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, 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 on 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. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

CAUTION:

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

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

See more information on MOS in the Appendix section.
# Table of Contents

Table of Contents .............................................................................................................................................. 3
List of Procedures .................................................................................................................................................. 5
List of Figures and Tables ...................................................................................................................................... 7
1.0 Introduction .................................................................................................................................................. 8
   1.1 Purpose and Scope ...................................................................................................................................... 8
   1.2 References ............................................................................................................................................... 8
   1.3 Acronyms ................................................................................................................................................ 9
   1.4 Terminology ........................................................................................................................................... 10
   1.5 Release Specific Hardware Support ........................................................................................................ 11
2.0 General Description ...................................................................................................................................... 11
   2.1 Acquiring Firmware ................................................................................................................................ 12
      2.1.1 HP .................................................................................................................................................. 12
      2.1.2 Oracle Rack Mount Server ............................................................................................................... 12
3.0 General Description ...................................................................................................................................... 13
   3.1 Required Materials .................................................................................................................................. 13
   3.2 Installation Overview ............................................................................................................................... 13
      3.2.1 Installation Matrix ............................................................................................................................ 13
      3.2.2 Installation Procedures .................................................................................................................... 15
   3.3 Optional Features .................................................................................................................................... 17
4.0 Software Installation Procedure ................................................................................................................ 18
   4.1 Prepare Servers for IPM ............................................................................................................................ 18
      4.1.1 Configure the HP/Oracle RMS BIOS Settings .................................................................................. 18
      4.1.2 Upgrade Rack Mount Server Firmware ......................................................................................... 19
   4.2 Install and Configure TVOE on First RMS (PMAC Host) ........................................................................ 19
   4.3 Install PMAC ........................................................................................................................................... 37
   4.4 Initialize the PMAC Application ............................................................................................................... 43
   4.5 Configure Cisco 4948E-F Aggregation Switches ..................................................................................... 48
      4.5.1 Configure netConfig Repository ................................................................................................. 48
      4.5.2 Configure Cisco 4948E-F Aggregation Switches ........................................................................... 56
   4.6 Configure PMAC Server ............................................................................................................................ 65
   4.7 Add Cabinet to PMAC .............................................................................................................................. 70
   4.8 Install TVOE on Additional Rack Mount Servers .................................................................................... 75
   4.9 Configure TVOE on Additional Rack Mount Servers ............................................................................. 80
   4.10 Create Virtual Machines for Applications ............................................................................................ 95
   4.11 Install Software on Virtual Machines .................................................................................................... 114
   4.12 Application Configuration: NOAMs ....................................................................................................... 119
   4.13 Application Configuration: NetBackup Client Installation (Optional) .................................................. 140
Appendix K: Upgrade Cisco 4948 PROM

Appendix G: Configuring for TVOE iLO Access

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

Appendix E: Changing the TVOE iLO4 Address

Appendix C: Changing the SNMP Configuration Settings

Appendix D.2: iLOM GUI Access (Oracle RMS)

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

Appendix B.2: Oracle RMS Servers (iLOM)

Appendix B.1: HP DL 380 Server

Appendix A.2.3: Configure HP Gen 9 Servers

Appendix A.2.2: Configure Oracle Rack Mount Servers

Appendix A.2.1: Configure HP Gen 8 Servers

Appendix A.2: Configure the RMS Server BIOS Settings

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

Appendix A: Pre-IPM Procedures

Appendix I.5: Configure PMAC Application NetBackup Virtual Disk

Appendix I.4: Open Ports for NetBackup Client Software

Appendix I.1: NetBackup Client Install using PLATCFG

Appendix I: Application NetBackup Client Installation Procedures

Appendix J: List of Frequently used Time Zones

Appendix K: Upgrade Cisco 4948 PROM
List of Procedures

Procedure 1. Configure the HP/Oracle RMS BIOS settings .......................................................... 18
Procedure 2. Upgrade Rack Mount Server Firmware ........................................................................ 19
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host) ........................................... 19
Procedure 4. First RMS Configuration .......................................................................................... 23
Procedure 5. PMAC Deployment .................................................................................................. 37
Procedure 6. Initialize the PMAC ................................................................................................ 43
Procedure 7. Configure netConfig Repository ............................................................................. 50
Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig) .................................... 57
Procedure 9. Configure the PMAC Server ...................................................................................... 65
Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory ...................................... 70
Procedure 11. Install TVOE on Additional Rack Mount Servers .................................................... 75
Procedure 12. Configure TVOE on Additional Rack Mount Servers .............................................. 80
Procedure 13. Load DSR and TPD ISO to the PMAC Server ......................................................... 95
Procedure 14. Create NOAM Guest VMs .................................................................................... 98
Procedure 15. Create SOAM Guest VMs .................................................................................... 102
Procedure 16. Create MP Guest VMs ........................................................................................ 106
Procedure 17. Create IP Front End (IPFE) Guest VMs ................................................................. 110
Procedure 18. IPM VMs ............................................................................................................. 114
Procedure 19. Install the DSR Application Software on the VMs ............................................... 116
Procedure 20. Configure First NOAM NE and Server ................................................................ 119
Procedure 21. Configure the NOAM Server Group .................................................................. 126
Procedure 22. Configure the Second NOAM Server ................................................................ 131
Procedure 23. Complete NOAM Server Group Configuration .................................................. 136
Procedure 24. Install NetBackup Client (Optional) ..................................................................... 140
Procedure 25. NOAM Configuration for DR Site (Optional) ..................................................... 141
Procedure 26. Pairing for DR-NOAM Site (Optional) ................................................................. 147
Procedure 27. Configure the SOAM NE ................................................................. 151
Procedure 28. Configure the SOAM Servers ......................................................... 153
Procedure 29. Configure the SOAM Server Group .............................................. 158
Procedure 30. Configure RMS-Specific B-Level Resources ............................... 163
Procedure 31. Configure the MP Servers ............................................................... 164
Procedure 32. Configure the MP Server Group(s) and Profile(s) ......................... 172
Procedure 33. Configure the Signaling Networks ............................................... 178
Procedure 34. Configure the Signaling Devices ................................................... 181
Procedure 35. Configure the Signaling Network Routes ...................................... 184
Procedure 36. Add VIP for Signaling networks (Active/Standby Configurations Only) ................................................................. 187
Procedure 37. Configure DSCP Values for Outgoing Traffic (Optional) ............... 189
Procedure 38. Configure SNMP Trap Receiver(s) (Optional) ............................... 192
Procedure 39. IP Front End (IPFE) Configuration (Optional) ............................. 197
Procedure 40. IDIH Installation (DSR 7.1-Optional) ........................................... 206
Procedure 41. Configure DSR Reference Data Synchronization for IDIH (DSR 7.1-Optional) ................................................................. 211
Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional) ................................................................. 213
Procedure 43. IDIH Configuration: Configure IDIH in the DSR (DSR 7.1-Optional)... 219
Procedure 44. IDIH Configuration: Configure Mail Server-Optional (DSR 7.1-Optional) ................................................................. 223
Procedure 45. IDIH Configuration: Configure SNMP Management Server-Optional (DSR 7.1-Optional) ................................................................. 225
Procedure 46. IDIH Configuration: Change Network Interface-Optional (DSR 7.1-Optional) ................................................................. 227
Procedure 47. IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (DSR 7.1-Optional) ................................................................. 228
Procedure 47. Activate Optional Features ............................................................ 229
Procedure 48. Backup TVOE Configuration ............................................................. 230
Procedure 49. Backup PMAC Application ............................................................... 232
Procedure 50. NOAM Database Backup ............................................................... 235
Procedure 51. SOAM Database Backup ............................................................... 237
Appendix A.2.1. Configure HP Gen 8 Server BIOS Settings .................................... 240
Appendix A.2.2. Configure Oracle Rack Mount Server BIOS Settings .................... 242
Appendix A.2.3. Configure HP Gen 9 Server BIOS Settings .................................... 244
Appendix B.1.1 Upgrade DL380 Server Firmware ................................................. 247
Appendix C.1. Changing SNMP Configuration Settings for HP DL 380 .................... 254
Appendix D.1. TVOE iLO4 GUI Access ................................................................. 256
Appendix D.1. TVOE iLO4 GUI Access ................................................................. 258
Appendix E.1. Changing the TVOE iLO Address ................................................... 261
Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4 .................... 264
Appendix F.2.1. HP DL380 Servers Mounting the ISO image via iLO4 .................... 267
Appendix G.1 Connecting to the TVOE iLO .......................................................... 271
Appendix I.1. Application NetBackup Client Installation (Using Platcfg) ............... 275
Appendix I.2. Application NetBackup Client Installation (NBAUTOINSTALL) ................................................................. 285
Appendix I.3. Create NetBackup Client Config File .................................................................................................................. 287
Appendix I.4. Open ports for NetBackup Client Software ......................................................................................................... 288
Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk ................................................................. 289
Appendix K.1. Upgrade Cisco 4948 PROM ................................................................................................................................. 295
Appendix M.1. Accessing the NOAM GUI using SSH Tunneling with Putty .................................................................................. 299
Appendix N.1. Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows ................................................... 301
Appendix P.1. DR-NOAM Feature Activation (DSR 6.0/7.0) ............................................................................................................ 306
Appendix Q.1. Creating a Bootable USB Drive on Linux ................................................................................................................ 307
Appendix R.1. IDIH External Drive Removal ............................................................................................................................... 308
Appendix T.1 Disable DTLS (DSR 7.1 Only) ............................................................................................................................... 313
Appendix T.2 Enable DTLS (DSR 7.1 Only) ............................................................................................................................... 315

List of Figures and Tables

Table 1. Acronyms ................................................................................................................................................................................. 9
Figure 1. Example of an instruction that indicates the server to which it applies ................................................................. 10
Table 2. Terminology .......................................................................................................................................................................... 10
Figure 2. Initial Application Installation Path-Example Shown ................................................................................................. 11
Figure 3 DSR Installation Procedure Map .............................................................................................................................. 14
Table 3. Installation Overview ......................................................................................................................................................... 15
Table 4. Time Zones ............................................................................................................................................................................. 294
Figure 4. Example Network Element XML File .......................................................................................................................... 298
Figure 5: HP Gen9 Server Hard Disk Drive Location for IDIH ............................................................................................... 311
1.0 Introduction

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to configure HP DL-380 Gen8/9 or Oracle Rack Mount Servers (RMS) to be used with Oracle Communication Diameter Signaling Router 6.0/7.0/7.1 (DSR 6.0/7.0/7.1) and to install DSR 6.0/7.0/7.1. It is assumed that the hardware installation and network cabling were executed beforehand.

The audience for this document includes Oracle customers as well as these groups: Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application.

Throughout the remainder of this document, the term RMS refers to either HP DL-380 Gen8/9 or Oracle Rack Mount Servers.

1.2 References

Software Centric Customers do not receive firmware upgrades through Oracle. Instead, refer to the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on https://docs.oracle.com under Platform documentation. The latest version is recommended if an upgrade is performed, otherwise version 2.2.8 is the minimum.

[1] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.8)
[2] TPD Initial Product Manufacture, E53017
[3] DSR 6.0/7.0 Hardware and Software Installation Procedure 1/2, E57789
[4] DSR 7.1 Hardware and Software Installation Procedure 1/2, E53488
[6] DSR Range Based Address Resolution (RBAR) Feature Activation, E58664
[9] DSR MAP-Diameter IWF Feature Activation Procedure, E58666
[10] DSR Meta Administration Feature Activation Procedure, E58661
[12] IDIH 6.0/7.0 Installation Procedure, E56571
### 1.3 Acronyms

An alphabetized list of acronyms used in the document:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS</td>
<td>Basic Input Output System</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disk</td>
</tr>
<tr>
<td>DSR</td>
<td>Diameter Signaling Router</td>
</tr>
<tr>
<td>DVD</td>
<td>Digital Versatile Disc</td>
</tr>
<tr>
<td>EBIPA</td>
<td>Enclosure Bay IP Addressing</td>
</tr>
<tr>
<td>FRU</td>
<td>Field Replaceable Unit</td>
</tr>
<tr>
<td>iLO</td>
<td>Integrated Lights Out manager</td>
</tr>
<tr>
<td>IPM</td>
<td>Initial Product Manufacture – the process of installing TPD on a hardware platform</td>
</tr>
<tr>
<td>MSA</td>
<td>Modular Smart Array</td>
</tr>
<tr>
<td>NB</td>
<td>NetBackup</td>
</tr>
<tr>
<td>OA</td>
<td>HP Onboard Administrator</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System (e.g. TPD)</td>
</tr>
<tr>
<td>RMS</td>
<td>Rack Mounted Server</td>
</tr>
<tr>
<td>PMAC</td>
<td>Platform Management &amp; Configuration</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>TPD</td>
<td>Tekelec Platform Distribution</td>
</tr>
<tr>
<td>TVOE</td>
<td>Tekelec Virtual Operating Environment</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VSP</td>
<td>Virtual Serial Port</td>
</tr>
</tbody>
</table>
1.4 Terminology

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

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

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

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

<table>
<thead>
<tr>
<th>5</th>
<th><strong>ServerX:</strong> Connect to the console of the server</th>
<th>Establish a connection to the server using cu on the terminal server/console.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* cu –l /dev/ttyS7</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Management Server</th>
<th>HP ProLiant DL380 or Oracle Rack Mount server deployed to run TVOE and host a virtualized PM&amp;C application. Can also host a virtualized NOAM. It is also used to configure the Aggregation switches (via the PMAC) and to serve other configuration purposes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMAC Application</td>
<td>PMAC is an application that provides platform-level management functionality for HP system, such as the capability to manage and provision platform components of the system so it can host applications.</td>
</tr>
<tr>
<td>Software Centric</td>
<td>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.</td>
</tr>
<tr>
<td>Enablement</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 2. Terminology
1.5 Release Specific Hardware Support

The following lists the DSR release and their corresponding hardware support covered in this installation procedure:

DSR 6.0/6.0.1:
- HP DL380 Gen8
- Oracle Sun Netra X3-2

DSR 6.0.2:
- HP DL380 Gen 8
- Oracle Sun Netra X3-2

DSR 7.0:
- HP DL380 Gen 8

DSR 7.0.1:
- HP DL380 Gen 8
- HP DL380 Gen 9

DSR 7.1
- HP DL380 Gen 8
- HP DL380 Gen 9

2.0 General Description

This document defines the steps to execute the initial installation of the Diameter Signaling Router 6.0/7.0/7.1 (DSR 6.0/7.0/7.1) application.

DSR 6.0/7.0/7.1 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 6.0/7.0/7.1 application on a RMS System.

Figure 2. Initial Application Installation Path-Example Shown
2.1 Acquiring Firmware

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

DSR 7.1 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

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 2.2.8 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 2.2.8. However, if a firmware upgrade is needed, the current GA release of the HP Solutions Firmware Upgrade Pack 2.x.x should be used.

Each version of the HP Solutions Firmware Upgrade Pack contains multiple items including media and documentation. If an HP FUP 2.x.x version newer than the minimum of HP FUP 2.2.8 is used, then the HP Solutions Firmware Upgrade Guide [1] should be used to upgrade the firmware. This document provides its own upgrade procedures for firmware.

The two pieces of required firmware media provided in the HP Solutions Firmware Upgrade Pack 2.x.x releases are:

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

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

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

2.1.2 Oracle Rack Mount Server

The Oracle Firmware Upgrade Pack (FUP) consists of documentation used to assist in the upgrading of Oracle rack mount servers. The pack consists of an upgrade guide and release notes. The current minimum supported release is 3.1.3. However, if a firmware update is required, it is recommended to use the latest available release. Firmware components can be downloaded from My Oracle Support at https://support.oracle.com. Refer to the appropriate FUP release notes for directions on how to acquire the firmware.
3.0 General Description

This section provides a brief overview of the recommended method for installing the Target Release software. The basic install process and approximate time required is outlined in.

3.1 Required Materials

1. One (1) target release Application Media, or a target-release ISO
2. One (1) ISO of TPD release, or later shipping baseline as per Oracle ECO

3.2 Installation Overview

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

3.2.1 Installation Matrix

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

1) An overall installation requirement is decided upon. Among the data that should be collected:
   - The Total number of Rack Mount Servers
   - The number of VMs and servers on each Rack Mount Server and their role(s)
   - Does the deployment include 4948 aggregation switches?
   - Will MP’s be in N+0 configurations or in active/standby?
   - What time zone should be used across the entire collection of DSR sites?
   - Will SNMP traps be viewed at the NOAM, or will an external NMS be used? (Or both?)
Figure 3 DSR Installation Procedure Map
### 3.2.2 Installation Procedures

The following table illustrates the progression of the installation process by procedure with estimated times. The estimated times and the phases that must be completed may vary due to differences in typing ability and system configuration. The phases outlined in are to be executed in the order they are listed.

**Table 3. Installation Overview**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Phase</th>
<th>Elapsed Time (Minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Procedure 1</strong></td>
<td>Configure the HP/Oracle RMS BIOS settings</td>
<td><strong>This Step</strong> 30 <strong>Cum.</strong> 30</td>
</tr>
<tr>
<td><strong>Procedure 2</strong></td>
<td>Upgrade Rack Mount Server Firmware</td>
<td>30</td>
</tr>
<tr>
<td><strong>Procedure 3</strong></td>
<td>Install and Configure TVOE on First RMS (PMAC Host)</td>
<td>30</td>
</tr>
<tr>
<td><strong>Procedure 4</strong></td>
<td>First RMS Configuration</td>
<td>30</td>
</tr>
<tr>
<td><strong>Procedure 5</strong></td>
<td>PMAC Deployment</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 6</strong></td>
<td>Initialize the PMAC Application</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 7</strong></td>
<td>Configure netConfig Repository</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 8</strong></td>
<td>Configure Cisco 4948E/4948E-F Switch using NetConfig*</td>
<td>30*</td>
</tr>
<tr>
<td><strong>Procedure 9</strong></td>
<td>Configure the PMAC Server</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 10</strong></td>
<td>Add Cabinet and Enclosure to the PM&amp;C system inventory</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 11</strong></td>
<td>Install TVOE on Additional Rack Mount Servers</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 12</strong></td>
<td>Configure TVOE on Additional Rack Mount Servers</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 13</strong></td>
<td>Load DSR and TPD ISO to the PMAC Server</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 14</strong></td>
<td>Create NOAMP Guest VMs</td>
<td>5</td>
</tr>
<tr>
<td><strong>Procedure 15</strong></td>
<td>Create SOAM Guest VMs</td>
<td>5</td>
</tr>
<tr>
<td><strong>Procedure 16</strong></td>
<td>Create MP Guest VMs</td>
<td>5</td>
</tr>
<tr>
<td><strong>Procedure 17</strong></td>
<td>Create IPFE Guest VMs*</td>
<td>5</td>
</tr>
<tr>
<td><strong>Procedure 18</strong></td>
<td>IPM VMs</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 19</strong></td>
<td>Install the DSR Application Software on the VMs</td>
<td>20</td>
</tr>
<tr>
<td><strong>Procedure 20</strong></td>
<td>Configure the First NOAM NE and Server</td>
<td>25</td>
</tr>
<tr>
<td><strong>Procedure 21</strong></td>
<td>Configure the NOAM Server Group</td>
<td>15</td>
</tr>
<tr>
<td><strong>Procedure 22</strong></td>
<td>Configure the Second NOAM Server</td>
<td>15</td>
</tr>
<tr>
<td><strong>Procedure 23</strong></td>
<td>Complete Configuring the NOAM Server Group</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 24</strong></td>
<td>Install NetBackup Client*</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 25</strong></td>
<td>NOAM Configuration for DR Site*</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 26</strong></td>
<td>NOAM Pairing for DSR NO DR Site*</td>
<td>10</td>
</tr>
<tr>
<td><strong>Procedure 27</strong></td>
<td>Configure the SOAM NE</td>
<td>15</td>
</tr>
</tbody>
</table>
Table 3. Installation Overview

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Phase</th>
<th>Elapsed Time (Minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure 28</td>
<td>Configure the SOAM Servers</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 29</td>
<td>Configure the SOAM Server Group</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 30</td>
<td>Configure RMS-specific B-level Resources</td>
<td>5</td>
</tr>
<tr>
<td>Procedure 31</td>
<td>Configure the MP Servers</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 32</td>
<td>Configure the MP Server Group(s) and Profiles</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 33</td>
<td>Configure the Signalling Network</td>
<td>30</td>
</tr>
<tr>
<td>Procedure 34</td>
<td>Configure the Signalling Devices</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 35</td>
<td>Configure the Signalling Network Routes</td>
<td>15</td>
</tr>
<tr>
<td>Procedure 36</td>
<td>Add VIP for Signalling Networks*</td>
<td>5</td>
</tr>
<tr>
<td>Procedure 37</td>
<td>Configure DSCP Values for Outgoing Traffic*</td>
<td>10</td>
</tr>
<tr>
<td>Procedure 38</td>
<td>Configure SNMP for Traps Receivers*</td>
<td>5</td>
</tr>
<tr>
<td>Procedure 39</td>
<td>IP Front End (IPFE) Configuration*</td>
<td>15</td>
</tr>
<tr>
<td>Procedure 40</td>
<td>IDIH Installation*</td>
<td>60</td>
</tr>
<tr>
<td>Procedure 41</td>
<td>IDIH Configuration-Data Synchornization*</td>
<td>15</td>
</tr>
<tr>
<td>Procedure 42</td>
<td>IDIH Configuration-SSO Domain*</td>
<td>30</td>
</tr>
<tr>
<td>Procedure 43</td>
<td>IDIH Configuration-DSR Configuration*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 44</td>
<td>IDIH Configuration-Mail Server*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 45</td>
<td>IDIH Configuration-SNMP Management Server*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 46</td>
<td>IDIH Configuration-Change Network Interface*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 47</td>
<td>Install Optional Features*</td>
<td>30</td>
</tr>
<tr>
<td>Procedure 48</td>
<td>Backup TVOE Configuration*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 49</td>
<td>Backup PMAC Application*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 50</td>
<td>Backup NOAM Database*</td>
<td>20</td>
</tr>
<tr>
<td>Procedure 51</td>
<td>Backup SOAM Database*</td>
<td>20</td>
</tr>
</tbody>
</table>

* denotes Optional Features.
### 3.3 Optional Features

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter Mediation</td>
<td>DSR Meta Administration Feature Activation, E58661</td>
</tr>
<tr>
<td>Range Based Address Resolution (RBAR)</td>
<td>DSR RBAR Feature Activation, E58664</td>
</tr>
<tr>
<td>MAP-Diameter IWF Feature</td>
<td>MAP-Diameter IWF Feature Activation, E58666</td>
</tr>
</tbody>
</table>
4.0 Software Installation Procedure

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

4.1 Prepare Servers for IPM

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

4.1.1 Configure the HP/Oracle RMS BIOS Settings

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

**Procedure 1. Configure the HP/Oracle RMS BIOS settings**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>RMS Server: Configure the BIOS Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Follow the appropriate Appendix procedure for the corresponding hardware type:</td>
</tr>
<tr>
<td></td>
<td>• HP DL 380 Gen 8 RMS: Appendix A.2.1: Configure HP Gen 8 Servers</td>
</tr>
<tr>
<td></td>
<td>• HP DL 380 Gen 9 RMS: Appendix A.2.3: Configure HP Gen 9 Servers</td>
</tr>
<tr>
<td></td>
<td>• Oracle Rack Mount Servers (Including Sun Netra X3-2): Appendix A.2.2: Configure Oracle Rack Mount Servers</td>
</tr>
</tbody>
</table>

This procedure explains the steps needed to configure HP DL380 and Oracle Server BIOS Settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
### 4.1.2 Upgrade Rack Mount Server Firmware

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

**Procedure 2. Upgrade Rack Mount Server Firmware**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure explains the steps needed to update the firmware if needed. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>
| 1 | **RMS Server**: Configure the BIOS Settings  
Follow the appropriate Appendix procedure for the corresponding hardware type:  
- Oracle Rack Mount Servers (Including Sun Netra X3-2): Appendix B.2: Oracle Rack Mount Server |

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure explains the steps needed to install TVOE on the first RMS Server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>
| 1 | **Connect to the First RMS Server**: Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE.  
**Note**: Appendix D: TVOE iLO/iLOM GUI Access and Appendix E: Changing the TVOE iLO4 Address explains how to access the rack mount server iLO and change the address if necessary. |
| 2 | **RMS Server**: Insert TVOE Media into Server  
Insert the OS IPM media (CD/DVD or USB) into the CD/DVD tray/USB slot of the rack mount server. Refer to Appendix Q: Creating a Bootable USB Drive on Linux for creating a bootable USB  
Alternatively ISO can be mounted using Virtual media as well. Refer to Appendix F: Attaching an ISO Image to a Server using the iLO or iLOM. |
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

3

**RMS Server:** Begin IPM Process

Once the Server reboots, it will reboot from the TVOE media and a boot prompt shall be displayed:

```bash
TPDnoraid diskconfig=HWRAID,force console=tty0
```

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

Welcome to Tokelau Platform Distribution!
Release: 7.0.0.0.0.06.11.0
Arch: x86_64

For a detailed description of all the supported commands and their options, please refer to the Initial Platform Manufacture document for this release.

In addition to `linux rescue` the following kickstart profiles may be used:

```
TPB : TPBnoraid : TPBblade : TPBcompact : H80
```

Commonly used options are:

- `console=(console_option){<console_option>}`
- `primaryConsole=(console_option)`
- `root=server_ip`
- `iscsi` (if) `iscsi
- `reserved=(size1: size2)`
- `diskconfig=H8RAID,force`
- `device=(device1:device2)`
- `guestArchive`

To install using a monitor and a local keyboard, add `console=tty0` to the boot:

```bash
TPDnoraid diskconfig=HWRAID,force console=tty0
```
### Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

#### 4. Monitor the IPM Installation

The IPM process takes about 30 minutes, you will see several messages and screens in the process.

The following screens will be displayed:

- **Formatting**
  - Formatting / file system...
  - 23%

- **Package Installation**
  - Install Starting
  - Starting install process, this may take several minutes...
  - Total Comple
  - Remaining 0%
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

<table>
<thead>
<tr>
<th>5</th>
<th>RMS Server: Install Complete-Reboot</th>
</tr>
</thead>
</table>

Once the IPM is complete, you will be prompted to press Enter as shown below. Remove the disk from the drive or unmount the TPD image from the iLO and press Enter to reboot the server.

![Reboot prompt](image-url)

After a few minutes and multiple reboots, the server boot sequence will start and eventually display that it is booting the new IPM load.

![Boot sequence](image-url)

**Note:** A successful IPM platform installation process results in a user login prompt.
Procedure 4. First RMS Configuration

This procedure will configure the First TVOE/Management Server.

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

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

1. **Determine Bridge Names and Interfaces**

   Determine the bridge interfaces to be used on the TVOE server and fill in the appropriate values in the table below. If netbackup is to be used, determine the bridge interface to be used for the netbackup network and fill in the `<TVOE_NetBackup_Bridge_Interface>` value.

<table>
<thead>
<tr>
<th>Guest Interface Alias</th>
<th>TVOE Bridge Name</th>
<th>TVOE Bridge Interface</th>
</tr>
</thead>
</table>
   | control               | control          | Fill in the appropriate value (default is bond0):
   |                       |                  | `<TVOE_Control_Bridge_Interface>` |
   | management            | management       | Fill in the appropriate value:
   |                       |                  | `<TVOE_Management_Bridge_Interface>` |
   | Xmi                   | xmi              | Fill in the appropriate value:
   |                       |                  | `<TVOE_XMI_Bridge_Interface>` |
   | Imi                   | imi              | Fill in the appropriate value, (default is bond0.4):
   |                       |                  | `<TVOE_IMI_Bridge_Interface>` |
   | xsi1                  | xsi1             | Fill in the appropriate value:
   |                       |                  | `<TVOE_XSI1_Bridge_Interface>` |
   | xsi2                  | xsi2             | Fill in the appropriate value:
   |                       |                  | `<TVOE_XSI2_Bridge_Interface>` |
   | netbackup (if applicable) | netbackup | Fill in the appropriate value:
   |                       |                  | `<TVOE_NetBackup_Bridge_Interface>` |
### Procedure 4. First RMS Configuration

#### 1st RMS iLO/iLOM: Login and Launch the Integrated Remote Console

- **Log in to iLO/iLOM**, follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI.

  ```
  https://<management_server_iLO_ip>
  ```

---

#### 1st RMS iLO/iLOM: Create Tagged Control Interface and Bridge (Optional)

- If you are using a **tagged control network** interface on this TVOE Server, then complete this step. Otherwise, **skip to the next step**.

  ```
  $ sudo /usr/TKLC/plat/bin/netAdm set
  --type=Bridge
  --name=control
  --delBridgeInt=bond0
  
  Interface bond0 updated
  Bridge control updated
  ```

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

  ```
  $ sudo /usr/TKLC/plat/bin/netAdm set
  --type=Bridge
  --name=control
  --bridgeInterfaces=<TVOE_Control_Bridge_Interface>
  ```

---

#### 1st RMS iLO/iLOM: Create the Management Network

- Create the Management network, execute the following command:

  **Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

  ```
  $ 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>
  ```

---
### Procedure 4. First RMS Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create the XMI Network:</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.</td>
</tr>
<tr>
<td></td>
<td>$sudo /usr/TKLC/plat/bin/netAdm add --device=&lt;TVOE_XMI_Bridge_Interface&gt; --onboot=yes</td>
</tr>
<tr>
<td></td>
<td>Interface bond0.3 added</td>
</tr>
<tr>
<td></td>
<td>$sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=&lt;TVOE_XMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td></td>
<td>Interface bond0.3 was updated. Bridge xmi added!</td>
</tr>
<tr>
<td>2</td>
<td>Create the IMI Network:</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.</td>
</tr>
<tr>
<td></td>
<td>$sudo /usr/TKLC/plat/bin/netAdm add --device=&lt;TVOE_IMI_Bridge_Interface&gt; --onboot=yes</td>
</tr>
<tr>
<td></td>
<td>Interface bond0.4 added</td>
</tr>
<tr>
<td></td>
<td>$sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=imi --onboot=yes --bridgeInterfaces=&lt;TVOE_IMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td></td>
<td>Interface bond0.4 was updated. Bridge imi added!</td>
</tr>
</tbody>
</table>
Procedure 4. First RMS Configuration

| 7 | **1st RMS**  
   **iLO/iLOM:**  
   Create the  
   XSI-1  
   Network  
   (with  
   Aggregation  
   Switches) |
|---|---|
|   | Execute this step if deploying with **Aggregation switches**, otherwise **skip this step**

**Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

Execute the following commands:

```
$ sudo /usr/TKLC/plat/bin/netAdm add  
   --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes

Interface bond0.5 added
```

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge  
   --name=xsi1 --onboot=yes  
   --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>

Interface bond0.5 was updated.  
Bridge xsi1 added!
```
Procedure 4. First RMS Configuration

Execute this step if deploying without Aggregation switches

Execute the following commands:

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add --device=bond1 --onboot=yes --type=Bonding --mode=active-backup --miimon=100
Interface bond1 added

$ sudo /usr/TKLC/plat/bin/netAdm set --device=eth03 --type=Ethernet --master=bond1 --slave=yes --onboot=yes
Interface eth03 updated

$ sudo /usr/TKLC/plat/bin/netAdm set --device=eth13 --type=Ethernet --master=bond1 --slave=yes --onboot=yes
Interface eth13 updated

$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes
Interface bond1.<XSI1_VLAN_ID> added

$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>
Interface bond1.<XSI1_VLAN_ID> was updated. Bridge xsi1 added!
```
Procedure 4. First RMS Configuration

1st RMS iLO/iLOM: Create the XSI-2 Network

Configure the XSI2 Network using option 1 OR option 2 below

**Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

**Option 1:** Deployment with Aggregation switches:

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_XSI2_Bridge_Interface> --onboot=yes

Interface bond0.6 added
```

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi2 --onboot=yes
--bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>

Interface bond0.6 was updated.
Bridge xsi2 added!
```

**Option 2:** Deployment without Aggregation switches:

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_XSI2_Bridge_Interface> --onboot=yes

Interface bond1.<XSI2_VLAN_ID> added
```

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi2
--onboot=yes --bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>

Interface bond1.<XSI2_VLAN_ID> was updated.

Bridge xsi2 added!
```
### Procedure 4. First RMS Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td><strong>1st RMS iLO/iLOM:</strong> Add the NetBackup Network-Option 1 <em>(Optional)</em>&lt;br&gt; If NetBackup is to be used, execute this step, otherwise skip to Step 13.&lt;br&gt;&lt;br&gt;<strong>Select only this option or the following options listed in steps 11-12.</strong>&lt;br&gt;&lt;br&gt;NetBackup is a tool that allows the customer to take remote backups of the system.&lt;br&gt;&lt;br&gt;Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.&lt;br&gt;&lt;br&gt;Note: The example below illustrates a TVOE Management Server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.&lt;br&gt;&lt;br&gt;Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.&lt;br&gt;&lt;br&gt;Create netbackup bridge using a bond containing an untagged interface&lt;br&gt;&lt;br&gt;$ sudo /usr/TKLC/plat/bin/netAdm add&lt;br&gt;  --device=&lt;TVOE_NetBackup_Bridge_Interface&gt;&lt;br&gt;  --onboot=yes --type=Bonding --mode=active-backup --&lt;br&gt;  miimon=100&lt;br&gt;  --MTU=&lt;NetBackup_MTU_size&gt;&lt;br&gt;Interface &lt;TVOE_NetBackup_Bridge_Interface&gt; added&lt;br&gt;&lt;br&gt;$ sudo /usr/TKLC/plat/bin/netAdm set&lt;br&gt;  --device=&lt;ethernet_interface_4&gt; --type=Ethernet&lt;br&gt;  --master=&lt;TVOE_NetBackup_Bridge_Interface&gt; --slave=yes&lt;br&gt;  --onboot=yes&lt;br&gt;Interface &lt;ethernet_interface_4&gt; updated&lt;br&gt;&lt;br&gt;$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge&lt;br&gt;  --name=&lt;TVOE_NetBackup_Bridge&gt; --onboot=yes --bootproto=none&lt;br&gt;  --MTU=&lt;NetBackup_MTU_size&gt;&lt;br&gt;  --bridgeInterfaces=&lt;TVOE_NetBackup_Bridge_Interface&gt;&lt;br&gt;  --address=&lt;TVOE_NetBackup_IP&gt;&lt;br&gt;  --netmask=&lt;TVOE_NetBackup_Netmask/Prefix&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td><strong>1st RMS iLO/iLOM:</strong> Add the NetBackup Network-Option 2 <em>(Optional)</em>&lt;br&gt; Select only this option or options in Steps 10 or 12&lt;br&gt;&lt;br&gt;Create NetBackup bridge using an untagged native interface:&lt;br&gt;&lt;br&gt;$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge&lt;br&gt;  --name=&lt;TVOE_NetBackup_Bridge&gt; --onboot=yes --bootproto=none&lt;br&gt;  --MTU=&lt;NetBackup_MTU_size&gt;&lt;br&gt;  --bridgeInterfaces=&lt;Ethernet_Interface_4&gt;&lt;br&gt;  --address=&lt;TVOE_NetBackup_IP&gt;&lt;br&gt;  --netmask=&lt;TVOE_NetBackup_Netmask/Prefix&gt;</td>
</tr>
</tbody>
</table>
Procedure 4. First RMS Configuration

| 12 | 1st RMS iLO/iLOM: Add the NetBackup Network-Option 3 (Optional) | Select only this option or options in 10-11
Create NetBackup bridge using a tagged device:

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

Interface <TVOE_NetBackup_Bridge_Interface> added
```

```
$ sudo /usr/TKL/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>
```

| 13 | 1st RMS iLO/iLOM: Configure Networking for NetBackup Interface (Optional) | Note: If you have configured NetBackup in the previous steps, execute this step; otherwise skip this step.

```
$ sudo /usr/TKL/plat/bin/netAdm add
   --route=net
   --device=netbackup --address=<TVOE_NetBackup_Network_ID>
   --netmask=<TVOE_NetBackup_NetMask/Prefix>
   --gateway=<TVOE_NetBackup_Gateway_IP_Address>
```

| 14 | 1st RMS iLO/iLOM: Create the Management Network | Management_Server_TVOE_IP

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

| 15 | 1st RMS iLO/iLOM: Restart the network interfaces | Restart the network interfaces, execute the following command:

```
$ sudo service network restart
```
### Procedure 4. First RMS Configuration

<table>
<thead>
<tr>
<th><strong>16</strong></th>
<th><strong>1st RMS iLO/iLOM:</strong> Set Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Set the server hostname by running the following:</strong></td>
</tr>
<tr>
<td></td>
<td><code>$ sudo su - platcfg</code></td>
</tr>
<tr>
<td></td>
<td><strong>Navigate to Server Configuration -&gt; Hostname -&gt; Edit.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image1.png" alt="Image of Hostname" /></td>
</tr>
<tr>
<td></td>
<td>Set TVOE Management Server hostname Press OK. Navigate out of Hostname</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>17</strong></th>
<th><strong>1st RMS iLO/iLOM:</strong> Set the Time Zone and/or Hardware Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Navigate to Server Configuration -&gt; Time Zone.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image2.png" alt="Image of Time Zone" /></td>
</tr>
<tr>
<td></td>
<td>Select Edit. Set the time zone and/or hardware clock to <strong>&quot;UTC&quot; (or appropriate time zone value)</strong> Press OK. Navigate out of Server Configuration</td>
</tr>
</tbody>
</table>
Procedure 4. First RMS Configuration

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

The **Time Servers** page will now be shown, which shows the configured NTP servers and peers (if there are NTP servers already configured).

Update NTP Information, select **Edit.** The **Edit Time Servers** menu is displayed.

Select the appropriate **Edit Time Servers** menu option. You can add new or edit any existing NTP server entry.

Set NTP server IP address to point to the customer provided NTP server (Remember that 3 distinct NTP sources are required)

Press **OK.**

Exit platcfg.

Ensure that the time is set correctly by executing the following commands:

```
$ sudo service ntpd stop
$ sudo ntpdate ntpserver1
$ sudo service ntpd start
```
Procedure 4. First RMS Configuration

19

1st RMS iLO/iLOM: Set SNMP

Set SNMP by running the following:

```
$ sudo su - platcfg
```

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

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

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

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

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

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

Exit platcfg.
## Procedure 4. First RMS Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Command/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Restart iLO/iLOM:</td>
<td><code>sudo init 6</code></td>
</tr>
<tr>
<td></td>
<td>Execute the following command to restart the server:</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Configure iLO/iLOM: NetBackup Part 1 (Optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute this step if the <strong>NetBackup</strong> feature is enabled for this system, otherwise skip this step. Configure the appropriate NetBackup client on the PMAC TVOE host.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open firewall ports for NetBackup using the following commands:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt /usr/TKLC/plat/etc/iptables/</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo /usr/TKLC/plat/bin/iptablesAdm reconfig</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable platcfg to show the Netbackup Menu Items by executing the following commands:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBConfig;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBInit;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBDeInit;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBInstall;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBVerifyEnv;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo platcfgadm --show NBVerify;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create LV and file system for Netbackup client software on the vgguests volume group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This will create the LV, format it with a filesystem, and mount it under <code>/usr/openv/</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example output is shown below:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Called with options: <code>/tmp/nb.lvm</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VG vgguests already exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Creating lv netbackup_lv.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume netbackup_lv will be created.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Success: Volume netbackup_lv was created.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Creating filesystem, this may take a while.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Updating fstab for lv netbackup_lv.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuring existing lv netbackup_lv.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The LV for netbackup has been created!</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 4. First RMS Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>22</strong></td>
<td><strong>1st RMS iLO/iLOM:</strong> Configure NetBackup-Part 2 (Optional)</td>
</tr>
<tr>
<td></td>
<td>Install the netbackup client software:</td>
</tr>
<tr>
<td></td>
<td>Refer to <strong>Appendix I:</strong> Application NetBackup Client Installation Procedures on instructions how to install the netbackup client.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Skip any steps relating to copying netbackup &quot;notify&quot; scripts to /usr/openv/netbackup/bin. The TVOE netbackup notify scripts are taken care of in the next step.</td>
</tr>
<tr>
<td></td>
<td>Create softlinks for TVOE specific netbackup notify scripts.</td>
</tr>
</tbody>
</table>
| | ```
| $ 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 following files form the TVOE host: |
| | • /var/TKLC/bkp/*.iso |
| **23** | **1st RMS iLO/iLOM:** Setup syscheck |
| | syscheck must be configured to monitor bonded interfaces. |
| | Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: |
| | ```
| $ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>
| $ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --enable
| $ sudo /usr/TKLC/plat/bin/syscheck net ipbond -v
| ``` |
| **24** | **1st RMS iLO/iLOM:** Verify Server Health |
| | Execute the following: |
| | ```
| $ alarmMgr -alarmStatus
| ``` |
| | This command should return no output on a healthy system. If any alarms are reported, contact **Appendix U:** My Oracle Support (MOS) |
Procedure 4. First RMS Configuration

1st RMS iLO/iLOM:
Perform a TVOE backup using TPD platcfg utility

Execute the following:

```
$ sudo su - platcfg
```

Navigate to **Maintenance -> Backup and Restore**

Select Backup Platform (CD/DVD)

**Note:** If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device." Press **Enter** to continue.

Select an applicable backup option, and press **Enter** to continue.

Exit from TPD platcfg utility.

The TVOE backup can be found in the "/var/TKLC/bkp/" directory, and is prefixed by the server hostname. An example of a TVOE backup ISO follows:

```
/var/TKLC/bkp/RMS503u14-plat-app-201210301505.iso
```

Move the TVOE backup to a customer provided backup server for safe keeping.
### 4.3 Install PMAC

#### Procedure 5. PMAC Deployment

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td><strong>1st RMS iLO/iLOM:</strong> Login and Launch the Integrated Remote Console. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>

**Prerequisite:** First RMS Network Configuration (PMAC Host) has been completed.

**Needed material:**
- PMAC Media on USB Drive or ISO

Log in to iLO/iLOM, follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. [https://<management_server_iLO_ip>](https://<management_server_iLO_ip>)

---

**Install PMAC**

**Procedure 5. PMAC Deployment**

This procedure will deploy PMAC on the TVOE Host.
# Procedure 5. PMAC Deployment

<table>
<thead>
<tr>
<th>TVOE iLO/iLOM:</th>
<th>Mount the PMAC Media to the TVOE Server</th>
</tr>
</thead>
</table>

Use one of the following 2 options to mount the PMAC Media:

**Option 1:**

If using a USB media, insert the PM&C USB into a USB port and execute the following to mount the iso:

```bash
$ ls /media/*/*.iso
```

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

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

**Option 2:**

If using an ISO image, run the following to mount it:

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

Next Validate the PM&C media by executing the following commands:

```bash
$ 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

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

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

If deploying PMAC without 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>
--isoimagesVolSizeGB=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 will deploy and boot. The management and control network will come up based on the settings that were provided to the PMAC-deploy script.

**Note:** This step takes between 5 and 10 minutes.

4. **TVOE iLO/iLOM:** Unmount the Media

The media should auto-unmount, if it does not, unmount the media using the following command:

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

Remove the media from the drive.
## Procedure 5. PMAC Deployment

### Step 5

**TVOE iLO/iLOM:**
SSH into the Management Server

- Using an SSH client such as putty, ssh to the TVOE host as `admusr`.

- Login using `virsh`, and wait until you see the login prompt:

  ```
  $ sudo /usr/bin/virsh list
  
  Id   Name    State
  ---------------------
  1    myTPD   running
  2    PM&C   running
  
  $ sudo /usr/bin/virsh console <PM&C>
  
  Starting ntdMgr: [ OK ]
  Starting atd: [ OK ]
  'TPD Up' notification(s) already sent: [ OK ]
  upstart: Starting tpdProv...
  upstart: tpdProv started.
  CentOS release 6.2 (Final)
  Kernel 2.6.32-220.17.1.el6prerele6.0.0_80.14.0.x86_64
  on an x86_64
  PM&Cdev7 login:
  ```

### Step 6

**Virtual PM&C:**
Verify the PMAC is configured correctly on first boot

- Establish an SSH session to the PMAC, login as `admusr`.

- Run the following command (there should be no output):

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

### Step 7

**Virtual PM&C:**
Error doing verification, if error is outputted

- If an error was made use the following command to delete the PM&C Guest and then re-deploy the guest again:

  ```
  $ sudo guestMgr --remove <PMAC_Name>
  ```
### Procedure 5. PMAC Deployment

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 8    | Virtual PM&C: Set the PMAC time zone | Determine the Time Zone to be used for the PMAC  

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

Run  

```bash  
$ sudo set_pmac_tz.pl <time zone>  
Example:  
$ sudo set_pmac_tz.pl America/New_York  
```

Verify that the time zone has been updated:  

```bash  
$ sudo date  
```
Procedure 5. PMAC Deployment

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9    | Virtual PMAC: Set SNMP | Set SNMP by running the following:  

```
$ sudo su - platcfg
```

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

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

Complete the form by entering in all information about the SNMP trap destination. Select **OK** to finalize the configuration. The ‘**NMS Server Action Menu**’ will now be displayed. Select **Exit.** The following dialogue will then be presented.

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

Exit platcfg.

| 10   | Virtual PMAC: Reboot the server | Reboot the server by running:  

```
$ sudo init 6
```
### 4.4 Initialize the PMAC Application

**Procedure 6. Initialize the PMAC**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TVOE Host:</td>
<td>Get the DSR ISO</td>
</tr>
</tbody>
</table>

Use this procedure to gather and prepare configuration files that are required to proceed with the DSR 6.0/7.0/7.1 installation.

**Needed material:**
- HP Misc. Firmware USB
- HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.8) [1]
- DSR USB or ISO

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

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

1. **TVOE Host:** Get the DSR ISO

   Once the PMAC is done rebooting, 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.

   Mount the media on the TVOE Host using one of the following commands:

   1. If using a USB Drive, run the following to mount it:

   ```
   $ sudo /bin/ls /media/*/*.iso

   /media/sdb1/DSR-6.0.0_60.7.0-x86_64.iso
   ```

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

   ```
   $ sudo /bin/mount -o loop /media/sdb1/DSR-6.0.0_60.7.0-
   x86_64.iso /mnt/upgrade
   ```

   2. If the DSR in on an ISO, mount it using the following commands

   ```
   $ sudo /bin/mount -o loop <path to DSR ISO>
   /mnt/upgrade
   ```
Procedure 6. Initialize the PMAC

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 2 | **TVOE iLO/iLO:** SSH into the Management Server | Using an SSH client such as putty, ssh to the TVOE host as **admusr**. Login using **virsh**, and wait until you see the login prompt:

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

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

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

[Output Removed]

Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prere16.0.0-80.14.0.x86_64
on an x86_64
PM&Cdev7 login:

| 3 | **Virtual PMAC:** Get support files from the DSR ISO | **Execute** the following commands to copy the required files

```bash
$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>: /mnt/upgrade/upgrade/overlay/* /usr/TKLC/smac/etc/
```

Logout of PMAC and Re-login to TVOE Host and unmount the ISO

**Note:** Hold **ctrl ]** to logout of the PM&C

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

Remove the DSR 6.0/7.0/7.1 DSR media from the TVOE Management Server.
Procedure 6. Initialize the PMAC

Virtual PMAC:
Copy ISO images into place (this will copy both the 4948E IOS images into place).

Insert the Misc. Firmware USB media into the USB drive.

For this step, be sure to use the correct IOS version specified by the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.8) [1].

Copy each ISO image called out by the release notes.

SSH to the TVOE Host server as admusr using the vsp/Host Console on the TVOE Management Server iLO/iLOM. Make the upgrade media available to the server.

Execute the following commands to copy the required files. Note: The `<PMAC Management_IP Address>` is the one used to deploy PMAC in procedure 4, step 4.

Mount the media on the TVOE Host using one of the following commands:
If using a USB Drive, run the following to mount it:

```bash
$ sudo /bin/ls /media/*/*.iso
```

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

```bash
$ sudo /bin/mount -o loop /media/sdb1/ <MISC file name> /mnt/upgrade
```

If the DSR in on an ISO, mount it using the following commands

```bash
$ sudo /bin/mount -o loop <path to DSR ISO> /mnt/upgrade
```

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

Logout of PM&C and Re-login to TVOE Host and unmount the ISO

Hold `ctrl ]` to logout of the PM&C

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

Remove the Misc. Firmware media from the drive.
**Procedure 6. Initialize the PMAC**

<table>
<thead>
<tr>
<th>Step</th>
<th>Virtual PMAC: Initialize the PMAC Application</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Initialize the PMAC Application; run the following commands:</td>
<td>$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE Profile successfully applied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState PMAC Feature State = InProgress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=&lt;mgmt_gateway_address&gt; --ip=0.0.0.0 --mask=0.0.0.0 --device=management Successful add of Admin Route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig Initialization has been started as a background task</td>
</tr>
<tr>
<td>6</td>
<td>Virtual PMAC: Initialize the PMAC Application</td>
<td>Wait for the background task to successfully complete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The command will show &quot;IN_PROGRESS&quot; for a short time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run the following command until a &quot;COMPLETE&quot; or &quot;FAILED&quot; response is seen similar to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1: Initialize PMAC COMPLETE - PMAC initialized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sinceUpdate: 47</td>
</tr>
<tr>
<td></td>
<td></td>
<td>taskRecordNum: 2 Server Identity:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical Blade Location:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blade Enclosure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blade Enclosure Bay:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest VM Location:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host IP:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPD IP:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rack Mount Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Some expected networking alarms may be present</td>
</tr>
</tbody>
</table>
Procedure 6. Initialize the PMAC

<table>
<thead>
<tr>
<th>Step</th>
<th>Virtual PMAC:</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Initialize the PMAC Application</td>
<td>Perform a system healthcheck on PMAC</td>
<td>$ sudo /usr/TKLC/plat/bin/alarmMgr -alarmStatus</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This command should return no output on a healthy system. <strong>Note:</strong> An NTP alarm will be detected if the system switches are not configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/sentry status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All Processes should be running, displaying output similar to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PM&amp;C Sentry Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sentryd started: Mon Jul 23 17:50:49 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Current activity mode: ACTIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Process PID Status StartTS NumR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>smacTalk 9039 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>smacMon 9094 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fri Aug 3 13:16:35 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Command Complete.</td>
</tr>
<tr>
<td>8</td>
<td>Verify the PMAC application release</td>
<td>Verify the PMAC application release</td>
<td>$ sudo /usr/TKLC/plat/bin/appRev</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Install Time: Fri Sep 28 15:54:04 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product Name: PM&amp;C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product Release: 5.0.0_50.10.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Part Number ISO: 872-2441-905</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Part Number USB: 872-2441-105</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Base Distro Product: TPD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Base Distro Release: 6.0.0_80.22.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Base Distro ISO: TPD.install</td>
</tr>
<tr>
<td>9</td>
<td>Logout of the virsh console</td>
<td>Logout of the virsh console</td>
<td>Hold ctrl ] to logout of the PMAC</td>
</tr>
<tr>
<td>10</td>
<td>Note</td>
<td>If configuring a system with Aggregation switches, continue to procedure 7. If configuring a system without aggregation switches, skip to procedure 8.</td>
<td></td>
</tr>
</tbody>
</table>
4.5 Configure Cisco 4948E-F Aggregation Switches

4.5.1 Configure netConfig Repository

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

For switches, use the following command:

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

For services, use the following command:

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

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

IPv4 and IPv6

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

Terminology

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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;management_server_iLO_ip&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;management_server_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;netConfig_server_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_backup_user&gt;</td>
<td>admusr</td>
</tr>
<tr>
<td>&lt;switch_backup_user_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;serial console type&gt;</td>
<td>u=USB, c=PCIe</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;switch_hostname&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;device_model&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;console_name&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_console_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_platform_username&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_platform_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_enable_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmt_netmask&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;mgmt_vlanID&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;control_vlanID&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;IOS_filename&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;ip_version&gt;</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;switch_hostname&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;device_model&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;console_name&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_console_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_platform_username&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_platform_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_enable_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmt_netmask&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;mgmt_vlanID&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;control_vlanID&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;IOS_filename&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;ip_version&gt;</td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 7. Configure netConfig Repository

### Prerequisite:
This procedure assumes a recently IPM'ed TVOE server with a VM hosting the PM&C application.

### Needed material:
- HP Misc. Firmware USB
- HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.8) [1]
- DSR USB or ISO

**Note:** Uplinks must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables.

**Note:** The generic XML configuration file referenced in this procedure needs to be updated to match the customer's network.

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

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | **1st RMS iLO/iLOM:** Log in to iLO/iLOM, follow **Appendix D**: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI.  

```bash
https://<management_server_iLO_ip>
```

Login as `admusr`. |
Procedure 7. Configure netConfig Repository

2. **TVOE iLO/iLO:**
   - SSH into the Management Server

Using an SSH client such as putty, ssh to the TVOE host as `admusr`.

Login using `virsh`, and wait until you see the login prompt:

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

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>myTPD</td>
<td>running</td>
</tr>
<tr>
<td>2</td>
<td>PM&amp;C</td>
<td>running</td>
</tr>
</tbody>
</table>
```

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

[Output Removed]
Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64
PM&Cdev7 login:
```
### Procedure 7. Configure netConfig Repository

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command and Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>Virtual PMAC: Setup netConfig Repository</strong></td>
<td>Use netConfig to create a repository entry that will use the ssh service. This command will provide the user with several prompts. The prompts shown with <code>&lt;variables&gt;</code> as the answers are site specific that the user MUST modify. Other prompts that don't have a <code>&lt;variable&gt;</code> shown as the answer must be entered EXACTLY as they are shown here:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Type? (tftp, ssh, conserver, oa) ssh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service host? <code>&lt;netConfig_server_mgmt_ip_address&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter an option name <code>&lt;q to cancel&gt;</code>: user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter the value for user: <code>&lt;switch_backup_user&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter an option name <code>&lt;q to cancel&gt;</code>: password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter the value for password: <code>&lt;switch_backup_user_password&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Password: <code>&lt;switch_backup_user_password&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter an option name <code>&lt;q to cancel&gt;</code>: q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add service for ssh_service successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To ensure that you entered the information correctly, use the following command and inspect the output, which will be similar to the one shown below.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Name: ssh_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: ssh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host: 10.250.8.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options: password: C20F7D639AE7E7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user: admusr</td>
</tr>
<tr>
<td>4</td>
<td><strong>Virtual PMAC: Configure TFTP service</strong></td>
<td>Use netConfig to create a repository entry that will use the TFTP service. This command will give the user several prompts. The prompts with <code>&lt;variables&gt;</code> as the answers are site specific that the user MUST modify. Other prompts that don't have a <code>&lt;variable&gt;</code> as the answer must be entered EXACTLY as they are shown here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service type? (tftp, ssh, conserver, oa) tftp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service host? <code>&lt;netConfig_server_mgmt_ip_address&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter an option name (q to cancel): dir</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter a value for user dir: <code>/var/TKLC/smac/image/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter an option name(q to cancel): q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add service for tftp_service successful</td>
</tr>
</tbody>
</table>
### Procedure 7. Configure netConfig Repository

| 5 | Virtual PMAC: Run conserverSetup | Execute the following command to run the conserverSetup:
|   |   | $ sudo /usr/TKLC/plat/bin/conserverSetup -u -s <management_server_mgmt_ip_address>
|   |   | You will be prompted 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

| 6 | 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>
**Procedure 7. Configure netConfig Repository**

<table>
<thead>
<tr>
<th>Virtual PMAC:</th>
<th>Use netConfig to create a repository entry for each switch. The initial command will prompt the user multiple times. The prompts with <code>&lt;variables&gt;</code> as the answers are site specific that the user MUST modify. Other prompts that don't have a <code>&lt;variable&gt;</code> as an answer must be entered EXACTLY as they are shown here. <strong>Note:</strong> The <code>&lt;device_model&gt;</code> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact Appendix U: My Oracle Support (MOS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setup the netConfig Repository with Aggregation Switch Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>sudo /usr/TKLC/plat/bin/netConfig --repo addDevice</strong></td>
<td></td>
</tr>
<tr>
<td><strong>name=&lt;switch_hostname&gt; --reuseCredentials</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device Vendor? Cisco</strong></td>
<td>Device Model? <code>&lt;device_model&gt;</code></td>
</tr>
<tr>
<td><strong>Device Model? <code>&lt;device_model&gt;</code></strong></td>
<td>What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <code>&lt;switch_mgmt_ip_address&gt;</code></td>
</tr>
<tr>
<td><strong>What is the management interface a port or a vlan? [vlan]: [Enter]</strong></td>
<td>Is the management interface a port or a vlan? [vlan]: [Enter]</td>
</tr>
<tr>
<td><strong>What is the VLAN ID of the management VLAN? [2]: &lt;mgmt_vlanID&gt;</strong></td>
<td>What is the VLAN ID of the management VLAN? [2]: [Enter]</td>
</tr>
<tr>
<td><strong>What is the switchport connects to the management server? [GE40]: [Enter]</strong></td>
<td>What is the switchport mode (access/trunk) for the management server port? [trunk]: [Enter]</td>
</tr>
<tr>
<td><strong>What is the VLAN ID of the management VLAN? [2]: &lt;mgmt_vlanID&gt;</strong></td>
<td>What are the allowed vlans for the management server port? [1,2]: <code>&lt;control_vlanID&gt;, &lt;mgmt_vlanID&gt;</code></td>
</tr>
<tr>
<td><strong>Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.XO.bin]: <code>&lt;IOS_filename&gt;</code></strong></td>
<td>Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.XO.bin]: <code>&lt;IOS_filename&gt;</code></td>
</tr>
<tr>
<td><strong>Firmware file to be used in upgrade: <code>&lt;IOS_filename&gt;</code></strong></td>
<td>File transfer service to be used in upgrade: <code>tftp_service</code></td>
</tr>
<tr>
<td><strong>Enter the name of the upgrade file transfer service: <code>tftp_service</code></strong></td>
<td>Should the init oob adapter be added (y/n)? y</td>
</tr>
<tr>
<td><strong>Adding consoleInit protocol for &lt;switch_hostname&gt; using oob...</strong></td>
<td>Adding consoleInit protocol for &lt;switch_hostname&gt; using oob...</td>
</tr>
<tr>
<td><strong>What is the name of the service used for OOB access? console_service</strong></td>
<td>What is the name of the console for OOB access? <code>&lt;console_name&gt;</code></td>
</tr>
<tr>
<td><strong>What is the platform access username? &lt;switch_platform_username&gt;`</strong></td>
<td>What is the device console password? <code>&lt;switch_console_password&gt;</code></td>
</tr>
<tr>
<td><strong>What is the device console password? <code>&lt;switch_console_password&gt;</code></strong></td>
<td>What is the platform user password? <code>&lt;switch_platform_password&gt;</code></td>
</tr>
<tr>
<td><strong>What is the device privileged mode password? <code>&lt;switch_enable_password&gt;</code></strong></td>
<td>What is the device privileged mode password? <code>&lt;switch_enable_password&gt;</code></td>
</tr>
<tr>
<td><strong>Verify password: <code>&lt;switch_platform_password&gt;</code></strong></td>
<td>Verify password: <code>&lt;switch_platform_password&gt;</code></td>
</tr>
<tr>
<td><strong>What is the device privileged mode password? <code>&lt;switch_enable_password&gt;</code></strong></td>
<td>Verify password: <code>&lt;switch_enable_password&gt;</code></td>
</tr>
<tr>
<td><strong>Should the live network adapter be added (y/n)? y</strong></td>
<td>Adding cli protocol for &lt;switch_hostname&gt; using network...</td>
</tr>
<tr>
<td><strong>Network device access already set: <code>&lt;switch_mgmt_ip_address&gt;</code></strong></td>
<td>Should the live oob adapter be added (y/n)? y</td>
</tr>
<tr>
<td><strong>Adding cli protocol for &lt;switch_hostname&gt; using oob...</strong></td>
<td>Adding cli protocol for &lt;switch_hostname&gt; using oob...</td>
</tr>
<tr>
<td><strong>OOB device access already set: console_service</strong></td>
<td>OOB device access already set: console_service</td>
</tr>
<tr>
<td><strong>Device named &lt;switch_hostname&gt; successfully added.</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 7. Configure netConfig Repository

<table>
<thead>
<tr>
<th>Step</th>
<th>Virtual PMAC:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Verification</td>
<td>To check that you entered the information correctly, use the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=&lt;switch_hostname&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The output should be similar to the one shown:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=&lt;switch_hostname&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device: &lt;switch_hostname&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor: Cisco</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model: &lt;device_model&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FW Ver: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FW Filename: &lt;IOS_image&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FW Service: tftp_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initialization Management Options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgmtIP: &lt;switch_mgmt_ip_address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgmtInt: vlan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgmtVlan: &lt;mgmt_vlanID&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgmtVlanName: management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface: GE40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mode: trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>allowedVlans: &lt;control_vlanID&gt;, &lt;mgmt_vlanID&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access: Network: &lt;switch_mgmt_ip_address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access: OOB:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service: console_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Console: &lt;console_name&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Init Protocol Configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Live Protocol Configured</td>
</tr>
</tbody>
</table>

| 9    | Virtual PMAC: | Repeat Steps 7-8 for the second Cisco 4948. |
|      | Repeat For Second 4948. | |
4.5.2 Configure Cisco 4948E-F Aggregation Switches

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

Procedure Reference Tables:

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;switch_platform_username&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_platform_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_enable_password&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;management_server_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;pmac_mgmt_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmtVLAN_id&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;mgmt_Vlan_subnet_id&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;netmask&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch1A_mgmtVLAN_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch_mgmt_netmask&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;switch1B_mgmtVLAN_ip_address&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;management_server_mgmtInterface&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;management_server_iLO_ip&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;customer_supplied_ntp_server_address&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;platcfg_password&gt;</td>
<td>Initial password as provided by Oracle</td>
</tr>
<tr>
<td>&lt;management_server_mgmtInterface&gt;</td>
<td>Value gathered from NAPD</td>
</tr>
<tr>
<td>&lt;switch_backup_user&gt;</td>
<td>admusr</td>
</tr>
<tr>
<td>&lt;switch_backup_user_password&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 1    | Virtual PMAC: Verify IOS image is on the system | Verify the IOS image is on the system. If the appropriate image does not exist, copy the image to the PMAC.  
$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file> |
| 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  

Note: Ignore the sentry restart instructions  
Note: This may take up to 60 seconds to complete. |
| 3    | Virtual PMAC TVOE HOST: Manipulate host server physical interfaces. | Exit from the virtual PMAC console, by entering <ctrl-d> and you will be returned to the server prompt. Ensure that the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:  
$ 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)

<table>
<thead>
<tr>
<th>4</th>
<th>Virtual PMAC: Determine if switch1A PROM upgrade is required</th>
</tr>
</thead>
</table>

Determine if switch1A PROM upgrade is required.

**Note:** ROM & PROM are intended to have the same meaning for this procedure

Connect serially to switch1A by issuing the following command.

```
$ 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 Appendix U: My Oracle Support (MOS)

Note the IOS image & ROM version for comparison in a following step. Exit from the console by entering `<ctrl-e>`<c><.> and you will be returned to the server prompt.

Check the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix K: Upgrade Cisco 4948 PROM to upgrade the PROM for switch1A.
### Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)

<table>
<thead>
<tr>
<th></th>
<th>Virtual PMAC: Modify configure xml file with information needed to initialize the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Extract the configuration files from the zip file copied in procedure 6</td>
</tr>
</tbody>
</table>

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

**Note:** This will create a directory called "DSR_NetConfig_Templates" which contains all the necessary configuration files. Copy the following files using the following commands

```
$ sudo cp DSR_NetConfig_Templates/init/Aggregation/*.xml /usr/TKLC/smac/etc
$ sudo cp DSR_NetConfig_Templates/config/DSR_RMS_Productization/4948E-F_L3_configure.xml /usr/TKLC/smac/etc
$ sudo chmod 644 /usr/TKLC/smac/etc/*.xml
```

**Note:** Update the 4948E init and configure xml files to match your network parameters. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has `<some_variable_name>` will need to be modified, removing the dollar sign and the less than, greater than sign.

```
$ 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
```
Initialize switch1A by issuing the following command:

```
$ 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 about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Appendix U: My Oracle Support (MOS). A successful completion of netConfig will return the user to the prompt.

Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.

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

Hostname: switch1A
```
$
```

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

Exit the PM&C with the escape character is `<ctrl]->`

Exit from the virtual PMAC console, by entering `<ctrl]->` and you will be returned to the server prompt. Ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_2>
$ sudo /sbin/ifdown <ethernet_interface_1>
```
### Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>TVOE iLO/iLO: SSH into the Management Server</td>
<td>Log back into the PMAC. Login using <code>virsh</code>, and wait until you see the login prompt:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo /usr/bin/virsh list</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Id</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo /usr/bin/virsh console &lt;PM&amp;C&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Output Removed]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starting ntdMgr: [ OK ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starting atd: [ OK ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'TPD Up' notification(s) already sent: [ OK ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upstart: Starting tpdProvd...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upstart: tpdProvd started.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CentOS release 6.2 (Final)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kernel 2.6.32-220.17.1.el6prerele6.0.0_x86_64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on an x86_64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PM&amp;Cdev7 login:</td>
</tr>
<tr>
<td>9</td>
<td>Virtual PMAC: Initialize switch1B</td>
<td>Initialize switch1B by issuing the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processing file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact <strong>Appendix U: My Oracle Support (MOS)</strong>. A successful completion of netConfig will return the user to the prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hostname: switch1B</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If this command fails, stop this procedure and contact <strong>Appendix U: My Oracle Support (MOS)</strong></td>
</tr>
</tbody>
</table>
### Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
</table>
| 10   | Virtual PM&C: Modify PMAC Feature to disable TFTP | Disable the DEVICE.NETWORK.NETBOOT feature.  

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

**Note:** Ignore the sentry restart instructions  

**Note:** This may take up to 60 seconds to complete.

| 11   | Virtual PMAC: Configure the switches | Configure both switches by issuing the following command:  

```
$ sudo /usr/TKLCL/plat/bin/netConfig --file=/usr/TKLCL/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 Appendix U: My Oracle Support (MOS).

| 12   | TVOE Management Server: Enable Interfaces on TVOE Host | Exit from the virtual PM&C console, by entering `<ctrl-d>` and you will be returned to the server prompt.  

Ensure that the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:  

```
$ sudo /sbin/ifup <ethernet_interface_1>  
$ sudo /sbin/ifup <ethernet_interface_2>
```
Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)

13. **TVOE iLO/iLO:** SSH into the Management Server

   Log back into the PMAC.

   Login using `virsh`, and wait until you see the login prompt:

   ```
   $ 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.
   CentOS release 6.2 (Final)
   Kernel 2.6.32-220.17.1.el6prerelease.0.14.0.x86_64
   on an x86_64
   PM&Cdev7 login:
   ```

14. **Virtual PMAC:** Verify switch configuration

   Ping each of the interfaces 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 the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

16. **Virtual PMAC:** Verify access to customer network

   Verify connectivity to the customer network by issuing the following command

   ```
   $ /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 the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.
**Procedure 8. Configure Cisco 4948E-F Aggregation Switches (netConfig)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Command</th>
</tr>
</thead>
</table>
| 18   | Verify access to customer network | Verify connectivity to the customer network by issuing the following command:  

```bash
$ /bin/ping <customer_supplied_ntp_server_address>
```

| 19   | Re-attach uplinks of switch1A | Re-attach switch1A customer uplink cables. Refer to the NAPD for which ports are uplink ports.  

**Note:** If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

| 20   | TVOE Management Server: Restore the TVOE host back to its original state | Exit from the virtual PM&C console, by entering `<ctrl-J>` and you will be returned to the server prompt.  

Restore the server networking back to original state:  

```bash
$ sudo /sbin/service network restart
```
4.6 Configure PMAC Server

Procedure 9. Configure the PMAC Server

This procedure will provide PMAC configuration using the web interface.

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

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

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

1. **PMAC GUI: Login**

   Open web browser and navigate to the PMAC GUI, Login as **PMACadmin** user:

   ```
   https://<pmac_network_ip>
   ```
**Procedure 9. Configure the PMAC Server**

2. **PMAC GUI:** Configure Optional Features

Navigate to **Main Menu -> Administration -> PM&C Configuration**

If **NetBackup** is to be used, enable the NetBackup feature. Otherwise use the selected features as is. The following image is for reference only:

**Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Role</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE.NETWORK.NETBOOT</td>
<td>Network device</td>
<td>management</td>
<td>[✓]</td>
</tr>
<tr>
<td>DEVICE.NTP</td>
<td>PMAC as a time server</td>
<td>management</td>
<td>[✓]</td>
</tr>
<tr>
<td>PMAC.MANAGED</td>
<td>Remote management of PMAC server</td>
<td>management</td>
<td>[✓]</td>
</tr>
<tr>
<td>PMAC.REMOTE.BACKUP</td>
<td>Remote server for backup</td>
<td>management</td>
<td>[✓]</td>
</tr>
<tr>
<td>PM&amp;C.NETBACK</td>
<td>NetBackup client</td>
<td>management</td>
<td>[✓]</td>
</tr>
</tbody>
</table>

Make sure that the roles for all the features are set to **management**.

Also make sure that the enabled checkbox is checked for the following:
- DEVICE.NETWORK.NETBOOT
- DEVICE.NTP
- PM&C.REMOTE.BACKUP
- PM&C.NETBACK (only if NetBackup is used)

And click on **Apply**. This foreground task will take a few moments, and then refresh the view with an Info or Error notice to verify the action. To discard changes, just navigate away from the view.
Procedure 9. Configure the PMAC Server

3. PMAC GUI: Settings summary

Go to In the Main Menu -> Administration -> PM&C Configuration

The following summary screen will be displayed. This will provide a summary of PM&C configuration.
### Procedure 9. Configure the PMAC Server

#### 4. PMAC Command Line: Configure a System Health Check

**Execute the following commands:**

```
$ alarmMgr -alarmStatus
```

This command should return no output on a healthy system.

```
$ sudo sentry status
```

All Processes should be running, displaying output similar to the following:

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Status</th>
<th>StartTS</th>
<th>NumR</th>
</tr>
</thead>
<tbody>
<tr>
<td>smacTalk</td>
<td>9039</td>
<td>running</td>
<td>Tue Jul 24 12:50:29 2012</td>
<td>2</td>
</tr>
<tr>
<td>smacMon</td>
<td>9094</td>
<td>running</td>
<td>Tue Jul 24 12:50:29 2012</td>
<td>2</td>
</tr>
<tr>
<td>hpiPortAudit</td>
<td>9137</td>
<td>running</td>
<td>Tue Jul 24 12:50:29 2012</td>
<td>2</td>
</tr>
<tr>
<td>snmpEventHandler</td>
<td>9176</td>
<td>running</td>
<td>Tue Jul 24 12:50:29 2012</td>
<td>2</td>
</tr>
<tr>
<td>eclipseHelp</td>
<td>9196</td>
<td>running</td>
<td>Tue Jul 24 12:50:30 2012</td>
<td>2</td>
</tr>
</tbody>
</table>

**Fri Aug 3 13:16:35 2012**

Command Complete.

#### 5. PMAC Command Line: Install NetBackup (Optional)

1. **If the NetBackup client installation will rely on the TPD “nbAutoInstall” process to configure the PM&C NetBackup client perform the following at the PMAC Command Line, otherwise continue to sub bullet 2 below.**

   **Command:**
   ```
   $ 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/
   ```

   Use TPD platcfg utility to add the NetBackup Server’s alias and IP to the “/etc/hosts” file.

Procedure 9. Configure the PMAC Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC Command Line: Perform a backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$ sudo pmacadm backup</td>
</tr>
</tbody>
</table>

Perform PMAC application backup using the following command:

```
$ sudo pmacadm backup
```

PM&C backup been successfully initiated as task ID 7

[usradm@pmacDev3 ~]$`

**Note:** The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPM&C_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

Next Verify that the backup was successful using the following command:

```
$ 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:

Once the backup has been verified that it was successful, copy the backup file to a remote location. The backup file is located under /var/TKLC/smac/backup.
### 4.7 Add Cabinet to PMAC

**Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>If you make a mistake, click Cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail.</td>
</tr>
<tr>
<td><strong>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</strong></td>
<td></td>
</tr>
</tbody>
</table>

**1. PMAC GUI: Login**

Open web browser and navigate to the PMAC GUI, Login as **PMACadmin** user:

```
https://<pmac_network_ip>
```

[Oracle System Login Image]
Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Configure Cabinets</th>
<th>Navigate to Main Menu -&gt; Hardware -&gt; System Configuration -&gt; Configure Cabinets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>Press the <strong>Add Cabinet</strong> Button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter the Cabinet ID, and press the <strong>Add Cabinet</strong> button:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Image of Add Cabinet button]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cabinet ID: <strong>1</strong>; Cabinet ID must be from 1 to 654</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Image of Add Cabinet dialog box]</td>
</tr>
<tr>
<td>3</td>
<td>PMAC GUI: Check Errors</td>
<td>If no error is reported to the user you will see the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Image of Configure Cabinets dialog box]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or you will see an error message:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Image of Add Cabinet error dialog box]</td>
</tr>
</tbody>
</table>
Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>PMAC GUI: Configure RMS</strong> Navigate to <strong>Main Menu -&gt; Hardware -&gt; System Configuration -&gt; Configure RMS</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Configure RMS Panel" /></td>
</tr>
<tr>
<td>5</td>
<td><strong>PMAC GUI: Add RMS</strong> On the Configure RMS panel, click the <strong>Add RMS</strong> button.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add RMS Panel" /></td>
</tr>
<tr>
<td>6</td>
<td><strong>PMAC GUI: Enter information</strong> Enter the IP Address of the rack mount server management port (iLO/iLOM). All the other fields are optional. Then click on the <strong>Add RMS</strong> button.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add RMS Details" /></td>
</tr>
</tbody>
</table>

**Note:** The PMAC contains default credentials for the rack mount server management port (not to be confused with OS or Application credentials), however if you know the default credentials will not work then enter the valid credentials for the rack mount server management port.
Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory

If no error is reported to the user you will see the following

Configure RMS

Or you will see an error message:

Add RMS

Error

- Both the user and the password must be specified or neither.
### Procedure 10. Add Cabinet and Enclosure to the PMAC system Inventory

| 8 | **PMAC GUI:** Verify RMS discovered |

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

The RMS inventory page is displayed.

![RMS inventory page](image)

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

**Note:** If **“Status”** displays an error, contact **Appendix U: My Oracle Support (MOS)**.
### 4.8 Install TVOE on Additional Rack Mount Servers

**Procedure 11. Install TVOE on Additional Rack Mount Servers**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>PMAC GUI: Login</strong></td>
</tr>
</tbody>
</table>

Open web browser and navigate to the PMAC GUI, Login as **PMACadmin** user:

```
https://<pmac_network_ip>
```

---

**Prerequisite:** PMAC (virtualized) has been installed on the First RMS Server.

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

If this procedure fails, contact **Appendix U: My Oracle Support (MOS)**, and ask for assistance.
Procedure 11. Install TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Task</th>
</tr>
</thead>
</table>
| 2    | Configure RMS on PM&C Server | Navigate to **Main Menu -> Hardware -> System Configuration -> Configure RMS.**  

![Diagram showing the navigation process](image)

**Click Add RMS**

<table>
<thead>
<tr>
<th>RMS IP</th>
<th>RMS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are no provisioned RMS

![Add RMS button](image)

**Click Add RMS**

Enter the IP Address of the rack mount server management port (iLO). All the other fields are optional. Then click on the **Add RMS** button.

**Click Add RMS**

![Add RMS form](image)

The iLO IP address and name of the new RMS should now be displayed.

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Repeat for Additional Rack Mount Servers</td>
<td>Repeat Step 2 for any additional rack mount servers you wish to configure.</td>
</tr>
</tbody>
</table>
### Procedure 11. Install TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>TVOE Host: Load TVOE ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Attach the USB device containing the ISO image to a USB port.</td>
</tr>
<tr>
<td></td>
<td>- Login to the PMAC GUI if not already done so (Step 1)</td>
</tr>
<tr>
<td></td>
<td>- In the &quot;VM Entities&quot; list, select the PMAC guest. On the resulting &quot;View VM Guest&quot; page, select the Media tab.</td>
</tr>
<tr>
<td></td>
<td>- Under the Media tab, find the ISO image in the &quot;Available Media&quot; list, and click its Attach button. After a pause, the image will appear in the &quot;Attached Media&quot; list.</td>
</tr>
<tr>
<td>2.</td>
<td>Using a TVOE 64 bit iso file</td>
</tr>
<tr>
<td></td>
<td>Use sftp to transfer the iso image to the PMAC server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as PMACftpusr user:</td>
</tr>
<tr>
<td></td>
<td># cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server)</td>
</tr>
<tr>
<td></td>
<td># Using sftp, connect to the PMAC management server</td>
</tr>
<tr>
<td></td>
<td>&gt; sftp pmacftpusr@&lt;PM&amp;C_management_network_ip&gt;</td>
</tr>
<tr>
<td></td>
<td>&gt; put &lt;image&gt;.iso</td>
</tr>
<tr>
<td></td>
<td># After the image transfer is 100% complete, close the connection</td>
</tr>
<tr>
<td></td>
<td>&gt; quit</td>
</tr>
</tbody>
</table>
Procedure 11. Install TVOE on Additional Rack Mount Servers

5 PMAC GUI: Add TVOE image

Navigate to Main Menu -> Software -> Manage Software Images

Press Add Image button. Use the drop down to select the image.

If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the TVOE Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the TVOE Management Server before you started this procedure, choose a correspondingly higher device number.

If in Step 4 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/..."

Select the appropriate path and Press Add New Image button.

You may check the progress using the Task Monitoring link. Observe the green bar indicating success.

Once the green bar is displayed, remove the TVOE Media from the optical drive of the TVOE Management Server.
Procedure 11. Install TVOE on Additional Rack Mount Servers

6 PMAC GUI: Select RMS Servers for TVOE OS install

Navigate to Software -> Software Inventory.

Select the RMS servers you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.

Click on Install OS

7 PMAC GUI: Initiate OS Install on RMS Server(s)

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

Click on Start Install, a confirmation window will pop up, click on Ok to proceed with the install.
Procedure 11. Install TVOE on Additional Rack Mount Servers

Navigate to Main Menu -> Task Monitoring to monitor the progress of the TVOE Installation background task. A separate task will appear for each server affected.

When the installation is complete, the task will change to green and the Progress bar will indicate “100%”.

4.9 Configure TVOE on Additional Rack Mount Servers

Procedure 12. Configure TVOE on Additional Rack Mount Servers

This procedure will configure TVOE on all remaining RMS Servers.

**Prerequisite:** RMS Server has been IPM’ed with TVOE OS

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

If this procedure fails, contact **Appendix U:** My Oracle Support (MOS), and ask for assistance.
## Procedure 12. Configure TVOE on Additional Rack Mount Servers

Determine the bridge interfaces to be used on the TVOE server and fill in the appropriate values in the table below. If netbackup is to be used, determine the bridge interface to be used for the netbackup network and fill in the `<TVOE_NetBackup_Bridge_Interface>` value.

The entries in this table should match the table that was filled out for the first RMS in **procedure 4, step 1**.

<table>
<thead>
<tr>
<th>Guest Interface Alias</th>
<th>TVOE Bridge Name</th>
<th>TVOE Bridge Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>control</td>
<td>control</td>
<td>Fill in the appropriate value (default is bond0):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_Control_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>management</td>
<td>management</td>
<td>Fill in the appropriate value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_Management_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>xmi</td>
<td>xmi</td>
<td>Fill in the appropriate value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_XMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>imi</td>
<td>imi</td>
<td>Fill in the appropriate value, (default is bond0.4):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_IMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>xsi1</td>
<td>xsi1</td>
<td>Fill in the appropriate value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_XSI1_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>xsi2</td>
<td>xsi2</td>
<td>Fill in the appropriate value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_XSI2_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>netbackup (if applicable)</td>
<td>netbackup</td>
<td>Fill in the appropriate value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;TVOE_NetBackup_Bridge_Interface&gt;</td>
</tr>
</tbody>
</table>
## Procedure 12. Configure TVOE on Additional Rack Mount Servers

### 2. RMS iLO/iLOM: Login and Launch the Integrated Remote Console

Log in to iLO/iLOM, follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI.

```
https://<management_server_iLO_ip>
```

### 3. RMS iLO/iLOM: Create Tagged Control Interface and Bridge (Optional)

If you are using a tagged control network interface on this TVOE Server, then complete this step. Otherwise, **skip to the next step**.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --delBridgeInt=bond0
Interface bond0 updated
Bridge control updated
```

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

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

### 4. RMS iLO/iLOM: Create the Management Network

Create the Management network, execute the following command:

**Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

```
$ 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>
--bridgeInterfaces=<TVOE_Management_Bridge_Interface>
```
Procedure 12. Configure TVOE on Additional Rack Mount Servers

5

RMS
iLO/iLOM:
Create the
XMI Network

Configure the XMI Network:

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

```
$sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_XMI_Bridge_Interface> --onboot=yes
Interface bond0.3 added

$sudo /usr/TKLC/plat/bin/netAdm add
--type=Bridge --name=xmi
--onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>
Interface bond0.3 was updated.
Bridge xmi added!
```

6

RMS
iLO/iLOM:
Create the
IMI Network

Configure the IMI Network:

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

```
$sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_IMI_Bridge_Interface> --onboot=yes
Interface bond0.4 added

$sudo /usr/TKLC/plat/bin/netAdm add
--type=Bridge --name=imi
--onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface>
Interface bond0.4 was updated.
Bridge imi added!
```
## Procedure 12. Configure TVoE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>7</th>
<th>RMS iLO/iLOM: Create the XSI-1 Network (with Aggregation Switches)</th>
</tr>
</thead>
</table>

Execute this step if deploying with Aggregation switches, otherwise skip this step.

**Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

Execute the following commands:

```
$ sudo /usr/TKLC/plat/bin/netAdm add
  --device=<TVOE_XSI1_Bridge_Interface>  --onboot=yes

Interface bond0.5 added
```

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge
  --name=xsil  --onboot=yes
  --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>

Interface bond0.5 was updated.
Bridge xsil added!
```
### Procedure 12. Configure TVOE on Additional Rack Mount Servers

- **RMS iLO/iLOM:** Create the XSI-1 Network (without Aggregation Switches)

  Execute this step if deploying **without Aggregation switches**

  Execute the following commands:

  ```
  $ sudo /usr/TKLC/plat/bin/netAdm add --device=bond1 --onboot=yes --type=Bonding --mode=active-backup --miimon=100
  Interface bond1 added
  
  $ sudo /usr/TKLC/plat/bin/netAdm set --device=eth03 --type=Ethernet --master=bond1 --slave=yes --onboot=yes
  Interface eth03 updated
  
  $ sudo /usr/TKLC/plat/bin/netAdm set --device=eth13 --type=Ethernet --master=bond1 --slave=yes --onboot=yes
  Interface eth13 updated
  
  $ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes
  Interface bond1.<XSI1_VLAN_ID> added
  
  $ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>
  Interface bond1.<XSI1_VLAN_ID> was updated. Bridge xsi1 added!
  ```
### Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Page</th>
<th>RMS iLO/iLOM: Create the XSI-2 Network (with Aggregation Switches)</th>
<th>RMS iLO/iLOM: Create the XSI-2 Network (without Aggregation Switches)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Execute the following commands for deployments without Aggregation switches:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Option 1: Deployment with Aggregation switches:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--device=&lt;TVOE_XSI2_Bridge_Interface&gt; --onboot=yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface bond0.6 added</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi2 --onboot=yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--bridgeInterfaces=&lt;TVOE_XSI2_Bridge_Interface&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface bond0.6 was updated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bridge xsi2 added!</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Execute the following commands for deployments without Aggregation switches:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--device=&lt;TVOE_XSI2_Bridge_Interface&gt; --onboot=yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface bond1.&lt;XSI2_VLAN_ID&gt; added</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xsi2 --onboot=yes --bridgeInterfaces=&lt;TVOE_XSI2_Bridge_Interface&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface bond1.&lt;XSI2_VLAN_ID&gt; was updated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bridge xsi2 added!</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th></th>
<th>RMS iLO/iLOM: Add the NetBackup Network- Option 1 (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>If NetBackup is to be used, execute this step, otherwise skip to Step 14.</td>
</tr>
<tr>
<td></td>
<td>Select only this option or the following options listed in steps 12-13.</td>
</tr>
<tr>
<td></td>
<td>Before selecting the configuration option, first read the description in each step to determine which configuration is applicable to your installation and network.</td>
</tr>
<tr>
<td></td>
<td>NetBackup is a tool that allows the customer to take remote backups of the system.</td>
</tr>
<tr>
<td></td>
<td>Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.</td>
</tr>
<tr>
<td></td>
<td>Note: The example below illustrates a TVOE Management Server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.</td>
</tr>
<tr>
<td></td>
<td>Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.</td>
</tr>
<tr>
<td></td>
<td>Create netbackup bridge using a bond containing an untagged interface</td>
</tr>
</tbody>
</table>

```
$ 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>
```
# Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 12   | **RMS iLO/iLOM:** Add the NetBackup Network-Option 2 (Optional)  
Select only this option or options in Steps 11 or 13  
Create NetBackup bridge using an untagged native interface:  
```bash
$ 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>
```
| 13   | **RMS iLO/iLOM:** Add the NetBackup Network-Option 3 (Optional)  
Select only this option or options in 11-12  
Create NetBackup bridge using a tagged device:  
```bash
$ sudo /usr/TKLC/plat/bin/netAdm add  
--device=<TVOE_NetBackup_Bridge_Interface>  
--onboot=yes
```

Interface `<TVOE_NetBackup_Bridge_Interface>` added  
```bash
$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>
```
| 14   | **RMS iLO/iLOM:** Restart the network interfaces  
Restart the network interfaces, execute the following command:  
```bash
$ sudo service network restart
```
## Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 15   | **RMS iLO/iLOM:** Set Hostname  
Set the server hostname by running the following:  
```
$ sudo su - platcfg
```
Navigate to **Server Configuration -> Hostname -> Edit.**  
Set TVOE Management Server hostname  
Press **OK.**  
Navigate out of Hostname |
| 16   | **RMS iLO/iLOM:** Set the Time Zone and/or Hardware Clock  
Navigate to **Server Configuration -> Time Zone.**  
Select **Edit.**  
Set the time zone and/or hardware clock to **“UTC” (or appropriate time zone value)**  
Press **OK.**  
Navigate out of **Server Configuration** |
Procedure 12. Configure TVOE on Additional Rack Mount Servers

RMS iLO/iLOM: Set NTP

Navigate to Network Configuration -> NTP.

The Time Servers page will now be shown, which shows the configured NTP servers and peers (if there are NTP servers already configured).

Update NTP Information, select Edit. The Edit Time Servers menu is displayed.

Select the appropriate Edit Time Servers menu option. You can add new or edit any existing NTP server entry.

Set NTP server IP address to point to the customer provided NTP server (Remember that 3 distinct NTP sources are required)

Press OK.

Exit platcfg.

Ensure that the time is set correctly by executing the following commands:

```
$ sudo service ntpd stop
$ sudo ntpdate ntpserver1
$ sudo service ntpd start
```
### Procedure 12. Configure TVOE on Additional Rack Mount Servers

| Page | RMS iLO/iLOM: Set SNMP | Set SNMP by running the following:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td></td>
<td>$ sudo su - platcfg</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

Exit platcfg.
Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 19   | **RMS iLO/iLOM:** Restart Server  
Execute the following command to restart the server:  

```bash
$ sudo init 6
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 20   | **RMS iLO/iLOM:** Configure NetBackup - Part 1 (Optional)  
Execute this step if the **NetBackup** feature is enabled for this system, otherwise skip this step. Configure the appropriate NetBackup client on the PMAC TVOE host.  
Open firewall ports for NetBackup using the following commands:  

```bash
$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt /usr/TKLC/plat/etc/iptables/
$ sudo /usr/TKLC/plat/bin/iptablesadm reconfig
```

Enable `platcfg` to show the Netbackup Menu Items by executing the following commands:

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

Create LV and file system for Netbackup client software on the vgguests volume group:

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

This will create the LV, format it with a filesystem, and mount it under `/usr/openv/`.  

Example output is shown below:

```
 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**

### RMS iLO/iLOM: Configure NetBackup-Part 2 (Optional)

21

- **RMS iLO/iLOM:** Configure NetBackup-Part 2 (Optional)

  **Install the netbackup client software:**

  Refer to Appendix I: Application NetBackup Client Installation Procedures on instructions how to install the netbackup client.

  **Note:** Skip any steps relating to copying netbackup "notify" scripts to /usr/openv/netbackup/bin. The TVOE netbackup notify scripts are taken care of in the next step.

  Create softlinks 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 following files form the TVOE host:

  - /var/TKLC/bkp/*.iso

### RMS iLO/iLOM: Setup syscheck

22

- **RMS iLO/iLOM:** Setup syscheck

  **Syscheck must be configured to monitor bonded interfaces.**

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

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

### RMS iLO/iLOM: Verify syscheck

23

- **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
  ```
### Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 24   | **RMS**<br>iLO/iLOM: **Verify Server Health**<br>Execute the following: <br>```
$ alarmMgr -alarmStatus
```
This command should return no output on a healthy system. If any alarms are reported, contact Appendix U: My Oracle Support (MOS) |
| 25   | **RMS**<br>iLO/iLOM: **Perform a TVOE backup using TPD platcfg utility**<br>Execute the following: <br>```
$ sudo su - platcfg
```
Navigate to **Maintenance -> Backup and Restore**<br>Select **Backup Platform (CD/DVD)**<br>Note: If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device.” Press **Enter** to continue.<br>Select an applicable backup option, and press **Enter** to continue. Exit from TPD platcfg utility.<br>The TVOE backup can be found in the “/var/TKLC/bkp/” directory, and is prefixed by the server hostname. An example of a TVOE backup ISO follows: <br>/var/TKLC/bkp/RMS503u14-plat-app-201210301505.iso<br>Move the TVOE backup to a customer provided backup server for safe keeping. |
| 26   | **Additional RMS:** **Repeat**<br>Repeat this procedure for additional Rack Mount Servers. |
### 4.10 Create Virtual Machines for Applications

**Procedure 13. Load DSR and TPD ISO to the PMAC Server**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| 1      | **TVOE Host: Load Application ISO** | Add the TPD ISO image to the PMAC, this can be done in one of three ways:  
1. Insert the CD containing the TPD image into the removable media drive.  
2. Attach the USB device containing the ISO image to a USB port.  
3. Copy the Application iso file to the PMAC server into the “/var/TKLC/smac/image/isoimages/home/smacftpusr/” directory as pmacftpusr user:  
   cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server)  
   Using sftp, connect to the PMAC server  
   ```bash  
   $ sftp pmacftpusr@<pmac_management_network_ip>  
   $ put <image>.iso  
   ```  
   After the image transfer is 100% complete, close the connection:  
   ```bash  
   $ quit  
   ``` |
| 2      | **PMAC GUI: Login** | Open web browser and enter:  
https://<PMAC_Mgmt_Network_IP>  
Login as pmacadmin user:  
![Oracle System Login](image) |

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
### Procedure 13. Load DSR and TPD ISO to the PMAC Server

<table>
<thead>
<tr>
<th></th>
<th><strong>PMAC GUI:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Attach the software Image to the PMAC Guest</td>
</tr>
</tbody>
</table>

If in Step 1 the ISO image was transferred directly to the PMAC guest via sftp, skip the rest of this step and continue with **step 4**. If the image is on a CD or USB device, continue with this step.

In the PMAC GUI, navigate to **Main Menu -> VM Management**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the **Media** tab.

Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its **Attach** button. After a pause, the image will appear in the "**Attached Media**" list.
## Procedure 13. Load DSR and TPD ISO to the PMAC Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Add TPD Image</td>
</tr>
</tbody>
</table>
|      | Navigate to **Main Menu -> Software -> Manage Software Images**  
|      | Press **Add Image** button. Use the drop down to select the image.  
|      | ![Image](device://...). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, **device://dev/sr1**. If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.  
|      | If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file `/var/TKLC/...`.  
|      | ![Image](Add Software Image)  
|      | Select the appropriate path and Press **Add New Image** button.  
|      | ![Image](Task Monitoring) link. Observe the green bar indicating success.  
|      | Once the green bar is displayed, remove the TPD Media from the optical drive of the management server. |
| 5    | Load DSR ISO |
|      | If the DSR ISO hasn’t been loaded onto the PMAC already, repeat steps 1 through 4 to load it using the DSR media or ISO. |
Procedure 14. Create NOAM Guest VMs

This procedure will provide the steps needed to create a DSR NOAM virtual machine (referred to as a “guest”) on a TVOE RMS. It must be repeated for every NOAM server you wish to install.

Prerequisite: TVOE has been installed and configured on the target RMS

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

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>PMAC GUI: Login</th>
<th>Open web browser and enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PMA C GUI: Login</td>
<td><a href="https://%3CPMAC_Mgmt_Network_IP%3E">https://&lt;PMAC_Mgmt_Network_IP&gt;</a></td>
</tr>
</tbody>
</table>

Login as *pmacadmin* user:
### Procedure 14. Create NOAM Guest VMs

<table>
<thead>
<tr>
<th></th>
<th><strong>PMAC GUI:</strong> Navigate to VM Management of the Target Server</th>
<th><strong>Navigate to Main Menu -&gt; VM Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Step 1:</strong> Navigate to Main Menu -&gt; VM Management of the Target Server. Select the TVOE rack mounted server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.</td>
<td></td>
</tr>
</tbody>
</table>

Select the TVOE rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server’s guest machine configuration will then be displayed in the remaining area of the window.

---

Click **Create Guest**
Procedure 14. Create NOAM Guest VMs

3 PMAC GUI: Configure VM Guest Parameters

- Select Import Profile

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

<table>
<thead>
<tr>
<th>NOAM VM TVOE Hardware Type(s)</th>
<th>Dedicated Netbackup Interface?</th>
<th>Choose Profile (&lt;Application ISO NAME&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP DL380 Gen 8 RMS, HP DL380 Gen 9 RMS, Sun Netra RMS</td>
<td>No</td>
<td>DSR_NOAMP_RMS</td>
</tr>
<tr>
<td>HP DL380 Gen 8 RMS, HP DL380 Gen 9 RMS, Sun Netra RMS</td>
<td>Yes</td>
<td>DSR_NOAMP_NETBACKUP_RMS</td>
</tr>
</tbody>
</table>

**Note:** Refer to Section 1.5 for the supported hardware for DSR 6.0, 7.0, and 7.1.

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

Press **Select Profile**.

Press **Create**.
Procedure 14. Create NOAM Guest VMs

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>Wait for Guest Creation to Complete</strong></td>
<td>Navigate to Main Menu -&gt; Task Monitoring to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched. Wait or refresh the screen until you see that the guest creation task has completed successfully.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Verify Guest Machine is Running</strong></td>
<td>Navigate to Main Menu -&gt; VM Management. Select the TVOE server on which the guest machine was just created. Look at the list of guests present on the and verify that you see a guest that matches the name you configured and that its status is “<strong>Running</strong>”. VM Creation for this guest is complete.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Repeat for remaining NOAM VMs</strong></td>
<td>Repeat from Step 2 for any remaining NOAM VMs (for instance, the standby NOAM) that must be created.</td>
</tr>
</tbody>
</table>
### Procedure 15. Create SOAM Guest VMs

This procedure will provide the steps needed to create a DSR SOAM virtual machine (referred to as a "guest") on a TVOE RMS. It must be repeated for every SOAM server you wish to install.

**Prerequisite:** TVOE has been installed and configured on the target RMS

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Step Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PMAC GUI: Login</td>
<td>Open web browser and enter: &lt;https://&lt;PMAC_Mgmt_Network_IP&gt;&gt;&lt;br&gt;Login as <code>pmacadmin</code> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
Procedure 15. Create SOAM Guest VMs

2. **PMAC GUI:**
   Navigate to VM Management of the Target Server

Navigate to Main Menu -> VM Management

Select the TVOE rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.

Click **Create Guest**
Procedure 15. Create SOAM Guest VMs

<table>
<thead>
<tr>
<th>3</th>
<th>PMAC GUI: Configure VM Guest Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select Import Profile</td>
</tr>
<tr>
<td></td>
<td>![Image of import profile setup]</td>
</tr>
<tr>
<td></td>
<td>From the “ISO/Profile” drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running on and your preference for NetBackup interfaces:</td>
</tr>
<tr>
<td></td>
<td>&lt;Application ISO NAME&gt; =&gt; DSR_SOAM_RMS</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM</td>
</tr>
<tr>
<td></td>
<td>Press Select Profile.</td>
</tr>
<tr>
<td></td>
<td>Press Create</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>PMAC GUI: Wait for Guest Creation to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Task Monitoring</strong> to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched.</td>
</tr>
<tr>
<td></td>
<td>Wait or refresh the screen until you see that the guest creation task has completed successfully.</td>
</tr>
</tbody>
</table>
**Procedure 15. Create SOAM Guest VMs**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>PMAC GUI:</strong> Verify Guest Machine is Running</td>
<td>Navigate to <em>Main Menu -&gt; VM Management</em>&lt;br&gt; Select the TVOE server on which the guest machine was just created.&lt;br&gt; Look at the list of guests present on the rack mount server and verify that you see a guest that matches the name you configured and that its status is <em>“Running”</em>. VM Creation for this guest is complete.</td>
</tr>
<tr>
<td>6</td>
<td><strong>PMAC GUI:</strong> Repeat for remaining SOAM VMs</td>
<td>Repeat from <em>Step 2</em> for any remaining SOAM VMs (for instance, the standby SOAM) that must be created.</td>
</tr>
</tbody>
</table>
### Procedure 16. Create MP Guest VMs

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>PMAC GUI: Login</strong>&lt;br&gt;Open web browser and enter: &lt;br&gt;<code>https://&lt;PMAC_Mgmt_Network_IP&gt;</code>&lt;br&gt;Login as <code>pmacadmin</code> user:</td>
</tr>
</tbody>
</table>

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

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

If this procedure fails, contact **Appendix U: My Oracle Support (MOS)**, and ask for assistance.
Procedure 16. Create MP Guest VMs

2. **PMAC GUI:**
   - Navigate to VM Management of the Target Rack Mount Server

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

   Select the rack mount server from the **VM Entities** listing on the left side of the screen. The selected server’s guest machine configuration will then be displayed in the remaining area of the window.

   Click **Create Guest**
Procedure 16. Create MP Guest VMs

3. PMAC GUI: Configure VM Guest Parameters

Select Import Profile

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

<Application ISO NAME> => DSR_MP_RMS

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

Press Select Profile.

You can edit the name, if you wish. For instance: “DSR_MP_A,” or DSR_MP_B”. (This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)

Press Create

4. PMAC GUI: Wait for Guest Creation to Complete

Navigate to Main Menu -> Task Monitoring to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched.

Wait or refresh the screen until you see that the guest creation task has completed successfully.
### Procedure 16. Create MP Guest VMs

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 5    | PMAC GUI: | Verify Guest Machine is Running | Navigate to **Main Menu -> VM Management**
|      |          |      | Select the TVOE server on which the guest machine was just created. Look at the list of guests present on the rack mount server and verify that you see a guest that matches the name you configured and that its status is **"Running"**. VM Creation for this guest is complete. |
| 6    | PMAC GUI: | Repeat for remaining MP VMs | Repeat from **Step 2** for any remaining MP VMs that must be created. |
**Procedure 17. Create IP Front End (IPFE) Guest VMs**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1      | PMAC GUI: Open web browser and enter:  
https://<PMAC_Mgmt_Network_IP>  
Login as pmacadmin user: |

This procedure will provide the steps needed to create an IPFE virtual machine (referred to as a "guest") on a TVOE server. It must be repeated for every server you wish to install.

**Prerequisite:** TVOE has been installed and configured on the target RMS.

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

If this procedure fails, contact **Appendix U: My Oracle Support (MOS), and ask for assistance.**
Procedure 17. Create IP Front End (IPFE) Guest VMs

2

PMAC GUI:
Navigate to VM Management of the Target Rack Mount Server

Navigate to Main Menu -> VM Management

Select the TVOE rack mount server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.

Click Create Guest
Procedure 17. Create IP Front End (IPFE) Guest VMs

3  PMAC GUI: Configure VM Guest Parameters

Select **Import Profile**

![Import Profile Image]

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

<Application ISO NAME> \(\rightarrow\) DSR_IPFE_RMS

**Note:** Application ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM.

Press **Select Profile**.

You can edit the name, if you wish. For instance: “DSR_IPFE_A,” or “DSR_IPFE_B”. (This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)

Press **Create**

4  PMAC GUI: Wait for Guest Creation to Complete

Navigate to **Main Menu -> Task Monitoring** to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched.

Wait or refresh the screen until you see that the guest creation task has completed successfully.
### Procedure 17. Create IP Front End (IPFE) Guest VMs

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Verify Guest Machine is Running</td>
<td>Navigate to Main Menu -&gt; VM Management. Select the TVOE rack mount server on which the guest machine was just created. Look at the list of guests present on the rack mount server and verify that you see a guest that matches the name you configured and that its status is “Running”. VM Creation for this guest is complete.</td>
</tr>
<tr>
<td>6</td>
<td>Repeat for remaining IPFE VMs</td>
<td>Repeat from Step 2 for any remaining IPFE VMs that must be created.</td>
</tr>
</tbody>
</table>
4.11 Install Software on Virtual Machines

Procedure 18. IPM VMs

This procedure will provide the steps to install TPD on rack mount server guest VMs.

**Prerequisite**: VM Guests creation has been completed.

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

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

<table>
<thead>
<tr>
<th>S T E P #</th>
<th>PMAC GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open web browser and enter:</td>
</tr>
<tr>
<td></td>
<td><strong>https://&lt;PMAC_Mgmt_Network_IP&gt;</strong></td>
</tr>
</tbody>
</table>

Login as *pmacadmin* user:
Procedure 18. IPM VMs

2

- PMAC GUI: Select Servers for OS install
  
  Navigate to Software -> Software Inventory.

  Select the VM servers (IPFEs, MPs, etc.) you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.

  **Note:** VM’s will have the text “Guest: <VM_GUEST_NAME>” underneath the physical RMS that hosts them.

  ![Software Inventory Screen]

  Click on Install OS
  
  ![Install, Upgrade, Refresh Buttons]

3

- PMAC GUI: Initiate OS Install
  
  The left side of this screen shows the servers to be affected by this TPD 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 and Images Tables]

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

  ![Start Install Button]
Procedure 18. IPM VMs

| 4 | PMAC GUI: Monitor OS Install | Navigate to Main Menu -> Task Monitoring to monitor the progress of the OS Installation background task. A separate task will appear for each VM affected. When the installation is complete, the task will change to green and the Progress bar will indicate "100%". |

Procedure 19. Install the DSR Application Software on the VMs

| STEP # | PMAC GUI: Login | Open web browser and enter: [https://<PMAC_Mgmt_Network_IP>]  

Login as pmacadmin user: | 1 |
Procedure 19. Install the DSR Application Software on the VMs

2  PMAC GUI: Select Servers for DSR Application Install

Navigate to Software -> Software Inventory.

Select the VM servers (IPFEs, MPs, Etc.) you want to install with DSR. If you want to install the same DSR image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.

Note: VM's will have the text “Guest: <VM_GUEST_NAME>” underneath the RMS that hosts them.

<table>
<thead>
<tr>
<th>ID</th>
<th>IP Address</th>
<th>Hostname</th>
<th>Plat Name</th>
<th>Plat Version</th>
<th>App Name</th>
<th>App Version</th>
<th>Design Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>192.168.1.4</td>
<td>mstSITOE-Kauai-B</td>
<td>TFO (x86_64)</td>
<td>6.3.0.0.0-184.17.0</td>
<td>TFOE</td>
<td>Pending Activation</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>192.168.1.1</td>
<td>mstSITOE-Kauai</td>
<td>TFO (x86_64)</td>
<td>6.3.0.0.0-184.17.0</td>
<td>TFOE</td>
<td>Pending Activation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>192.168.1.6</td>
<td>mstSITOE-Kauai-A</td>
<td>TFO (x86_64)</td>
<td>6.3.0.0.0-184.17.0</td>
<td>TFOE</td>
<td>Pending Activation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>192.168.1.1</td>
<td>mstSITOE-Kauai-B</td>
<td>TFO (x86_64)</td>
<td>6.3.0.0.0-184.17.0</td>
<td>TFOE</td>
<td>Pending Activation</td>
<td></td>
</tr>
</tbody>
</table>

Click on Upgrade

3  PMAC GUI: Initiate DSR Application Install

The left side of this screen shows the servers to be affected by this DSR application installation. Select the DSR image to install to all of the selected servers.

Click on Start Software Upgrade, a confirmation window will pop up, click on Ok to proceed with the install.
Procedure 19. Install the DSR Application Software on the VMs

4. **PMAC GUI: Monitor DSR Application Install**

Navigate to **Main Menu -> Task Monitoring** to monitor the progress of the OS installation background task. A separate task will appear for each VM affected.

When the installation is complete, the task will change to green and the Progress bar will indicate “100%”.

5. **PMAC GUI: Accept/Reject Upgrade**

Navigate to **Software -> Software Inventory** to accept the software installation. Select all the servers on which the application has been installed in the previous steps and click on **Accept Upgrade** as shown below.

Note: On some Rack mount servers, the GUI may not provide the option to accept upgrade. So first verify in “task monitoring” that the upgrade is not in progress, then manually accept or reject the upgrade by ssh'ing into the server and execute:

- To accept:

  ```
  $ sudo /var/TKLC/backout/accept
  ```

  **Note:** Once the upgrade has been accepted, the App version will change from “Pending Acc/Rej” to the version number of the application.
4.12 Application Configuration: NOAMs

Procedure 20. Configure First NOAM NE and Server

This procedure will provide the steps to configure the First NOAM server.

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

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

1. Save the NOAM Network Data to an XML file

   Using a text editor, create a NOAM Network Element file that describes the networking of the target install environment of your first NOAM server.
   Select an appropriate file name and save the file to a known location on your computer.
   A suggested filename format is “Appname_NEname_NetworkElement.XML”, so for example a DSR2 NOAM network element XML file would have a filename “DSR2_NOAM_NetworkElement.xml”.
   Alternatively, you can update the sample DSR 6.0/7.0/7.1 Network Element file. It can be found on the management server at:
   
   /usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml
   
   A sample XML file can also be found in Appendix L: Sample Network Element.

   **Note:** The following limitations apply when specifying a Network Element name: A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.

2. Exchange SSH keys between PMAC and first NOAM server

   Use the PMAC GUI to determine the Control Network IP address of the server that is to be the first NOAM server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.
   
   Note the IP address for the first NOAM server.
   Login to the PMAC terminal as the admusr.
   
   From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the 1st NOAM server using the keyexchange utility, using the Control network IP address for the NOAM server.
   When prompted for the password, enter the password for the admusr user of the NOAM server.
   
   $ keyexchange admusr@<NO1_Control_IP_Address>
### Procedure 20. Configure First NOAM NE and Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 3    | **Connect a Web Browser to the NOAM GUI** | Plug a laptop Ethernet cable onto an unused, un-configured port on the 4948 switch (if available in your installation) or use SSH Tunneling through the PMAC to connect the laptop to the NOAM server.  
If you are using tunneling, then you can skip the rest of this step and instead complete the instructions in Appendix M: Accessing the NOAM GUI using SSH Tunneling with Putty (for using Putty) Appendix N: Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows (for OpenSSH). OpenSSH is recommended if you are using a Windows 7 PC.  
From the PMAC, enable the switch port that the laptop is plugged into.  
Enable that laptop Ethernet port to acquire a DHCP address and then access the NOAM-"A" GUI via its control IP address. |
| 4    | **NOAM GUI: Login**         | Login to the NOAM GUI as the guiadmin user:                                                                                             |

![Oracle System Login](image-url)

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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 20. Configure First NOAM NE and Server

Create the NOAM Network Element using the XML File

Navigate to Main Menu->Configuration->Network Elements

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

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

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

```
Browse... No file selected.  
```

Insert  Delete  Export  Report

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

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network Address</th>
<th>Netmask</th>
<th>VLAN ID</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAL/MI</td>
<td>10.240.10.0/24</td>
<td>255.255.255.0</td>
<td>8</td>
<td>10.240.10.35</td>
</tr>
<tr>
<td>INTERNAL/MI</td>
<td>10.240.10.0/24</td>
<td>255.255.255.0</td>
<td>4</td>
<td>10.240.10.3</td>
</tr>
</tbody>
</table>
Procedure 20. Configure First NOAM NE and Server

Map Services to Networks

Navigate to Main Menu -> Configuration -> Services.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Intra-NE Network</th>
<th>Inter-NE Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;XMI Network&gt;</td>
</tr>
<tr>
<td>Replication</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;XMI Network&gt;</td>
</tr>
<tr>
<td>Signaling</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>HA Secondary</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>HA_MP_Secondary</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Replication_MP</td>
<td>&lt;IMI Network&gt;</td>
<td>Unspecified</td>
</tr>
<tr>
<td>ComAgent</td>
<td>&lt;IMI Network&gt;</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

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

Select the Ok button to apply the Service-to-Network selections.
Procedure 20. Configure First NOAM NE and Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 7 | **Insert the 1st NOAM server** | Navigate to **Main Menu -> Configuration -> Servers.**
    
    Select the **Insert** button to insert the new NOAM server into servers table (the first or server).
    
    | Attribute | Value | Description |
    |-----------|-------|-------------|
    | Hostname | ND-Server1 | Unique name for the server (ID string. Valid characters are alphabetic with an quotation mark and end with ”) |
    | Role | NETWORK OAM&P | Select the function of the server |
    | System ID | ND-Server1 | System ID for the NOAM of SON 64-character string. Valid values are |
    | Hardware Profile | DSR TVOE Guest | Hardware profile of the server |
    | Network Element Name | NOAMMEMORYTEST | Select the network element |
    | Location | | Location description [Default = "*", value is any text string] |

    Fill in the fields as follows:
    
    **Hostname**: `<Hostname>`
    
    **Role**: **NETWORK OAM&P**
    
    **System ID**: `<Site System ID>`
    
    **Hardware Profile**: **DSR TVOE Guest**
    
    **Network Element Name**: **[Choose NE from Drop Down Box]**
    
    The network interface fields will now become available with selection choices based on the chosen hardware profile and network element.
    
    | Network | IP Address | Interface |
    |---------|------------|-----------|
    | INTERNAL.XMI (10.249.84.129/25) | 10.249.84.166 | xmi | VLAN (3) |
    | INTERNAL.IMI (10.240.85.0/25) | 10.240.85.10 | imi | VLAN (4) |

    Fill in the server IP addresses for the XMI network. Select **xmi** for the interface. Leave the "VLAN" checkbox unchecked.
    
    Fill in the server IP addresses for the IMI network. Select **imi** for the interface. Leave the "VLAN" checkbox unchecked.
    
    Next, add the following NTP servers:
    
    | NTP Server | Preferred? |
    |------------|------------|
    | `<RMS1-TVOE-IP-Address>` | Yes |

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 8 | **Export the Initial Configuration** | Navigate to **Main Menu -> Configuration -> Servers.**

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

    ![Buttons](Image)
### Procedure 20. Configure First NOAM NE and Server

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM iLO:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9    | **Copy Configuration File to 1st NOAM Server** | Obtain a terminal window to the 1st NOAM server, logging in as the *admusr* user. (See Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the NOAM from iLO)  
Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the /var/tmp directory.  
The configuration file will have a filename like TKLCCfgData.<hostname>.sh.  
The following is an example:  

```bash  
$ sudo cp /var/TKLC/db/filemgmt/TKLCCfgData.RMS01.sh /var/tmp/TKLCCfgData.sh  
```

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM iLO:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 10   | **Wait for Configuration to Complete** | The automatic configuration daemon will look for the file named “TKLCCfgData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.  
Wait to be prompted to reboot the server, but **DO NOT** reboot the server, it will be rebooted later on in this procedure.  
**Note:** Ignore the warning about removing the USB key, since no USB key is present. |

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM iLO:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 11   | **Set the Time zone and Reboot the Server** | From the command line prompt, execute `set_ini_tz.pl`. This will set the system time zone.  
The following command example uses the America/New_York time zone.  
Replace as appropriate with the time zone you have selected for this installation.  
For a full list of valid time zones, see Appendix J: List of Frequently used Time Zones  

```bash  
$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl  
"America/New_York" /dev/null 2>&1  
```

```bash  
$ sudo init 6  
```
## Procedure 20. Configure First NOAM NE and Server

### 1st NOAM: Configure Networking for Dedicated NetBackup Interface (Optional)

**Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.

Obtain a terminal window to the 1st NOAM server, logging in as the `admusr` user.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP_Address> --netmask=<NO1_NetBackup_NetMask>
```

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address>
```

### 1st NOAM Server: Verify Server Health

Execute the following command on the 1st 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
```
### Procedure 21. Configure the NOAM Server Group

<table>
<thead>
<tr>
<th><strong>STEP #</strong></th>
<th><strong>NOAM GUI:</strong> Login</th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login</td>
<td>Establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of:</td>
</tr>
</tbody>
</table>

```
https://<NO1_XMI_IP_Address>
```

Login as the *guiadmin* user:

![Oracle System Login](image)

- Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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 21. Configure the NOAM Server Group

NOAM GUI:
Enter NOAM Server Group Data

Navigate to Main Menu -> Configuration -> Server Groups

Select Insert and fill the following fields:

- Server Group Name: <Enter Server Group Name>
- Level: A
- Parent: None
- Function: DSR (Active/Standy Pair)
- WAN Replication Connection Count: Use Default Value

Select OK when all fields are filled in.
Procedure 21. Configure the NOAM Server Group

From the GUI Main Menu -> Configuration -> Server Groups.

Select the new server group, and then select Edit.

Select the Network Element that represents the NOAM.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPC3NO</td>
<td>Include in SG</td>
<td>Preferred Spare</td>
</tr>
</tbody>
</table>

In the portion of the screen that lists the servers for the server group, find the NOAM server being configured.

Click the Include in SG checkbox.

Leave other boxes blank.

Press OK.
Procedure 21. Configure the NOAM Server Group

| NOAM: Verify NOAM server role | From terminal window to the iLO of the first NOAM server, execute the following command:

```
$ha.mystate
```

Verify that the `DbReplication` and `VIP` item under the `resourceId` column has a value of `Active` under the `role` column.

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

Example:

```
<table>
<thead>
<tr>
<th>resourceId</th>
<th>role</th>
<th>node</th>
<th>subResources</th>
<th>lastUpdate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DbReplication</td>
<td>Active</td>
<td>A1027.209</td>
<td>0 0316:161158.499</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>Active</td>
<td>A1027.209</td>
<td>0 0316:161158.501</td>
<td></td>
</tr>
<tr>
<td>pSbrBaseRep1</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.074</td>
<td></td>
</tr>
<tr>
<td>pSbrBindingRes</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.074</td>
<td></td>
</tr>
<tr>
<td>pSbrBaseRep1</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.075</td>
<td></td>
</tr>
<tr>
<td>pSbrSessionRes</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.075</td>
<td></td>
</tr>
<tr>
<td>PERR_B_Proc</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.074</td>
<td></td>
</tr>
<tr>
<td>PERR_S_Proc</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.075</td>
<td></td>
</tr>
<tr>
<td>CmdProcessRes</td>
<td>Active</td>
<td>A1027.209</td>
<td>0 0316:161158.501</td>
<td></td>
</tr>
<tr>
<td>DB_MP_reader</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.071</td>
<td></td>
</tr>
<tr>
<td>DBR_SDD</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.071</td>
<td></td>
</tr>
<tr>
<td>VIP_DA_MP</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.072</td>
<td></td>
</tr>
<tr>
<td>EXSTACK_Process</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.072</td>
<td></td>
</tr>
<tr>
<td>DSR_Process</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.072</td>
<td></td>
</tr>
<tr>
<td>CERN_KFID_Proc</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.070</td>
<td></td>
</tr>
<tr>
<td>DSNOM_Proc</td>
<td>Active</td>
<td>A1027.209</td>
<td>0 0316:161158.497</td>
<td></td>
</tr>
<tr>
<td>CERN_KFID2_Proc</td>
<td>OS</td>
<td>A1027.209</td>
<td>0 0316:161554.070</td>
<td></td>
</tr>
<tr>
<td>SS7_MP_Proces</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.073</td>
<td></td>
</tr>
<tr>
<td>SS7_MP_Process</td>
<td>OS</td>
<td>A1027.209</td>
<td>0-63 0316:161554.074</td>
<td></td>
</tr>
</tbody>
</table>
```
Procedure 21. Configure the NOAM Server Group

5

NOAM GUI: Restart 1st NOAM Server

From the NOAM GUI, select the Main menu -> Status & Manage -> Server menu.

Select the first NOAM server. Select the Restart button.

Answer OK to the confirmation popup.

Are you sure you wish to restart application software on the following server(s)?
Jetta-NO-1

Wait for restart to complete.
Procedure 22. Configure the Second NOAM Server

This procedure will provide the steps to configure the Second NOAM server.

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

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

1

Exchange SSH keys between PMAC and Second NOAM server

Use the PMAC GUI to determine the Control Network IP address of the server that is to be the second NOAM server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.

Note the IP address for the Second NOAM server.

Login to the PMAC terminal as the admusr.

From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the 2nd NOAM server using the keyexchange utility, using the Control network IP address for the NOAM server. When prompted for the password, enter the password for the admusr user of the NOAM server.

$ keyexchange admusr@<NO2_Control_IP_Address>

Note: if keyexchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.

2

NOAM GUI: Login

If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of:

https://<NO1_XMI_IP_Address>

Login to the NOAM GUI as the guiadmin user:
Procedure 22. Configure the Second NOAM Server

3

**NOAM GUI:** Insert the 2\(^{nd}\) NOAM server

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

Select the **Insert** button to insert the 2\(^{nd}\) NOAM server into servers table (the first or server).

![Adding a new server](image)

Fill in the fields as follows:

**Hostname:** `<Hostname>`

**Role:** NETWORK OAM&P

**System ID:** `<Site System ID>`

**Hardware Profile:** DSR TVOE Guest

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

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

![Network interface fields](image)

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

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

Next, add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RMS2-TVOE-IP-Address&gt;</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Select the **Ok** button when you have completed entering all the server data.
# Procedure 22. Configure the Second NOAM Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4    | **NOAM GUI:** Export the Initial Configuration | Navigate to Main Menu -> Configuration -> Servers.  
From the GUI screen, select the NOAM server and then select **Export** to generate the initial configuration data for that server. |
| 5    | **1st NOAM Server:** Copy Configuration File to 2nd NOAM Server | Obtain a terminal session to the 1st NOAM as the **admusr** user.  
Use the **awpushcfg** utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the 2nd NOAM server, using the Control network IP address for the 2nd NOAM server.  
The configuration file will have a filename like “TKLCCfgData.<hostname>.sh”.  
```bash  
$ sudo awpushcfg  
```
The **awpushcfg** utility is interactive, so the user will be prompted for the following:  
* IP address of the local PMAC server: Use the local control network address from the PMAC.  
* Username: Use **admusr**  
* Control network IP address for the target server: In this case, enter the control IP for the 2nd NOAM server.  
* Hostname of the target server: Enter the server name configured in **step 3**
## Procedure 22. Configure the Second NOAM Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 6    | **PMAC:** Verify awpushcfg was called and Reboot the Server. Obtain a terminal window connection on the 2<sup>nd</sup> NOAM. SSH from the 1<sup>st</sup> NOAM to the 2<sup>nd</sup> NOAM server by executing the following command: 

```
$ ssh admusr@<NO2_Control_IP_Address>
```

Login as the `admusr` user. 

The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. 

Verify awpushcfg was called by checking the following file: 

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

Verify the following message is displayed: 

 `[SUCCESS] script completed successfully!`

Now Reboot the Server: 

```
$ sudo init 6
```

Wait for the server to reboot.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 7    | **2<sup>nd</sup> NOAM Server:** Establish an SSH session and Login. Obtain a terminal window to the 2<sup>nd</sup> NOAM server, logging in as the `admusr` user.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8    | **2<sup>nd</sup> NOAM Server:** Configure Networking for Dedicated NetBackup Interface (Optional). **Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup. 

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask>
```

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>
```
### Procedure 22. Configure the Second NOAM Server

<table>
<thead>
<tr>
<th>9</th>
<th><strong>2nd NOAM Server</strong></th>
<th>Verify Server Health</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Execute the following command on the 2nd NOAM server and make sure that no errors are returned:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>$ sudo syscheck</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class hardware...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class disk...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class net...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class system...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class proc...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 23. Complete NOAM Server Group Configuration

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>NOAM GUI:</strong> Login</td>
<td>Establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td><strong>https://&lt;NO1_XMI_IP_Address&gt;</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Login as the <em>guiadmin</em> user:</td>
<td></td>
</tr>
</tbody>
</table>

If this procedure fails, contact **Appendix U: My Oracle Support (MOS)**, and ask for assistance.
Procedure 23. Complete NOAM Server Group Configuration

2

NOAM GUI:
Edit the NOAM Server Group Data

Navigate to Main Menu->Configuration->Server Groups.

Select the NOAM Server group and click on Edit

Add the 2\textsuperscript{nd} NOAM server to the Server Group by clicking the Include in SG checkbox for the 2\textsuperscript{nd} NOAM server.

Click Apply.

Add a NOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below.
Procedure 23. Complete NOAM Server Group Configuration

3. NOAM VIP: Establish GUI Session
   Establish a GUI session on the NOAM by using the XMI VIP address:
   https://<NOAM_VIP_IP_Address>
   Login as user guiadmin.

4. NOAM VIP: Wait for Remote Database Alarm to Clear
   Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.
   Navigate to Main menu->Alarms & Events->View Active

<table>
<thead>
<tr>
<th>Seq #</th>
<th>Event ID</th>
<th>Timestamp</th>
<th>Severity</th>
<th>Product</th>
<th>Process</th>
<th>NE</th>
<th>Server</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>414</td>
<td>10200</td>
<td>2015-03-20 09:39:00 EDT</td>
<td>CLEAR</td>
<td>apgw Gomez server</td>
<td>Compass_NO</td>
<td>Compass-NOA</td>
<td>CFG</td>
<td></td>
</tr>
<tr>
<td>413</td>
<td>10200</td>
<td>2015-03-20 09:41:11 EDT</td>
<td>NONE</td>
<td>apgw Gomez server</td>
<td>Compass_NO</td>
<td>Compass-NOA</td>
<td>CFG</td>
<td></td>
</tr>
</tbody>
</table>
**Procedure 23. Complete NOAM Server Group Configuration**

<table>
<thead>
<tr>
<th>5</th>
<th><strong>NOAM GUI:</strong> Restart 2nd NOAM Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From the NOAM GUI, select the <strong>Main menu -&gt; Status &amp; Manage -&gt; Server</strong> menu.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>Select the 2nd NOAM server. Select the <strong>Restart</strong> button.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Restart" /></td>
</tr>
<tr>
<td></td>
<td>Answer <strong>OK</strong> to the confirmation popup.</td>
</tr>
<tr>
<td></td>
<td>Are you sure you wish to restart application software on the following server(s)?</td>
</tr>
<tr>
<td></td>
<td>Jetta-NO-2</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="OK Cancel" /></td>
</tr>
<tr>
<td></td>
<td>Wait for restart to complete. Wait approximately 3-5 minutes before proceeding.</td>
</tr>
</tbody>
</table>
### 4.13 Application Configuration: NetBackup Client Installation (Optional)

**Procedure 24. Install NetBackup Client (Optional)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>This procedure will download and install NetBackup Client software on the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- /usr/TKLC/appworks/sbin/bpstart_notify</td>
</tr>
<tr>
<td></td>
<td>- /usr/TKLC/appworks/sbin/bpend_notify</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>

1. **Install NetBackup Client Software**  
   If a customer has a way of transferring and installing the net Backup client without the aid of TPD tools (push configuration) then use Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL
   **Note:** This is not common. If the answer to the previous question is not known then use Appendix I.1: NetBackup Client Install using PLATCFG

2. **Install NetBackup Client Software**  
   Choose the same method used in step 1 to install NetBackup on the 2nd NOAM.
## 4.14 Application Configuration: Disaster Recovery NOAM (Optional)

**Procedure 25. NOAM Configuration for DR Site (Optional)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This procedure will provide the steps to configure the First DR NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
<td></td>
</tr>
</tbody>
</table>

1. **PRIMARY NOAM VIP GUI: Login**

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

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

   Login as the `guiadmin` user:

   ![Oracle System Login](image)

   Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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 25. NOAM Configuration for DR Site (Optional)

**Primary NOAM VIP GUI:** Insert the DR NOAM Network Element

Navigate to Main Menu—>Configuration—>Network Elements

The **Network Elements** screen will display select the **Browse** (scroll to bottom left corner of screen).

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

<table>
<thead>
<tr>
<th>Insert</th>
<th>Edit</th>
<th>Delete</th>
<th>Lock/Unlock</th>
<th>Report</th>
<th>Export</th>
</tr>
</thead>
</table>

A dialogue will pop up, browse to the location of the DSR DR NOAM Site Element XML File and click the **Open** button.

Then click **Upload File** as shown below

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

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Network Name</th>
<th>Network Address</th>
<th>Netmask</th>
<th>VLAN ID</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_900805</td>
<td>INTERNAL1WI</td>
<td>10.240.10.32</td>
<td>255.255.256.0</td>
<td>2</td>
<td>10.240.10.35</td>
</tr>
<tr>
<td>NO_900805</td>
<td>INTERNAL1WI</td>
<td>10.240.10.0</td>
<td>255.255.256.0</td>
<td>4</td>
<td>10.240.10.3</td>
</tr>
</tbody>
</table>
Procedure 25. NOAM Configuration for DR Site (Optional)

3 PRIMARY NOAM VIP GUI: Insert the 1st DR-NOAM server

Navigate to Main Menu -> Configuration -> Servers.

Select the Insert button to insert the new DR-NOAM server into servers table.

![Add server interface]

Fill in the fields as follows:

Hostname: <Hostname>

Role: NETWORK OAM&P

System ID: <Site System ID>

Hardware Profile: DSR TVOE Guest

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

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

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

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

Next, add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DRNO1-RMS-TVOE-IP-Address&gt;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Select the Ok button when you have completed entering all the server data.
### Procedure 25. NOAM Configuration for DR Site (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>PRIMARY NOAM VIP</strong>&lt;br&gt;<strong>GUI:</strong> Export the Initial Configuration&lt;br&gt;&lt;br&gt;Navigate to <strong>Main Menu -&gt; Configuration -&gt; Servers.</strong>&lt;br&gt;From the GUI screen, select the DR-NOAM server and then select <strong>Export</strong> to generate the initial configuration data for that server.</td>
</tr>
<tr>
<td>5</td>
<td><strong>PMAC:</strong> Exchange SSH keys between PMAC and DR-NOAM server&lt;br&gt;&lt;br&gt;Use the PMAC GUI to determine the Control Network IP address of the server that is to be the first NOAM server. From the PMAC GUI, navigate to <strong>Main Menu -&gt; Software -&gt; Software Inventory.</strong>&lt;br&gt;Note the IP address for the first DR-NOAM server.&lt;br&gt;&lt;br&gt;Login to the PMAC terminal as the <strong>admusr.</strong>&lt;br&gt;From a terminal window connection on the PMAC as the <strong>admusr</strong> user, exchange SSH keys for <strong>admusr</strong> between the PMAC and the 1st DR-NOAM server using the keyexchange utility, using the Control network IP address for the NOAM server. When prompted for the password, enter the password for the <strong>admusr</strong> user of the NOAM server.</td>
</tr>
<tr>
<td>6</td>
<td><strong>NOAM VIP:</strong> Exchange SSH keys between NOAM and PMAC at the DR site.&lt;br&gt;&lt;br&gt;From a terminal window connection on the NOAMP VIP as the <strong>admusr.</strong>&lt;br&gt;Exchange SSH keys for admusr between the NOAM and the DR NO’s PMAC using the keyexchange utility. When prompted for the password, enter the appropriate password for <strong>admusr</strong> on the PMAC server.</td>
</tr>
</tbody>
</table>
Procedure 25. NOAM Configuration for DR Site (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 7 | **Primary NOAM:** Copy Configuration File to 1st DR-NOAM Server | Obtain a terminal session to the primary NOAM as the *admusr* user. Use the `awpushcfg` utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the primary NOAM to the 1st DR-NOAM server, using the Control network IP address for the DR-NOAM server. The configuration file will have a filename like "TKLCConfigData.<Hostname>.sh".  

```
$ sudo awpushcfg
```

The `awpushcfg` utility is interactive, so the user will be prompted for the following:

- IP address of the local PMAC server: Use the local control network address from the PMAC.
- Username: Use *admusr*
- Control network IP address for the target server: In this case, enter the control IP for the 1st DR-NOAM server.
- Hostname of the target server: Enter the server name configured in step 3.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8 | **1st DR-NOAM Server:** Verify awpushcfg was called and Reboot the Server | Obtain a terminal window connection on the 1st DR-NOAM iLO from the OA. (Use the procedure in Appendix D: TVOE iLO/iLOM GUI Access). Login as the *admusr* user. The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the `/var/tmp` directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify `awpushcfg` was called by checking the following file

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

Verify the following message is displayed:

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

Now Reboot the Server:

```
$ sudo init 6
```

Wait for the server to reboot
Procedure 25. NOAM Configuration for DR Site (Optional)

9  **1st DR-NOAM:** Configure Networking for Dedicated NetBackup Interface (Optional)

   **Note:** You will only execute this step if your DR-NOAM is using a dedicated Ethernet interface for NetBackup.

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup
       --type=Ethernet --onboot=yes
       --address=<NO1_NetBackup_IP_Address>
       --netmask=<NO1_NetBackup_NetMask>
   
   $ sudo /usr/TKLC/plat/bin/netAdm add --route=net
       --device=netbackup --address=<NO1_NetBackup_Network_ID>
       --netmask=<NO1_NetBackup_NetMask>
       --gateway=<NO1_NetBackup_Gateway_IP_Address>
   ``

10 **1st DR-NOAM:** Establish an SSH session and Login

   Obtain a terminal window to the 1st DR-NOAM server, logging in as the *admusr* user.

11 **1st DR-NOAM Server:** Verify Server Health

   Execute the following command on the 1st DR-NOAM server and make sure that no errors are returned:

   ```bash
   $ 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
   ``

12 **Repeat for 2nd DR NOAM Server**

   Repeat Steps 3 through 11 to configure 2nd DR-NOAM Server. When inserting the 2nd DR-NOAM server, change the NTP server address to the following:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DRNO2-RMS-TVOE-IP-Address&gt;</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Procedure 26. Pairing for DR-NOAM Site (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure will provide the steps to pair the DR-NOAM site.</td>
</tr>
<tr>
<td></td>
<td><strong>Prerequisite</strong>: Installation for DR-NOAM Site complete</td>
</tr>
<tr>
<td></td>
<td>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact <strong>Appendix U</strong>: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>

1. **Primary NOAM VIP GUI: Login**

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

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

   Login as the *guiadmin* user:

   ![Oracle System Login](image-url)
Procedure 26. Pairing for DR-NOAM Site (Optional)

2

Primary NOAM VIP GUI: Enter DR-NOAM Server Group Data

Navigate to Main Menu -> Configuration -> Server Groups

Select Insert and fill the following fields:

- Server Group Name: <Enter Server Group Name>
- Level: A
- Parent: None
- Function: DSR (Active/Standby Pair)
- WAN Replication Connection Count: Use Default Value

Select OK when all fields are filled in.

3

Primary NOAM VIP GUI: Update Server Group

Select the Server Group that was created in the previous step, and click on Edit.

The user will be presented with the Server Groups [Edit] screen

Check the checkbox labeled Include in SG for both DR-NOAM Servers as shown below and click on Apply
Procedure 26. Pairing for DR-NOAM Site (Optional)

4. Primary NOAM VIP GUI: Add DR-NOAM VIP

Click the Add dialogue button for the VIP Address and enter an IP Address for the VIP as shown below.

<table>
<thead>
<tr>
<th>VIP Address</th>
<th>Add</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.250.55.163</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Then click the Apply dialogue button. Verify that the banner information message states Data committed.

Ok  Apply  Cancel

5. Primary NOAM VIP GUI: Wait for Remote Database Alarm to Clear

Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.

Navigate to Main menu->Alarms & Events->View Active

<table>
<thead>
<tr>
<th>Seq #</th>
<th>Event ID</th>
<th>Timestamp</th>
<th>Severity</th>
<th>Product</th>
<th>Process</th>
<th>NE</th>
<th>Server</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>414</td>
<td>10260</td>
<td>2015-03-20 09:59:00.000 EDT</td>
<td>CLEAR</td>
<td>awpGroupServer</td>
<td>Compass_NOA</td>
<td>CG</td>
<td>Compass-NOA</td>
<td>Remote Database re-initialization in progress</td>
</tr>
<tr>
<td>413</td>
<td>10260</td>
<td>2015-03-20 09:28:16.411 EDT</td>
<td>WARN</td>
<td>awpGroupServer</td>
<td>Compass_NOA</td>
<td>CG</td>
<td>Compass-NOA</td>
<td>Remote Database re-initialization in progress</td>
</tr>
</tbody>
</table>
### Procedure 26. Pairing for DR-NOAM Site (Optional)

**6**  
**Primary NOAM VIP GUI:** Restart 1st DR-NOAM Server  
From the NOAM GUI, select the `Main menu -> Status & Manage -> Server` menu.

![Status & Manage menu](image)

Select the 1st DR-NOAM server. Select the **Restart** button.

Answer **OK** to the confirmation popup.

![Confirmation popup](image)

Wait for restart to complete. Wait approximately 3-5 minutes before proceeding.

**7**  
**Primary NOAM VIP GUI:** Restart the application on the 2nd DR-NOAM Server  
Repeat Steps 6, but select the 2nd DR-NOAM Server.

**8**  
**DR-NOAM:** Expected Alarm (DSR 7.1)  
For DSR 7.1, the following alarm is expected to be present on the DR-NOAM:

**HA Service Start Failure:**

<table>
<thead>
<tr>
<th>Sec #</th>
<th>Event ID</th>
<th>Timestamp</th>
<th>Severity</th>
<th>Product</th>
<th>Process</th>
<th>NE</th>
<th>Server</th>
<th>Type</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4529</td>
<td>31525</td>
<td>2016-07-17 17:23:23</td>
<td>MAJOR</td>
<td>Jema</td>
<td>EVO-OK 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: This alarm is only cosmetic and not service affecting.
### 4.15 Application Configuration: SOAMs

#### Procedure 27. Configure the SOAM NE

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

1. **NOAM VIP GUI: Login**

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

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

   Login as the `guiadmin` user:
**Procedure 27. Configure the SOAM NE**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2. | **NOAM VIP GUI: Create the SOAM Network Element using an XML File**

   - Make sure to have an SOAM Network Element XML file available on the PC that is running the web browser. The SOAM Network Element XML file is similar to what was created and used in **Procedure 20**, but defines the SOAM "Network Element".

   - Refer to **Appendix L: Sample Network Element** for a sample Network Element xml file.

   - Navigate to **Main Menu->Configuration->Network Elements**

   ![Diagram of Configuration menu]

   - Select the **Browse** button, and enter the path and name of the SOAM network XML file.

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

<table>
<thead>
<tr>
<th>Insert</th>
<th>Delete</th>
<th>Export</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Insert button" /></td>
<td><img src="image" alt="Delete button" /></td>
<td><img src="image" alt="Export button" /></td>
<td><img src="image" alt="Report button" /></td>
</tr>
</tbody>
</table>
**Procedure 28. Configure the SOAM Servers**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Exchange SSH keys between SOAM site's local PMAC and the SOAM Server</strong>&lt;br&gt;Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From the PMAC GUI, navigate to <strong>Main Menu -&gt; Software -&gt; Software Inventory</strong>.&lt;br&gt;Note the IP address for the SOAM server.&lt;br&gt;Login to the PMAC terminal as the <em>admusr</em>.&lt;br&gt;From a terminal window connection on the PMAC as the <em>admusr</em> user, exchange SSH keys for <em>admusr</em> between the PMAC and the SOAM server using the keyexchange utility, using the Control network IP address for the SOAM server. When prompted for the password, enter the password for the <em>admusr</em> user of the NOAM server.&lt;br&gt;$ keyexchange admusr@&lt;SO1_Control_IP Address&gt;</td>
</tr>
<tr>
<td>2</td>
<td><strong>Exchange SSH keys between NOAM and PMAC at the SOAM site (If necessary)</strong>&lt;br&gt;Note: If this SOAM shares the same PMAC as the NOAM, then you can skip this step.&lt;br&gt;From a terminal window connection on the NOAM VIP, as the <em>admusr</em>, exchange SSH keys for <em>admusr</em> between the NOAM and the PMAC for this SOAM site using the keyexchange utility.&lt;br&gt;When prompted for the password, enter the admusr password for the PMAC server.&lt;br&gt;$ keyexchange admusr@&lt;SO1_Site_PMAC_Mgmt_IP_Address&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Repeat</strong> this step for the standby NOAM Server</td>
</tr>
</tbody>
</table>
Procedure 28. Configure the SOAM Servers

<table>
<thead>
<tr>
<th>3</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If not already done, establish a GUI session on the NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of: <code>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</code></td>
</tr>
</tbody>
</table>

Login to the NOAM GUI as the `guiadmin` user:
NOAM VIP GUI: Insert the 1st SOAM server

Navigate to Main Menu -> Configuration -> Servers.

Select the Insert button to insert the 1st SOAM server into servers table (the first or server).

Fill in the fields as follows:
- Hostname: <Hostname>
- Role: SYSTEM OAM
- System ID: <Site System ID>
- Hardware Profile: DSR TVOE Guest
- Network Element Name: [Choose NE from Drop Down Box]

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

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

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

Next, add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;RMS1-TVOE-IP-Address&gt;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Select the Ok button when you have completed entering all the server data.
## Procedure 28. Configure the SOAM Servers

### 5 NOAM VIP

**GUI:** Export the Initial Configuration

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

![Configuration Menu](image)

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

### 6 NOAM VIP

**Copy Configuration File to 1st SOAM Server**

Obtain a terminal session to the NOAM VIP as the **admusr** user.

Use the **awpushcfg** utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the NOAM to the 1st SOAM server, using the Control network IP address for the 1st SOAM server.

The configuration file will have a filename like “TKLCConfigData.<hostname>.sh”.

```bash
$ sudo awpushcfg
```

The awpushcfg utility is interactive, so the user will be prompted for the following:

- IP address of the local PMAC server: Use the local control network address from the PMAC.
- Username: Use **admusr**
- Control network IP address for the target server: In this case, enter the control IP for the 1st SOAM server.
- Hostname of the target server: Enter the server name configured in **step 4**
**Procedure 28. Configure the SOAM Servers**

<table>
<thead>
<tr>
<th>7</th>
<th>1st SOAM Server: Verify awpushcfg was called and Reboot the Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the NOAM VIP terminal console.</td>
<td></td>
</tr>
<tr>
<td>$ ssh admusr@&lt;SO1_Control_IP&gt;</td>
<td></td>
</tr>
<tr>
<td>Login as the <code>admusr</code> user.</td>
<td></td>
</tr>
<tr>
<td>The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.</td>
<td></td>
</tr>
<tr>
<td>Verify awpushcfg was called by checking the following file</td>
<td></td>
</tr>
<tr>
<td>$ sudo cat /var/TKLC/appw/logs/Process/install.log</td>
<td></td>
</tr>
<tr>
<td>Verify the following message is displayed:</td>
<td></td>
</tr>
<tr>
<td>[SUCCESS] script completed successfully!</td>
<td></td>
</tr>
<tr>
<td>Now Reboot the Server:</td>
<td></td>
</tr>
<tr>
<td>$ sudo init 6</td>
<td></td>
</tr>
<tr>
<td>Wait for the server to reboot</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8</th>
<th>1st SOAM Server: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the NOAM VIP terminal console.</td>
<td></td>
</tr>
<tr>
<td>$ ssh admusr@&lt;SO1_Control_IP&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9</th>
<th>1st SOAM Server: Verify Server Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute the following command on the 1st SOAM server and make sure that no errors are returned:</td>
<td></td>
</tr>
<tr>
<td>$ sudo syscheck</td>
<td></td>
</tr>
<tr>
<td>Running modules in class hardware...OK</td>
<td></td>
</tr>
<tr>
<td>Running modules in class disk...OK</td>
<td></td>
</tr>
<tr>
<td>Running modules in class net...OK</td>
<td></td>
</tr>
<tr>
<td>Running modules in class system...OK</td>
<td></td>
</tr>
<tr>
<td>Running modules in class proc...OK</td>
<td></td>
</tr>
<tr>
<td>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 28. Configure the SOAM Servers

| Step | Insert and Configure the 2nd SOAM server | Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;RMS2-TVOE-IP-Address&gt;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Instead of data for the 1st SOAM Server, insert the network data for the 2nd SOAM server, transfer the TKLCCConfigData file to the 2nd SOAM server, and reboot the 2nd SOAM server when prompted at a terminal window.

| Step | Install Netbackup Client Software on SOAMs (Optional) | If you are using NetBackup at this site, then execute Procedure 24 again to install the NetBackup Client on all SOAM servers.

Procedure 29. Configure the SOAM Server Group

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
### Procedure 29. Configure the SOAM Server Group

<table>
<thead>
<tr>
<th></th>
<th><strong>NOAM VIP GUI: Login</strong></th>
<th>If not already done, establish a GUI session on the NOAM server by using the XMI VIP address of the first NOAM server. Open the web browser and enter a URL of: <strong>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong></th>
</tr>
</thead>
</table>

Login to the NOAM GUI as the **guiadmin** user:
## Procedure 29. Configure the SOAM Server Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2 | **NOAM VIP**  
GUI: Enter SOAM Server Group Data  

After approximately 5 minutes for the 2nd SOAM server to reboot,  
Navigate to the GUI **Main Menu->Configuration->Server Groups**  

![Configuration Menu](image)

Select **Insert**  

Add the SOAM Server Group name along with the values for the following fields:  
- **Name:** `<Hostname>`  
- **Level:** B  
- **Parent:** [Select the NOAM Server Group]  
- **Function:** DSR (Active/Standby Pair)  
- **WAN Replication Connection Count:** Use Default Value  

Select **OK** when all fields are filled. |
Procedure 29. Configure the SOAM Server Group

3. **NOAM VIP GUI:** Edit the SOAM Server Group and add VIP

From the GUI, **Main Menu -> Configuration -> Server Groups**

Select the new SOAM server group, and then select **Edit.**

Add both SOAM servers to the Server Group Primary Site by clicking the **Include in SG** checkbox. Do not check any of the **Preferred Spare** checkboxes.

Click **Apply.**

Add a SOAM VIP by click on **Add.** Fill in the **VIP Address** and press **Ok** as shown below:
## Procedure 29. Configure the SOAM Server Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4 | **NOAM VIP GUI:** Wait for Remote Database Alarm to Clear  
   - Wait for the alarm **Remote Database re-initialization in progress** to be cleared before proceeding.  
   - Navigate to **Main menu->Alarms & Events->View Active**  
     ![alarm screen](image)
| 5 | **NOAM VIP GUI:** Restart 1st SOAM server  
   - From the NOAMP GUI, select **Main menu->Status & Manage->Server**.  
     ![status & manage](image)  
   - Select the **1st** SOAM server.  
   - Select the **Restart** button. Answer **OK** to the confirmation popup. Wait for restart to complete.  
     ![restart screen](image)
### Procedure 29. Configure the SOAM Server Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>NOAM VIP GUI:</strong> Restart 2&lt;sup&gt;nd&lt;/sup&gt; SOAM server</td>
</tr>
</tbody>
</table>

From the NOAMP GUI, select **Main menu->Status & Manage->Server.**

Select the 2<sup>nd</sup> SOAM server.
Select the **Restart** button. Answer **OK** to the confirmation popup. Wait for restart to complete.

### Procedure 30. Configure RMS-Specific B-Level Resources

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Active SOAM:</strong> Login</td>
</tr>
</tbody>
</table>

Obtain a terminal window connection on the **Active SOAM** server. Login as **admusr.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Active SOAM:</strong> Execute B-Level Resource Script</td>
</tr>
</tbody>
</table>

Execute the following on the command line. Wait until the script completes and you are returned to the command line:

```
$ sudo /usr/TKLC/dsr/bin/rmsResourceConfig.sh
```

Verify that no errors are displayed. If any errors are displayed, halt this procedure and contact **Appendix U:** My Oracle Support (MOS).
### 4.16 Application Configuration: MPs

#### Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>STEP #</th>
<th><strong>PMAC:</strong> Exchange SSH keys between MP site’s local PMAC and the MP server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Use the MP site’s PMAC GUI to determine the Control Network IP address of the server that is to be an MP server. From the MP site’s PMAC GUI, navigate to <strong>Main Menu -&gt; Software -&gt; Software Inventory.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Main Menu" /></td>
</tr>
<tr>
<td></td>
<td><strong>Enc: 9102 Bar: 3E</strong> 192.168.1.239 Compass-DAMP-03</td>
</tr>
<tr>
<td></td>
<td>Note the IP address for an MP server.</td>
</tr>
<tr>
<td></td>
<td>Login to the MP site’s PMAC terminal as the <strong>admusr.</strong></td>
</tr>
<tr>
<td></td>
<td>From a terminal window connection on the MP site’s PMAC as the <strong>admusr.</strong></td>
</tr>
<tr>
<td></td>
<td>Exchange SSH keys for <strong>admusr between</strong> the PMAC and the MP server using the keyexchange utility, using the Control network IP address for the MP server.</td>
</tr>
<tr>
<td></td>
<td><code>$ keyexchange admusr@&lt;MP_Control_IP Address&gt;</code></td>
</tr>
<tr>
<td></td>
<td>When prompted for the password, enter the password for the <strong>admusr</strong> user of the MP server.</td>
</tr>
</tbody>
</table>

This procedure will provide the steps to configure an MP Servers (IPFE, SBR, SS7-MP, DA-MP). Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact **Appendix U: My Oracle Support (MOS), and ask for assistance.**
Procedure 31. Configure the MP Servers

| 2 | NOAM VIP GUI: Login | If not already done, establish a GUI session on the NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of:  
|   |                   | `https://<Primary_NOAM_VIP_IP_Address>`

Login to the NOAM GUI as the `guiadmin` user:

![Oracle System Login](image)

```plaintext
Enter your username and password to log in

Username: guiadmin
Password: ********

Welcome to the Oracle System Login.
Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 6.0, 9.0, or 10.0 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 31. Configure the MP Servers

3

**NOAM VIP GUI: Insert the MP server** (Part 1)

Navigate to **Main Menu->Configuration->Servers**

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

**Fill out the following values:**
- **Hostname:** `<Hostname>`
- **Role:** MP
- **Network Element:** [Choose the Corresponding SOAM Network Element]
- **Hardware Profile:** DSR TVOE Guest
- **Location:** `<enter an optional location description>`

The interface configuration form will now appear.

For the XMI network, enter the MP's XMI IP address. Select “xmi” for the interface. Leave the “VLAN” checkbox unchecked.

For the IMI network, enter the MP's IMI IP address. Select “imi” for the interface. Leave the “VLAN” checkbox unchecked.

4

**NOAM VIP GUI: Insert the MP server** (Part 2)

Next, add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MP RMS-TVOE-IP-Address&gt;</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Select **OK** when all fields are filled in to finish MP server insertion.
Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>NOAM VIP GUI:</strong> Export the Configuration</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Configuration -&gt; Servers.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="GUI Screen" /></td>
</tr>
<tr>
<td></td>
<td>From the GUI screen, select the MP server and then select <strong>Export</strong> to generate the initial configuration data for that server.</td>
</tr>
<tr>
<td></td>
<td><strong>Insert</strong> <strong>Edit</strong> <strong>Delete</strong> <strong>Export</strong> <strong>Report</strong></td>
</tr>
<tr>
<td>6</td>
<td><strong>NOAM VIP:</strong> Copy Configuration File to MP Server</td>
</tr>
<tr>
<td></td>
<td>Obtain a terminal session to the NOAM VIP as the <strong>admusr</strong> user.</td>
</tr>
<tr>
<td></td>
<td>Use the <strong>awpushcfg</strong> utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the NOAM to the MP server, using the Control network IP address for the MP server.</td>
</tr>
<tr>
<td></td>
<td>The configuration file will have a filename like “TKLCConfigData.&lt;hostname&gt;.sh”.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo awpushcfg</code></td>
</tr>
<tr>
<td></td>
<td>The awpushcfg utility is interactive, so the user will be prompted for the following:</td>
</tr>
<tr>
<td></td>
<td>- IP address of the local PMAC server: Use the local control network address from the PMAC.</td>
</tr>
<tr>
<td></td>
<td>- Username: Use <strong>admusr</strong></td>
</tr>
<tr>
<td></td>
<td>- Control network IP address for the target server: In this case, enter the control IP for the MP server).</td>
</tr>
<tr>
<td></td>
<td>- Hostname of the target server: Enter the server name configured in step 1</td>
</tr>
</tbody>
</table>
Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>MP Server</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Obtain a terminal window connection on the MP server console by establishing an ssh session from the NOAM VIP terminal console.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>$ ssh admusr@&lt;MP_Control_IP&gt;</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Login as the <strong>admusr</strong> user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify awpushcfg was called by checking the following file:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>$ sudo cat /var/TKLC/appw/logs/Process/install.log</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify the following message is displayed:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>[SUCCESS] script completed successfully!</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reboot the server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>$ sudo init 6</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Proceed to the next step once the Server finished rebooting. The server is done rebooting once the login prompt is displayed.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Verify Server Health</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After the reboot, login as <strong>admusr</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute the following command as super-user on the server and make sure that no errors are returned:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>$ sudo syscheck</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class hardware...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class disk...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class net...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class system...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running modules in class proc...OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network-Part1 (Optional)</th>
</tr>
</thead>
</table>
| 9    | **Note:** THIS STEP IS **OPTIONAL** AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALLING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. (Not executing this step will mean that a default route will not be configurable on this MP and you will have to create separate network routes for each signaling network destination.) Using the iLO facility, log into the MP as the admusr user. (Alternatively, you can log into the site’s PMAC then SSH to the MP’s control address.) Determine `<XMI_Gateway_IP>` from your SO site network element info. Gather the following items:  
- `<NO_XMI_Network_Address>`  
- `<NO_XMI_Network_Netmask>`  
- `<DR_NO_XMI_Network_Address>`  
- `<DR_NO_XMI_Network_Netmask>`  
- `<TVOE_Mgmt_XMI_Network_Address>`  
- `<TVOE_Mgmt_XMI_Network_Netmask>`  
**Note:** You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the **Main Menu -> Configuration -> Network Elements** screen.  
Proceed to the next step to modify the default routes on the MP servers. |
Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td><strong>MP Server:</strong> Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network-Part2 (Optional)</td>
</tr>
</tbody>
</table>

After gathering the network information from **step 9**, proceed with modifying the default routes on the MP server.

Establish a connection to the MP server, login as *admusr*.

Create network routes to the NO's XMI(OAM) network:

**Note:** If your NOAM XMI network is exactly the same as your MP XMI network, then you should skip this command and only configure the DR NO route.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=net
   --address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask>
   --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>
Route to <MP_XMI_Interface> added.
```

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>
Route to <MP_XMI_Interface> added.
```

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_XMI_Network_Address>
   --netmask=<TVOE_Mgmt_XMI_Network_Netmask>
   --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>
Route to <MP_XMI_Interface> added.
```

(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>
Route to <MP_XMI_Interface> added.
```

(Repeat for any existing customer NMS stations)

Delete the existing default route:

```
$ sudo /usr/TKLC/plat/bin/netAdm delete --route=default
   --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>
Route to <MP_XMI_Interface> removed.
```
Procedure 31. Configure the MP Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>MP Server:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Verify connectivity</td>
<td>After steps 9 and 10 have been executed, verify network connectivity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establish a connection to the MP server, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ping active NO XMI IP address to verify connectivity:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ ping &lt;ACTIVE_NO_XMI_IP_Address&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>(Optional)</em> Ping Customer NMS Station(s):</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ ping &lt;Customer_NMS_IP&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not get a response, then verify your network configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you continue to get failures then halt the installation and contact Oracle customer support.</td>
</tr>
<tr>
<td>12</td>
<td>Repeat for remaining MPs</td>
<td>Repeat this entire procedure for all remaining MP servers.</td>
</tr>
</tbody>
</table>
Procedure 32. Configure the MP Server Group(s) and Profile(s)

This procedure will provide the steps to configure MP Server Groups

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI: Login</th>
<th>Determine Server Group Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: https://&lt;Primary_NOAM_VIP_IP_Address&gt; Login to the NOAM GUI as the guiadmin user:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determine what server group function will be configured, make note the following configuration decisions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Group Function</th>
<th>MPs Will Run</th>
<th>Redundancy Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR (multi-active cluster)</td>
<td>Diameter Relay and Application Services</td>
<td>Multiple MPs active Per SG</td>
</tr>
<tr>
<td>DSR (active-standby pair)</td>
<td>Diameter Relay and Application Services</td>
<td>1 Active MP and 1 Standby MP / Per SG</td>
</tr>
<tr>
<td>IP Load Balancer</td>
<td>IPFE application</td>
<td>1 Active MP Per SG</td>
</tr>
<tr>
<td>SS7-IWF</td>
<td>MAP IWF Application</td>
<td>1 Active MP Per SG</td>
</tr>
</tbody>
</table>
### Procedure 32. Configure the MP Server Group(s) and Profile(s)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 3    | NOAM VIP GUI: Enter MP Server Group Data | From the data collected from step 2, create the server group with the following: Navigate to **Main Menu -> Configuration -> Server Groups**  

Select **Insert**  

![Menu Screenshot](image)  

Select **Server Group Name:** `<Server Group Name>`  
Select **Level:** `C`  
Select **Parent:** `[SOAMP Server Group That is Parent To this MP]`  
Select **Function:** **Select the Proper Function for this MP Server Group (Gathered in Step 2)**  
Select **OK** when all fields are filled in. |
| 4    | NOAM VIP GUI: Repeat For Additional Server Groups | Repeat **Steps 2-3** for any remaining MP server groups you wish to create.  
For instance, if you are installing IPFE, you will need to create an IP Load Balancer server group. |
Procedure 32. Configure the MP Server Group(s) and Profile(s)

<table>
<thead>
<tr>
<th></th>
<th><strong>NOAM VIP GUI</strong>: Edit the MP Server Groups to include MPs</th>
<th>From the GUI, navigate to <strong>Main Menu-&gt;Configuration-&gt;Server Groups</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>[Image] From the GUI, navigate to <strong>Main Menu-&gt;Configuration-&gt;Server Groups</strong></td>
<td>Select a server group that you just created and then select <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the Network Element that represents the MP server group you wish to edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the <strong>Include in SG</strong> box for every MP server that you wish to include in this server group. Leave other checkboxes blank.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Each IPFE server should be in its own server group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select <strong>OK</strong>.</td>
</tr>
<tr>
<td>6</td>
<td><strong>NOAM VIP GUI</strong>: Repeat For Additional Server Groups</td>
<td>Repeat Steps 5 for any remaining MP server groups you need to edit.</td>
</tr>
<tr>
<td>7</td>
<td><strong>NOAM VIP GUI</strong>: Wait for Remote Database Alarm to Clear</td>
<td>Wait for the alarm <strong>Remote Database re-initialization in progress</strong> to be cleared before proceeding.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Navigate to <strong>Main menu-&gt;Alarms &amp; Events-&gt;View Active</strong></td>
</tr>
</tbody>
</table>

**Main Menu: Alarms & Events -> View History (Filtered)**

<table>
<thead>
<tr>
<th>Seq #</th>
<th>Event ID</th>
<th>Timestamp</th>
<th>Severity</th>
<th>Product</th>
<th>Process</th>
<th>NE</th>
<th>Server</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>416</td>
<td>10200</td>
<td>2015-03-20 00:50:00:50:00:50</td>
<td>CLEAR</td>
<td>Compass_NOA CF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>413</td>
<td>10200</td>
<td>2015-03-20 00:50:00:50:00:50</td>
<td>IN PROGRESS</td>
<td>Compass_NOA CF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 32. Configure the MP Server Group(s) and Profile(s)

<table>
<thead>
<tr>
<th></th>
<th><strong>SOAM VIP GUI: Login</strong></th>
<th>If not already done, establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><strong>SOAM VIP GUI: Login</strong></td>
<td>Open the web browser and enter a URL of: <strong>https://&lt;Primary_SOAM_VIP_IP_Address&gt;</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login to the SOAM GUI as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image-url)
Procedure 32. Configure the MP Server Group(s) and Profile(s)

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

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

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

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

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM:Relay</td>
<td>Virtualized DA-MP on TVOE Guest running the relay application</td>
</tr>
<tr>
<td>VM:Database</td>
<td>Virtualized DA-MP on TVOE Guest running relay and database applications</td>
</tr>
<tr>
<td>VM:Session</td>
<td>Virtualized DA-MP on TVOE Guest running relay and session applications</td>
</tr>
<tr>
<td>VM:MD-IWF</td>
<td>Virtualized SS7-MP on TVOE Guest running MD-IWF applications</td>
</tr>
</tbody>
</table>

Note: If the DA-MPs at this site are configured for Active/Standby then there will be a single selection box visible that assigns profiles for all MPs.

When finished, press the Assign button
Procedure 32. Configure the MP Server Group(s) and Profile(s)

10. **SOAM VIP GUI:** Update DpiOption table from the active SOAM (DSR 7.0 ONLY)

    **DSR 7.0 ONLY, if DSR 7.1 skip this step**

    If IPFE Hash load balance algorithm is being used (Load Balance Algorithm: 
    Execute the following step, and **skip this step**.

    Log on to the active SOAM console as `admusr` via the SOAM VIP.

    Execute the following command (advise cut and paste to prevent errors):

    ```
    $ sudo iset -fvalue="50" DpiOption where 
    "name='MpEngIngressMpsPercentile'"
    
    *** changed 1 records ===
    ```

11. **NOAM VIP GUI:** Login

    If not already done, establish a GUI session on the NOAM server by using the VIP 
    IP address of the NOAM server.

    Open the web browser and enter a URL of:

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

    Login to the NOAM GUI as the *guiadmin* user:
Procedure 32. Configure the MP Server Group(s) and Profile(s)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>NOAM VIP GUI: Restart MP servers</td>
</tr>
<tr>
<td></td>
<td>Navigate to Main menu-&gt;Status &amp; Manage-&gt;Server</td>
</tr>
<tr>
<td></td>
<td>For each MP server:</td>
</tr>
<tr>
<td></td>
<td>- Select the MP server.</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>Restart</strong> button.</td>
</tr>
<tr>
<td></td>
<td>- Answer <strong>OK</strong> to the confirmation popup. Wait for the message which tells you that the restart was successful.</td>
</tr>
</tbody>
</table>

4.17 Application Configuration: Signaling Network

Procedure 33. Configure the Signaling Networks

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure will provide the steps to configure the signaling networks</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact <strong>Appendix U</strong>: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>
|   | NOAM VIP GUI: Login | If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.  
Open the web browser and enter a URL of:  
https://<Primary_NOAM_VIP_IP_Address>  
Login to the NOAM GUI as the guiadmin user: |
|---|---|---|
|   |   | ![ORACLE System Login](image)  
Welcome to the Oracle System Login.  
Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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. |
|   | NOAM VIP GUI: Navigate to Signaling Network Configuration Screen | Navigate to Main Menu -> Configuration -> Network  
Click on Insert in the lower left corner. |
Procedure 33. Configure the Signaling Networks

3. **NOAMP VIP: Add Signaling Networks**

You will see the following screen:

Enter the **Network Name**, **VLAN ID**, **Network Address**, **Netmask**, and **Router IP** that matches the Signaling network.

**Note:** Even if the network does not use VLAN Tagging, you should enter the correct VLAN ID here as indicated by the NAPD.

- **IMPORTANT:** Leave the **Network Element** field as **Unassigned**.
- Select **No** for Default Network.
- Select **Yes** for Routable.

Press **OK**. if you are finished adding signaling networks.

- **OR**-

Press **Apply** to save this signaling network and repeat this step to enter additional signaling networks.
## Procedure 34. Configure the Signaling Devices

This procedure will provide the steps to configure the signaling devices. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOAM VIP GUI: Login</td>
<td>If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <strong>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong>. Login to the NOAM GUI as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
Procedure 34. Configure the Signaling Devices

NOAM VIP GUI: Make Signaling Devices Configurable (Un-bonded, non-VLAN signaling interfaces only)

Note: You will only execute this step if you are using un-bonded, non-VLAN tagged Ethernet interfaces for signaling traffic.

Navigate to Main Menu -> Configuration -> Network -> Devices

You should see several tabs each representing a server in the system. Click on the tab representing the first MP.

Main Menu: Configuration -> Network -> Devices

You should see a list of network devices installed on the MP.

Select all Ethernet devices that will be used as un-bonded signaling interfaces and have “Discovered” as their Configuration Status.

Next, press the Take Ownership button.

After a brief moment, the selected devices should now show a Configuration Status of “Configured”.

Select the first signaling interface (xsi1) and click on Edit
Procedure 34. Configure the Signaling Devices

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Configure the Signaling Interfaces of the MP</th>
</tr>
</thead>
</table>

The following screen should be displayed. Verify that the server name on the top corresponds to the MP.

Edit Ethernet device xsi2 on mp-DRA-CHTM-1-1

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td></td>
<td>Select the device type. It cannot be changed after device is created. [Default = N/A, Range = Bonding, VLAN, Alias.]</td>
</tr>
<tr>
<td>Device Monitoring</td>
<td></td>
<td>Choose a monitoring style to use with a bonding device. Disabled for non-bonding devices. [Default = MI, Options = MI, ARP]</td>
</tr>
<tr>
<td>Start On Boot</td>
<td></td>
<td>Start the device, and also start on boot. [Default = enabled]</td>
</tr>
<tr>
<td>Boot Protocol</td>
<td></td>
<td>Select the boot protocol. [Default = None, Range = None, DHCP]</td>
</tr>
<tr>
<td>Base Device(s)</td>
<td></td>
<td>The base device(s) for bonding, alias and VLAN device types. Alias and VLAN devices require 1 selection. Bonding devices require 2 selections. It cannot be changed after device is created. [Default = N/A, Range = available base devices per device type.]</td>
</tr>
</tbody>
</table>

Device Type: **Ethernet**

Start on Boot: **Verify that the checkbox is selected.**

Boot Protocol: **None**

Now Click on the **IP Interfaces** tab as shown below.

**Insert Device on blade09**

Now Click on **Add Row**, the following will be displayed

Select the first Signaling Network from the drop down menu.

If configuring an IPv6 only and your site has IPv6 auto-configuration, there’s no need to enter an IP address, it will be assigned automatically. If configuring an IPv4 or IPv4/IPv6, enter the IP address that corresponds to the IPv4 interface.

Click on **Ok** at the bottom of the screen.

To configure additional Signaling Interfaces, re-select the MP and click on **Edit** again and **repeat** this step, otherwise continue with the **next step**.
Procedure 34. Configure the Signaling Devices

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>NOAM VIP GUI: Configure the Interfaces of the other MPs. Repeat this procedure to configure the signaling devices of all other MPs.</td>
</tr>
</tbody>
</table>

Procedure 35. Configure the Signaling Network Routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOAM VIP GUI: Login If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: https://&lt;Primary_NOAM_VIP_IP_Address&gt; Login to the NOAM GUI as the guiadmin user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image-url)
### Procedure 35. Configure the Signaling Network Routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2 | **NOAM VIP GUI:** Navigate to Routes Configuration Screen

Navigate to **Main Menu -> Configuration -> Network -> Routes**

Select the first MP Server you see listed on the first row of tabs as shown, then click the **Entire Server Group** link. Initially, no routes should be displayed.

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Scope Status</th>
</tr>
</thead>
</table>

| 3 | **NOAM VIP GUI:** Add Route

Click on **Insert** at the bottom of the screen to add additional routes.

| Insert | Edit | Delete | Report | Report All |

| 4 | **NOAM VIP GUI:** Add Default Route for MPs Going Through Signaling Network Gateway (Optional)

**OPTIONAL** - Only execute this step if you performed **Procedure 31 Step 10:** which removed the XMI gateway default route on MPs

If your MP servers no longer have a default route, then you can now insert a default route here which uses one of the signaling network gateways.

**Route Type:** Default

**Device:** Select the signaling device that is directly attached to the network where the XSI default gateway resides.

**Gateway IP:** The XSI gateway you wish to use for default signaling network access.

Select **OK**
Procedure 35. Configure the Signaling Network Routes

| 5 | NOAM VIP GUI: Add Network Routes for Diameter Peers |

Use this step to add IP and/or IPv6 routes to *diameter* peer destination networks. The goal here is to ensure that diameter traffic uses the gateway(s) on the signaling networks.

*Route Type: Net*

**Device:** Select the appropriate signaling interface that will be used to connect to that network.

**Destination:** Enter the Network ID of Network to which the peer node is connected to.

**Netmask:** Enter the corresponding Netmask.

**Gateway IP:** Enter the Int-XSI switch VIP of the chosen Network for L3 deployments (either of Int-XSI-1 or of Int-XSI2). Or the IP of the customer gateway for L2 deployments.

If you have more routes to enter, Press **Apply** to save the current route entry and repeat this step to enter more routes.

If you are finished entering routes, Press **OK** to save the latest route and leave this screen.

If *aggregation switches* are used, routes should be configured on the aggregation switches so that the destination networks configured in this step are reachable. This can be done by running the following `netconfig` commands from the site’s local PMAC (examples shown -- actual values will vary):

**Add routes (IPv4 & IPv6):**

```
$ sudo netConfig -device=switch1A addRoute
network=10.10.10.0 mask=255.255.255.0 nexhop=10.50.76.81
$ sudo netConfig -device=switch1A addRoute
network6=2001::/64 nexthop=fd0f::1
```

**Delete routes (IPv4 & IPv6):**

```
$ sudo netConfig -device=switch1A deleteRoute
network=10.10.10.0 mask=255.255.255.0 nexhop=10.50.76.81
$ sudo netConfig -device=switch1A deleteRoute
network6=2001::/64 nexthop=fd0f::1
```

After the routes are added via netconfig, a **netconfig backup** should be taken so that the new routes are retained in the backup.
Procedure 35. Configure the Signaling Network Routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>NOAM VIP GUI: Repeat for all other MP server groups. The routes entered in this procedure should now be configured on all MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from step 2, but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups.</td>
</tr>
</tbody>
</table>

Procedure 36. Add VIP for Signaling networks (Active/Standby Configurations Only)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOAM VIP GUI: Login If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <code>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</code> Login to the NOAM GUI as the <code>guiadmin</code> user:</td>
</tr>
</tbody>
</table>
Procedure 36. Add VIP for Signaling networks (Active/Standby Configurations Only)

NOAM VIP GUI: Edit the MP Server Group and add VIPs (ONLY FOR 1+1)

IF YOUR MPs ARE IN A DSR MULTI-ACTIVE CLUSTER SERVER GROUP CONFIGURATION (N+0), THEN SKIP THIS STEP

From Main Menu->Configuration->Server Groups

Select the MP server group, and then select Edit

Click on Add to add the VIP for XSI1
Enter the VIP of int-XSI-1 and click on Apply

Click on Add again to add the VIP for XSI2
Enter the VIP of int-XSI-2 and click on Apply

If more Signaling networks exist, add their corresponding VIP addresses.

Finally Click on OK.
### 4.18 Application Configuration: DSCP (Optional)

#### Procedure 37. Configure DSCP Values for Outgoing Traffic (Optional)

This procedure will provide the steps to configure the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network will utilize packet DSCP markings for Quality-of-Service purposes.

**Note:** If your enclosure switches already have DSCP configuration for the signaling VLANs, then the switch configuration will override the settings in this procedure. It is strongly recommended, however, that you configure DSCP here at the application level where you have the most knowledge about outgoing traffic patterns and qualities.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.</td>
</tr>
<tr>
<td></td>
<td>Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td><strong>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong></td>
</tr>
<tr>
<td></td>
<td>Login to the NOAM GUI as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
Procedure 37. Configure DSCP Values for Outgoing Traffic (Optional)

| NOAM VIP GUI: Option 1: Configure Interface DSCP | Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. |

Navigate to Main Menu -> Configuration -> DSCP -> Interface DSCP

Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with Entire Network selected; or limit yourself to a particular server group by clicking on that server group name's tab).

Click Insert

Main Menu: Configuration -> DSCP -> Interface DSCP

Select the network interface from the drop down box, then enter the DSCP value you wish to have applied to packets leaving this interface.

Insert DSCP by Interface on FZTEST-MP1

Click OK if there are no more interfaces on this server to configure, or Apply to finish this interface and continue on with more interfaces by selecting them from the drop down and entering their DSCP values.
### Procedure 37. Configure DSCP Values for Outgoing Traffic (Optional)

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

| 4    | **NOAM VIP GUI:** Repeat for additional servers. |
|      | Repeat **Steps 2-3** for all remaining servers. |
### 4.19 Application Configuration: SNMP (Optional)

**Procedure 38. Configure SNMP Trap Receiver(s) (Optional)**

This procedure will provide the steps to configure forwarding of SNMP Traps from each individual server.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOAM VIP GUI: Login</td>
</tr>
</tbody>
</table>

If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.

Open the web browser and enter a URL of:

```
http://<Primary_NOAM_VIP_IP_Address>
```

Login to the NOAM GUI as the *guiadmin* user:

![Oracle System Login](image-url)

*Username*: guiadmin

*Password*: *********

Login
Procedure 38. Configure SNMP Trap Receiver(s) (Optional)

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

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

- Remote Servers
  - LDAP Authentication
  - SNMP Trapping
  - Data Export
  - DNS Configuration

Verify that **Traps Enabled** is checked:

<table>
<thead>
<tr>
<th>Traps Enabled</th>
<th>Enabled</th>
</tr>
</thead>
</table>

Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP’s “XMI” network.

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager 1</td>
<td>10.10.55.88</td>
</tr>
</tbody>
</table>

Enter the **SNMP Community Name**:

- SNMPv2c Read-Only Community Name: snmppublic
- SNMPv2c Read-Write Community Name: snmppublic

Leave all other fields at their default values.

Press **OK**
Procedure 38. Configure SNMP Trap Receiver(s) (Optional)

3  NOAMP VIP: Enable Traps from Individual Servers (Optional)

<table>
<thead>
<tr>
<th>Traps from Individual Servers</th>
<th>[Default: enabled]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enable or disable SNMP traps from insert from individual servers, otherwise NOAMP server. [Default: disabled]</td>
</tr>
<tr>
<td>Configured Community Name (SNMP)</td>
<td></td>
</tr>
</tbody>
</table>

Note: By default SNMP traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable.

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

Make sure the checkbox next to Enabled is checked, if not, check it as shown below

Then click on Apply and verify that the data is committed.

4  PMAC GUI: Login (DSR 7.0 Only)

DSR 7.0 Only. For DSR 7.1, skip to step 7

Open web browser and enter:

http://<PMAC_Mgmt_Network_IP>

Login as pmacadmin user:
Procedure 38. Configure SNMP Trap Receiver(s) (Optional)

5

PMAC GUI: Update the TVOE Host SNMP Community String (DSR 7.0 Only)

DSR 7.0 Only. For DSR 7.1, skip to step 7

Navigate to Main Menu -> Administration -> Credentials -> SNMP

Select the Read Only or ReadWrite button depending on which SNMP community string is to be updated.

Note: If this the first time the SNMP Community Strings has been updated for this PMAC, perform the following:

1. Leave the Use Site Specific checkbox (TPDverejny) unchecked.
2. Enter the community string configured in step 2 of this procedure.
### Procedure 38. Configure SNMP Trap Receiver(s) (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI: Update the TVOE Host SNMP Community String <em>(DSR 7.0 Only)</em></th>
<th>DSR 7.0 Only. For DSR 7.1, skip to step 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Continued from the previous step, enter the new Community String into the Community string textbox. Click the <strong>Update Servers</strong> button</td>
<td></td>
</tr>
</tbody>
</table>

The following warning will be displayed:

```
You are about to update the per-DSR-only SNMP Dictionary on all known supporting TVOE servers and the PMAC guest on the control network of this PMAC. Changing of SNMP Community Strings is only supported across product release versions that support this functionality and attempting to do so with products/versons not supporting it has caused the system to become unstable.
Are you sure you want to continue?
```

Select **OK**

**Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Establish an SSH Session</th>
<th>DSR 7.1 Only. For DSR 7.0, skip this step.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Establish an SSH session to the PMAC, login as <em>admusr</em>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Update the PMAC Community String</th>
<th>DSR 7.1 Only. For DSR 7.0, skip this step.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Execute the following command to update the PMAC community string to the one configured in <strong>step 2</strong> of this document:</td>
<td></td>
</tr>
</tbody>
</table>

```
$ sudo pmaccli setCommStr --accessType=rw --commStr=<community string from step 2>
```

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Verify Updated Community String</th>
<th>DSR 7.1 Only. For DSR 7.0, skip this step.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Execute the following command to verify the updated community string. The output of the command should display the community string set in <strong>step 8</strong>:</td>
<td></td>
</tr>
</tbody>
</table>

```
$ sudo pmaccli getCommStrStatus
```
4.20 Application Configuration: IP Front End (IPFE)

Procedure 39. IP Front End (IPFE) Configuration (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI: Login</th>
<th>Note: If you converted a Discovered device to a Configured device on the Configuration -&gt; Network -&gt; Devices and are using the converted device for an IPFE XSI interface, complete this procedure. Otherwise, skip to step 4. Note: If you do not recall whether any IPFE devices were converted, complete the following step.</th>
</tr>
</thead>
</table>
| 1 | If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
https://<Primary_NOAM_VIP_IP_Address>  
Login to the NOAM GUI as the guiadmin user:  
![Oracle System Login](image) |  |
<p>| 2 | Determine whether the Appworks update Script needs to be executed |  |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>3</th>
<th><strong>NOAM VIP:</strong> Execute the AppWorks update Scripts. (DSR 7.0)</th>
<th>DSR 7.0 ONLY, DSR 7.1 skip to step 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Execute the following command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>$ sudo ipfeAppworksUpdate.sh</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOAM VIP GUI:</strong> Verify the AppWorks update Script ran. (DSR 7.0)</td>
<td>Select <strong>Configuration -&gt; Network -&gt; Devices</strong></td>
</tr>
</tbody>
</table>
|      |   | Select the tabs for the IPFE.                             | ![Configuration and Network Tree](image)
|      |   | Verify that, for devices that were converted to **Configured** from **Discovered**, the following information is seen in the Device Options column: |
|      |   | `ethtoolOpts = --set-ring eth04 rx 4078; --offload eth04 gro off gso off onboot = no` |
|      |   | **1st IPFE Server:** Establish an SSH session to the IPFE server. Login as **admusr**. |
|      |   | Execute the following command:                            |                                     |
|      |   | $ sudo ipfeNetUpdate.sh                                   |                                     |
|      |   | Now reboot the IPFE Server:                               | $ sudo init 6                       |
### Procedure 39. IP Front End (IPFE) Configuration (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6    | 1st IPFE: Verify the ipfeNetUpdate script ran. (DSR 7.0) | After the IPFE server reboots, re-establish the ssh session and login as `admusr`. Execute the following commands:  

```bash
$ sudo cat /etc/sysconfig/network
```

```
NETWORKING=yes  
NETWORKING_IPV6=yes  
NTPSERVERARGS=iburst  
HOSTNAME= <hostname of IPFE Server>  
IPV6INIT=yes  
IPV6FORWARDING=yes
```

Execute the following command:

```bash
$ sudo cat /etc/modprobe.d/bnx2x.conf
```

```
options bnx2x num_queues=25 disable_tpa=1
```

Execute the following command:

```bash
$ sudo cat /etc/sysconfig/network-scripts/ifcfg-eth01
```

```
ETHTOOL_OPTS="--set-ring eth01 rx 4078; --offload eth01 gro off gso off"
```

| 7    | Additional IPFE servers: Repeat for additional IPFE Servers. (DSR 7.0) | Repeat steps 5-6 for additional IPFE servers. |
### Procedure 39. IP Front End (IPFE) Configuration (Optional)

| 8 | SOAM VIP GUI: Login | Establish a GUI session on the SOAM server the VIP IP address of the SOAM server.  
Open the web browser and enter a URL of:  
https://<Primary_SOAM_VIP_IP_Address>  
Login to the SOAM GUI as the `guiadmin` user: |

![Oracle System Login](image_url)

*Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
Procedure 39. IP Front End (IPFE) Configuration (Optional)

**SOAM VIP GUI:** Configuration of replication IPFE association data.

Select Main Menu -> IPFE -> Configuration -> Options

![Options Menu](image)

Enter the IP address of the 1st IPFE in the IPFE-A1 IP Address field and the IP address of the 2nd IPFE in the IPFE-A2 IP Address field.

If applicable, enter the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPFE-A1 IP Address</td>
<td>10.240.79.103 - VIPser/IPFE1</td>
</tr>
<tr>
<td>IPFE-A2 IP Address</td>
<td>10.240.79.104 - VIPser/IPFE2</td>
</tr>
<tr>
<td>IPFE-B1 IP Address</td>
<td><code>&lt;unset&gt;</code></td>
</tr>
<tr>
<td>IPFE-B2 IP Address</td>
<td><code>&lt;unset&gt;</code></td>
</tr>
</tbody>
</table>

**Note:** It is recommended that the address reside on the IMI (Internal Management Interface) network.

**Note:** IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2.

**SOAM VIP GUI:** Configuration of IPFE Target sets-Part 1 (Insert Target Set)

Select Main Menu -> IPFE -> Configuration -> Target Sets

![Target Sets Menu](image)

Select either **Insert IPv4** or **Insert IPv6** button, depending on the IP version of the target set you plan to use.

![Buttons](image)
### Procedure 39. IP Front End (IPFE) Configuration (Optional)

<table>
<thead>
<tr>
<th>SOAM VIP GUI: Configuration of IPFE Target sets - Part 2 (Target Set Configuration)</th>
<th>Continued from the previous step, the following are configurable:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols: protocols the target set will support.</td>
<td><strong>Delete Age</strong>: 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 <strong>Delete Age</strong> configuration will be treated as a new connection and will not automatically go to the same application server.</td>
</tr>
<tr>
<td>Protocols:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="" /></td>
</tr>
<tr>
<td>Load Balance Algorithm: <strong>Hash</strong> or <strong>Least Load</strong> options</td>
<td></td>
</tr>
<tr>
<td>Load Balance Algorithm:</td>
<td>![image2]</td>
</tr>
</tbody>
</table>

**Note**: In order for the IPFE to provide Least Load distribution, **Main Menu -> IPFE -> Configuration -> Options**, Monitoring Protocol must be set to **Heartbeat** so that the application servers can provide the load information the IPFE uses to select the **least-loaded** server for connections.

**Note**: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.
**Procedure 39. IP Front End (IPFE) Configuration (Optional)**

<table>
<thead>
<tr>
<th>SOAM VIP GUI: Configuration of IPFE Target sets-Part 3 (Target Set Configuration)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Optional):</strong> If you have selected the <strong>Least Load algorithm</strong>, you may configure the following fields to adjust the algorithm's behavior:</td>
</tr>
<tr>
<td><strong>MPS Factor</strong> – 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.</td>
</tr>
<tr>
<td><strong>Connection Count Factor</strong> – 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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

To configure **Reserved Ingress MPS**, go to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> Capacity Configuration Sets**. If you choose not to use **Reserved Ingress MPS**, set **MPS Factor** to 0 and **Connection Count Factor**, described below, to 100.
### Procedure 39. IP Front End (IPFE) Configuration (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td><strong>SOAM VIP GUI:</strong> Configuration of IPFE Target sets - Part 4 (Target Set Configuration)</td>
</tr>
<tr>
<td></td>
<td><strong>Primary Public IP Address:</strong> IP address for the target set</td>
</tr>
<tr>
<td></td>
<td><strong>Secondary Public IP Address:</strong> If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.</td>
</tr>
</tbody>
</table>

**Note:** This address must reside on the XSI (External Signaling Interface) network because it will be used by the application clients to reach the application servers. This address **MUST NOT** be a real interface address (that is, must not be associated with a network interface card).  

**Active IPFE:** IPFE to handle the traffic for the target set address.  

**Secondary Public IP Address:** If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.  

**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.  

**Note:** The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also match the IP version of the target set address (IPv4 or IPv6). If the Secondary Public IP Address is configured, it must reside on the same application server as the first IP address.  

**Note:** If all application servers have an equal weight (e.g., 100, which is the default), they have an equal chance of being selected. Application servers with larger weights have a greater chance of being selected.  

Click the **Add** button to add more application servers (Up to 16)  

Click the **Apply** button.
Procedure 39. IP Front End (IPFE) Configuration (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td><strong>SOAM VIP GUI:</strong> Repeat for additional Configuration of IPFE Target sets. At least one target set must be configured.</td>
</tr>
</tbody>
</table>

Repeat for steps 10-13 for each target set (Up to 16).
4.21 IDIH Installation and Configuration (DSR 7.1-Optional)

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

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

**Note:** For HP Gen9 Rack Mount Servers, follow Appendix S: HP Gen9 Server Hard Disk Drive Locations for IDIH for server hard disk drive locations.

### 4.21.1 IDIH Installation

This procedure is part of DSR 7.1 software installation. The installation procedure uses the “fast deployment” utility (fdconfig) bundled with the PMAC server to install and configure IDIH.

#### Procedure 40. IDIH Installation (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>TVOE Host:</strong> Load Application ISO</td>
</tr>
</tbody>
</table>

Add the Application ISO images (*Mediation, application, and Oracle*) to the PM&C, this can be done in one of three ways:

1. Insert the CD containing the IDIH media into the removable media drive.
2. Attach the USB device containing the ISO image to a USB port.
3. Copy the Application iso file to the PM&C server into the `/var/TKLC/smac/image/isoimages/home/smacftpsr/` directory as pmacftpsr user:

   cd into the directory where your ISO image is located on the TVOE Host (*not on the PMAC server*)

   Using sftp, connect to the PM&C server

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

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

   ```
   $ quit
   ```
### Procedure 40. IDIH Installation (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2    | PMAC GUI: Login | Open web browser and enter:  
  **https://<PMAC_Mgmt_Network_IP>**  
  Login as **pmacadmin** user: |
| 3    | PMAC GUI: Attach the software Image to the PMAC Guest | If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step.  
In the PM&C GUI, navigate to **Main Menu -> VM Management**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the **Media** tab.  
Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its **Attach** button. After a pause, the image will appear in the "**Attached Media**" list. |
### Procedure 40. IDIH Installation (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4    | **PMAC GUI:** Add Application Image  
Navigate to **Main Menu -> Software -> Manage Software Images**  
Press **Add Image** button. Use the drop down to select the image.  
If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://...”). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.  
If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...".  
Select the appropriate path and Press **Add New Image** button.  
You may check the progress using the **Task Monitoring** link. Observe the green bar indicating success.  
Once the green bar is displayed, remove the DSR application Media from the optical drive of the management server. |
| 5    | **PMAC:** Establish Terminal Session  
Establish an SSH session to the PMAC. Login as **admusr**. |
| 6    | **PMAC:** Copy the fdc.cfg file to the guest-dropin Directory  
Copy the fdc.cfg file to the pmac guest-dropin directory.  
Execute the following command:  

```bash  
$ sudo cp /usr/TKLC/smac/html/TPD/mediation-7.1.0.0.0_x.x.x_x/fdc.cfg /var/TKLC/smac/guest-dropin  
```
Procedure 40. IDIH Installation (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Configure the fdc.cfg file</td>
<td>Configure the fdc.cfg file. See Appendix O: IDIH Fast Deployment Configuration for a breakdown of the parameters. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.</td>
</tr>
<tr>
<td>8</td>
<td>Run the FDC creation script Fdc.sh</td>
<td>Run the FDC creation script Fdc.sh. Execute the following commands:</td>
</tr>
</tbody>
</table>

```
$cd /var/TKLC/smac/guest-dropin/
$cd /usr/TKLC/smac/html/TPD/mediation-7.1.0.0.0_x.x.x-x86_64/fdc.sh fdc.cfg
```

**Note:** Rename the fdc.cfg file to your preference; also note that two files are generated by the fdc shell script. One is for the Installation procedure and the other file is used for the upgrade procedure. The upgrade FDC is named upgrade.

Example: hostname.cfg

Note: The following hostname for guests has been reserved for internal use. Please try to avoid them:
- oracle
- mediation
- appserver

Here are the suggested hostname for guests:
- `<server hostname>-ora` example, thunderbolt-ora
- `<server hostname>-med` example, thunderbolt-med
- `<server hostname>-app` example, thunderbolt-app

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Run the fdconfig</td>
<td>Run the fdconfig configuration. Execute the following commands:</td>
</tr>
</tbody>
</table>

```
$sudo fdconfig config –file=hostname_xx-xx-xx.xml
```

Example:

```
$sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml
```
**Procedure 40. IDIH Installation (DSR 7.1-Optional)**

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI: Monitor the Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>If not already done so, establish a GUI session on the PMAC server. Navigate to <strong>Main Menu -&gt; Task Monitoring</strong></td>
</tr>
</tbody>
</table>

Monitor the IDIH configuration to completion.

Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:

Example:
4.21.2 Post IDIH Installation Configuration

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

4.21.2.1 IDIH Configuration: Configure DSR Reference Data Synchronization

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

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

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

Procedure 41. Configure DSR Reference Data Synchronization for IDIH (DSR 7.1-Optional)

This procedure will provide the steps to configure DSR reference data synchronization for IDIH

Note: For DSR 6.0/7.0, refer to [12].

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>IDIH Application Server: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish an SSH session to the IDIH Application Server. Login as user admusr. Issue the following commands to login as tekelec user.</td>
</tr>
<tr>
<td></td>
<td>$ sudo su - tekelec</td>
</tr>
</tbody>
</table>
Procedure 41. Configure DSR Reference Data Synchronization for IDIH (DSR 7.1-Optional)

2

IDIH Application Server:
Execute Configuration Script.

Execute the following script:

```
$ apps/trda-config.sh
```

Example output:

demol-app:/usr/TKLC/xIH apps/trda-config.sh
dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-adapter.properties to UNIX format ...
Please enter DSR SOAM server IP address: 10.240.39.175
dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-adapter.properties to UNIX format ...
Buildfile: build.xml

app.disable:

common.weblogic.stop:

[java] weblogicDeployer invoked with options: -adminurl http://appserver:7001 ...
userconfigfile /usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile /usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop

[java] Task 4 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
[java] Task 4 completed: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
[java] Target state: stop completed on Server nsp

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds
Buildfile: build.xml

app.enable:

common.weblogic.start:

[java] weblogicDeployer invoked with options: -adminurl http://appserver:7001 ...
userconfigfile /usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile /usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start

[java] Oct 17, 2013 11:36:36 AM EDT <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating start operation for application, xIH Trace Reference Data Adapter [archive: null], to configured targets.>
[java] Task 5 initiated: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
[java] Task 5 completed: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
[java] Target state: start completed on Server nsp

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds

For prompt "Please enter DSR SOAM server IP address", enter the VIP of the DSR SOAM and press Enter.

Note: If the address entered is unreachable the script will exit with error "Unable to connect to <ip-address>!"
Procedure 41. Configure DSR Reference Data Synchronization for IDIH (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>STEP</th>
<th>IDIH App Server: Monitor Completion</th>
<th>Monitor the log file located at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Monitor the log file located at:</td>
<td><code>/var/TKLC/xIH/log/apps/weblogic/apps/application.log</code></td>
</tr>
<tr>
<td></td>
<td>Examine the log file for entries containing text “Trace Reference Data Adapter”</td>
<td></td>
</tr>
</tbody>
</table>

4.21.2.2 IDIH Configuration: Configuring the SSO Domain

Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional)

STEP # | This procedure will provide the steps to configure SSO Domain for IDIH

**Note:** For DSR 6.0/7.0, refer to [12].

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

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

<table>
<thead>
<tr>
<th>STEP</th>
<th>NOAM VIP GUI: Login</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login as the <code>guiadmin</code> user:</td>
<td><code>https://&lt;Primary_NOAM_VIP_IP_Address&gt;</code></td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
<table>
<thead>
<tr>
<th>NOAM VIP GUI: Configure DNS</th>
<th>navigate to Main Menu -&gt; Administration -&gt; Remote Servers -&gt; DNS Configuration</th>
</tr>
</thead>
</table>

Configure values for the following fields:

- Domain Name
- Name Server
- Search Domain 1

If values have already been configured, select the **Cancel** button; otherwise configure the above values and select the **Ok** button.
Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional)

3

NOAM VIP GUI:
Establish SSO Local Zone

Navigate to Main Menu -> Access Control -> Certification Management

Select the Establish SSO Zone button

Enter a value for Zone Name:

Select the Ok button.

Information for the new Certificate type of SSO Local is now displayed.

Select the Report button.

The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access.

Example of Certificate report:

-----BEGIN CERTIFICATE-----
MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWI1aDEFMA0GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDV
QQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgc
T3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYDVQQIDA
JQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2x
lMQswCQYDVQQIDAJQVjEQMA4GA1UEAwHGT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4
GA1UEBgcT3JhY2xlMQswCQYDVQQIDAJQVjEQMA4GA1UEBgcT3JhY2xlMQswCQYD
-----END CERTIFICATE-----
### Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>IDIH Application Server GUI: Login</strong>&lt;br&gt;Establish a GUI session on the IDIH app server:&lt;br&gt;Login as the <strong>idihadmin</strong> user:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="IDIH Maintenance login screen" /></td>
</tr>
<tr>
<td>5</td>
<td><strong>IDIH Application Server GUI: Launch the OAM portal</strong>&lt;br&gt;Navigate to the OAM portal Icon to Launch the OAM web application:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Maintenance menu" /></td>
</tr>
</tbody>
</table>
**Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional)**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Server GUI:</strong> Configure the SSO Domain</td>
<td></td>
</tr>
</tbody>
</table>

Navigate to **System -> Single Sign on**

![IDIH GUI](image)

Select the **SSO Parameters** Tab

![SSO Parameters Tab](image)

Select the **Edit Value** Icon Button

![Edit Value Button](image)

Enter a value for the Domain Name.

**Note:** This should be the same domain name assigned in the DSR NOAM DNS Configuration (Step 2)

Select the **Save** icon button.

![Save Button](image)

Select the **Refresh** icon button to display data saved for the Remote Zone.

![Refresh Value Button](image)
### Procedure 42. IDIH Configuration: Configuring the SSO Domain (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>7</th>
<th><strong>DIH Application Server GUI:</strong> Configure the SSO Remote Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Navigate to System -&gt; Single Sign on</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td><strong>Select the SSO Zones Tab</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Remote Zone Configuration" /></td>
</tr>
<tr>
<td></td>
<td><strong>Select the Add icon button</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add Remote Zone" /></td>
</tr>
<tr>
<td></td>
<td><strong>Enter a value for field Remote Name</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Remote Name Entry" /></td>
</tr>
<tr>
<td></td>
<td><strong>For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Certificate Paste" /></td>
</tr>
<tr>
<td></td>
<td><strong>Select the save icon</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Save Icon" /></td>
</tr>
<tr>
<td></td>
<td><strong>Select the Refresh icon to display the data saved for remote zone.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Refresh Icon" /></td>
</tr>
</tbody>
</table>
4.21.2.3 IDIH Configuration: Configuring IDIH in the DSR

Procedure 43. IDIH Configuration: Configure IDIH in the DSR (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOAM VIP GUI: Login</td>
</tr>
</tbody>
</table>

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

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

Login as the `guiadmin` user:

![Oracle System Login](image)

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
Procedure 43. IDIH Configuration: Configure IDIH in the DSR (DSR 7.1-Optional)

2

NOAM VIP GUI: Configure CommAgent Connection

Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers

Select the Insert button

Add the IDIH Mediation Server

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

Set the Remote Server Mode to Server
### Procedure 43. IDIH Configuration: Configure IDIH in the DSR (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>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:</td>
</tr>
</tbody>
</table>

```
https://<Primary_SOAM_VIP_IP_Address>
```

Login as the **guiadmin** user:

![Oracle System Login](image)

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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 43. IDIH Configuration: Configure IDIH in the DSR (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>4</th>
<th>SOAM VIP GUI: Configure IDIH Hostname</th>
</tr>
</thead>
</table>

Navigate to Main Menu -> Diameter -> Troubleshooting with IDIH -> Configuration -> Options

Enter the fully qualified IDIH host name in the **IDIH Visualization Address field**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max bandwidth</td>
<td>25</td>
<td>Maximum amount of bandwidth specified in Mbps that is used for a maximum. Node will discard TTPs so that the bandwidth required is less than the configured maximum. (Default: 2Mbps, Range: 0-25)</td>
</tr>
<tr>
<td>IDIH Host Name</td>
<td>- Select -</td>
<td>The Host Name of the peer IDIH server used for sending the messages. (Default: trial)</td>
</tr>
<tr>
<td>IDIH Visualization address</td>
<td>100.65.135.179</td>
<td>The IP address or FQDN of the remote IDIH server that visualizes the &quot;Maintenance&quot; screen. If an IP address is used in place of a FQDN then IDIH SSO function is disabled.</td>
</tr>
</tbody>
</table>

Click the **Apply** button
### 4.21.2.4 IDIH Configuration: Configuring Mail Server (Optional)

**Procedure 44. IDIH Configuration: Configure Mail Server-Optional (DSR 7.1-Optional)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>IDIH Application Server: Login</strong> Establish an SSH session to the IDIH Application Server, login as <code>admusr</code>.</td>
</tr>
</tbody>
</table>

This procedure will provide the steps to configure the SMTP mail server.

**Note:** This procedure is optional; however, this option is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined) and is available only on the Application server.

**Note:** For DSR 6.0/7.0, refer to [12].

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
**Procedure 44. IDIH Configuration: Configure Mail Server-Optional (DSR 7.1-Optional)**

<table>
<thead>
<tr>
<th>Step</th>
<th>IDIH Application Server: Configure the Authenticated Mail Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Enter the platcfg menu, execute the following command:</strong></td>
</tr>
<tr>
<td></td>
<td>$ sudo su - platcfg</td>
</tr>
</tbody>
</table>

Select **Application Server Configuration**

Select **SMTP Configuration**

Select **Edit**

Enter the following parameters:

1. Mail Server IP Address
2. User
3. Password
4. Email Address (From)
5. Mail smtp timeout
6. Mail smtp connectiontimeout
7. SNMP over SSL used?

Select **OK**

Select **Exit** to exit the platcfg menu.
### 4.21.2.5 IDIH Configuration: Configuring SNMP Management Server (Optional)

**Procedure 45. IDIH Configuration: Configure SNMP Management Server-Optional (DSR 7.1-Optional)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IDIH Application Server: Login</td>
</tr>
</tbody>
</table>

This procedure will provide the steps to configure the SNMP management server.

**Note:** This procedure is optional; however, this option is required for Forwarding (forwarding by SNMP filter defined) and is available only on the application server.

**Note:** For DSR 6.0/7.0, refer to [12].

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

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

Establish an SSH session to the IDIH Application Server, login as admusr.
## Procedure 45. IDIH Configuration: Configure SNMP Management Server-Optional (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>IDIH Application Server: Configure SNMP Management Server</th>
</tr>
</thead>
</table>

Enter the platcfg menu, execute the following command:

```
$ sudo su - platcfg
```

Select **Application Server Configuration**

Select **SNMP Agent Configuration**

Select **Edit**

Enter the IP address of the SNMP Management Server

**Note:** The SNMP agent configuration is updated and the SNMP Management server is automatically restarted.

Select **OK**

Select **Exit** to exit the platcfg menu.
### 4.21.2.6 IDIH Configuration: Change Network Interface (Optional)

**Procedure 46. IDIH Configuration: Change Network Interface-Optional (DSR 7.1-Optional)**

This procedure will provide the steps to change the default network interface.

**Note:** Initially the default network interface used to transport TTRs from DSR to DIH uses the internal imi network; however, this can be changed if required. It should be noted that changing this interface could degrade performance of TTR transmission.

**Note:** A script is provided to manage the settings so that the operator doesn’t need to know the details required to apply the settings. There are two settings ‘interface.name’ and ‘interface.enabled’.

- When `interface.enabled=True` then communications over the `interface.name =value` where value is the name of the network interface as defined on the platform, is the only specified interface that is used for communications.

- When `interface.enabled=False` then communications over the named interface is not enforced, that is, all interfaces configured on the platform are allowed to be used for communications.

For example, if it is required to use the xmi interface for communication instead of the default internal imi interface, then the operator would supply ‘xmi’ when prompted for the interface name and ‘True’ when prompted if interface filtering should be applied.

**Note:** For DSR 6.0/7.0, refer to [12].

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>IDIH Mediation Server: Login</th>
<th>Establish an SSH session to the IDIH Mediation Server. Login as user <strong>admusr</strong>. Issue the following commands to login as <strong>tekelec</strong> user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$ sudo su --tekelec</td>
<td>$ sudo su --tekelec</td>
</tr>
</tbody>
</table>

---

Note: For DSR 6.0/7.0, refer to [12].

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

If this procedure fails, contact **Appendix U: My Oracle Support (MOS)**, and ask for assistance.
Procedure 46. IDIH Configuration: Change Network Interface-Optional (DSR 7.1-Optional)

<table>
<thead>
<tr>
<th>Step #</th>
<th>IDIH Mediation Server: Execute the Change Interface Script</th>
<th>Execute the change interface script with the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Execute the change interface script with the following command: $ chgIntf.sh</td>
<td></td>
</tr>
</tbody>
</table>

Answer the following questions during execution of the script:

This script is used to change the interface name (default = imi) used for mediation communications and whether to enable network interface filtering or not. Please answer the following questions or enter CTRL-C to exit out of the script.

Current setting are: interface.name=imi interface.enabled=True

Enter new network interface name, return to keep current [imi]: xmi

Do you want to enable network interface filtering [True|False], return to keep current [True]:

Updating configuration properties file with 'interface.name=xmi' and 'interface.enable=True', and restarting mediation configuration bundle...

4.21.2.7 IDIH Configuration: Generate Disaster Recovery FDC File (Optional)

Procedure 47 IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (DSR 7.1-Optional)

This procedure will provide the steps to generate a disaster recovery fdc file.

Note: For DSR 6.0/7.0, refer to [12].

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

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Identify Backup Server</th>
<th>Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:</th>
</tr>
</thead>
</table>
| 1      | Identify Backup Server | TVOE
|        |                        | PMAC
|        |                        | DSR NOAM
|        |                        | DSR SOAM

<table>
<thead>
<tr>
<th>Step #</th>
<th>PMAC: Establish Terminal Session</th>
<th>Establish an SSH session to the PMAC. Login as admusr.</th>
</tr>
</thead>
</table>
### Procedure 47 IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (DSR 7.1-Optional)

#### Step 3

**PMAC:** Verify Upgrade fdc file exists

Execute the following commands to verify the upgrade FDC file for IDIH exists:

```bash
$ cd /var/TKLC/smac/guest-dropin
$ ls -l *.xml
```

The following 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.

#### Step 4

**PMAC:** Transfer the FDC file to a remote server.

Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.

```bash
$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/guest-dropin/<idih_upgrade>.xml /path/to/destination/
```

When prompted, enter the admusr user password and press **Enter**.

If the Customer System is a Windows system please refer to reference [3] (DSR 6.0/7.0)/[4] (DSR 7.1) Using WinSCP to copy the backup image to the customer system.

### 4.22 Activate Optional Features

**Procedure 47. Activate Optional Features**

**Prerequisite:** All previous DSR installation steps have been completed.

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

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

**Refer to Install Guides for Optional Features to Complete Installation**

Refer to Section 3.3 for a list of feature install documents whose procedures are to be executed at this moment.
### 4.23 Post-Install Activities

**Procedure 48 Backup TVOE Configuration**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Identify Backup Server</strong></td>
<td>Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- TVOE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PMAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- DSR NOAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- DSR SOAM</td>
</tr>
<tr>
<td>2</td>
<td><strong>TVOE Server: Login</strong></td>
<td>Establish an SSH session to the TVOE host server, login as <code>admusr</code>.</td>
</tr>
</tbody>
</table>
Procedure 48 Backup TVOE Configuration

TVOE Server: Build ISO backup file

Execute the following command from the TVOE server:

```
$ sudo su - - platcfg
```

Select the following menu options sequentially:
- Maintenance -> Backup and Restore -> Backup Platform (CD/DVD).
- The “Backup TekServer Menu” page will now be shown.

Build the backup ISO image by selecting:
- Build ISO file only

Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.

After the ISO is created, platcfg will return to the Backup TekServer Menu. The ISO has now been created and is located in the `/var/TKLC/bkp/` directory. An example filename of a backup file that was created is: “hostname1307466752-app-201104171705.iso”

Exit out of platcfg by selecting Exit.
## Procedure 48 Backup TVOE Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 4    | Backup Server: Transfer TVOE Files to Backup Server | Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.  

```
$ sudo scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
```

When prompted, enter the tvoexfer user password and press Enter.  

If the Customer System is a Windows system please refer to reference [3] (DSR 6.0/7.0) / [4] (DSR 7.1) Using WinSCP to copy the backup image to the customer system.  

The TVOE backup file has now been successfully placed on the backup server. |
| 5    | Repeat for Additional TVOE Servers | Repeat steps 3-4 for additional TVOE servers                                |

## Procedure 49 Backup PMAC Application

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
|      | This procedure will provide instruction on how to back up each PMAC application installed in this procedure.  
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.  
If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance. | Identify an external server to be used as a backup server for the following steps.  
The server should not be co-located with any of the following items:  
  - TVOE  
  - PMAC  
  - DSR NOAM  
  - DSR SOAM  

PMAC Server: Login Establish an SSH session to the PMAC server, login as admusr. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 1    | Identify Backup Server        | Identify an external server to be used as a backup server for the following steps.  
The server should not be co-located with any of the following items:  
  - TVOE  
  - PMAC  
  - DSR NOAM  
  - DSR SOAM  

PMAC Server: Login Establish an SSH session to the PMAC server, login as admusr. |
### Procedure 49 Backup PMAC Application

#### PMAC Server: Build backup File

Execute the following command from the PMAC server:

```bash
$ 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 `pmaccli getBgTasks`. The result should eventually be "PMAC Backup successful" and the background task should indicate "COMPLETE".

#### PMAC GUI: Login

Open web browser and enter:

```
http://<PMAC_Mgmt_Network_IP>
```

Login as `pmacadmin` user:

![Oracle System Login](image_url)
### Procedure 49 Backup PMAC Application

#### 5 PMAC Server GUI:
**Monitor/Verify Backup Task Completion**

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

![Background Task Monitoring](image)

Monitor the Backup PM&C Task:

**Note:** Alternatively, you can monitor the Backup task by executing the following command:

```
$ sudo pmaccli getBgTasks
```

#### 6 Backup Server:
**Transfer PMAC File to Backup Server**

Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.

```
$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/
```

When prompted, enter the admusr user password and press **Enter**.

If the Customer System is a Windows system please refer to reference [3] (DSR 6.0/7.0) [4] (DSR 7.1) Using WinSCP to copy the backup image to the customer system.

#### 5 Repeat for Additional TVOE Servers

Repeat **steps 2-6** for additional TVOE servers
Procedure 50 NOAM Database Backup

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Identify Backup Server</th>
<th>Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>• TVOE&lt;br&gt;• PMAC&lt;br&gt;• DSR NOAM&lt;br&gt;• DSR SOAM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI: Login</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td><strong>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong>&lt;br&gt;Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image-url)
Procedure 50 NOAM Database Backup

4

NOAM VIP
GUI: Perform Database Backup

Navigate to Main Menu -> Status & Manage -> Database

Select the Active NOAM

Select the Backup Button:

Select the desired file compression method

Set the archive file name if needed.

Select OK

6

Backup Server: Transfer PMAC File to Backup Server

Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.

```
$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/
```

When prompted, enter the admusr user password and press Enter.

If the Customer System is a Windows system please refer to reference [3] (DSR 6.0/7.0) [4] (DSR 7.1) Using WinSCP to copy the backup image to the customer system.
Procedure 51 SOAM Database Backup

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| 1      | Identify Backup Server | Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:  
- TVOE  
- PMAC  
- DSR NOAM  
- DSR SOAM |
| 2      | SOAM VIP GUI: Login | Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of:  
http://<Primary_SOAM_VIP_IP_Address>  
Login as the guiadmin user: |

[ Oracle System Login Image ]

If this procedure fails, contact **Appendix U: My Oracle Support (MOS), and ask for assistance.**
### Procedure 51: SOAM Database Backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **4** | **SOAM VIP GUI: Perform Database Backup**  
Navigate to **Main Menu -> Status & Manage -> Database**  
Select the Active SOAM  
Select the **Backup** Button:  
Select the desired file compression method  
Set the archive file name if needed.  
Select **OK**  
| **5** | **Backup Server: Transfer PMAC File to Backup Server**  
Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.  
```
$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/
```
When prompted, enter the admusr user password and press **Enter**.  
If the Customer System is a Windows system please refer to reference [3] (DSR 6.0/7.0) [4] (DSR 7.1) Using WinSCP to copy the backup image to the customer system.  
| **6** | **Repeat for Additional TVOE Servers**  
Repeat **steps 2-6** for additional SOAM Sites |
Important: Before configuring Diameter connections (SCTP Only), please refer to Appendix T: Disable/Enable DTLS.
Appendix A: Pre-IPM Procedures

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

The date and time in the server’s CMOS clock must be set accurately before running the IPM procedure. There are a number of different ways to set the server’s CMOS clock.

Appendix A.2: Configure the RMS Server BIOS Settings

Appendix A.2.1: Configure HP Gen 8 Servers

Follow these steps to configure HP Gen 8 server BIOS settings

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HP DL380 Server: Reboot</td>
</tr>
</tbody>
</table>

Reboot the server and after the server is powered on, press the <F9> key when prompted to access the ROM-Based Setup Utility:

![ROM-Based Setup Utility, Version 3.00](image)

Copyright 1982, 2012 Hewlett-Packard Development Company, L.P.

- System Options
- Power Management Options
- PCI IRQ Settings
- PCI Device Enable/Disable
- Standard Boot Order (IPL)
- Boot Controller Order
- Network Login
- Server Availability
- Server Security
- BIOS Serial Console & EMS
- Server Asset Text
- Advanced Options
- System Default Options
- Utility Language

HP ProLiant DL380p Gen8
S/M: USE2162BHC
Product ID: 653200-821
HP BIOS F70 02/25/2012
Backup Version 02/21/2012
Bootblock 00/30/2011
Power Management Controller - 3.0
131072MB Memory Configured

Proc 1: Intel 2.60GHz, 2MB L3 Cache
Proc 2: Intel 2.60GHz, 2MB L3 Cache

Press <TAB> for More Information

(Enter) to View/Modify Date and Time
(1/4) for Different Selection: <TAB> for More Info: <ESC> to Exit Utility
## Appendix A.2. Configure HP Gen 8 Server BIOS Settings

<table>
<thead>
<tr>
<th>Step</th>
<th>HP DL380 Server:</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Configure HP Gen 8 Server BIOS Settings</strong></td>
<td>From the above screen (Step 1), set the data and time to GMT (Greenwich Mean Time). Press &lt;Esc&gt; to navigate to the main menu</td>
</tr>
<tr>
<td>2</td>
<td><strong>Select the Date and Time</strong></td>
<td>From the above screen (Step 1), set the data and time to GMT (Greenwich Mean Time). Press &lt;Esc&gt; to navigate to the main menu</td>
</tr>
</tbody>
</table>
| 3    | **Select Server Availability** | From the above screen (Step 1), select Server Availability.  
- Change Automatic Power-On to Enabled  
- Change Power-On Delay to No Delay  
- Press <Esc> to navigate to the main menu |
| 4    | **System Options** | From the above screen (Step 1), Select System Options.  
- Select Power Management Options  
- Select HP Power Regulator  
- Select HP Status High Performance Mode  
- Press <ESC> to navigate to the main menu |
| 5    | **Power Management Options** | From the above screen (Step 1), Select System Options.  
- Select Processor Options.  
- Change Intel® Virtualization Technology to **Enabled**.  
- Press <ESC> to return to System Options.  
- Select Serial Port Options. |
| 6    | **Exit ROM-Based Utility** | Press <ESC> to Save and Exit from the ROM-Based Setup Utility. |
## Appendix A.2.2: Configure Oracle Rack Mount Servers

### Appendix A.2. Configure Oracle Rack Mount Server BIOS Settings

This procedure explains the steps needed to configure Oracle rack mount server BIOS settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Oracle RMS:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reboot</td>
<td>Reboot the server. After the server is powered on, press the <strong>F2</strong> key when prompted to access the Setup Utility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Setup Utility Screenshot" /></td>
</tr>
<tr>
<td>2</td>
<td>Set Server Data and Time</td>
<td>From the above screen (Step 1), set the data and time to GMT (Greenwich Mean Time).</td>
</tr>
</tbody>
</table>
### Appendix A.2.2. Configure Oracle Rack Mount Server BIOS Settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Oracle RMS: Exit and Save Changes</th>
<th>Oracle RMS: Advanced Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td>From the above screen (Step 1) Go to the <strong>Advanced Menu</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select Processors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select CPU Power Management Configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If Energy Performance is not set to [Performance], select <strong>Energy Performance</strong> and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the resulting menu, select the <strong>Performance</strong> option and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Press &lt;ESC&gt; to return to the advanced menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select <strong>UEFI Configuration Synchronization</strong> and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If <strong>Synchronization Late</strong> is not [Disabled], press <strong>Enter</strong> to modify the option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. In the resulting menu, select the Disabled option and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Press the Escape key once to return to the <strong>Advanced menu</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>⚠️ If this is an X3-2 Server, skip to Step 4. ⚠️</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the <strong>Exit</strong> or <strong>Save &amp; Exit</strong> menu and press <strong>Enter</strong> on Save Changes and Reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Answer Yes to the prompt for confirmation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Go to the <strong>Save &amp; Exit</strong> menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select <strong>Save Changes and Reset</strong>.</td>
</tr>
</tbody>
</table>

Go to the **Save & Exit** menu.  
Select **Save Changes and Reset**.
Appendix A.2.3: 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 Gen9s should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided below.

Appendix A.2.3. Configure HP Gen 9 Server BIOS Settings

<table>
<thead>
<tr>
<th>STEP #</th>
<th>HP Gen9 Server:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect:</td>
<td>Connect via a VGA monitor and USB keyboard.</td>
</tr>
<tr>
<td>2</td>
<td>Reboot</td>
<td>Reboot the server. After the server is powered on, press the F9 key when prompted to access the System Utilities menu:</td>
</tr>
<tr>
<td>3</td>
<td>System Configuration</td>
<td>From the above screen (Step 2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the System Configuration menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the BIOS/Platform Configuration (RBSU) menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the Boot Options menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the Boot Mode is NOT Legacy BIOS mode, press &lt;Enter&gt; to open the BIOS mode menu. Otherwise skip to step 5.</td>
</tr>
<tr>
<td>4</td>
<td>Legacy BIOS Mode</td>
<td>Continued from the step 3, select Legacy BIOS Mode.</td>
</tr>
<tr>
<td>5</td>
<td>Press &lt;Esc&gt; once to back out to the BIOS/Platform Configuration (RBSU) menu.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Serial Port Options</td>
<td>From the above screen (Step 2), Select the System Options menu, then select the Serial Port Options menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change Embedded Serial Port to COM2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change Virtual Serial Port to COM1</td>
</tr>
<tr>
<td>7</td>
<td>Exit</td>
<td>Press &lt;Esc&gt; twice to back out to the BIOS/Platform Configuration (RBSU) menu.</td>
</tr>
</tbody>
</table>
### Appendix A.2.3. Configure HP Gen 9 Server BIOS Settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8    | **HP Gen9 Server:** Server Availability  
From the above screen (Step 2), Select the **Server Availability** menu.  
- Set the **Automatic Power-On** to **Restore Last Power State**  
- Set **Power-On Delay** to **No Delay** |
| 9    | **HP Gen9 Server:** Exit  
Press <Esc> twice to back out to the **BIOS/Platform Configuration (RBSU)** menu. |
| 10   | **HP Gen9 Server:** Power Management  
From the above screen (Step 2), select the **Power Management** menu  
- Select the Power Management menu.  
- Set HP Power Profile to Maximum Performance. Press <Esc> once to back out to the **BIOS/Platform Configuration (RBSU)** menu. |
| 11   | **HP Gen9 Server:** Save Settings and Exit  
Press <F10> to save the updated settings, then <y> to confirm the settings change.  
Press <Esc> twice to back out to the System Utilities menu. |
| 12   | **HP Gen9 Server:** Reboot  
Select **Reboot the System** and press <Enter> to confirm. |
Appendix B: Upgrade Server Firmware

Appendix B.1: HP DL 380 Server

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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ilo_ip&gt;</td>
<td>Fill in the IP address of the iLO for the server being upgraded</td>
</tr>
<tr>
<td>&lt;ilo_admin_user&gt;</td>
<td>Fill in the username of the iLO’s Administrator user</td>
</tr>
<tr>
<td>&lt;ilo_admin_password&gt;</td>
<td>Fill in the password for the iLO’s Administrator user</td>
</tr>
<tr>
<td>&lt;local_HPSPP_image_path&gt;</td>
<td>Fill in the filename for the HP Support Pack for ProLiant ISO</td>
</tr>
<tr>
<td>&lt;admusr_password&gt;</td>
<td>Fill in the password for the admusr user for the server being upgraded</td>
</tr>
</tbody>
</table>

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

Note: For the "Update Firmware Errata" step check the HP Solutions Firmware Upgrade Pack Release notes [1] to see if there are any firmware errata items that apply to the server being upgraded. If there is, there will be a directory matching the errata’s ID in the /errata directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.
## Appendix B.1.1 Upgrade DL380 Server Firmware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | **Local Work Station:** Insert the USB Flash Drive  
Insert Update Firmware USB into a USB port of the RMS server. Refer to steps for creating a bootable SPP USB media or refer to Appendix Q: Creating a Bootable USB Drive on Linux  
**Note:** There is also the option of mounting a virtual image for this process. If this option is used, **skip this step.** |
| 2    | **Local Work Station:** Login to the iLO web GUI  
Access the iLO web GUI.  
https://<iLO_IP>/  
Username = <iLO_admin_user>  
Password = <iLO_admin_password> |
Appendix B.1.1 Upgrade DL380 Server Firmware

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>ILO4 Web GUI:</strong> Launch Remote Console.</td>
</tr>
</tbody>
</table>

Launch the Java Integrated Remote Console applet.

On the menu to the left navigate to the **Remote Console** page. Under Java Integrated Remote Console (Java IRC), click **Launch**

![Java Integrated Remote Console (Java IRC)](image)

The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java applet-based console. Java IRC requires the availability of Java.

Acknowledge the security warning if presented:
Appendix B.1.1 Upgrade DL380 Server Firmware

4

**ILO4 Remote Console:**
- Create Virtual Drive Connection

⚠️ If using SPP USB media plugged into the server, skip this step.

Click on the **Virtual Drives** drop down menu. Go to **CD/DVD** then click on **Virtual Image**.

Navigate to the HP Support Pack for ProLiant ISO ISO file copied to the workstation.

Select the ISO image file and click **Open**.

At the bottom of the remote console window you should now see a green highlighted drive icon and **VirtualM** written next to it.
## Appendix B.1.1 Upgrade DL380 Server Firmware

<table>
<thead>
<tr>
<th></th>
<th>iLO4 Remote Console:</th>
<th>Login to the server as admusr.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Password: &lt;admusr_password&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>iLO4 Remote Console:</th>
<th>Reboot the server by executing the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><code>$ sudo init 6</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>iLO4 Remote Console:</th>
<th>The server will reboot into the HP Support Pack for ProLiant ISO and present the following boot prompt.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Press [Enter] to select the <strong>Automatic Firmware Update</strong> procedure.</td>
</tr>
</tbody>
</table>

![Automatic Firmware Update Version 2012.42.0](image)

**Note:** If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.
## Appendix B.1.1 Upgrade DL380 Server Firmware

| 8 | ILO4 Remote Console: Monitor Installation. |

**Important:** Do not click inside the remote console during the rest of the firmware upgrade process.

The firmware install will stay at the EULA acceptance screen for a short period of time. The time it takes this process to complete will vary by server and network connection speed and will take several minutes.

Depending on the hardware, the following screens will be displayed:

1. **Please Wait.**
   - Analyzing the system for unattended installation.
   - This could take several minutes...

2. **HP Service Pack for ProLiant 2014.09.0**
   - Please wait, analyzing system....

**Note:** No progress indication is displayed. The installation will proceed automatically to the next step.
Appendix B.1.1 Upgrade DL380 Server Firmware

Once analysis is complete, the installer will begin to upgrade inventory and deploy the eligible firmware components.

A progress indicator is displayed at this time, as shown below. If iLO firmware is applied, the Remote Console will disconnect, but will continue upgrading.

If the Remote Console closes due to the iLO upgrading, wait 3-5 minutes and log back in to the iLO Web GUI and re-connect to the Remote Console. The server might already be done upgrading and might have rebooted.

Depending on the hardware, the following screens will be displayed:

Note: If the iLO firmware is to be upgraded, it will be upgraded last. At this point the iLO 2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.
Appendix B.1.1 Upgrade DL380 Server Firmware

10  Local Work Station: Clean Up

Once the firmware updates have been completed the server will automatically be rebooted.

Closing the remote console window will disconnect the Virtual Image and you can close the iLO3/iLO4 Web GUI browser session.

If you are using SPP USB media plugged into the server you can now remove it.

11  Local Work Station: Verify Server Availability

Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.

12  Local Work Station: Update Firmware Errata

Refer to the ProLiant Server Firmware Errata section of [13] to determine if this HP Solutions Firmware Update Pack contains additional firmware errata updates that should be applied to the server at this time.

13  Repeat for Additional RMS Servers

Repeat this procedure for additional HP DL380 rack mount servers.

Appendix B.2: Oracle Rack Mount Server

Needed Material:

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

Note: The minimum supported Oracle Firmware Upgrade Pack for DSR 7.1 is release 3.1.3. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, and then follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.
## Appendix C: Changing the SNMP Configuration Settings

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th><strong>Local Work Station:</strong> Login to the iLO web GUI</th>
</tr>
</thead>
</table>
| 1      | Access the iLO web GUI.  
|        | [https://<iLO_IP>/](https://<iLO_IP>)/  
|        | **Username** = `<iLO_admin_user>`  
|        | **Password** = `<iLO_admin_password>` |

<table>
<thead>
<tr>
<th>STEP #</th>
<th><strong>iLO4 GUI:</strong> Navigate to Management Screen</th>
</tr>
</thead>
</table>
| 2      | Expand the [Administration] menu item in the left hand navigation pane.  
|        | Select the [Management] sub-menu item to display the Management configuration page. |
### Appendix C.1. Changing SNMP Configuration Settings for HP DL 380

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>iLO4 GUI:</strong> Disable SNMP Alerts</td>
<td>From the above screen (Step 2): Select setting [Disabled] for each of the 3 SNMP Alerts options as shown to the right. <img src="image.png" alt="Image of SNMP settings" /> Click [Apply] to save the change. <strong>Note:</strong> To verify the setting changes navigate away from the Management configuration page and then go page back to it to verify the SNMP settings as shown on the right.</td>
</tr>
<tr>
<td>4</td>
<td><strong>iLO4 GUI:</strong> Exit</td>
<td>Click [Sign Out] link in upper right corner of page to log out of the iLO GUI.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Repeat for Additional RMS Servers.</strong></td>
<td>Repeat this procedure for additional HP DL 380 rack mount servers.</td>
</tr>
</tbody>
</table>
Appendix D: TVOE iLO/iLOM GUI Access

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

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| 1      | Launch Internet Explorer  
Navigate to 192.168.100.5 (manufacturing default) or customer IP set during installation. |
| 2      | Internet Explorer may display a warning message regarding the Security Certificate. |
Appendix D.1. TVOE iLO4 GUI Access

3. Select the option to Continue to the website (not recommended)

4. Log in to the iLO4

5. The iLO4 Home page is displayed.

6. Click on Launch to start the PMAC iLO4 CLI
Appendix D.2: iLOM GUI Access (Oracle RMS)

Appendix D.2. TVOE iLO4 GUI Access

This procedure contains the steps to 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, contact Appendix U: My Oracle Support (MOS), and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Launch Internet Explorer</td>
<td><img src="image" alt="Login Screen" /></td>
</tr>
<tr>
<td></td>
<td>Navigate to 192.168.100.5 (manufacturing default) or customer IP set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>during installation.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Internet Explorer may display a warning message regarding the Security</td>
<td><img src="image" alt="Certificate Error" /></td>
</tr>
<tr>
<td></td>
<td>Certificate.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Select the option to Continue to the website (not recommended)</td>
<td><img src="image" alt="Certificate Error Warning" /></td>
</tr>
</tbody>
</table>

- Log in - Tekelec Platform Management & Configuration - Windows Internet Explorer
- There is a problem with this website’s security certificate.
- We recommend that you close this webpage and do not continue to this website.
## Appendix D.2. TVOE iLO4 GUI Access

<table>
<thead>
<tr>
<th>Step</th>
<th>Oracle RMS:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Login</td>
<td>Login to the Oracle rack mount server ILOM:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image1" alt="Login Screen" /></td>
</tr>
<tr>
<td>5</td>
<td>Access the Remote Console</td>
<td>Navigate to Remote Control -&gt; Redirection Select Launch Remote Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image2" alt="Remote Control Screen" /></td>
</tr>
</tbody>
</table>
Appendix D.2. TVOE iLO4 GUI Access

6

Oracle RMS: Access the Remote Console

Select **OK** and open with Java Web Start Launcher

Select **Continue** and **Run** for any security warning prompts
Appendix E: Changing the TVOE iLO4 Address

Appendix E.1. Changing the TVOE iLO Address

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HP DL 380: Connect to the TVOE iLO GUI</td>
<td>Using the instructions in Appendix D: TVOE iLO/iLOM GUI Access, connect to the iLO4 GUI</td>
</tr>
<tr>
<td>2</td>
<td>iLO4 GUI: Navigate to Network Menu</td>
<td>Navigate to Network -&gt; iLO Dedicated Network Port</td>
</tr>
</tbody>
</table>

Select the tab for either IPv4 or IPv6
Appendix E.1. Changing the TVOE iLO Address

### 3
**iLO4 GUI:**
- Change **IP information** Subnet Mask and **Gateway IP Address** to the values supplied in the NAPD for the TVOE iLO.
- Select **Apply**.

**Note:** You will lose access after you hit the **Apply** button.

**Change the IP address, subnet Mask/prefix, and Gateway address to the values supplied in the NAPD for the TVOE iLO.**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route #1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Static Route #2</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Static Route #3</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Select **Submit**

**Note:** You will lose access after you hit the **Submit** button.

### 4
**Local Machine:**
- Reset PC’s network connection.

Using the instructions found in **Appendix G:** Configuring for TVOE iLO Access; reset the PC’s network connection replacing the **Subnet Mask** and **Gateway** with those just used for the TVOE iLO.

Use an appropriate **IP address** for this subnet.
Appendix E.1. Changing 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 entered in Step 3
Appendix F: Attaching an ISO Image to a Server using the iLO or iLOM

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

Appendix F.1: HP DL380 Servers (iLO4)

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

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>iLO 4 Web GUI: Launch Remote Console</td>
<td>Launch the Java Integrated Remote Console applet. On the menu to the left navigate to the Remote Console page. Under Java Integrated Remote Console (Java IRC), click Launch</td>
</tr>
</tbody>
</table>
## Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4

### Table

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>iLO 4 Web GUI: Java Security Prompt</strong></td>
</tr>
<tr>
<td></td>
<td>Acknowledge Security Warning.</td>
</tr>
<tr>
<td></td>
<td>If a dialog similar to the one below is presented, click <strong>Yes</strong> to acknowledge the issue and proceed.</td>
</tr>
</tbody>
</table>

![Warning Security](image_url)
Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4

3. Click on the Virtual Drives drop down menu. Go to CD/DVD, then click on Virtual Image.

Navigate to the location of the ISO image file specified by the procedure which referenced this appendix.

4. Verify Virtual Image Connection.

Select the desired file and click Open.

At the bottom of the remote console window, there should now be a green highlighted drive icon and Virtual M written next to it.
Appendix F.2: Oracle RMS Servers (iLOM)

Appendix F.2.2. HP DL380 Servers Mounting the ISO image via iLO4

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Oracle RMS:</strong> Login</td>
</tr>
<tr>
<td></td>
<td>Login to the Oracle rack mount server ILOM:</td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="Login Image" /></td>
</tr>
<tr>
<td>2</td>
<td><strong>Oracle RMS:</strong> Access the Remote Console</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Remote Control -&gt; Redirection</strong></td>
</tr>
<tr>
<td></td>
<td>Select Launch <strong>Remote Console</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="Remote Console Image" /></td>
</tr>
</tbody>
</table>
Appendix F.2.2. HP DL380 Servers Mounting the ISO image via iLO4

3. Oracle RMS: Access the Remote Console

Select OK and open with Java Web Start Launcher

Select Continue and Run for any security warning prompts
### Oracle RMS: Mount the ISO from the Remote Console

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Navigate to KVMS</td>
</tr>
<tr>
<td></td>
<td>Select Storage</td>
</tr>
</tbody>
</table>

1. Navigate to KVMS
2. Select Storage
3. Select Add, browse to the ISO located on the local machine.
4. Click Select
5. Once the ISO image is selected, now select Connect
### Appendix F.2. HP DL380 Servers Mounting the ISO image via iLO4

<table>
<thead>
<tr>
<th>Oracle RMS: Change the Device for Next Boot</th>
<th>Oracle RMS: Power Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the Next Boot Device by navigating to Host Management -&gt; Host Control. In the drop down box, select CDROM.</td>
<td>Reboot the rack mount server to start the install by navigating to Host Management -&gt; Power Control. From the drop down box, select Reset.</td>
</tr>
</tbody>
</table>
## Appendix G: Configuring for TVOE iLO Access

### Appendix G.1 Connecting to the TVOE iLO

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

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

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

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

2. Click **Use the following IP address**
   - Set the **IP address** to 192.168.100.100
   - Set the **Subnet mask** to 255.255.255.0
   - Set the **Default gateway** to 192.168.100.1
   - Select **OK**.
   - Select **Close** from the network interface card’s main **Properties** screen.

3. Connect the laptop’s Ethernet port directly to the TVOE iLO port using a standard Cat-5 cross-over cable.
Appendix H: SNMP Configuration

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

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

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

DSR application servers can be configured to:

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

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

3. Send SNMP traps from individual servers like MPs of all types if Traps from Individual Servers check box is selected on Main Menu > Administration > Remote Servers > SNMP Trapping screen.
Application server SNMP configuration is done from the NOAM GUI, near the end of DSR installation.

See the procedure list for details.

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

The recommended configuration is as follows:
The following components:
• PMAC (TVOE)
• PMAC (App)
• Applicable Switch types
• TVOE for DSR Servers
Should have their SNMP trap destinations set to:
1. The local SOAM VIP
2. The customer NMS, if available

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

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

Appendix I: Application NetBackup Client Installation Procedures

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

Please note that at the writing of this document, the supported versions of Netbackup in DSR 6.0/7.0/7.1 are 7.1, 7.5 and 7.6.
## Appendix I.1: NetBackup Client Install using PLATCFG

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

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

Table of Contents

2

Application server iLO: Navigate to NetBackup Configuration

Configure NetBackup Client on application server

```
$ sudo su - platcfg
```

Navigate to NetBackup -> Configuration

3

Application server iLO: Enable Push of NetBackup Client

Navigate to NetBackup Configuration -> Enable Push of NetBackup Client

```
Do you wish to initialize this server for NetBackup Client?
Yes No
```

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

Enter the NetBackup password:

Note: If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.
### Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

<table>
<thead>
<tr>
<th>5</th>
<th><strong>Application server iLO:</strong> Verify NetBackup Client software push is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Navigate to</strong> NetBackup Configuration -&gt; Verify NetBackup Client Push</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="NetBackup Configuration Utility 3.06 (c) 2003 - 2011 Symantec, Inc." /></td>
</tr>
<tr>
<td></td>
<td>- Password: master366666</td>
</tr>
<tr>
<td></td>
<td>- Verify NetBackup Client Environment</td>
</tr>
<tr>
<td></td>
<td>- Users must set up: netbackup</td>
</tr>
<tr>
<td></td>
<td>- Users netbackup shell set up: /usr/bin/bash</td>
</tr>
<tr>
<td></td>
<td>- Home directory: /home/cshh/home/netbackup</td>
</tr>
<tr>
<td></td>
<td>- Top directory: /home/cshh/top</td>
</tr>
<tr>
<td></td>
<td>- Top directory permissions 1777</td>
</tr>
</tbody>
</table>

Verify list entries indicate **OK** for NetBackup client software environment.

Select **Exit** to return to NetBackup Configuration menu.
### Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>NetBackup server: Push appropriate NetBackup Client software to application server</td>
</tr>
</tbody>
</table>

**Note:** 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. Below are the steps that 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.

**Note:** 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 that is being used at this site.

**Login** to the NetBackup server using password provided by customer:

Navigate to the appropriate NetBackup Client software path:

**Note:** The input below is only used as an example. (7.5 in the path below refer to the NetBackup version. If installed a different version (e.g. 7.1 or 7.6), replace 7.5 with 7.1 or 7.6)

```
$ cd /usr/openv/netbackup/client/Linux/7.5
```

**Execute** the `sftp_to_client` NetBackup utility using the application IP address and application netbackup user:

```
$ ./sftp_to_client <application IP> netbackup
```

**Note:** The optional argument, `-L`, is used to avoid modification of the client's current bp.conf file.
<table>
<thead>
<tr>
<th>Step</th>
<th>Application server iLO: Install NetBackup Client software on application server.</th>
</tr>
</thead>
</table>
| 7    | **Execute the command:**  

```bash
$ sudo chmod 555 /var/TKLC/home/rssh/tmp/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 the following: "'/tmp/bp.XXXX/"

Navigate to **NetBackup Configuration -> Install NetBackup Client**

![Install NetBackup Client dialog box](image)

Verify list entries indicate **OK** for NetBackup client software installation

Select **Exit** to return to NetBackup Configuration menu
## Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

<table>
<thead>
<tr>
<th>Step</th>
<th>Application Server iLO:</th>
<th>Task Description</th>
<th>Navigation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Verify NetBackup Client software installation on the application server.</td>
<td>Navigate to NetBackup Configuration -&gt; Verify NetBackup Client Installation.</td>
<td><img src="image" alt="Verify NetBackup Client Installation" /></td>
</tr>
<tr>
<td></td>
<td>Verify list entries indicate OK for NetBackup Client software installation. Select Exit to return to NetBackup Configuration menu.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Disable NetBackup Client software transfer to the application server.</td>
<td>Navigate to NetBackup Configuration -&gt; Remove File Transfer User</td>
<td><img src="image" alt="Remove File Transfer User" /></td>
</tr>
<tr>
<td></td>
<td>Select Yes to remove the NetBackup file transfer user from the application server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Exit platform configuration utility (platcfg)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

<table>
<thead>
<tr>
<th>11</th>
<th>Application server iLO: Verify Server bp.conf file</th>
<th>Verify that the server has been added to the <code>/usr/openv/netbackup/bp.conf</code> file: Issue the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><code>$ sudo cat /usr/openv/netbackup/bp.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLIENT_NAME = 10.240.34.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SERVER = NB71server</td>
</tr>
</tbody>
</table>
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

Application server iLO:
Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.

Note: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup "/usr/openv/netbackup/bp.conf" file, identified by the SERVER configuration parameter.

The NetBackup server hostname and IP address must be added to the application server's host's file. List NetBackup servers hostname:

```bash
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```bash
$ sudo su - platcfg
```

Navigate to Network Configuration -> Modify Hosts File

Select Edit, the Host Action Menu will be displayed.

Select Add Host, and enter the appropriate data.

Select OK, confirm the host alias add, and exit Platform Configuration Utility.
<table>
<thead>
<tr>
<th>13</th>
<th><strong>Application server iLO:</strong> Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Copy the notify scripts from appropriate path on application server for given application:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo ln -s &lt;path&gt;/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify</code></td>
</tr>
<tr>
<td></td>
<td><code>$ sudo ln -s &lt;path&gt;/bpend_notify /usr/openv/netbackup/bin/bpend_notify</code></td>
</tr>
<tr>
<td></td>
<td>An example of <code>&lt;path&gt;</code> is “/usr/TKLC/appworks/sbin”</td>
</tr>
</tbody>
</table>
## Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application server iLO: Login and launch the integrated remote console. SSH to the application Server (PMAC or NOAM) as <em>admusr</em> using the management network for the PMAC or XMI network for the NOAM.</td>
</tr>
<tr>
<td>2</td>
<td>Application server iLO: Enable nbAutoInstall Execute the following command: <code>$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable</code></td>
</tr>
</tbody>
</table>
| 3      | Application server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them. Execute the following commands ``` $ 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 ```  
  *Note: An example of <path> is “/usr/TKLC/plat/sbin”* |
### Application NetBackup Client Installation (NBAUTOINSTALL)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Application server iLO: Verify NetBackup configuration file</td>
<td>Open <code>/usr/openv/netbackup/bp.conf</code> and make sure it points to the NetBackup Server using the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo vi /usr/openv/netbackup/bp.conf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SERVER = nb75server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLIENT_NAME = 10.240.10.185</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONNECT_OPTIONS = localhost 1 0 2</td>
</tr>
</tbody>
</table>

**Note:** Verify that the above server name matches the NetBackup Server, and verify that the CLIENT_NAME matches the hostname or IP of the local client machine, if they do not, update them as necessary.

Edit `/etc/hosts` using the following command and add the NetBackup server:

$ sudo vi /etc/hosts

e.g.: 192.168.176.45    nb75server

**Note:** The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly. At any time, the customer may now push and install a new version of Netbackup Client.
### Appendix I.3: Create NetBackup Client Config File

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

#### Appendix I.3. Create NetBackup Client Config File

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| 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 the following naming conventions: `NB$ver.conf`  
Where $ver is the client version number with the periods removed. For the 7.5 client the value of $ver would be 75 and the full path to the file would be: `/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. |
| 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 the following is applicable:  
**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: Open Ports for NetBackup Client Software

This procedure will use iptables and ip6tables (if applicable) to open the applicable ports for the NetBackup client to communicate to the NetBackup Server.

## Appendix I.4. Open ports for NetBackup Client Software

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Active NOAM Server:</strong> Establish an SSH session to the active NOAM server. Login as <em>admusr</em>.</td>
<td>If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>
| 2    | **Active NOAM Server:** Change directories to `/usr/TKLC/plat/etc/iptables`  
Change directories to `/usr/TKLC/plat/etc/iptables`  
Using `vi`, create a file named `60netbackup.ipt`  
Using `vi`, create a file named `60netbackup.ipt`  
Insert the following contents into the file:  
# NetBackup ports.  
# *filter  
-A INPUT -m state --state NEW -m tcp --tcp --dport 1556 -j ACCEPT  
-A INPUT -m state --state NEW -m tcp --tcp --dport 13724 -j ACCEPT  
-A INPUT -m state --state NEW -m tcp --tcp --dport 13782 -j ACCEPT  
Now save and close the file using `:wq` |
| 3    | **Standby NOAM:** Repeat Steps 1-2 for the standby NOAM to open ports for NetBackup client software. |

Note: If system servers are to use IPv6 networks for NetBackup client-to-server communication, then repeat this procedure to create a file named `60netbackup.ip6t`, with the same contents as shown above, in the directory `/usr/TKLC/plat/etc/ip6tables`. 

---

288 | Page  
E 5 5 2 3 5 - 0 3
Appendix I.4. Open ports for NetBackup Client Software

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>Active SOAM:</strong> Open Ports for NetBackup Client Software. Repeat <strong>Steps 1-2</strong> for the active SOAM to open ports for NetBackup client software.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Standby SOAM:</strong> Open Ports for NetBackup Client Software. Repeat <strong>Steps 1-2</strong> for the standby SOAM to open ports for NetBackup client software.</td>
</tr>
</tbody>
</table>

Appendix I.5: Configure PMAC Application NetBackup Virtual Disk

Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>PMAC GUI:</strong> Login. Open web browser and navigate to the PMAC GUI, Login as <strong>PMACadmin</strong> user: <code>https://&lt;pmac_network_ip&gt;</code></td>
</tr>
</tbody>
</table>
Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk

2 PMAC GUI: Create netBackup Virtual Disk

Navigate to Main Menu -> VM Management

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

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

Confirm the PMAC application guest edit.

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

Click OK to continue.

3 PMAC GUI: Verify netBackup Virtual Disk

Confirm the Edit VM Guest task has completed successfully.

Navigate to Main Menu -> Task Monitoring

Confirm that the guest edit task has completed successfully.
Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk

<table>
<thead>
<tr>
<th>PMAC GUI:</th>
<th>Navigate to Main Menu -&gt; Task Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify &quot;In-Progress&quot; tasks</td>
<td></td>
</tr>
</tbody>
</table>

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

**Note:** If desired, you can delete all of the Complete and Failed tasks using the “Delete Completed” and “Delete Failed” buttons. This will leave only the in-progress tasks.
## Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk

### Management Server TVOE iLO/iLOM:
SSH into the Management Server

Using an SSH client such as putty, ssh to the TVOE host as `admusr`.

Login using `virsh`, and wait until you see the login prompt:

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

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>myTPD</td>
<td>running</td>
</tr>
<tr>
<td>2</td>
<td>PM&amp;C</td>
<td>running</td>
</tr>
</tbody>
</table>

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

```
Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64
on an x86_64
PM&Cdev7 login:
```

### PMAC:
Shutdown the PMAC Guest

Assuming no in-progress tasks exists, it is safe to shutdown the PMAC guest. Execute the following 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!

```
[admusr@pmac ~]$
```

Eventually the virsh console session is closed and you are returned to the TVOE host command prompt:

```
Halting system...
Power down.
[admusr@tvoe ~]$
```
Appendix I.5. Configure the PMAC Application Guest NetBackup Virtual Disk

<table>
<thead>
<tr>
<th>Management Server TVOE iLO/iLOM: Verify PMAC Guest is shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the TVOE host command prompt execute the following command:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>[admusr@tvoe ~]$</td>
</tr>
<tr>
<td>This should show the guest state as “shut off”. You will want to be sure all guests are in the shut off state as well.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management Server TVOE iLO/iLOM: Start PMAC Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue the following command to start the PMAC guest:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
## Appendix J: List of Frequently used Time Zones

Table 4. Time Zones

<table>
<thead>
<tr>
<th>Time Zone Value</th>
<th>Description</th>
<th>Universal Time Code (UTC) Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>America/New_York</td>
<td>Eastern Time</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Chicago</td>
<td>Central Time</td>
<td>UTC-06</td>
</tr>
<tr>
<td>America/Denver</td>
<td>Mountain Time</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Phoenix</td>
<td>Mountain Standard Time - Arizona</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Los_Angeles</td>
<td>Pacific Time</td>
<td>UTC-08</td>
</tr>
<tr>
<td>America/Anchorage</td>
<td>Alaska Time</td>
<td>UTC-09</td>
</tr>
<tr>
<td>Pacific/Honolulu</td>
<td>Hawaii</td>
<td>UTC-10</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>America/Mexico_City</td>
<td>Central Time - most locations</td>
<td>UTC-06</td>
</tr>
<tr>
<td>Africa/Monrovia</td>
<td></td>
<td>UTC+00</td>
</tr>
<tr>
<td>Asia/Tokyo</td>
<td></td>
<td>UTC+09</td>
</tr>
<tr>
<td>America/Jamaica</td>
<td></td>
<td>UTC-05</td>
</tr>
<tr>
<td>Europe/Rome</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Asia/Hong_Kong</td>
<td></td>
<td>UTC+08</td>
</tr>
<tr>
<td>Pacific/Guam</td>
<td></td>
<td>UTC+10</td>
</tr>
<tr>
<td>Europe/Athens</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>Europe/London</td>
<td></td>
<td>UTC+00</td>
</tr>
<tr>
<td>Europe/Paris</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Madrid</td>
<td>mainland</td>
<td>UTC+01</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>Europe/Copenhagen</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Berlin</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Prague</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>America/Vancouver</td>
<td>Pacific Time - west British Columbia</td>
<td>UTC-08</td>
</tr>
<tr>
<td>America/Edmonton</td>
<td>Mountain Time - Alberta, east British Columbia &amp; westSaskatchewan</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Toronto</td>
<td>Eastern Time - Ontario - most locations</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Montreal</td>
<td>Eastern Time - Quebec - most locations</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Sao_Paulo</td>
<td>South &amp; Southeast Brazil</td>
<td>UTC-03</td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Australia/Perth</td>
<td>Western Australia - most locations</td>
<td>UTC+08</td>
</tr>
<tr>
<td>Australia/Sydney</td>
<td>New South Wales - most locations</td>
<td>UTC+10</td>
</tr>
<tr>
<td>Asia/Seoul</td>
<td></td>
<td>UTC+09</td>
</tr>
<tr>
<td>Africa/Lagos</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Warsaw</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>America/Puerto_Rico</td>
<td></td>
<td>UTC-04</td>
</tr>
<tr>
<td>Europe/Moscow</td>
<td>Moscow+00 - west Russia</td>
<td>UTC+04</td>
</tr>
<tr>
<td>Asia/Manila</td>
<td></td>
<td>UTC+08</td>
</tr>
</tbody>
</table>
## Appendix K: Upgrade Cisco 4948 PROM

### Appendix K.1. Upgrade Cisco 4948 PROM

<table>
<thead>
<tr>
<th>STE #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Virtual PMAC:</strong> Verify PROM image is on the system</td>
<td>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>
|       | Determine if the PROM image for the 4948E-F is on the system. | Execute the following 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 HP Solutions Firmware Upgrade Pack Release Notes [1] |
| 2     | **Virtual PMAC:** Attach to switch Console | Connect serially to the switch by issuing the following command as admusr on the server: 

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
```

```
switch1A_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ee?' for help]
Press Enter
```

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# 
```
### Appendix K.1. Upgrade Cisco 4948 PROM

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3    | Configure ports on the switch | Configure ports on the 4948E-F switch. To ensure connectivity, ping the management server's management vlan ip `<pmac_mgmt_ip_address>` address from the switch. Execute the following commands:  

```
Switch# conf t  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# spanning-tree portfast trunk  
Switch(config-if)# end  
Switch# write memory  
```

Now issue ping command:

```
Switch# ping <pmac_mgmtVLAN_ip_address>
```

If ping is not successful, double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Appendix U: My Oracle Support (MOS).

| 4    | Upgrade PROM | To upgrade PROM, execute the following commands:  
```
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#  
```

Reload the switch, execute the following commands:

```
Switch# reload  
System configuration has been modified. Save? [yes/no]: no  
Proceed with reload? [confirm] [Enter]  
=== Boot messages removed ===  
```

**Note:** Type `[Control-C]` when "*Type control-C to prevent autobooting*" is displayed on the screen.
Appendix K.1. Upgrade Cisco 4948 PROM

<table>
<thead>
<tr>
<th></th>
<th><strong>4948E-F:</strong></th>
<th>Initiates the PROM upgrade by executing the following commands:</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td></td>
<td><strong>Initiate PROM Upgrade</strong></td>
</tr>
<tr>
<td></td>
<td>rommon 1 &gt; boot</td>
<td>bootflash:&lt;PROM_image_file&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*** PROM upgrade messages removed ***</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System will reset itself and reboot within few seconds....</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>4948E-F:</strong></th>
<th>The switch will reboot when the firmware upgrade completes. Allow it to boot up. Wait for the following line to be printed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td><strong>Verify PROM Upgrade</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Press RETURN to get started! Would you like to terminate autoinstall? [yes]: [Enter]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switch&gt; show version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ROM: 12.2(31r)SGA1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System returned to ROM by reload</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Review the output and look for the ROM version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong ROM version, contact Appendix U: My Oracle Support (MOS).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>4948E-F:</strong></th>
<th>Reset switch to factory defaults. Execute the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><strong>Reset Switch Factory Defaults</strong></td>
<td><strong>Switch# write erase</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Switch# reload</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Wait until the switch reloads, then exit from console, enter &lt;ctrl-e&gt;&lt;c&gt;&lt;c&gt;&lt;c&gt; and you will be returned to the server prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> There might be messages from the switch, if asked to confirm, press enter. If asked yes or no, type in 'no' and press enter.</td>
</tr>
</tbody>
</table>

Appendix L: Sample Network Element

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

It is expected that the maintainer/creator of this file has networking knowledge of this product and the customer site at which it is being installed. This network element XML file is used for DSR deployments using Cisco 4948 switches and HP Rack Mount servers. The following is an example of a Network Element XML file.

The SOAM Network Element XML file needs to have same network names for the networks as the NOAMP Network Element XML file has. It is easy to accidentally create different network names for NOAMP and SOAM Network Element, and then the mapping of services to networks will not be possible.
Figure 4. Example Network Element XML File

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

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

## Appendix M.1. Accessing the NOAM GUI using SSH Tunneling with Putty

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | Log in to PMAC Server using PuTTY  
Launch the PuTTY application from your station and open a session to the PMAC’s management address. Login as `admusr` |
2. **Create SSH Tunnel through the PMAC in PuTTY**

Click the icon in the upper left hand corner of the PuTTY window to bring down the main menu.

Select **Change Settings**

Select **Connections -> SSH -> Tunnels**

![PuTTY Tunnel Configuration](image)

1. Verify that the **Local** and **Auto** buttons are selected. Leave other fields blank
2. In **Source Port**, enter **443**
3. In **Destination**, enter `<NOAM-Control-IP>:443`
4. Click **Add**

![PuTTY Forwarded Ports](image)

You should now see a display similar to the following in the text box at the center of this dialog.

5. Click **Apply**
6. **Connect** to the PMAC, and login as **admusr**
Appendix M.1. Accessing the NOAM GUI using SSH Tunneling with Putty

<table>
<thead>
<tr>
<th></th>
<th>Use Local Web Browser to Connect to GUI</th>
<th>Using your web browser, navigate to the following URL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td><img src="https://localhost/" alt="Image" /></td>
</tr>
</tbody>
</table>

You should arrive at the login screen for the NOAM GUI.

**Note:** If using windows 7 and a blank screen is displayed, enable **Compatibility Mode** in IE, or use a different browser (Firefox or Chrome)

---

Appendix N: Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

Appendix N.1. Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

<table>
<thead>
<tr>
<th>S T E P #</th>
<th>Note: This procedure assumes that the NOAM server you wish to create a tunnel to has been IPM’d with the DSR application ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> This procedure assumes that you have exchanged SSH keys between the PMAC and the first NOAM server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This procedure assumes that you have obtained the control network IP address for the first NOAM server. You can get this from the PMAC GUI’s Software Inventory screen. That variable will be referred to as &lt;NOAM-Control-IP&gt; in these instructions.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is the recommended tunneling method if you are using Windows 7.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>1</th>
<th>If Needed, Download and Install OpenSSH for Windows</th>
<th>Download OpenSSH for Windows from <a href="#">here</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Extract the installer from the ZIP file, then run the installer. <strong>openssh</strong> is now installed on your PC.</td>
</tr>
</tbody>
</table>
## Appendix N.1. Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Create SSH Tunnel Through the PMAC</strong></td>
<td>Open up a Command Prompt shell</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Within the command shell, enter the following to create the SSH tunnel to the 1st NO, through the PMAC:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&gt; ssh -L 443:&lt;1st_NO_Control_IP_Address&gt;:443 admusr@&lt;PMAC_Management_IP_Address&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Answer <strong>Yes</strong> if it asks if you want to continue connecting)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="SSH Tunnel Establishment" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The tunnel to the 1st NOAM is now established.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Use Local Web Browser to Connect to GUI</strong></td>
<td>Using your web browser, navigate to the following URL:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>https://localhost/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Web Browser Connection" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You should arrive at the login screen for the NOAM GUI.</td>
</tr>
</tbody>
</table>
Appendix O: IDIH Fast Deployment Configuration

The fdc.cfg file contains 8 sections. The following is a list of those sections with a short description:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Images</td>
<td>A list of the TVOE, TPD, and iDIH application versions.</td>
</tr>
<tr>
<td>TVOE RMS</td>
<td>Includes Hardware Type and ILO address of the Rack Mount Server.</td>
</tr>
<tr>
<td>Type</td>
<td>Management or Standalone</td>
</tr>
<tr>
<td>TVOE Configuration</td>
<td>Contains all ip addresses, hostname and network devices for the TVOE host.</td>
</tr>
<tr>
<td>Guest Configurations</td>
<td>The guest sections contain network and hostname configuration for the Oracle,</td>
</tr>
<tr>
<td>(3)</td>
<td>Mediation and Application guests.</td>
</tr>
</tbody>
</table>

**Software Images**

Be sure to update the software images section based on software versions you intend to install. The following table outlines typical installation failures caused by incorrect software versions. Use the “fdconfig dumpsteps –file=” command to produce output of a Fast Deployment Session.

<table>
<thead>
<tr>
<th>Software Image</th>
<th>Element</th>
<th>Command Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>TVOE ISO</td>
<td>mgmtsrvrtvoe</td>
<td>IPM Server</td>
</tr>
<tr>
<td>TPD ISO</td>
<td>Oracle,tpd</td>
<td>IPM Server</td>
</tr>
<tr>
<td></td>
<td>Mediation,tpd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application,tpd</td>
<td></td>
</tr>
<tr>
<td>iDIH Mediation ISO</td>
<td>Mgmtsrvrtvoe,configExt</td>
<td>Transfer File</td>
</tr>
<tr>
<td>iDIH Oracle ISO</td>
<td>Oracle,ora</td>
<td>Upgrade Server</td>
</tr>
<tr>
<td>iDIH Mediation ISO</td>
<td>Mediation,med</td>
<td></td>
</tr>
<tr>
<td>iDIH Application ISO</td>
<td>Application,app</td>
<td></td>
</tr>
</tbody>
</table>

**TVOE RMS**

The TVOE RMS section contains the ILO ip address and Hardware profile. If the ILO IP address is incorrect the PMAC will not be able to discover the Rack Mount Server, server discovery must occur before the installation can begin.
TYPE

If your IDIH system is to be collocated with a PMAC on the same TVOE host make sure “Type=Management” is not commented out. It will setup a management network instead of an xmi network and it will remove the software stanza inside of the TVOE server stanza. If you are setting up a standalone IDIH then comment out “Type=Management” which will setup an xmi bridge.

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.

Below is FDC configuration template included on the mediation ISO:
# Software Images
TvoeIso="TVOE-3.0.0.0.0_86.20.0-x86_64"
TpdIso="TPD.install-7.0.1.0.0_86.20.0-OracleLinux6.6-x86_64"
OraIso="oracle-7.1.0.0.0_71.14.0-x86_64"
MedIso="mediation-7.1.0.0.0_71.14.0-x86_64"
AppIso="apps-7.1.0.0.0_71.14.0-x86_64"

# Tvoe Blade OA IP and Bay uncomment if this server is blade #EncId="1401"
#Oa1="10.250.51.197"
#Oa2="10.250.51.198"
#Bay="15F"
#Hw="ProLiantBL460cGen8"
#Hw="ProLiantBL460cGen6"

# Tvoe RMS Out of Band Management IP and Hw # Comment these lines if server is blade OobIp="10.250.34.24"
Hw="ProLiantDL380pGen8"
#Hw="SUNNETRA4270M3"

# Comment this line out if server is standalone Type="Management"

# Tvoe Config
#
TvoeName="thunderbolt"
TvoeIp="10.250.51.8"
Mask="255.255.255.0"
Gateway="10.250.51.1"
TvoeNtp="2607:f0d0:1002:51::4/64"
TvoeIp6Gw="fe80::0"
# xmlbond
XmiDev="bond0"
XmiEth="eth01,eth02"
# imibond
ImiDev="bond1"
ImiEth="eth03,eth04"
# xml/management
MgmtInt="bond0.1"
MgmtIntType="Vlan"
MgmtIntVlanid="3"
# imi
ImiInt="bond1.5"
ImiIntType="Vlan"
ImiIntVlanid="5"

# Oracle Guest Config
OraName="thunderbolt-ora"
OraIp="10.250.51.6"
OraMask=$Mask
OraGw=$Gateway
OraIp6="2607:f0d0:1002:51::5/64"
OraIp6Gw="STvoeIp6Gw"

# Mediation Guest Config
MedName="thunderbolt-med"
MedIp="10.250.51.10"
MedMask=$Mask
MedGw=$Gateway
MedIp6="2607:f0d0:1002:51::6/64"
MedIp6Gw="STvoeIp6Gw"

# Application Guest Config
AppName="thunderbolt-app"
AppIp="10.250.51.11"
AppMask=$Mask
AppGw=$Gateway
AppIp6="2607:f0d0:1002:51::7/64"
AppIp6Gw="STvoeIp6Gw"
Appendix P: DR-NOAM Feature Activation (DSR 6.0/7.0)

### Appendix P.1. DR-NOAM Feature Activation (DSR 6.0/7.0)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>DR-NOAM: Feature Activation</th>
<th>If the DR NOAM was configured in <strong>Procedure 25</strong> AND MAP-Diameter IWF is activated, SSH to the active DR-NOAM, login as <strong>admusr</strong>. Execute the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>$ cd /usr/TKLC/dsr/prod/maint/loaders/activate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ ./load.mapinterworkingActivateAsourced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Repeat this step for the standby DR-NOAM.</td>
</tr>
</tbody>
</table>

This procedure will activate optional features for DR-NOAM servers.

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

If this procedure fails, contact **Appendix U: My Oracle Support (MOS)**, and ask for assistance.
## Appendix Q: Creating a Bootable USB Drive on Linux

### Appendix Q.2. Creating a Bootable USB Drive on Linux

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | **Insert USB Media**<br>Insert the USB Media into the USB Port. It should automatically be mounted under `/media`<br>Obtain the path of the USB drive by running:<br>
```bash
$ ls /media
```

The output should be similar to the following:<br>`sdb1`

Note down the path without the partition number (in this case, it would be `/dev/sdb`)<br><br>**Linux Machine**<br>Obtain the TVOE `.usb` file and copy it onto the local linux machine (e.g. under `/var/TKL`/upgrade)<br><br>**Copy the `.USB file onto the USB drive**<br>Use the `dd` command to copy the `.usb` file onto the USB drive<br><br>**Note:** Make sure you **do not** use the partition number when copying the file<br>
```bash
$ sudo dd if=<path_to_usb_image> of=/dev/sdb bs=4M oflag=direct
```
Appendix R: IDIH External Drive Removal

This procedure should only be run if the user intends to do a fresh installation on an existing IDIH.

Appendix R.3. IDIH External Drive Removal

This procedure will destroy all of the data in the Oracle Database.

Warning: Do not perform this procedure on an IDIH system unless you intend to do a fresh TVOE installation.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PMAC GUI: Login</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open web browser and enter: https://&lt;PMAC_Mgmt_Network_IP&gt;</td>
<td>Login as pmacadmin user:</td>
</tr>
</tbody>
</table>

[Oracle System Login]

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 6.0, 7.0, or 8.0 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, 2015, Oracle and/or its affiliates. All rights reserved.
### Appendix R.3. IDIH External Drive Removal

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>PMAC GUI:</strong> Delete VMs if Needed</td>
<td>Before a re-installation can be performed, the IDIH VMs must be removed first. Navigate to Main Menu -&gt; VM Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select each of the IDIH VMs and select the <strong>Delete</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>3</td>
<td><strong>IDIH TVOE HOST:</strong> Login</td>
<td>Establish an SSH session to the TVOE host, login as <strong>admusr</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>IDIH TVOE HOST:</strong> Verify External Drive Exists</td>
<td>Execute the following command to verify the external drive exists: HP DL380:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo hpssaclic ctrl slot=2 Id all show</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Sun Netra X3-2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>`$ sudo megacli -ldinfo -11 -a0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following information should be displayed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="table" alt="Table" /></td>
</tr>
</tbody>
</table>
Appendix R.3. IDIH External Drive Removal

<table>
<thead>
<tr>
<th>5</th>
<th>IDIH TVOE HOST:</th>
<th>Remove the External Drive and Volume Group</th>
</tr>
</thead>
</table>

Execute the following command to remote the external drive and volume group:

HP DL380:

```
$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2
```

Oracle Sun Netra X3-2:

```
$ sudo /usr/TKLC/plat/sbin/storageClean pool \  
  --poolName=external3 --level=pv

$ sudo /usr/TKLC/plat/sbin/storageClean lvm \  
  --vgName=external3 --level=vg

$ sudo /usr/TKLC/plat/sbin/storageClean pool \  
  --poolName=external2 --level=pv

$ sudo /usr/TKLC/plat/sbin/storageClean lvm \  
  --vgName=external2 --level=vg

$ sudo /usr/TKLC/plat/sbin/storageClean pool \  
  --poolName=external1 --level=pv

$ sudo /usr/TKLC/plat/sbin/storageClean lvm \  
  --vgName=external1 --level=vg

$ sudo megacli -cfglddel -l3 -a0
$ sudo megacli -cfglddel -l2 -a0
$ sudo megacli -cfglddel -l1 -a0
```
Appendix S: HP Gen9 Server Hard Disk Drive Locations for IDIH

The following figure shows hard disk drive placement for the HP Gen9 Rack mount servers:

Figure 5: HP Gen9 Server Hard Disk Drive Location for IDIH

Install the first two 900GB HDD for the OS in HDD Bay3 Slots 1 and 2.

After installing the 900GB HDD in Bay 3 slots 1 and 2 for the OS Install all the remaining 900GB HDD in BAY 2 starting with slot 1 through slot 4.
Appendix T: Disable/Enable DTLS

DSR 7.1 ONLY
Oracle is introducing SCTP Datagram Transport Layer Security (DTLS) in DSR 7.1 by enabling SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers installing DSR 7.1 should prepare clients before the DSR connections are established after installation. This will ensure the DSR to Client SCTP connection will establish with SCTP AUTH extensions enabled. See RFC 6083. If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices WILL 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 the following procedure to Disable DTLS:

Appendix T.1 Disable DTLS (DSR 7.1 Only)

| STEP # | MP Server: Login | Execute the following command to disable the SCTP Auth Flag:
|        |                | $ sudo sysctl -w net.sctp.auth_enable=0
|        | Disable SCTP Auth Flag | Note: It is recommended to copy and paste directly as listed below to avoid errors
|        | Verify SCTP Auth Flag is Disabled | Note: It is recommended to copy and paste directly as listed below to avoid errors
|        | Make SCTP Auth Flag changes Persistent | Note: It is recommended to copy and paste directly as listed below to avoid errors

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS), and ask for assistance.
### Appendix T.1 Disable DTLS (DSR 7.1 Only)

<table>
<thead>
<tr>
<th>Step</th>
<th>MP Server:</th>
<th>Task</th>
</tr>
</thead>
</table>
| 5    | Verify Auth Flag is Disabled | Execute the following command to verify the SCTP Auth Flag has been disabled:  
**Note:** It is recommended to copy and paste directly as listed below to avoid errors  
$ sudo grep net.sctp.auth_enable /etc/dpi_init  
The following output should be displayed:  
`sysctl -w net.sctp.auth_enable=0` |
| 6    | Additional MP Servers: Repeat | Repeat for all remaining MP servers. |
If DTLS connections are to be configured AFTER DTLS has been disabled as performed in Procedure T.1, then the procedure below for Enabling DTLS needs to be followed before DTLS connections are configured.

**Appendix T.2 Enable DTLS (DSR 7.1 Only)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>MP Server:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Login</strong></td>
<td>Establish an SSH session to the MP server. Login as admusr.</td>
</tr>
</tbody>
</table>
| 2      | **Enable SCTP Auth Flag** | Execute the following command to Enable the SCTP Auth Flag:  
  
  **Note:** It is recommended to copy and paste directly as listed below to avoid errors  
  
  ```bash
  $ sudo sysctl -w net.sctp.auth_enable=1
  ``` |
| 3      | **Verify SCTP Auth Flag changes** | Execute the following command to verify the SCTP Auth Flag changes:  
  
  **Note:** It is recommended to copy and paste directly as listed below to avoid errors  
  
  ```bash
  $ sudo sysctl -a | grep net.sctp.auth_enable  
  ```  
  The following output is expected:  
  
  ```bash
  net.sctp.auth_enable = 1
  ``` |
| 4      | **Make SCTP Auth Flag Changes persistent** | Execute the following command to make the SCTP Auth Flag changes persistent:  
  
  **Note:** It is recommended to copy and paste directly as listed below to avoid errors  
  
  ```bash
  $ sudo sed -i 's/sysctl -w net.sctp.auth_enable=0/sysctl -w net.sctp.auth_enable=1/g' /etc/dpi_init
  ``` |
| 5      | **Verify Auth Flag changes** | Execute the following command to verify the SCTP Auth Flag has been disabled:  
  
  **Note:** It is recommended to copy and paste directly as listed below to avoid errors  
  
  ```bash
  $ sudo grep net.sctp.auth_enable /etc/dpi_init  
  ```  
  The following output should be displayed:  
  
  ```bash
  sysctl -w net.sctp.auth_enable=1
  ``` |
Appendix T.2 Enable DTLS (DSR 7.1 Only)

<table>
<thead>
<tr>
<th></th>
<th>Additional MP Servers:</th>
<th>Repeat for all remaining MP servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Repeat</td>
<td></td>
</tr>
</tbody>
</table>

Appendix U: My Oracle Support (MOS)

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

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

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1) For the first set of menu options, select 2, “New Service Request”. You will hear another set of menu options.
2) In this set of menu options, select 3, “Hardware, Networking and Solaris Operating System Support”. A third set of menu options begins.
3) In the third set of options, select 2, “Non-technical issue”. Then you will be connected to a live agent who can assist you with MOS registration and provide Support. Identifiers. Simply mention you are a Tekelec Customer new to MOS.