

Oracle® Communications

Diameter Signaling Router

C-Class Software Installation and Configuration
Procedure 2/2

Release 8.0

E76181-02

June 2017

ORACLE®

DSR 8.0 C-Class Software Installation and Configuration 2/2

Oracle © Communication Diameter Signaling Router DSR C-Class Software Installation and Configuration Procedure 2/2

Copyright © 2017 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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



CAUTION: Use only the Upgrade procedure included in the Upgrade Kit. Before upgrading any system, please access My Oracle Support (MOS) (<https://support.oracle.com>) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

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

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

Note: This document represents the 2nd part of the DSR Installation Process. Prior to executing this document, make sure that the 1st part was fully executed:

- **DSR Hardware and Software Installation:** Use document [7] DSR Hardware and Software Installation Part 1, E76180.

Table of Contents

1. Introduction	7
1.1 References	7
1.2 Acronyms.....	7
1.3 Terminology.....	8
2. General Description	10
3. Installation Overview	11
3.1 Required Materials	11
3.2 Installation Strategy.....	11
3.3 SNMP Configuration.....	15
3.4 Optional Features	15
4. Software Installation Procedure	16
4.1 Install and Configure NOAM Servers	17
4.1.1 Load Application and TPD ISO onto the PMAC Server	17
4.1.2 Execute DSR Fast Deployment for NOAMs	20
4.1.3 Configure NOAMs.....	24
4.1.4 Install NetBackup Client (Optional).....	41
4.2 Install and Configure DR-NOAM Servers (Optional).....	42
4.2.1 Execute DSR Fast Deployment for DR-NOAMs.....	42
4.2.2 Pair DR-NOAMs.....	50
4.2.3 Install NetBackup Client (Optional).....	53
4.3 Install and Configure SOAM Servers	54
4.3.1 Configure SOAM TVOE Server Blades	54
4.3.2 Configure SOAMs.....	72
4.4 Configure MP Servers	85
4.4.1 Configure MP Blade Servers	85
4.4.2 Configure Signaling Network Routes.....	113
4.4.3 Configure DSCP (Optional)	118
4.4.4 Configure IP Front End Servers (Optional).....	121
4.5 SNMP Configuration.....	126
4.6 IDIH Installation and Configuration (Optional).....	134
4.6.1 IDIH Installation.....	135
4.6.2 Post IDIH Installation Configuration.....	140
4.7 Post-Install Activities.....	158
4.7.1 Activate Optional Features	158
4.7.2 Configure ComAgent Connections (DSR + SDS)	159
4.7.3 Shared Secret Encryption Key Revocation (RADIUS ONLY)	165
4.7.4 Backup TVOE Configuration.....	165
4.7.5 Backup PMAC Application.....	167
4.7.6 Backup NOAM Database.....	169
4.7.7 Backup SOAM Database.....	172
4.7.8 Enable/Disable DTLS (SCTP Diameter Connections Only)	175

Appendix A: Sample Network Element and Hardware Profiles	175
Appendix B: Configure for TVOE iLO Access	178
Appendix C: TVOE iLO Access	181
Appendix D: TVOE iLO4 GUI Access	184
Appendix E: Change the TVOE iLO Address	185
Appendix F: PMAC/NOAM/SOAM Console iLO Access	188
Appendix G: List of Frequently Used Time Zones	189
Appendix H: Application NetBackup Client Installation Procedures	191
Appendix H.1: NETBACKUP Client Installation Using PLATCFG.....	191
Appendix H.2: NetBackup Client Install/Upgrade with NBAutoInstall.....	198
Appendix H.3: Create NetBackup Client Configuration File	200
Appendix H.4: Open Ports for NetBackup Client Software	200
Appendix I: IDIH Fast Deployment Configuration	201
Appendix J: IDIH External Drive Removal	205
Appendix K: DSR Fast Deployment Configuration	209
Appendix L: Growth/De-Growth	211
Appendix L.1: Growth	211
Appendix L.2: De-Growth	220
Appendix O: Restore SNMP Configuration to SNMPv3 (Optional)	237
Appendix P: My Oracle Support (MOS)	238

List of Tables

Table 1. Acronyms	7
Table 2. Optional Features.....	15
Table 3. List of Selected Time Zone Values	189

List of Figures

Figure 1. Example of an instruction that indicates the server to which it applies	8
Figure 2. Example of Initial Application Installation Path	11
Figure 3. DSR Installation: High Level Sequence.....	13
Figure 4. DSR Single Site Installation Procedure Map	14
Figure 5. Example Network Element XML File	176
Figure 6. Example Server Hardware Profile XML-HP c-Class Blade	177
Figure 7. Example Server Hardware Profile XML- Virtual Guest on TVOE.....	178

List of Procedures

Procedure 1.	Load Application and TPD ISO onto PMAC Server.....	17
Procedure 2.	Configure NOAM Servers	20
Procedure 3.	Configure the First NOAM NE and Server.....	24
Procedure 4.	Configure the NOAM Server Group.....	30
Procedure 5.	Configure the Second NOAM Server.....	34
Procedure 6.	Complete NOAM Server Group Configuration.....	38
Procedure 7.	Install NetBackup Client (Optional).....	41
Procedure 8.	NOAM Configuration for DR Site (Optional)	42
Procedure 9.	Pairing for DR-NOAM site (Optional).....	50
Procedure 10.	Install NetBackup Client (Optional).....	53
Procedure 11.	Configure SOAM TVOE Server Blades	54
Procedure 12.	Create SOAM Guest VMs	63
Procedure 13.	IPM Blades and VMs.....	67
Procedure 14.	Install the Application Software	69
Procedure 15.	Configure SOAM NE	72
Procedure 16.	Configure the SOAM Servers	74
Procedure 17.	Configure the SOAM Server Group	79
Procedure 18.	Activate PCA (PCA Only).....	84
Procedure 19.	Activate DCA (DCA Only)	84
Procedure 20.	Configure MP Blade Servers	85
Procedure 21.	Configure Places and Assign MP Servers to Places (PCA/DCA Only).....	99
Procedure 22.	Configure the MP Server Group(s) and Profile(s).....	102
Procedure 23.	Add VIP for Signaling Networks (Active/Standby Configurations Only)	111
Procedure 24.	Configure the Signaling Network Routes.....	113
Procedure 25.	Configure DSCP Values for Outgoing Traffic	118
Procedure 26.	Procedure 26: IP Front End (IPFE) Configuration	121
Procedure 27.	Configure SNMP Trap Receiver(s).....	126
Procedure 28.	IDIH Configuration.....	135
Procedure 29.	Configure DSR Reference Data Synchronization for IDIH	140
Procedure 30.	IDIH Configuration: Configuring the SSO Domain (Optional).....	143
Procedure 31.	IDIH Configuration: Configure IDIH in the DSR	149
Procedure 32.	IDIH Configuration: Configure Mail Server (Optional).....	152
Procedure 33.	IDIH Configuration: Configure SNMP Management Server (Optional).....	154
Procedure 34.	IDIH Configuration: Change Network Interface (Optional)	155
Procedure 35.	IDIH Configuration: Backup the Upgrade and Disaster Recovery FDC File (Optional).	156
Procedure 36.	IDIH Configuration: Change Alarm Ignore List (Optional)	157

Procedure 37.	Activate Optional Features.....	158
Procedure 38.	Configure ComAgent Connections (DSR + SDS).....	159
Procedure 39.	Shared Secret Encryption Key Revocation (RADIUS Only)	165
Procedure 40.	Backup TVOE Configuration.....	165
Procedure 41.	Backup PMAC Application	167
Procedure 42.	NOAM Database Backup.....	169
Procedure 43.	SOAM Database Backup	172
Procedure 44.	Enable/Disable DTLS (SCTP Diameter Connections Only)	175
Procedure 45.	Connect to the TVOE iLO	178
Procedure 46.	Access the TVOE iLO	181
Procedure 47.	TVOE iLO4 GUI Access.....	184
Procedure 48.	Change the TVOE iLO Address.....	185
Procedure 49.	PMAC/NOAM/SOAM Console iLO Access.....	188
Procedure 50.	Application NetBackup Client Installation (Using Platcfg).....	191
Procedure 51.	Application NetBackup Client Installation (NBAutoInstall).....	198
Procedure 52.	Create NetBackup Client Configuration File	200
Procedure 53.	Open Ports for NetBackup Client Software	200
Procedure 54.	IDIH External Drive Removal	205
Procedure 55.	Perform Backups.....	212
Procedure 56.	Perform Health Check.....	213
Procedure 57.	Add a New Server/VMs.....	215
Procedure 58.	Growth: DR-NOAM	216
Procedure 59.	Growth: SOAM spare (PCA Only).....	216
Procedure 60.	Growth: MP	217
Procedure 61.	Post Growth Health Check.....	218
Procedure 62.	Post Growth Backups.....	219
Procedure 63.	Perform Backups.....	220
Procedure 64.	Perform Health Check.....	221
Procedure 65.	Remove Server from Server Group	224
Procedure 66.	Post Growth Health Check.....	234
Procedure 67.	Post Growth Backups.....	236

1. Introduction

This document describes the application-related installation procedures for an HP C-class Diameter Signaling Router system.

This document assumes that platform-related configuration has already been done. Before executing this document, please ensure that all procedures from [7] DSR Hardware and Software Installation Part 1, E76180 have already been performed successfully.

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.

In scenarios where the DSR installation has already been executed, and system growth, de-growth is necessary; refer to Appendix L: Growth/De-Growth.

1.1 References

- [1] DSR Meta Administration Feature Activation Procedure, E58661
- [2] DSR Full Address Based Resolution (FABR) Feature Activation Procedure, E78925
- [3] DSR Range Based Address Resolution (RBAR) Feature Activation Procedure, E78926
- [4] SDS SW Installation and Configuration Guide, E79531
- [5] MAP-Diameter IWF Feature Activation Procedure. E78927
- [6] DSR IPv6 Migration Guide, E57517
- [7] DSR Hardware and Software Installation Part 1, E76180
- [8] DSR GLA Feature Activation Procedure, E78916
- [9] DSR PCA Activation Guide, E81528
- [10] DSR DTLS Feature Activation Procedure, E78942
- [11] DSR RADIUS Shared secret encryption key revocation MOP MO008572
- [12] Platform 7.2 Configuration Procedure, E64363
- [13] DSR Security Guide, E76974
- [14] DCA Framework and Application Activation and Deactivation Guide, E80801

1.2 Acronyms

An alphabetized list of acronyms used in the document

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array

Acronym	Definition
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
RMS	Rack Mounted Server
PMAC	Platform Management & Configuration
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port
IPFE	IP Front End
PCA	Policy and Charging Application
IDIH	Integrated Diameter Intelligence Hub

1.3 Terminology

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

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

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

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

5 <input type="checkbox"/>	ServerX: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. <pre>\$ cu -l /dev/ttyS7</pre>
-------------------------------	--	---

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

Table 2. Terminology

Term	Definition
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.
Health Check	Procedure used to determine the health and status of the DSR's internal network. This includes status displayed from the DSR GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.

Term	Definition
Management Server	HP ProLiant DL360/ DL380 deployed to run TVOE and host a virtualized PMAC application. Can also host a virtualized NOAM or IDIH. It is also used to configure the Aggregation switches (via the PMAC) and to serve other configuration purposes.
Place Association	Applicable for various applications, a Place Association is a configured object that allows places to be grouped together. A place can be a member of more than one place association. The Policy & Charging DRA application defines two place association types: policy binding region and policy & charging mated sites.
PMAC Application	PMAC is an application that provides platform-level management functionality for HP G6/G8/G9 system, such as the capability to manage and provision platform components of the system so it can host applications.
SBR Server Group Redundancy	The Policy and Charging application uses SBR server groups to store the application data. The SBR server groups support both two and three site redundancy. The server group function name is SBR .
Server Group Primary Site	A server group primary site is a term used to represent the principle location within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single Policy and Charging Mated Sites place association. For the Diameter Custom Application (DCA), these sites (Places) are configured in Applications Region place association. The primary site may be in a different site (place) for each configured SOAM or SBR server group. A primary site is described as the location in which the active and standby servers to reside; however, there cannot be any preferred spare servers within this location. All SOAM and SBR server groups have a primary site.
Server Group Secondary Site	A server group secondary site is a term used to represent location in addition to the primary site within a SOAM or SBR SERVER GROUP. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single Policy and Charging Mated Sites place association. For the Diameter Custom Application (DCA), these sites (places) are configured in Applications Region place association. The secondary site may be in a different site (place) for each configured SOAM or SBR server group. A secondary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. If two or three site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups.

Term	Definition
Server Group Tertiary Site	<p>A server group tertiary site is a term used to represent location in addition to the primary and secondary sites within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy & Charging DRA application, these sites (places) are all configured within a single Policy and Charging Mated Sites place association.</p> <p>The tertiary site may be in a different site (place) for each configured SOAM or SBR server group.</p> <p>A tertiary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. A tertiary site only applies if three site redundancy is wanted for SOAM and SBR server groups.</p>
Session Binding Repository Server Group Redundancy	<p>The DCA application may use SBR server groups to store application session data. The SBR server groups with support both two and three site redundancy. The server group function name is Session and Binding Repository.</p>
Site	<p>Applicable for various applications, a site is type of place. A place is configured object that allows servers to be associated with a physical location.</p> <p>A site place allows servers to be associated with a physical site. For example, sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one site when the server is configured.</p> <p>For the Policy & Charging DRA application, when configuring a site, only put DA-MPs and SBR MP servers in the site. Do not add NOAM, SOAM, or IPFE MPs to a site.</p>
Software Centric	<p>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.</p>
Three Site Redundancy	<p>Three site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of two sites in a Policy and Charging Mated Sites Place Association containing three sites.</p> <p>Three site redundancy is a feature provided by server groups configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in three geographically separate sites (locations). This feature ensures there is always a functioning active server in a server group even if all the servers in two sites fail.</p>
Two Site Redundancy	<p>Two site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy and Charging Mated Sites Place Association containing two sites.</p> <p>Two site redundancy is a feature provided by server group configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in two geographically separate sites (locations). This feature ensures there is always a functioning active server in a server group even if all the servers in a single site fail.</p>

2. General Description

This document defines the steps to execute the initial installation of the Diameter Signaling Router (DSR) application on new HP C-Class Hardware.

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

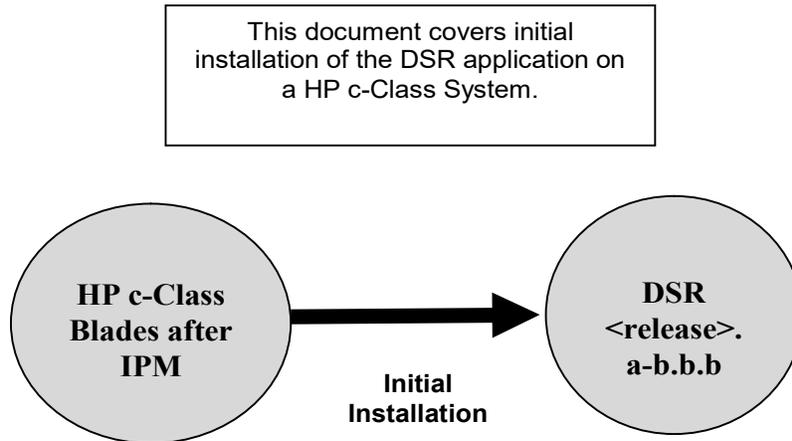


Figure 2. Example of Initial Application Installation Path

3. Installation Overview

This section provides a brief overview of the recommended method for installing DSR software on an HP C-Class system. The basic installation process and approximate time required is outlined in Figure 4. DSR Single Site Installation Procedure Map.

This section describes the overall strategy to employ for a single or multi-site DSR installation. It also lists the procedures required for installation with estimated times. Section 3.2 Installation Strategy discusses the overall install strategy and includes an installation flow chart that can be used to determine exactly which procedures should be run for an installation.

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 Strategy

A successful installation of DSR requires careful planning and assessment of all configuration materials and installation variables. Once a site survey has been conducted with the customer, the installer should use this section to map out the exact procedure list that is executed at each site.

Figure 3. DSR Installation: High Level Sequence illustrates the overall process that each DSR installation involves. In summary:

1. An overall installation requirement is decided upon. Among the data that should be collected:
 - The total number of sites
 - The number of servers at each site and their role(s)
 - Does DSR's networking interface terminate on a Layer 2 or Layer 3 boundary?
 - Number of enclosures at each site -- if any at all.
 - Will NOAMs use rack-mount servers or server blades?
 - (Per Site) Will MP's be in N+ 0 configurations 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 an external NMS be used? (Or both?)
2. A site survey (NAPD) is conducted with the customer to determine exact networking and site details.
Note: XMI and IMI addresses are difficult to change once configured. It is very important that these addresses are well planned and not expected to change after a site is installed.
 3. For each SOAM /MP/DR-NOAM only site (i.e., sites NOT containing the main NOAM server), the installer executes the procedures in document [7] DSR Hardware and Software Installation Part 1, E76180 to set up the PMAC, HP enclosures, and switches. Then, using the procedures in this document, all servers are IPMed with the proper TPD and DSR application ISO image. Figure 4. DSR Single Site Installation Procedure Map details the exact procedures that are to be executed for the 2nd part of this install. When this is complete, all non-NOAM sites are reachable through the network and ready for further installation when the primary NOAM site is brought up.
 4. The installer moves to the **main** site that contains the primary NOAM. Again, [7] DSR Hardware and Software Installation Part 1, E76180 is executed for this site first and then use the procedures in this document. Consult Figure 4. DSR Single Site Installation Procedure Map to determine the procedure list. During this install, the user brings up the other sub-sites (if they exist) configured in step 3. For single sites where the NOAM/SOAM/MPs are all located together, then step 3 is skipped and the entire install is covered by this step.
 5. Once the primary NOAM site has been installed according to [7] DSR Hardware and Software Installation Part 1, E76180 and this document, and then full DSR installation is complete.

Note: An alternative install strategy swaps steps 3 and 4. The main NOAM site is installed first, and then the sub-sites (DR-NOAM, SOAM/MP only) are installed and brought up on the NOAM as they are configured. This approach is perfectly valid, but is not reflected in the flow-charts/diagrams shown here.

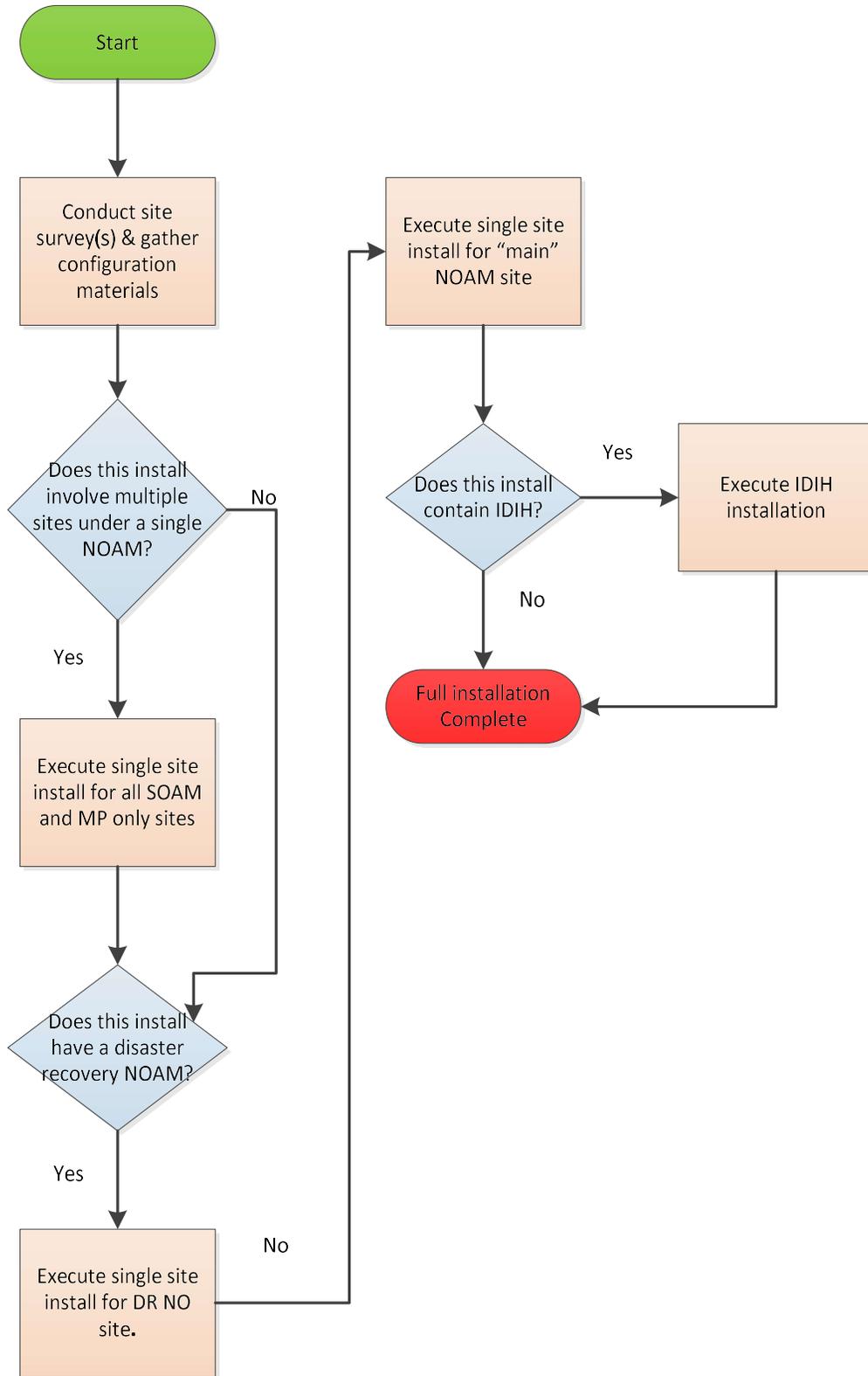


Figure 3. DSR Installation: High Level Sequence

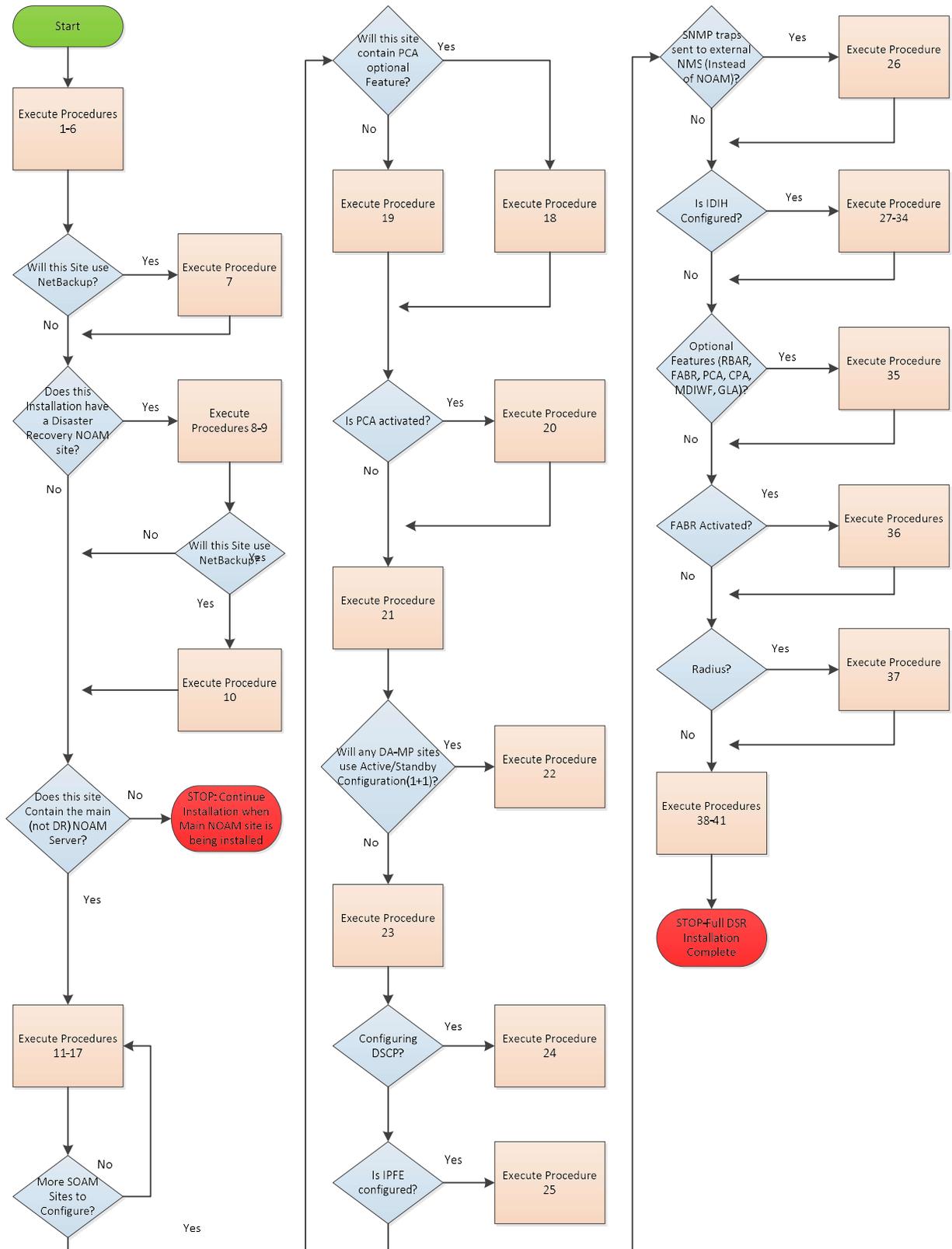


Figure 4. DSR Single Site Installation Procedure Map

3.3 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 (OA, 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 terminate at the NOAM and are viewable from the NOAM GUI (entire network) and the SOAM GUI (site specific). Traps are displayed on the GUI both as alarms and logged in trap history. This is the default configuration option and no changes are required for this to take effect.
2. Send all their SNMP traps to an external Network Management Station (NMS). The traps are seen at the SOAM AND/OR NOAM as alarms AND they are viewable at the configured NMS(s) as traps.

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 SOAMP VIP, or an external (customer) NMS. The recommended configuration is as follows:

The following components:

- PMAC (TVOE)
- PMAC (App)
- OAs
- All Switch types (4948, 3020, 6120.6125G)
- TVOE for DSR servers

Should have their SNMP trap destinations set to:

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

3.4 Optional Features

When DSR installation is complete, further configuration and/or installation steps 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 2. Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure, E58661
Policy and Charging Application (PCA)	DSR PCA Activation Guide, E81528
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide, E80801
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E78925
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure, E78926

Feature	Document
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure, E78927
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure, E78916
Host Intrusion Detection System (HIDS)	DSR Security Guide, E76974 (Section 3.2)

4. Software Installation Procedure

As mentioned earlier, the hardware installation and network cabling should be done before executing the procedures in this document. It is assumed that at this point, the user has access to:

- ILO consoles of all server blades at all sites
- ssh access to the PMAC servers at all sites
- GUI access to PMAC servers at all sites
- A configuration station with a web browser, ssh client, and scp client

SUDO

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

IPv6

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

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

If a dual-stack (IPv4 & IPv6) network is required, it is recommended that you first configure the topology, and then migrate to IPv6. Reference [6] DSR IPv6 Migration Guide, E57517 for instructions on how to accomplish this IPv6 migration.

4.1 Install and Configure NOAM Servers

4.1.1 Load Application and TPD ISO onto the PMAC Server

Procedure 1. Load Application and TPD ISO onto PMAC Server

S T E P #	<p>This procedure loads the DSR application and TPD ISO into the PMAC server.</p> <p>Needed material:</p> <ul style="list-style-type: none"> Application Media <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	TVOE Host: Load application ISO	<p>Add the Application ISO image to the PMAC, this can be done in one of three ways:</p> <ol style="list-style-type: none"> 1. Insert the Application CD required by the application 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). 4. Using sftp, connect to the PMAC server. <pre>\$ sftp pmacftpusr@<pmac_management_network_ip> \$ put <image>.iso</pre> 5. After the image transfer is 100% complete, close the connection: <pre>\$ quit</pre>

Procedure 1. Load Application and TPD ISO onto PMAC Server

<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser and enter:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<PMAC_Mgmt_Network_IP></code></p> </div> <p>Login as guiadmin user:</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Attach the software image to the PMAC guest</p>	<p>If the image is on a CD or USB device, continue with this step. 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.</p> <p>In the PMAC GUI, navigate to Main Menu -> VM Management. Select the PMAC guest. On the resulting View VM Guest page, select the Media tab.</p> <p>Under the Media tab, find the ISO image in the Available Media list, and click its Attach button. After a pause, the image displays in the Attached Media list.</p>

Procedure 1. Load Application and TPD ISO onto PMAC Server

<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Add application image</p>	<p>Navigate to Main Menu -> Software -> Manage Software Images.</p> <p>Click Add Image. Select the image from the list.</p> <p>If the image was supplied on a CD or a USB drive, it displays as a virtual device (device://...). These devices are assigned in numerical order as CD and USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally 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, select a correspondingly higher device number.</p> <p>If in step 1 the image was transferred to PMAC via sftp, it displays in the list as a local file /var/TKLC/....</p> <p>Select the appropriate path and click Add New Image.</p> <p>You may check the progress using the Task Monitoring link. Observe the green bar indicating success.</p> <p>Once the green bar is displayed, remove the DSR application Media from the optical drive of the management server.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Load TPD ISO</p>	<p>If the TPD ISO has not been loaded onto the PMAC already, repeat steps 1 through 4 to load it using the TPD media or ISO.</p>

4.1.2 Execute DSR Fast Deployment for NOAMs

Procedure 2. Configure NOAM Servers

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure extends the TVOE networking configuration on the first RMS server (if necessary), configure the networking on additional rack mount servers, create the NOAM VMs, and deploy the DSR and TPD images.</p> <p>Prerequisite: TVOE and PMAC (virtualized) have been installed on the first RMS server as described in [7] DSR Hardware and Software Installation Part 1, E76180.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>TVOE Host (Not PMAC): Configure control network bond for back-back configurations</p>	<p>Establish an SSH session to the second RMS server via the control IP address accessed from the site PMAC. Login as admusr.</p> <p>If the control network for the RMS servers consists of direct connections between the servers with no intervening switches (known as a back-to-back configuration), execute this step to set the primary interface of bond0 to <ethernet_interface_1>, otherwise skip to the next step.</p> <p>Note: Section TVOE Network Configuration, step 2, should have already been executed on the TVOE host that hosts the PMAC server.</p> <p>Note: The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm set --device=bond0 --primary=eth01 Interface bond0 updated</pre>
<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC Server: Login</p>	<p>Establish an SSH session to the PMAC server and login as admusr.</p>

Procedure 2. Configure NOAM Servers

3	PMAC Server: Update the DSR fast deployment template (Part 1)	<p>Perform the following command to navigate to the directory containing the DSR fast deployment template:</p> <pre>\$ cd /usr/TKLC/smac/etc</pre> <p>DSR Fast Deployment Template Names:</p> <p>NOAM on Rack Mount Servers: DSR_NOAM_FD_RMS.xml</p> <p>NOAM on Blade Servers: DSR_NOAM_FD_Blade.xml</p> <p>Note: If the fast deployment template is not present, then please re-execute section Setup PMAC step 10, sub step C from [7] DSR Hardware and Software Installation Part 1, E76180.</p> <p>Update the following items within the Fast deployment xml:</p> <p>TPD and DSR ISO:</p> <pre><software> <!--Target TPD release Image here --> <image id="tpd"> <name>TPD.install-7.0.2.0.0_86.34.0- OracleLinux6.6-x86_64</name> </image> <!--Target DSR release Image here --> <image id="dsr"> <name>DSR-8.0.0.0_80.8.0-x86_64</name> </image> </software></pre> <p>Note: These are the images uploaded from Procedure 1. Load Application and TPD ISO onto PMAC Server. Do NOT append .iso to the image name. To copy and paste the image name from the command line, issue the following command:</p> <pre>\$ ls /var/TKLC/smac/image/repository</pre>
---	---	---

Procedure 2. Configure NOAM Servers

4	<input type="checkbox"/> PMAC Server: Update the DSR fast deployment template for bond 1 – optional (Part 2)	Bond 1 Creation: Skip this step if Bond1 will not be created. Uncomment the following items from BOTH tvoe host id="NOAM1" and tvoe host id="NOAM2" by removing the encapsulated '<!--' '-->' brackets as highlighted below: Update the Ethernet interfaces that are to be enslaved by bond1. <pre> <!-- <tpdinterface id="bond1"> <device>bond1</device> <type>Bonding</type> <bonddata> <bondinterfaces><bond1_eth_interface1>,<bond1_eth_interface 2></bondinterfaces> <bondopts>mode=active-backup,miimon=100</bondopts> </bonddata> <onboot>yes</onboot> <bootproto>none</bootproto> </tpdinterface> --> </pre>
5	<input type="checkbox"/> PMAC Server: Update the DSR fast deployment template management/XMI combination (Part 3)	Only execute this step if your management network and xmi networks are combined, otherwise skip this step. Modify the template to reflect the following on BOTH tvoe host id="NOAM1" and tvoe host id="NOAM2": Remove the following stanzas: <pre> <mgmtbondinterface> <mgmtvlan> <mgmtsubnet> <mgmtdefaultgateway> <tpdinterface id="management"> (and all sub elements) <tpdbridge id="management"> (and all sub elements) </pre> Replace the following under <tpdroute id="management_default">: management with xmi for <device>management</device> \$\$mgmtdefaultgateway\$\$ with \$\$xmidefaultgateway\$\$ for <gateway>\$\$mgmtdefaultgateway\$\$</gateway> Add the following under <tpdbridge id="xmi">: <pre> <address><TVOE_Host_Server_XMI_IP></address> <netmask> \$\$xmisubnet\$\$</netmask> </pre>

Procedure 2. Configure NOAM Servers

8 <input type="checkbox"/>	PMAC Server: Backup FDC file	<p>Create the fdc directory so the NOAM fdc file is backed up by PMAC: Issue the following commands:</p> <p>Create the fdc backup directory:</p> <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc</pre> <p>Copy the fdc file to the fdc backup directory:</p> <pre>\$ sudo cp /usr/TKLC/smac/etc/<fdc_file> /usr/TKLC/smac/etc/fdc/</pre>
-------------------------------	--	---

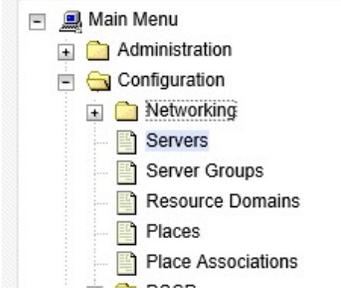
4.1.3 Configure NOAMs**Procedure 3. Configure the First NOAM NE and Server**

S	This procedure configures the first NOAM server.	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	Save the NOAM network data to an XML file	<p>Using a text editor, create a NOAM network element file that describes the networking of the target install environment of your first NOAM server.</p> <p>Select an appropriate file name and save the file to a known location on your computer.</p> <p>A suggested filename format is Appname_NName_NetworkElement.XML, so for example a DSR2 NOAM network element XML file would have a filename DSR2_NOAM_NetworkElement.xml.</p> <p>Alternatively, you can update the sample DSR network element file. It can be found on the management server at:</p> <pre style="border: 1px solid black; padding: 2px;">/usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml</pre> <p>A sample XML file can also be found in Appendix A: Sample Network Element and Hardware Profiles.</p> <p>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.</p>

Procedure 3. Configure the First NOAM NE and Server

<p>2 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>Using the XMI IP address configured in Procedure 2. Configure NOAM Servers (\$NOAM1_xmi_IP_address), login to the NOAM GUI as the guiadmin user:</p>
<p>3 <input type="checkbox"/></p>	<p>Create the NOAM network element using the XML file</p>	<p>Navigate to Main Menu->Networking -> Networks.</p> <p>Click Browse and type the pathname to the NOAM network XML file.</p> <p>Click Upload File to upload the XML file and configure the NOAM network element.</p> <p>Once the data has been uploaded, a tab displays with the name of your network element. Click this tab to display a screen with the individual networks that are now configured.</p>

Procedure 3. Configure the First NOAM NE and Server

<p>5</p> <p><input type="checkbox"/></p>	<p>Insert the 1st NOAM server</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>Click Insert to insert the new NOAM server into servers table (the first or server).</p> <p>Enter the fields as follows:</p> <p>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]</p> <p>The network interface fields become available with selection choices based on the chosen hardware profile and network element.</p> <p>Type the server IP addresses for the XMI network. Select XMI for the interface. Leave the VLAN checkbox unchecked.</p> <p>Note: The XMI server IP must match \$NOAM1_xmi_IP_address configured in Procedure 2.</p> <p>Type the server IP addresses for the IMI network. Select IMI for the interface. Leave the VLAN checkbox unchecked.</p> <p>Note: The IMI server IP must match \$NOAM1_imi_IP_address configured in Procedure 2.</p>
--	-----------------------------------	--

Procedure 3. Configure the First NOAM NE and Server

		<p>Next, add the following NTP servers:</p> <table border="1" data-bbox="479 279 1349 401"> <thead> <tr> <th data-bbox="479 279 906 321">NTP Server</th> <th data-bbox="906 279 1349 321">Preferred?</th> </tr> </thead> <tbody> <tr> <td data-bbox="479 321 906 401"><TVOE_XMI_IP_Address(NO1)/ TVOE_Mgmt_IP_Address(NO1)></td> <td data-bbox="906 321 1349 401">Yes</td> </tr> </tbody> </table> <p>Click OK when you have completed entering all the server data.</p>	NTP Server	Preferred?	<TVOE_XMI_IP_Address(NO1)/ TVOE_Mgmt_IP_Address(NO1)>	Yes
NTP Server	Preferred?					
<TVOE_XMI_IP_Address(NO1)/ TVOE_Mgmt_IP_Address(NO1)>	Yes					
<p>6</p> <p><input type="checkbox"/></p>	<p>Export the initial configuration</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <p>From the GUI screen, select the NOAM server and click Export to generate the initial configuration data for that server.</p>				
<p>7</p> <p><input type="checkbox"/></p>	<p>NOAM: Copy configuration file to 1st NOAM server</p>	<p>Establish an SSH session to the 1st NOAM server by logging in as the admusr user.</p> <p>Copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the 1st NOAM to the <code>/var/tmp</code> directory.</p> <p>The configuration file has a filename like TKLCConfigData.<hostname>.sh. The following is an example:</p> <pre data-bbox="456 1213 1360 1318">\$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.blade01.sh /var/tmp/TKLCConfigData.sh</pre>				
<p>8</p> <p><input type="checkbox"/></p>	<p>NOAM: Wait for configuration to complete</p>	<p>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the <code>/var/tmp</code> directory, implement the configuration in the file, and then prompt the user to reboot the server.</p> <p>Wait to be prompted to reboot the server, but DO NOT reboot the server, it is rebooted later on in this procedure.</p> <p>Note: Ignore the warning about removing the USB key, since no USB key is present.</p>				

Procedure 3. Configure the First NOAM NE and Server

9	<input type="checkbox"/> NOAM: Set the time zone and reboot the server	<p>From the command line prompt, execute set_ini_tz.pl. This sets the system time zone. The following command example uses the America/New_York time zone.</p> <p>Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix G: List of Frequently Used Time Zones.</p> <pre>\$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York"</pre> <pre>\$ sudo init 6</pre>
10	<input type="checkbox"/> 1st NOAM: Configure networking for dedicated netbackup interface (optional)	<p>Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the 1st NOAM server by logging in as the admusr user.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=NetBackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP_Address> --netmask=<NO1_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NetBackup_Svr_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address></pre>
11	<input type="checkbox"/> 1st NOAM Server: Verify server health	<p>Execute the following command on the 1st NOAM server and make sure that no errors are returned:</p> <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 4. Configure the NOAM Server Group

<p>S T E P #</p>	<p>This procedure configures the NOAM server group.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of:</p> <div data-bbox="456 541 1312 592" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<NO1_XMI_IP_Address>">http://<NO1_XMI_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

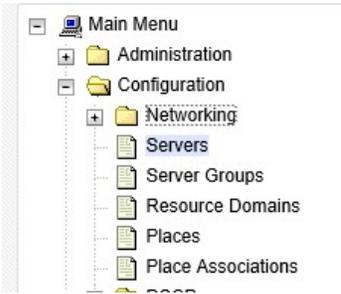
Procedure 4. Configure the NOAM Server Group

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM GUI: Edit the NOAM server group</p>	<p>From the GUI, navigate to Main Menu -> Configuration -> Server Groups.</p> <p>Select the new server group, and then select Edit.</p> <p>Select the network element that represents the NOAM.</p> <p>In the portion of the screen that lists the servers for the server group, find the NOAM server being configured.</p> <p>Click the Include in SG checkbox.</p> <p>Leave other boxes blank.</p> <p>Click OK.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM: Verify NOAM blade server role</p>	<p>From terminal window to the iLO of the first NOAM server, execute the following command:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">\$ha.mystate</pre> <p>Verify the DbReplication and VIP items under the resourceId column have a value of Active under the role column.</p> <p>You might have to wait a few minutes for it to become in that state.</p> <p>Example:</p>

Procedure 4. Configure the NOAM Server Group

5 <input type="checkbox"/>	NOAM GUI: Restart NOAM server	From the NOAM GUI, navigate to Main menu -> Status & Manage -> Server. Select the NOAM server. Click Restart. Answer OK to the confirmation screen. Wait for restart to complete.
-------------------------------	---	---

Procedure 5. Configure the Second NOAM Server

<p>S T E P #</p>	<p>This procedure configures the second NOAM server.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>If not already done, establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><code>http://<NO1_XMI_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>2 <input type="checkbox"/></p>	<p>NOAM GUI: Insert the 2nd NOAM server</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>Click Insert to insert the 2nd NOAM server into servers table (the first or server).</p>

Procedure 5. Configure the Second NOAM Server

Enter 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 become available with selection choices based on the chosen hardware profile and network element.

Type the server IP addresses for the XMI network. Select **XMI** for the interface. Leave the **VLAN** checkbox unchecked.

Note: The XMI server IP must match '\$NOAM2_xmi_IP_address' configured in Procedure 2.

Type the server IP addresses for the IMI network. Select **IMI** for the interface. Leave the **VLAN** checkbox unchecked.

Note: The IMI server IP must match '\$NOAM2_imi_IP_address' configured in Procedure 2.

Next, add the following NTP servers:

NTP Server	Preferred?
<TVOE_XMI_IP_Address(NO2)/ TVOE_Mgmt_IP_Address(NO2)>	Yes

Click **OK** when you have completed entering all the server data.

Procedure 5. Configure the Second NOAM Server

3 <input type="checkbox"/>	NOAM GUI: Export the initial configuration	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <p>From the GUI screen, select the NOAM server and click Export to generate the initial configuration data for that server.</p>
4 <input type="checkbox"/>	1st NOAM Server: Copy configuration file to 2 nd NOAM server	<p>Obtain a terminal session to the 1st NOAM as the admusr user.</p> <p>Execute the following command to configure the 2nd NOAM server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>.sh admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
5 <input type="checkbox"/>	2nd NOAM Server: Verify configuration was called and reboot the server	<p>Establish an SSH session to the 2nd NOAM server (NOAM2_xmi_IP_address)</p> <p>Login as the admusr user.</p> <p>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server.</p> <p>Verify configuration was called by checking the following file.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cat /var/TKLC/appw/logs/Process/install.log Verify the following message is displayed: [SUCCESS] script completed successfully!</pre> <p>Now reboot the server.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo init 6</pre> <p>Wait for the server to reboot.</p>

Procedure 5. Configure the Second NOAM Server

6	<input type="checkbox"/> 2nd NOAM Server: Configure networking for dedicated netbackup interface (optional)	<p>Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the 2nd NOAM server by logging in as the admusr user.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NetBackup_Svr_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>
7	<input type="checkbox"/> 2nd NOAM Server: Verify server health	<p>Execute the following command on the 2nd NOAM server and make sure that no errors are returned.</p> <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 6. Complete NOAM Server Group Configuration

<p>S T E P #</p>	<p>This procedure finishes configuring the NOAM server group.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of:</p> <div data-bbox="456 541 1312 590" style="border: 1px solid black; padding: 2px;"> <p><a href="http://<NO1_XMI_IP_Address>">http://<NO1_XMI_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

Procedure 6. Complete NOAM Server Group Configuration

2 <input type="checkbox"/>	NOAM GUI: Edit the NOAM server group data and add the VIP address	Navigate to Main Menu -> Configuration -> Server Groups. Select the NOAM server group and click Edit. Add the 2 nd NOAM server to the server group by clicking the Include in SG checkbox for the 2 nd NOAM server. Click Apply. Add a NOAM VIP by clicking Add. Type the VIP Address and click OK.
-------------------------------	---	--

Procedure 6. Complete NOAM Server Group Configuration

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Establish GUI session</p>	<p>Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:</p> <div data-bbox="456 310 1312 359" style="border: 1px solid black; padding: 2px;"> <p><code>http://<NOAM_XMI_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Wait for remote database alarm to clear</p>	<p>Navigate to Main Menu -> Alarms & Events -> View Active.</p> <p>Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.</p>

4.2 Install and Configure DR-NOAM Servers (Optional)

4.2.1 Execute DSR Fast Deployment for DR-NOAMs

Procedure 8. NOAM Configuration for DR Site (Optional)

S T E P #	<p>This procedure extends the TVOE networking configuration on the first DR-NOAM RMS server (if necessary), configures the networking on additional rack mount servers, creates the DR-NOAM VMs, and deploys the DSR and TPD images.</p> <p>Prerequisite: TVOE and PMAC (virtualized) have been installed on the First DR-NOAM RMS server as described in [7] DSR Hardware and Software Installation Part 1, E76180.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>PMAC Server: Login</p> <p>Establish an SSH session to the PMAC server and login as admusr.</p>
2 <input type="checkbox"/>	<p>PMAC Server: Update the DSR fast deployment template</p> <p>Perform the following command to navigate to the directory containing the DSR fast deployment template:</p> <pre style="border: 1px solid black; padding: 2px;">\$ cd /usr/TKLC/smac/etc</pre> <p>DSR Fast Deployment Template Names:</p> <p>NOAM on Rack Mount Servers: DSR_NOAM_FD_RMS.xml</p> <p>NOAM on Blade Servers: DSR_NOAM_FD_Blade.xml</p> <p>Note: If the fast deployment template is not present, then please re-execute section Setup PMAC step 10, sub step C from [7] DSR Hardware and Software Installation Part 1, E76180.</p> <p>Update the following items within the fast deployment xml:</p> <p>TPD and DSR ISO:</p> <pre><software> <!--Target TPD release Image here --> <image id="tpd"> <name>TPD.install-7.0.2.0.0_86.34.0- OracleLinux6.6-x86_64</name> </image> <!--Target DSR release Image here --> <image id="dsr"> <name>DSR-8.0.0.0_72.8.0-x86_64</name> </image> </software></pre> <p>Note: These are the images uploaded from Section 4.1.1 Load Application and TPD ISO onto the PMAC Server. Do NOT append .iso to the image name. To copy and paste the image name from the command line, issue the following command:</p> <pre style="border: 1px solid black; padding: 2px;">\$ ls /var/TKLC/smac/image/repository</pre> <p>Bond 1 Creation:</p> <p>Skip this step if Bond1 will not be created.</p>

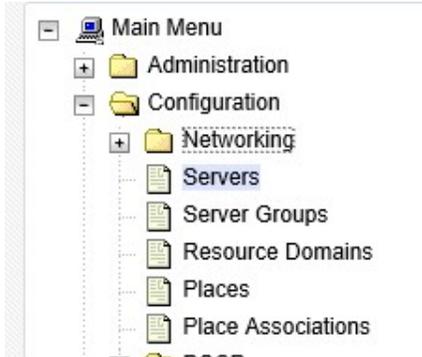
Procedure 8. NOAM Configuration for DR Site (Optional)

		<p>Uncomment the following items from BOTH tvoe host id="NOAM1" and tvoe host id="NOAM2" by removing the encapsulated '<!--' '-->' brackets as highlighted below:</p> <p>Update the ethernet interfaces that are to be enslaved by bond1.</p> <pre> <!-- <tpdinterface id="bond1"> <device>bond1</device> <type>Bonding</type> <bonddata> <bondinterfaces><bond1_eth_interface1>,<bond1_eth_interface2> </bondinterfaces> <bondopts>mode=active-backup,miimon=100</bondopts> </bonddata> <onboot>yes</onboot> <bootproto>none</bootproto> </tpdinterface> --> </pre>
3	<input type="checkbox"/> <p>PMAC Server: Update the DSR fast deployment template management/XMI combination (Part 3)</p>	<p>Only execute this step if your management network and XMI networks are combined, otherwise skip this step.</p> <p>Modify the template to reflect the following on BOTH tvoe host id="NOAM1" and tvoe host id="NOAM2":</p> <p>Remove the following stanzas:</p> <pre> <mgmtbondinterface> <mgmtvlan> <mgmtsubnet> <mgmtdefaultgateway> <tpdinterface id="management"> (and all sub elements) <tpdbridge id="management"> (and all sub elements) </pre> <p>Replace the following under <tpdroute id="management_default">:</p> <pre> management with xmi for <device>management</device> \$\$mgmtdefaultgateway\$\$ with \$\$xmidefaultgateway\$\$ for <gateway>\$\$mgmtdefaultgateway\$\$</gateway> </pre> <p>Add the following under <tpdbridge id="xmi">:</p> <pre> <address><TVOE_Host_Server_XMI_IP></address> <netmask> \$\$xmisubnet\$\$</netmask> </pre>

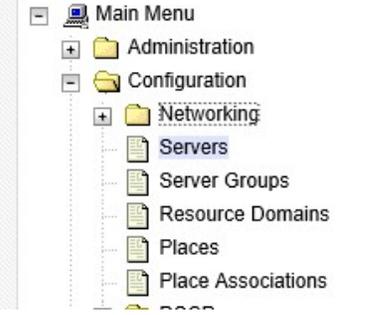
Procedure 8. NOAM Configuration for DR Site (Optional)

<p>6</p> <p><input type="checkbox"/></p>	<p>PMAC Server: Backup FDC file</p>	<p>Create the fdc directory so the NOAM fdc file is backed up by PMAC.</p> <p>Issue the following commands:</p> <pre style="border: 1px solid black; padding: 5px;"> Create the fdc backup directory: \$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc Copy the fdc file to the fdc backup directory: \$ sudo cp /usr/TKLC/smac/etc/<fdc_file> /usr/TKLC/smac/etc/fdc/ </pre>
<p>7</p> <p><input type="checkbox"/></p>	<p>Save the DR-NOAM network data to an XML file</p>	<p>Using a text editor, create a DR-NOAM network element file that describes the networking of the target install environment of your first DR-NOAM server.</p> <p>Select an appropriate file name and save the file to a known location on your computer.</p> <p>A suggested filename format is Appname_NName_NetworkElement.XML, so for example a DSR2 NOAM network element XML file would have a filename DSR2_NOAM_NetworkElement.xml.</p> <p>Alternatively, you can update the sample DSR network element file. It can be found on the management server at:</p> <pre style="border: 1px solid black; padding: 5px;"> /usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml </pre> <p>A sample XML file can also be found in Appendix A: Sample Network Element and Hardware Profiles.</p> <p>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.</p>
<p>8</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:</p> <pre style="border: 1px solid black; padding: 5px;"> http://<NOAM_XMI_VIP_IP_Address> </pre> <p>Login as the guiadmin user.</p>

Procedure 8. NOAM Configuration for DR Site (Optional)

<p>9</p> <p><input type="checkbox"/></p>	<p>PRIMARY NOAM VIP GUI: Insert the DR NOAM network element</p>	<p>Navigate to Main Menu -> Networking -> Networks.</p> <p>Click Browse and type the pathname of the DR NOAM network XML file.</p> <p>Click Upload File to upload the XML file and configure the NOAM network element.</p> <p>Once the data has been uploaded, a tab displays with the name of your network element. Select the tab to display a window that describes the individual networks now configured.</p>
<p>10</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Insert the 1st DR-NOAM server</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>Click Insert to insert the new DR-NOAM server into servers table.</p> <p>Enter the fields as follows:</p> <p>Hostname: <Hostname> Role: NETWORK OAM&P</p>

Procedure 8. NOAM Configuration for DR Site (Optional)

11 <input type="checkbox"/>	PRIMARY NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>From the GUI screen, select the DR-NOAM server and click Export to generate the initial configuration data for that server.</p>
12 <input type="checkbox"/>	1st NOAM Server: Copy configuration file to DR-NOAM NOAM server	<p>Obtain a terminal session to the primary NOAM as the admusr user.</p> <p>Execute the following command to configure the DR-NOAM server.</p> <pre data-bbox="456 884 1382 989">\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DR-NOAM_Hostname>.sh admusr@<DR-NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
13 <input type="checkbox"/>	1st DR-NOAM Server: Verify configuration was called and reboot the server	<p>Establish an SSH session to the DR-NOAM server (DR-NOAM_XMI_IP_address)</p> <p>Login as the admusr user.</p> <p>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server.</p> <p>Verify configuration was called by checking the following file.</p> <pre data-bbox="456 1272 1357 1388">\$ sudo cat /var/TKLC/appw/logs/Process/install.log Verify the following message is displayed: [SUCCESS] script completed successfully!</pre> <p>Now reboot the server:</p> <pre data-bbox="456 1451 1357 1503">\$ sudo init 6</pre> <p>Wait for the server to reboot.</p>

Procedure 8. NOAM Configuration for DR Site (Optional)

<p>14</p> <p><input type="checkbox"/></p>	<p>1st DR-NOAM: Configure networking for dedicated NetBackup interface (optional)</p>	<p>Note: Only execute this step if your DR-NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the 1st DR-NOAM server by logging in as the admusr user.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP_Address> --netmask=<NO1_NetBackup_NetMask></pre> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NetBackup_Svr_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address></pre>				
<p>15</p> <p><input type="checkbox"/></p>	<p>1st DR-NOAM Server: Verify server health</p>	<p>Execute the following command on the 1st DR-NOAM server and make sure that no errors are returned.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>				
<p>16</p> <p><input type="checkbox"/></p>	<p>Repeat for 2nd DR NOAM server</p>	<p>Repeat steps 7 through 12 to configure 2nd DR-NOAM server. When inserting the 2nd DR-NOAM server, change the NTP server address to the following:</p> <table border="1" data-bbox="475 1207 1349 1327"> <thead> <tr> <th style="background-color: #e1eef6;">NTP Server</th> <th style="background-color: #e1eef6;">Preferred?</th> </tr> </thead> <tbody> <tr> <td><TVOE_XMI_IP_Address(DR-NO2)/ TVOE_Mgmt_IP_Address(DR-NO2)></td> <td>Yes</td> </tr> </tbody> </table>	NTP Server	Preferred?	<TVOE_XMI_IP_Address(DR-NO2)/ TVOE_Mgmt_IP_Address(DR-NO2)>	Yes
NTP Server	Preferred?					
<TVOE_XMI_IP_Address(DR-NO2)/ TVOE_Mgmt_IP_Address(DR-NO2)>	Yes					

4.2.2 Pair DR-NOAMs

Procedure 9. Pairing for DR-NOAM site (Optional)

<p>S T E P #</p>	<p>This procedure pairs the DR-NOAM site.</p> <p>Prerequisite: Installation for DR-NOAM site complete.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the NOAM server by using the VIP IP address of the primary NOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="456 600 1312 646" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<Primary_NOAM_VIP_IP_Address>">http://<Primary_NOAM_VIP_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

Procedure 9. Pairing for DR-NOAM site (Optional)

<p>4 <input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Add DR NOAM VIP</p>	<p>Click Add for the VIP Address and enter an IP Address for the VIP.</p> <p>Click Apply. Verify the banner information message states Data committed.</p>
<p>5 <input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Wait for remote database alarm to clear</p>	<p>Navigate to Main Menu -> Alarms & Events -> View Active.</p> <p>Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.</p>
<p>6 <input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Restart 1st DR NOAM server</p>	<p>From the NOAM GUI, navigate to Main Menu -> Status & Manage -> Server.</p> <p>Select the 1st DR NOAM server. Click Restart.</p> <p>Click OK on the confirmation screen.</p> <p>Wait for the restart to complete in approximately 3-5 minutes before proceeding.</p>

Procedure 9. Pairing for DR-NOAM site (Optional)

<p>7</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Restart the application on the 2nd DR NOAM server</p>	<p>Repeat steps 6, but this time, select the 2nd DR NOAM server.</p>
<p>8</p> <p><input type="checkbox"/></p>	<p>Primary NOAM: Modify DSR OAM process</p>	<p>Establish an SSH session to the primary NOAM, login as admusr.</p> <p>Execute the following commands:</p> <p>Retrieve the cluster ID of the DR-NOAM:</p> <pre style="background-color: #f0f0f0; padding: 10px;">\$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>' " Server_ID NodeID ClusterID 1 Oahu-DSR-DR-NOAM-2 A1055</pre> <p>Execute the following command to start the DSR OAM process on the DR-NOAM:</p> <pre>\$ echo "<clusterID> DSROAM_Proc Yes" iload -ha -xun - fcluster -fresource -foptional HaClusterResourceCfg</pre>

4.2.3 Install NetBackup Client (Optional)

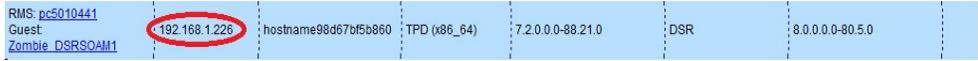
Procedure 10. Install NetBackup Client (Optional)

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>		<p>This procedure downloads and installs NetBackup client software on the server.</p> <p>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:</p> <ul style="list-style-type: none"> • /usr/TKLC/appworks/sbin/bpstart_notify • /usr/TKLC/appworks/sbin/bpend_notify <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<p>Install NetBackup client software</p>	<p>If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools (push configuration), then use Appendix H.2: NetBackup Client Install/Upgrade with NBAutoInstall.</p> <p>Note: This is not common. If the answer to the previous question is not known, then use Appendix H.1: NETBACKUP Client Installation Using PLATCFG.</p>
<p>2</p> <p><input type="checkbox"/></p>	<p>Install NetBackup client software</p>	<p>Choose the same method used in step 1 to install NetBackup on the 2nd NOAM.</p>

4.3 Install and Configure SOAM Servers

4.3.1 Configure SOAM TVOE Server Blades

Procedure 11. Configure SOAM TVOE Server Blades

S T E P #	<p>This procedure configures TVOE on the server blades that host DSR SOAM VMs. It details the configuration for a single server blade and should be repeated for every TVOE blade that was IPMed for this install.</p> <p>Note: TVOE should only be installed on Blade servers run as DSR SOAMs. They should NOT be installed on Blade servers intended to run as DSR MPs.</p> <p>Prerequisite: TVOE OS has been installed on the target server blades as per instructions in [7] DSR Hardware and Software Installation Part 1, E76180.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>PMAC Server: Exchange SSH keys between PMAC and TVOE server</p>	<p>Use the PMAC GUI to determine the control network IP address of the TVOE server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.</p>  <p>Note the IP address TVOE server.</p> <p>From a terminal window connection on the PMAC, login as the admusr user, exchange SSH keys between the PMAC and the TVOE server using the keyexchange utility, using the Control network IP address for the TVOE blade server. When asked for the password, type the password for the TVOE server.</p> <pre style="border: 1px solid black; padding: 5px;">\$ keyexchange admusr@<TVOE_Control_Blade_IP_address></pre>
2 <input type="checkbox"/>	<p>TVOE Server: Login and copy configuration scripts from PMAC</p>	<p>Login as admusr on the TVOE server using the control IP address noted above.</p> <p>Execute the following commands:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp admusr@<Mgmt_Server_Control_IP_address>:/usr/TKLC/smac/etc/TVOE* /usr/TKLC/</pre> <pre style="border: 1px solid black; padding: 5px;">\$ sudo chmod 777 /usr/TKLC/TVOE*</pre> <p>Note: If no TVOE configuration scripts are found here, then please re-execute section 4.2.2, step #13 of [7] DSR Hardware and Software Installation Part 1, E76180.</p>

Procedure 11. Configure SOAM TVOE Server Blades

3 <input type="checkbox"/>	TVOE Server: Mezzanine card/ segregated OAM/XMI network configuration	<p>Perform this step if your TVOE server blade DOES have mezzanine cards AND you are running OAM/XMI traffic on a separate physical network (example below). If you do not have mezzanine cards, skip this step.</p> <p>Execute the following command:</p> <pre>\$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID> mezz</pre>
-------------------------------	--	---

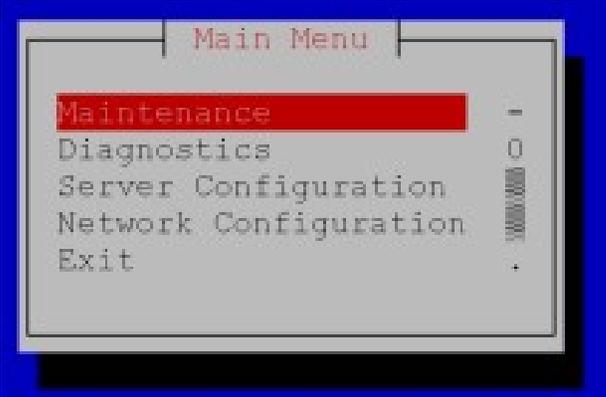
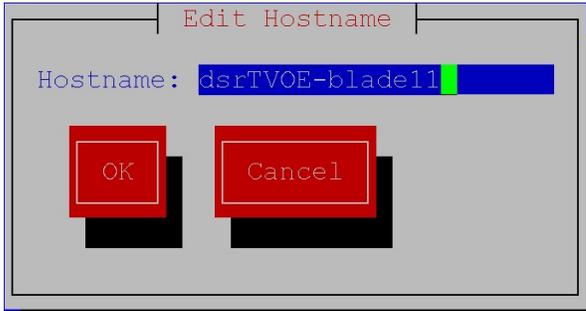
Procedure 11. Configure SOAM TVOE Server Blades

<p>4</p> <p><input type="checkbox"/></p>	<p>TVOE Server: No mezzanine card/ No segregated OAM/XMI network configuration</p>	<p>Perform this step if your TVOE server blade DOES NOT have mezzanine cards AND/OR you are NOT running OAM/XMI traffic over a separate physical network (example below).</p> <p>Execute the following command:</p> <pre>\$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID></pre>
<p>5</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Verify TVOE configuration</p>	<p>XMI_VLAN_ID is the VLAN ID for the XMI network in this installation, and IMI_VLAN_ID is the VLAN ID for the IMI network in this installation. For deployments with aggregation switches, the IMI and XMI VLAN IDs are the values of the INTERNAL-IMI and INTERNAL-XMI VLAN IDs, respectively. For layer-2 only deployments, the IMI and XMI VLAN IDs are obtained from the customer.</p> <p>Upon executing the proper version of the TVOEcfg.sh script, you should see an output similar to the following (example shows output without the “mezz” parameter):</p> <pre>Using onboard NICs ... Interface bond0.3 added Interface bond0.4 added Setting up the bridge and unsetting network info Interface bond0.3 was updated. Bridge xmi added! Setting up the bridge and unsetting network info Interface bond0.4 was updated. Bridge imi added!</pre> <p>The prompt displays.</p> <p>Note: If for any reason, you run the wrong version of the TVOEcfg.sh command, you can execute the following command to reset the network configuration so you can repeat either step 3 or 4.</p> <pre>sudo ./usr/TKLC/TVOEclean.sh</pre>

Procedure 11. Configure SOAM TVOE Server Blades

6	<p>TVOE Server: Configure XMI IP and default route</p>	<p>Configure IP address on the XMI network:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=xmi --address=<TVOE_XMI_IP_ADDRESS> --netmask=<TVOE_XMI_Netmask/Prefix> /sys/class/net/bond1/bonding/primary has 0 lines, nothing to do. Interface xmi was updated.</pre> <p>Restart network services:</p> <pre>\$ sudo service network restart [wait for the prompt to return]</pre> <p>Set the default route:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=xmi --gateway=<TVOE_XMI_Gateway_IP_Address> Route to xmi added.</pre>
7	<p>TVOE Server: Configure NetBackup dedicated interface and bridge (optional)</p>	<p>In these examples, <interface> is replaced with the actual ethernet interface that is used as the dedicated NetBackup port. For instance, eth01 or eth22.</p> <p>Un-bonded ethernet interface:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Ethernet interface> --slave=no --onboot=yes</pre> <p>[OPTIONAL] If this installation is using jumbo frames, set the ethernet interface MTU to the desired jumbo frame size:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Ethernet interface> --MTU=<NetBackup_MTU_size></pre> <p>Create NetBackup VM bridge interface:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=netbackup --bridgeInterfaces=<Ethernet interface> --onboot=yes</pre>
8	<p>TVOE Server: Configure networking for dedicated NetBackup interface (optional)</p>	<p>Note: Only execute this step if using a dedicated ethernet interface for NetBackup.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=NetBackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP_Adress> --netmask=<NO1_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NetBackup_Svr_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address></pre>

Procedure 11. Configure SOAM TVOE Server Blades

<p>9</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Set hostname</p>	<pre>\$ sudo su - platcfg</pre>  <p>Navigate to Server Configuration -> Hostname -> Edit and enter a new hostname for your server:</p>  <p>Click OK and click Exit until you are at the platcfg main menu again.</p> <p>Note: Although the new hostname has been properly configured and committed at this point, it does not display on your command prompt unless you log out and log back in again.</p>
--	--	---

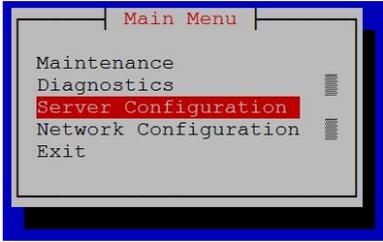
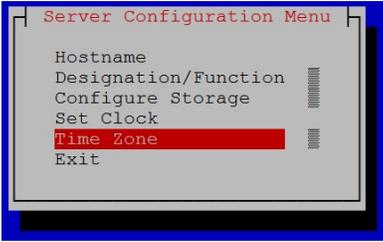
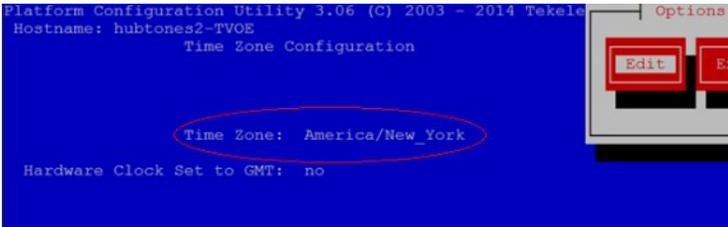
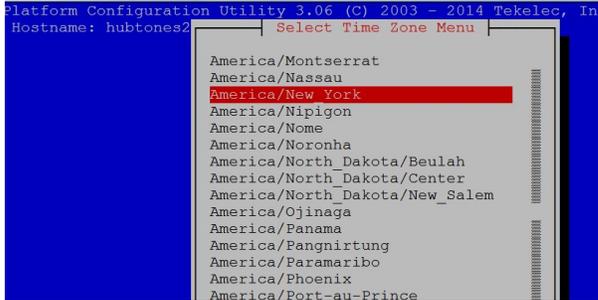
Procedure 11. Configure SOAM TVOE Server Blades

<p>10</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Configure SNMP</p>	<p>From the platcfg main menu, navigate to Network Configuration -> SNMP Configuration -> NMS Configuration.</p> <p>Click Edit.</p> <p>Click Add a New NMS Server.</p> <p>Enter the following NMS servers, clicking OK after each one and then selecting the Add NMS option again:</p> <ul style="list-style-type: none"> • Enter the Hostname/IP of the customer NMS server, for port, enter 162, and for Community String enter the community string provided in the customer NAPD Document. • Enter the IP of the SOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document <p>Click Exit.</p> <p>Select Yes when asked to restart the Alarm Routing Service.</p> <p>Once done, click Exit to quit to the platcfg main menu.</p>
---	---	--

Procedure 11. Configure SOAM TVOE Server Blades

<p>12</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Configure NTP. Edit an existing NTP server</p>	<p>Edit an existing NTP server.</p> <p>The NTP server to edit Menu screen displays.</p> <pre>lu NTP server to edit Menu tk x x x ntpserver1 x x ntpserver2 x x ntpserver3 a x x 10.75.156.6 a x x Exit x x x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj</pre> <p>Select appropriate NTP server and edit the details.</p> <pre>lqqqqqqqqqqqu Edit an NTP Server tqqqqqqqqqqqk x x x Address: 10.75.156.6 x x Hostname (optional): x x Options: iburst x x x x lqqqqk lqqqqqqqqk x x x OK x x Cancel x x x mqqqqj mqqqqqqqqj x x x x x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj</pre> <p>Enter appropriate data and click OK.</p> <p>Click Exit to return to the platcfg menu.</p>
---	---	--

Procedure 11. Configure SOAM TVOE Server Blades

<p>13</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Configure time zone</p>	<pre>\$ sudo su - platcfg</pre> <p>Navigate to Server Configuration -> Time Zone.</p>    <p>If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction.</p> <p>Click Edit.</p>  <p>Select the desired time zone from the list and click Enter.</p> <p>Continue clicking Exit until you are out of the platcfg program.</p>
<p>14</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Reboot</p>	<p>Reboot the server by executing the following command:</p> <pre>\$ sudo init 6</pre>
<p>15</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Repeat procedure for other TVOE blades</p>	<p>Configuration of this TVOE server blade is complete. Repeat this procedure from the beginning for other TVOE hosts that need to be configured.</p>
<p>16</p> <p><input type="checkbox"/></p>	<p>Install SDS (optional)</p>	<p>If this deployment contains SDS, SDS can now be installed.</p> <p>Refer to document referenced in [4] SDS SW Installation and Configuration Guide, E79531.</p>

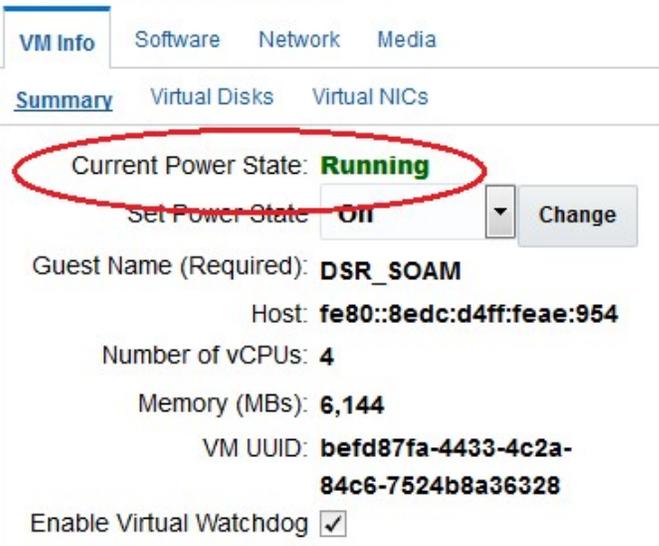
Procedure 12. Create SOAM Guest VMs

<p>S T E P #</p>	<p>This procedure creates a DSR SOAM virtual machine (referred to as a guest) on a TVOE server blade. It must be repeated for every SOAM server you want to install.</p> <p>Prerequisite: TVOE has been installed and configured on the target blade server.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser, navigate to the PMAC GUI, and enter a URL of:</p> <div data-bbox="446 527 1302 577" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<pmac_network_Network_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 12. Create SOAM Guest VMs

2 <input type="checkbox"/>	PMAC GUI: Navigate to VM management of the target server blade	Navigate to Main Menu -> VM Management . Select the TVOE server blade server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window. Click Create Guest .
-------------------------------	--	---

Procedure 12. Create SOAM Guest VMs

<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Wait for guest creation to complete</p>	<p>Navigate to Main Menu -> Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you have launched.</p> <p>Wait or refresh the screen until you see that the guest creation task has completed successfully.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify guest machine is running</p>	<p>Navigate to Main Menu -> VM Management.</p> <p>Select the TVOE server blade on which the guest machine was just created.</p> <p>Look at the list of guests present on the blade and verify that you see a guest that matches the name you configured and that its status is Running.</p> <p>View guest DSR_SOAM</p>  <p>VM Creation for this guest is complete. Repeat from step 2 for any remaining SOAM VMs (for instance, the standby SOAM) that must be created.</p>

Procedure 13. IPM Blades and VMs

<p>S T E P #</p>	<p>This procedure installs TPD on blade servers and blade server guest VMS.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • Enclosures containing the blade servers targeted for IPM that have been configured. • TVOE has been installed and configured on blade servers that will host DSR NOAM VMs. • DSR NOAM and SOAM guest VMs have been created successfully. <p>Needed material:</p> <ul style="list-style-type: none"> • TPD Media (64-bits) <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
	<p>1</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>

Procedure 13. IPM Blades and VMs

<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Select servers for OS install</p>	<p>Navigate to Software -> Software Inventory.</p> <p>Select the servers (VMs, 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 are highlighted in green.</p> <p>Note: VMs have the text Guest: <VM_GUEST_NAME> underneath the physical blade or RMS that hosts them.</p> <p>Click Install OS.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Initiate OS install</p>	<p>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.</p> <p>Click Start Software Install.</p> <p>When a confirmation screen displays, click OK to proceed.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Monitor OS install</p>	<p>Navigate to Main Menu -> Task Monitoring to monitor the progress of the OS Installation background task. A separate task displays for each blade affected.</p> <p>When the installation is complete, the task changes to green and the progress bar indicates 100%.</p>

Procedure 14. Install the Application Software

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure installs Diameter Signaling Router on the blade servers.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser, navigate to the PMAC GUI, and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<pmac_network_Network_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 14. Install the Application Software

<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Select servers for application install</p>	<p>Navigate to Software -> Software Inventory.</p> <p>Select the servers on which the application is to be installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows are highlighted in green.</p> <p>Note: VMs have the text Guest: <VM_GUEST_NAME> underneath the physical blade that hosts them.</p> <p>Click Upgrade.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Initiate application install</p>	<p>The left side of this screen shows the servers affected by this application installation. From the list of available bootable images on the right side of the screen, select one application image to install to all of the selected servers.</p> <p>Click Start Software Upgrade.</p> <p>When a confirmation screen displays, click OK to proceed with the install.</p>

4.3.2 Configure SOAMs

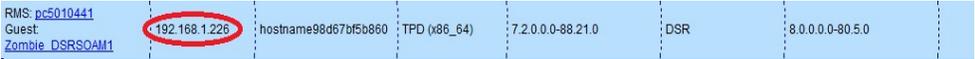
Procedure 15. Configure SOAM NE

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures the SOAM network element.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 15. Configure SOAM NE

2 <input type="checkbox"/>	NOAM VIP GUI: Create the SOAM network element using an XML file	<p>Navigate to Main Menu->Networking -> Networks.</p> <p>Refer to Appendix A: Sample Network Element and Hardware Profiles for a sample network element xml file</p> <p>Click Browse and type the pathname to the SOAM network XML file.</p> <p>Click Upload File to upload the XML file and configure the SOAM network element.</p> <p>Once the data has been uploaded, a tab displays with the name of your network element. Click this folder to display the list of individual networks now configured.</p>
-------------------------------	---	--

Procedure 16. Configure the SOAM Servers

<p>S T E P #</p>	<p>This procedure configures the SOAM servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Exchange SSH keys between SOAM site's local PMAC and the SOAM server</p>	<p>Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.</p>  <p>Note the IP address for the SOAM server.</p> <p>Log into the PMAC terminal as the admusr.</p> <p>From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the SOAM server using the keyexchange utility, using the Control network IP address for the SOAM server. When asked for the password, type the password for the admusr.</p> <pre>\$ keyexchange admusr@<SO1_Control_IP Address></pre>
<p>2 <input type="checkbox"/></p>	<p>Exchange SSH keys between NOAM and PMAC at the SOAM site (if necessary)</p>	<p>Note: If this SOAM shares the same PMAC as the NOAM, then you can skip this step.</p> <p>From a terminal window connection on the NOAM VIP, as the admusr, exchange SSH keys for admusr between the NOAM and the PMAC for this SOAM site using the keyexchange utility.</p> <p>When asked for the password, enter the admusr password for the PMAC server.</p> <pre>\$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address></pre>

Procedure 16. Configure the SOAM Servers

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:</p> <div data-bbox="406 310 1263 359" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<NOAM_XMI_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Insert the 1st SOAM server</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <div data-bbox="406 1312 747 1564" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> </div> <p>Click Insert to insert the 1st SOAM server into servers table (the first or server).</p> <p>Enter the fields as follows:</p> <p>Hostname: <code><Hostname></code> Role: SYSTEM OAM System ID: <code><Site System ID></code> Hardware Profile: <code>DSR TVOE Guest</code> Network Element Name: [Choose NE from Drop Down Box]</p>

Procedure 16. Configure the SOAM Servers

		<p>The network interface fields become available with selection choices based on the chosen hardware profile and network element</p> <p>Type the server IP addresses for the XMI network. Select XMI for the interface. Leave the VLAN checkbox unchecked.</p> <p>Type the server IP addresses for the IMI network. Select IMI for the interface. Leave the VLAN checkbox unchecked.</p> <p>Next, add the following NTP servers:</p> <table border="1" data-bbox="428 1211 1312 1297"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><TVOE_XMI_IP_Address(SO1)></td> <td>Yes</td> </tr> </tbody> </table> <p>Click OK when you have completed entering all the server data.</p>	NTP Server	Preferred?	<TVOE_XMI_IP_Address(SO1)>	Yes
NTP Server	Preferred?					
<TVOE_XMI_IP_Address(SO1)>	Yes					

Procedure 16. Configure the SOAM Servers

5 <input type="checkbox"/>	NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <p>From the GUI screen, select the SOAM server and click Export to generate the initial configuration data for that server.</p>
6 <input type="checkbox"/>	NOAM VIP: Copy configuration file to 1 st SOAM server	<p>Obtain a terminal session to the NOAM VIP as the admusr user.</p> <p>Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the NOAM to the 1st SOAM server, using the Control network IP address for the 1st SOAM server.</p> <p>The configuration file has a filename like TKLCConfigData.<hostname>.sh.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo awpushcfg</pre> <p>The awpushcfg utility is interactive, so the user is asked for the following:</p> <ul style="list-style-type: none"> • IP address of the local PMAC server: Use the management network address from the PMAC. • Username: Use admusr • Control network IP address for the target server: In this case, enter the control IP for the 1st SOAM server. • Hostname of the target server: Enter the server name configured in step 4.

Procedure 16. Configure the SOAM Servers

<p>7</p> <p><input type="checkbox"/></p>	<p>1st SOAM Server: Verify awpushcfg was called and reboot the server</p>	<p>Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the NOAM VIP terminal console.</p> <pre style="border: 1px solid black; padding: 5px;">\$ ssh admusr@<SO1_Control_IP></pre> <p>Login as the admusr user.</p> <p>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server.</p> <p>Verify awpushcfg was called by checking the following file.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify the following message is displayed:</p> <pre style="border: 1px solid black; padding: 5px;">[SUCCESS] script completed successfully!</pre> <p>Now reboot the server.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo init 6</pre> <p>Wait for the server to reboot.</p>				
<p>8</p> <p><input type="checkbox"/></p>	<p>1st SOAM Server: Verify server health</p>	<p>Execute the following command on the 1st SOAM server and make sure that no errors are returned:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>				
<p>9</p> <p><input type="checkbox"/></p>	<p>Insert and Configure the 2nd SOAM server</p>	<p>Repeat this procedure to insert and configure the 2nd SOAM server:</p> <table border="1" data-bbox="428 1283 1300 1367"> <thead> <tr> <th style="background-color: #e1eef6;">NTP Server</th> <th style="background-color: #e1eef6;">Preferred?</th> </tr> </thead> <tbody> <tr> <td style="background-color: #e1eef6;"><TVOE_XMI_IP_Address(SO2)></td> <td style="background-color: #e1eef6;">Yes</td> </tr> </tbody> </table> <p>Instead of data for the 1st SOAM server, insert the network data for the 2nd SOAM server, transfer the TKLCConfigData file to the 2nd SOAM server, and reboot the 2nd SOAM server when prompted at a terminal window.</p>	NTP Server	Preferred?	<TVOE_XMI_IP_Address(SO2)>	Yes
NTP Server	Preferred?					
<TVOE_XMI_IP_Address(SO2)>	Yes					
<p>10</p> <p><input type="checkbox"/></p>	<p>Install Netbackup client software on SOAMs (optional)</p>	<p>If you are using NetBackup at this site, then execute Procedure 13. IPM Blades and VMs again to install the NetBackup Client on all SOAM servers.</p>				

Procedure 17. Configure the SOAM Server Group

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures the SOAM server group.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<NOAM_XMI_VIP_IP_Address>">http://<NOAM_XMI_VIP_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

Procedure 17. Configure the SOAM Server Group

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

Procedure 17. Configure the SOAM Server Group

3 <input type="checkbox"/>	NOAM VIP GUI: Edit the SOAM server group and add a VIP address	<p>From the GUI, navigate to Main Menu -> Configuration -> Server Groups.</p> <p>Select the new SOAM server group and click Edit.</p> <p>Add both SOAM servers to the server group primary site by marking the Include in SG checkbox.</p> <p>Do not check any of the Preferred Spare checkboxes.</p> <p>Click Apply.</p> <p>Add a SOAM VIP by clicking Add. Type the VIP Address and click OK.</p>
-------------------------------	--	---

Procedure 17. Configure the SOAM Server Group

<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Edit the SOAM server group and add preferred spares for site redundancy (optional)</p>	<p>If the Two Site Redundancy feature is wanted for the SOAM server group, add a SOAM server that is located in its server group secondary site by marking the Include in SG checkbox. Also, check the Preferred Spare checkbox.</p> <table border="1" data-bbox="467 342 1286 657"> <thead> <tr> <th>Server</th> <th>SG Inclusion</th> <th>Preferred HA Role</th> </tr> </thead> <tbody> <tr> <td>ZombieSOAM1</td> <td><input checked="" type="checkbox"/> Include in SG</td> <td><input type="checkbox"/> Prefer server as spare</td> </tr> <tr> <td>ZombieSOAM2</td> <td><input checked="" type="checkbox"/> Include in SG</td> <td><input type="checkbox"/> Prefer server as spare</td> </tr> <tr> <td>ZombieSOAMsp</td> <td><input checked="" type="checkbox"/> Include in SG</td> <td><input checked="" type="checkbox"/> Prefer server as spare</td> </tr> </tbody> </table> <p>If the Three Site Redundancy feature is wanted for the SOAM server group, add an additional SOAM server that is located in its server group tertiary site by marking the Include in SG checkbox. Also, check the Preferred Spare checkbox.</p> <p>Note: The preferred spare servers must be server group secondary and tertiary sites. There should be servers from three separate sites (locations).</p> <p>For more information about server group secondary site, tertiary site, or site redundancy, see the 1.3 Terminology section.</p>	Server	SG Inclusion	Preferred HA Role	ZombieSOAM1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	ZombieSOAM2	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	ZombieSOAMsp	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role												
ZombieSOAM1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare												
ZombieSOAM2	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare												
ZombieSOAMsp	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare												
<p>5</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Edit the SOAM server group and add additional SOAM VIPs (optional)</p>	<p>Add additional SOAM VIPs by clicking Add. Type the VIP Address and click OK.</p> <p>Note: Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.</p>												
<p>6</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Wait for remote database alarm to clear</p>	<p>Wait for the Remote Database re-initialization in progress alarm to clear before proceeding.</p> <p>Navigate to Main Menu->Alarms & Events->View Active.</p>												

Procedure 18. Activate PCA (PCA Only)

S	This procedure activates PCA.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	(PCA Only) Activate PCA Feature	<p>If you are installing PCA, execute applicable procedures (added SOAM site activation or complete system activation) from [9] DSR PCA Activation Guide, E81528 to activate PCA.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online.</p> <p>Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.</p>

Procedure 19. Activate DCA (DCA Only)

S	This procedure activates DCA.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	(DCA Only) Activate PCA Feature	<p>If you are installing DCA, execute procedures [14] to activate DCA Framework and Feature.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online.</p> <p>Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.</p>

4.4 Configure MP Servers

4.4.1 Configure MP Blade Servers

Procedure 20. Configure MP Blade Servers

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures MP blade servers (IPFE, SBR, SS7-MP, DA-MP).</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 20. Configure MP Blade Servers

2 <input type="checkbox"/>	NOAM VIP GUI: Navigate to signaling network configuration screen	Navigate to Main Menu -> Configuration -> Networking -> Networks. Select the associated SOAM tab for the MP server. Click Insert in the lower left corner.
-------------------------------	--	---

Procedure 20. Configure MP Blade Servers

additional service to networks mapping

Click **Edit**.

Set the services according to one of these scenarios:

- If the dual path HA configuration is required:
 - Set up the inter-NE network to the XMI network
 - Set up the intra-NE network to the IMI network for HA_MP secondary.

This configuration uses the XMI network as a secondary path to preserve the HA status of SBRs grouped between multiple sites. If the primary HA path **SBR DB Replication Network** becomes lost or impaired, the XMI network preserves the HA state and prevents the servers from entering into a scenario known as **HA Split-Brain**. Preventing HA Split-Brain keeps the existing database in sync, but the DSR mate site is isolated from the active SBR and results in traffic loss until SBR DB replication network is restored.

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

The screenshot shows a configuration table with three rows and two columns of dropdown menus. The first row is for 'HA_MP_Secondary', with 'INTERNALIMI' in the first dropdown and 'INTERNALXMI' in the second. The second row is for 'Replication_MP', with 'INTERNALIMI' in the first dropdown and 'Replication' in the second. The third row is for 'ComAgent', with 'INTERNALIMI' in the first dropdown and 'Replication' in the second.

- If the dual path HA configuration is NOT required:
 - Set up the inter-NE network to SBR DB replication (configured in step 5).
 - Set up the intra-NE network to the IMI network for HA_MP secondary.

This condition allows an **HA Split-Brain** condition between the SBRs if the SBR DB replication network becomes lost or impaired. During an HA Split-Brain condition, an active SBR server exists at each site, but the database is not in sync between the SBRs.

Procedure 20. Configure MP Blade Servers

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

Click **OK** to apply the Service-to-Network selections.

Note: It is recommended that dual-path HA heartbeats be enabled in support of geo-diverse SBRs. This requires participating servers to be attached to at least two routable networks.

Note: For **HA_MP_Secondary**, it is recommended the **Inter-NE Network** be set as the PCA replication network (configured in step 5) or the XMI network and **Intra-NE Network** be set as the IMI network.

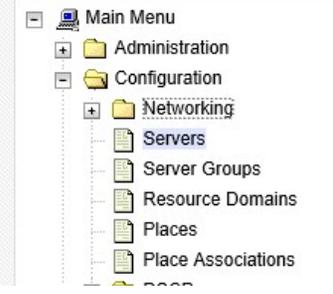
Procedure 20. Configure MP Blade Servers

<p>7</p> <p><input type="checkbox"/></p>	<p>PMAC: Exchange SSH keys between MP site's local PMAC and the MP server</p>	<p>Use the MP site's PMAC GUI to determine the Control Network IP address of the blade server that is to be an MP server. From the MP site's PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.</p> <p>Note the IP address for an MP server.</p> <p>Login to the MP site's PMAC terminal as the admusr.</p> <p>From a terminal window connection on the MP site's PMAC as the admusr.</p> <p>Exchange SSH keys for admusr between the PMAC and the MP blade server using the keyexchange utility, using the Control network IP address for the MP blade server.</p> <pre>\$ keyexchange admusr@<MP_Control_Blade_IP Address></pre> <p>When prompted for the password, enter the password for the admusr user of the MP server.</p>
--	--	---

Procedure 20. Configure MP Blade Servers

<p>8</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Insert the MP server (Part 1)</p>	<p>Before creating the MP blade server, first identify the hardware profile</p> <p>Hardware Profile: In the following step, you select the profile that matches your MP physical hardware and enclosure networking environment.</p> <p>Note: You must go through the process of identifying the enclosure switches, mezzanine cards and Ethernet interfaces of the network prior and blade(s) used before selecting the profile.</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #d9e1f2;"> <th style="padding: 5px;">Profile Name</th> <th style="padding: 5px;">Number of Enclosure Switches (Pairs)?</th> <th style="padding: 5px;">Bonded Signaling Interfaces?</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">1-Pair</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">Yes</td> </tr> <tr> <td style="padding: 5px;">2-Pair</td> <td style="padding: 5px;">2</td> <td style="padding: 5px;">Yes</td> </tr> <tr> <td style="padding: 5px;">3-Pair-bonded</td> <td style="padding: 5px;">3</td> <td style="padding: 5px;">Yes</td> </tr> <tr> <td style="padding: 5px;">3-Pair-un-bonded</td> <td style="padding: 5px;">3</td> <td style="padding: 5px;">No</td> </tr> </tbody> </table> <p>Note: If none of the above profiles properly describe your MP server blade, then you create your own in a text editor (see Figure 7 of Appendix A: Sample Network Element and Hardware Profiles) and copy it into the /var/TKLC/appworks/profiles/ directory of the active NOAM server, the standby NOAM server, and both the DR NOAM servers (if applicable).</p> <p>Note: After transferring the above file, set the proper file permission by executing the following command:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre style="font-family: monospace; font-size: 0.9em;">\$ sudo chmod 777 /var/TKLC/appworks/profiles/<profile name></pre> </div> <p>Make note of the profile used here since it is used in server creation in the following step.</p>	Profile Name	Number of Enclosure Switches (Pairs)?	Bonded Signaling Interfaces?	1-Pair	1	Yes	2-Pair	2	Yes	3-Pair-bonded	3	Yes	3-Pair-un-bonded	3	No
Profile Name	Number of Enclosure Switches (Pairs)?	Bonded Signaling Interfaces?															
1-Pair	1	Yes															
2-Pair	2	Yes															
3-Pair-bonded	3	Yes															
3-Pair-un-bonded	3	No															

Procedure 20. Configure MP Blade Servers

<p>9</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Insert the MP server (Part 2)</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>Click Insert to insert the new MP server into servers table.</p> <p>Enter the following values:</p> <p>Hostname: <Hostname> Role: MP Network Element Name: [Choose NE from Drop Down Box] Hardware Profile: Select the profile that matches your MP physical hardware and enclosure networking environment from step 8. Location: <Enter an optional location description></p> <p>The interface configuration form displays.</p> <p>Note: If networks have been configured previously, but are not required on the server, simply remove the populated network IP from the IP address field and this device is not created on the server.</p> <p>Type the IP addresses for all networks. Select the correct bond or interface. Ensure the correct bond and VLAN tagging (if required) is selected.</p> <p>Optional: If dedicated network for SBR replication has been defined, enter the SBR replication IP address. Select the proper bond or interface, and select the VLAN checkbox if VLAN tagging is required.</p>
--	---	--

Procedure 20. Configure MP Blade Servers

<p>10</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Insert the MP server (Part 3)</p>	<p>Next, add the following NTP servers:</p> <table border="1" data-bbox="472 279 1411 449"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><TVOE_XMI_IP_Address(SO1)></td> <td>Yes</td> </tr> <tr> <td><TVOE_XMI_IP_Address(SO2)></td> <td>No</td> </tr> <tr> <td><MP_Site_PMAC_TVOE_IP_Address></td> <td>No</td> </tr> </tbody> </table> <p>Note: For multiple enclosure deployments, prefer the SOAM TVOE Host that is located in the same enclosure as the MP server.</p> <p>Click OK when all fields are entered to finish MP server insertion.</p>	NTP Server	Preferred?	<TVOE_XMI_IP_Address(SO1)>	Yes	<TVOE_XMI_IP_Address(SO2)>	No	<MP_Site_PMAC_TVOE_IP_Address>	No
NTP Server	Preferred?									
<TVOE_XMI_IP_Address(SO1)>	Yes									
<TVOE_XMI_IP_Address(SO2)>	No									
<MP_Site_PMAC_TVOE_IP_Address>	No									
<p>11</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Export the configuration</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <p>From the GUI screen, select the MP server and click Export to generate the initial configuration data for that server.</p>								
<p>12</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy configuration file to MP server</p>	<p>Obtain a terminal session to the NOAM VIP as the admusr user.</p> <p>Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the MP server, using the Control network IP address for the MP server.</p> <p>The configuration file has a filename like TKLCConfigData.<hostname>.sh.</p> <pre data-bbox="451 1318 1354 1367">\$ sudo awpushcfg</pre> <p>The awpushcfg utility is interactive, so the user is asked for the following:</p> <ul style="list-style-type: none"> • IP address of the local PMAC server: Use the management network address from the PMAC. • Username: Use admusr • Control network IP address for the target server: In this case, enter the control IP for the MP server). • Hostname of the target server: Enter the server name configured in step 9. 								

Procedure 20. Configure MP Blade Servers

13 <input type="checkbox"/>	MP Server: Verify awpushcfg was called and reboot the configured server	<p>Obtain a terminal window connection on the MP server console by establishing an ssh session from the NOAM VIP terminal console.</p> <pre>\$ ssh admusr@<MP_Control_IP></pre> <p>Login as the admusr user.</p> <p>Verify awpushcfg was called by checking the following file:</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify the following message is displayed:</p> <pre>[SUCCESS] script completed successfully!</pre> <p>Reboot the server:</p> <pre>\$ sudo init 6</pre> <p>Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt is displayed.</p>
14 <input type="checkbox"/>	MP Server: Verify server health	<p>After the reboot, login as admusr.</p> <p>Execute the following command as super-user on the server and make sure that no errors are returned:</p> <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 20. Configure MP Blade Servers

<p>15 <input type="checkbox"/></p>	<p>MP Server: Delete auto-configured default route on MP and replace it with a network route via the XMI network-Part1 (optional)</p>	<p>Note: THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK.</p> <p>Not executing this step means a default route is not configurable on this MP and you have to create separate network routes for each signaling network destination.</p> <p>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.</p> <p>Determine <XMI_Gateway_IP> from your SO site network element info.</p> <p>Gather the following items:</p> <ul style="list-style-type: none"> • <NO_XMI_Network_Address> • <NO_XMI_Network_Netmask> • <DR_NO_XMI_Network_Addres> • <DR_NO_XMI_Network_Netmask> • <TVOE_Mgmt_XMI_Network_Address> • <TVOE_Mgmt_XMI_Network_Netmask> <p>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.</p> <p>Proceed to the next step to modify the default routes on the MP servers.</p>
<p>16 <input type="checkbox"/></p>	<p>MP Server: Delete auto-configured default route on MP and replace it with a network route via the XMI network-Part2 (optional)</p>	<p>After gathering the network information from step 15, proceed with modifying the default routes on the MP server.</p> <p>Establish a connection to the MP server and login as admusr.</p> <p>Create network routes to the NO's XMI(OAM) network:</p> <p>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.</p> <pre style="border: 1px solid black; padding: 5px;">\$ 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></pre> <p>Create network routes to the DR NO's XMI (OAM) network:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm add -route=net --address=<DR-NO Site Network ID> --netmask=<<DR-</pre>

Procedure 20. Configure MP Blade Servers

```
NO_Site_Network_Netmask>
--gateway=<MP_XMI_Gateway_IP_Address> --
device=<MP_XMI_Interface>
```

Create network routes to the management server TVOE XMI (OAM) network for NTP:

```
$ sudo /usr/TKLC/plat/bin/netAdm add -route=net
--address=<TVOE_Mgmt_Network_Address>
--netmask=<TVOE_Mgmt_Network_Netmask>
--gateway=<MP_XMI_Gateway_IP_Address> --
device=<MP_XMI_Interface>
```

(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>
```

Repeat for any existing customer NMS stations.

Delete the existing default route:

1. Login to primary NOAM VIP GUI.
2. Navigate to **Configuration -> Networking -> Networks**.
3. Select the respective SOAM tab.
4. Select the XMI network and click **Unlock**. Click **OK** to confirm.
5. Navigate to **Configuration -> Networking -> Routes**.
6. Select the **XMI route** and click **Delete**.
7. Click **OK** to confirm.
8. Repeat steps 1 through 7 for all required MPs to delete the XMI routes.
9. Navigate to **Configuration -> Networking -> Networks**.
10. Select the respective SOAM tab.
11. Select the SMI network and click **Lock**.
12. Click **OK** to confirm.

Procedure 20. Configure MP Blade Servers

<p>17 <input type="checkbox"/></p>	<p>MP Server: Verify connectivity</p>	<p>After steps 15 and 16 have been executed, verify network connectivity. Establish a connection to the MP server and login as admusr. Ping active NO XMI IP address to verify connectivity:</p> <pre style="border: 1px solid black; padding: 5px;">\$ ping <ACTIVE_NO_XMI_IP_Address> PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data. 64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms</pre> <p>(Optional) Ping Customer NMS Station(s):</p> <pre style="border: 1px solid black; padding: 5px;">\$ ping <Customer_NMS_IP> PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data. 64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms</pre> <p>If you do not get a response, then verify your network configuration. If you continue to get failures, then stop the installation and contact Oracle customer support.</p>
<p>18 <input type="checkbox"/></p>	<p>Repeat for remaining MP at all sites</p>	<p>Repeat this entire procedure for all remaining MP blades (SS7-MP, DA-MP, and IPFE).</p>

Procedure 21. Configure Places and Assign MP Servers to Places (PCA/DCA Only)

<p>S T E P #</p>	<p>This procedure adds places in the Policy and Charging DRA network.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div data-bbox="456 541 1312 590" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 21. Configure Places and Assign MP Servers to Places (PCA/DCA Only)

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Assign MP servers to places</p>	<p>Select the place configured in step 2, click Edit.</p> <p>For each place you have defined, select the set of MP servers that are assigned to those places.</p> <p>Check all the checkboxes for PCA DA-MP and SBR servers assigned to this place.</p> <p>Repeat this step for all other DA-MP or SBR servers you want to assign to places.</p> <p>Note: All PCA DA-MPs, SS7MPs, and SBR MPs must be added to the Site Place that corresponds to the physical location of the server.</p> <p>See the Terminology section for more information on sites.</p>
--	---	---

Procedure 22. Configure the MP Server Group(s) and Profile(s)

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures MP server groups.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 22. Configure the MP Server Group(s) and Profile(s)

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Determine server group function</p>	<p>Determine what server group function to configured, make note the following configuration decisions.</p> <table border="1"> <thead> <tr> <th>Server Group Function</th> <th>MPs Will Run</th> <th>Redundancy Model</th> </tr> </thead> <tbody> <tr> <td>DSR (multi-active cluster)</td> <td>Diameter Relay and Application Services</td> <td>Multiple MPs active Per SG</td> </tr> <tr> <td>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>Session Binding Repository</td> <td>Session Binding Repository Function</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>SBR</td> <td>Policy and Charging Session/or Policy Binding Function</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> <p>For PCA application:</p> <ul style="list-style-type: none"> • Online Charging function (only) <ul style="list-style-type: none"> • At least one MP server group with the SBR function must be configured. • At least one MP server group with the DSR (multi-active cluster) function must be configured. • MP server groups with the IP Load Balancer function (IPFE) are optional. • Policy DRA function <ul style="list-style-type: none"> • At least two MP server groups with the SBR function must be configured. One stores Session data and one stores Binding data. • At least one MP server group with the DSR (multi-active cluster) function must be configured. • MP server groups with the IP Load Balancer function (IPFE) are optional. • For DCA application: <ul style="list-style-type: none"> • At least one MP server group with the DSR (multi-active cluster) function must be configured. • At least one MP server group with the Session Binding Repository function may be configured in case of Session-based DCA application. <p>Note: If PCA application is already functional, then an existing Policy and Charging SBR for session SBR may be re-used instead of configuring a new Session Binding Repository.</p> <p>WAN Replication Connection Count:</p> <ul style="list-style-type: none"> • For non-Policy and Charging SBR server groups and Session Binding Repository: Default Value • For Policy and Charging server groups and Session Binding Repository SGs: 8 	Server Group Function	MPs Will Run	Redundancy Model	DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active Per SG	DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP Per SG	Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP Per SG	IP Load Balancer	IPFE application	1 Active MP Per SG	SBR	Policy and Charging Session/or Policy Binding Function	1 Active MP Per SG	SS7-IWF	MAP IWF Application	1 Active MP Per SG
Server Group Function	MPs Will Run	Redundancy Model																					
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active Per SG																					
DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP Per SG																					
Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP Per SG																					
IP Load Balancer	IPFE application	1 Active MP Per SG																					
SBR	Policy and Charging Session/or Policy Binding Function	1 Active MP Per SG																					
SS7-IWF	MAP IWF Application	1 Active MP Per SG																					

Procedure 22. Configure the MP Server Group(s) and Profile(s)

		<p>For the PCA application, the following types of MP server groups must be configured:</p> <ul style="list-style-type: none"> • DA-MP (Function: DSR (multi-active cluster)) • SBR (Function: SBR • IPFE (Function: IP Load Balancer) – Optional) <p>For the DCA application, the following types of MP server groups must be configured:</p> <ul style="list-style-type: none"> • DA-MP (Function: DSR (multi-active cluster)) • SBR (Function: Session Binding Repository) = Optional for Session-less Apps or SBR (Function: SBR assigned to Session Resource Domain) • IPFE (Function: IP Load Balancer) – Optional
<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Enter MP server group data</p>	<p>From the data collected from step 2, create the server group with the following: Navigate to Main Menu ->Configuration ->Server Groups.</p> <p>Select Insert.</p> <p>Enter the following fields:</p> <p>Server Group Name: <Server Group Name> Level: C Parent: [SOAMP server group that is parent to this MP] Function: Select the proper function for this MP server group (gathered in step 2)</p> <p>Click OK when all fields are filled in.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Repeat for additional server groups</p>	<p>Repeat steps 2-3 for any remaining MP server groups you wish to create. For instance, if you are installing IPFE, create an IP Load Balancer server group.</p>

Procedure 22. Configure the MP Server Group(s) and Profile(s)

<p>5 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Edit the MP server groups to include MP blades.</p>	<p>From the GUI, navigate to Main Menu -> Configuration -> Server Groups.</p> <p>Select a server group you just created and click Edit.</p> <p>Select the network element representing the MP server group you want to edit.</p> <p>Click the Include in SG checkbox for every MP server you want to include in this server group. Leave other checkboxes blank.</p> <p>Note: Each IPFE and SS7MP server should be in its own server group.</p> <p>Click OK.</p>
<p>6 <input type="checkbox"/></p>	<p>NOAM VIP GUI: [PCA/DCA Only]</p> <p>Edit the MP server group and add preferred spares for site redundancy (optional)</p>	<p>If two site redundancy for the Policy and Charging SBR server group/Session Binding Repository SBR server group is wanted, add a MP server that is physically located in a separate site (location) to the server group by marking the Include in SG checkbox and the Preferred Spare checkbox.</p> <p>If Three Site Redundancy for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the Include in SG checkbox and the Preferred Spare checkbox for both servers.</p> <p>Note: The Preferred Spare servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations).</p> <p>For more information about site redundancy for Policy and Charging SBR/Session Binding Repository server groups, see the Terminology section.</p> <p>Select OK to save</p>
<p>7 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Repeat for additional server groups</p>	<p>Repeat steps 5- 6 for any remaining MP server groups you need to edit.</p>

Procedure 22. Configure the MP Server Group(s) and Profile(s)

<p>8 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Wait for remote database alarm to clear</p>	<p>Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main Menu->Alarms & Events->View Active.</p>
<p>9 <input type="checkbox"/></p>	<p>SOAM VIP GUI: Login</p>	<p>If not already done, establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="467 617 1325 663" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_SOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 22. Configure the MP Server Group(s) and Profile(s)

10	<input type="checkbox"/> SOAM VIP GUI: Assign Profiles to DA-MPs from SOAM GUI.	<p>Navigate to Main Menu -> Diameter Common ->MPs -> Profile Assignments.</p> <p>Refer to the DA-MP section. If the site has both DSR and MAP-IWF server groups, a DA-MP section and SS7-MP section display.</p> <p>For each MP, select the proper profile assignment based on the MP's hardware type and the function it serves:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e1eef6;"> <th style="text-align: left;">Profile Name</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>G8/G9:Relay</td> <td>G8/G9 DA-MP half height blade running the relay application</td> </tr> <tr> <td>G8/G9:Database</td> <td>G8/G9 DA-MP half height blade running a database application (e.g., FABR, RBAR)</td> </tr> <tr> <td>G8/G9:Session</td> <td>G8/G9 DA-MP half height blade running a session application (e.g., CPA, PCA)</td> </tr> </tbody> </table> <p>Note: If the DA-MPs at this site are configured for Active/Standby, then there is a single selection box visible that assigns profiles for all MPs.</p> <p>When finished, click Assign.</p>	Profile Name	Description	G8/G9:Relay	G8/G9 DA-MP half height blade running the relay application	G8/G9:Database	G8/G9 DA-MP half height blade running a database application (e.g., FABR, RBAR)	G8/G9:Session	G8/G9 DA-MP half height blade running a session application (e.g., CPA, PCA)
Profile Name	Description									
G8/G9:Relay	G8/G9 DA-MP half height blade running the relay application									
G8/G9:Database	G8/G9 DA-MP half height blade running a database application (e.g., FABR, RBAR)									
G8/G9:Session	G8/G9 DA-MP half height blade running a session application (e.g., CPA, PCA)									

Procedure 22. Configure the MP Server Group(s) and Profile(s)

12 <input type="checkbox"/>	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: <div data-bbox="467 310 1325 359" style="border: 1px solid black; padding: 2px;"><code>http://<Primary_NOAM_VIP_IP_Address></code></div> Login as the guiadmin user.
--------------------------------	--------------------------------	--

Procedure 22. Configure the MP Server Group(s) and Profile(s)

13 <input type="checkbox"/>	NOAM VIP GUI: Restart MP blade servers	<p>Navigate to Main Menu->Status & Manage->Server.</p> <p>For each MP server:</p> <ul style="list-style-type: none"> • Select the MP server. • Click Restart. • Click OK on the confirmation screen. Wait for the message that tells you that the restart was successful. <p>Note: Policy and Charging DRA installations/DCA installations: You may continue to see alarms related to ComAgent until you complete the PCA/DCA installation.</p>
14 <input type="checkbox"/>	NOAM VIP: Clear DA_MP_Leader alarm	<p>Active/Standby DA-MP Configurations Only:</p> <p>If DSR (active/standby pair) server group function was configured for the DA-MPs, execute this step.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DA-MP Server Hostname>'" Server_ID NodeID ClusterID 7 ZombieDAMP2 C2479</pre> <p>Using the ClusterID above, enter the following:</p> <pre style="border: 1px solid black; padding: 5px;">\$ echo "<Cluster_ID> DA_MP_Leader Yes" iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</pre>

Procedure 23. Add VIP for Signaling Networks (Active/Standby Configurations Only)

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures the VIPs for the signaling networks on the MPs.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 23. Add VIP for Signaling Networks (Active/Standby Configurations Only)

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Edit the MP server group and add VIPs (only for 1+1)</p>	<p>IF YOUR MPs ARE IN A DSR MULTI-ACTIVE CLUSTER SERVER GROUP CONFIGURATION (N+0), THEN SKIP THIS STEP.</p> <p>From Main Menu->Configuration->Server Groups.</p> <p>Select the MP server group and click Edit.</p> <p>Click Add to add the VIP for XSI1. Enter the VIP of int-XSI-1 and click Apply. Click Add again to add the VIP for XSI2. Enter the VIP of int-XSI-2 and click Apply. If more signaling networks exist, add their corresponding VIP addresses. Click OK.</p>
--	--	--

4.4.2 Configure Signaling Network Routes

Procedure 24. Configure the Signaling Network Routes

S T E P #	<p>This procedure configures signaling network routes on MP-type servers (DA-MP, IPFE,SS7-MP, etc.)</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<Primary_NOAM_VIP_IP_Address>">http://<Primary_NOAM_VIP_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

Procedure 24. Configure the Signaling Network Routes

2 <input type="checkbox"/>	NOAM VIP GUI: Navigate to routes configuration screen	Navigate to Main Menu -> Configuration -> Network -> Routes . Select the MP server group tab on the top row and verify the Entire Server Group link is selected; if not, select the link.
3 <input type="checkbox"/>	NOAM VIP GUI: Add route	Click Insert at the bottom of the screen to add additional routes.

Procedure 24. Configure the Signaling Network Routes

<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Add default route for mps going through signaling network gateway (optional)</p>	<p>Optional – Execute this step only if you performed Procedure 20. Configure MP Blade Servers step 10, which removed the XMI gateway default route on MPs.</p> <p>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.</p> <p>Route Type: Default</p> <p>Device: Select the signaling device that is directly attached to the network where the XSI default gateway resides.</p> <p>Gateway IP: The XSI gateway you wish to use for default signaling network access.</p> <p>Click OK.</p>
--	--	---

Procedure 24. Configure the Signaling Network Routes

5 <input type="checkbox"/>	NOAM VIP GUI: Add Network Routes for Diameter Peers	<p>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.</p> <p>Route Type: Net, Default, Host Device: Select the appropriate signaling interface that is 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 (if configuring Net routes). 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.</p> <p>If you have more routes to enter, click Apply to save the current route entry and repeat this step to enter more routes</p> <p>If you are finished entering routes, click OK to save the latest route and leave this screen.</p> <p>Layer 3 Configurations Aggregation Switch Configurations Only: 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 vary):</p> <p>Add routes (IPv4 & IPv6):</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo netConfig --device=switch1A addRoute network=10.10.10.0/24 nexthop=10.50.76.81 \$ sudo netConfig --device=switch1A addRoute network6=2001::/64 nexthop=fd0f::1</pre> <p>Delete routes (IPv4 & IPv6):</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo netConfig --device=switch1A deleteRoute network=10.10.10.0/24 nexthop=10.50.76.81 \$ sudo netConfig -device=switch1A deleteRoute network6=2001::/64 nexthop=fd0f::1</pre>
-------------------------------	--	---

Procedure 24. Configure the Signaling Network Routes

6 <input type="checkbox"/>	Local PMAC: Perform a netConfig backup	<p>After the routes are added to the aggregation switches via netconfig, perform a netconfig backup so the new routes are retained in the backup.</p> <p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ netConfig backupConfiguration --device=<Switch Hostname service=<ssh_Service> filename=<Backup Filename></pre> <p>Copy the files to the backup directory:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /bin/mv -i ~<switch_backup_user>/<switch_name>- backup* /usr/TKLC/smac/etc/switch/backup</pre>
7 <input type="checkbox"/>	NOAM VIP GUI: Repeat for all other MP server groups	<p>The routes entered in this procedure should now be configured on all MPs in the server group for the first MP you selected.</p> <p>If you have additional MP server groups, repeat from step 2, but this time, select an MP from the next MP server group.</p> <p>Continue until you have covered all MP server groups. This includes DAMP, IPFE, and SS7MP servers.</p> <p>Note: IPFE and DAMP servers must have the same routes configured.</p>

4.4.3 Configure DSCP (Optional)

Procedure 25. Configure DSCP Values for Outgoing Traffic

<p>S T E P #</p>	<p>This procedure configures the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network uses packet DSCP markings for quality-of-service purposes.</p> <p>Note: If your enclosure switches already have DSCP configuration for the signaling VLANs, then the switch configuration 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.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 25. Configure DSCP Values for Outgoing Traffic

<p>2 ☐</p>	<p>NOAM VIP GUI: Option 1: Configure interface DSCP</p>	<p>Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site vary.</p> <p>Navigate to Main Menu -> Configuration -> DSCP -> Interface DSCP.</p> <p>Select the server you want 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.</p> <p>Click Insert.</p> <p>Main Menu: Configuration -> DSCP -> Interface DSCP</p>  <p>Select the network interface from the drop down box. Enter the DSCP value you wish to have applied to packets leaving this interface and select the transport protocol.</p> <p>Click OK if there are no more interfaces on this server to configure, or click Apply to finish this interface and continue with more interfaces by selecting them from the drop down and entering their DSCP values.</p>
----------------	--	--

Procedure 25. Configure DSCP Values for Outgoing Traffic

<p>3 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Option 2: Configure port DSCP</p>	<p>Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site vary.</p> <p>Navigate to Main Menu -> Configuration -> DSCP -> Port DSCP.</p> <p>Select the server you want 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.</p> <p>Click Insert.</p> <p>Enter the source port, DSCP value, and select the transport protocol.</p> <p>Click OK if there are no more port DSCPs on this server to configure, or Apply to finish this port entry and continue entering more port DSCP mappings.</p>
<p>4 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Repeat for additional servers</p>	<p>Repeat steps 2-3 for all remaining servers.</p>

4.4.4 Configure IP Front End Servers (Optional)

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure configures IP Front End (IPFE), and optimize performance.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_SOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

<p>2</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Configuration of replication IPFE association data</p>	<p>Navigate to Main Menu -> IPFE -> Configuration -> Options.</p> <p>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</p> <p>If applicable, enter the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields.</p> <p>Note: It is recommended that the address reside on the IMI (Internal Management Interface) network.</p> <p>Note: IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2.</p> <p>Note: Accept default configuration for remaining entries.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Configuration of IPFE target sets, Part 1 (insert target set)</p>	<p>Navigate to Main Menu -> IPFE -> Configuration -> Target Sets.</p> <p>Click either Insert IPv4 or Insert IPv6 depending on the IP version of the target set you plan to use.</p>

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

4 <input type="checkbox"/>	SOAM VIP GUI: Configure IPFE target sets, Part 2 (target set configuration)	<p>Continued from the previous step, the following are configurable:</p> <p>Protocols: protocols the target set supports.</p> <p>Delete Age: Specifies when the IPFE should remove its association data for a connection. Any packets presenting a source IP address/port combination that had been previously stored as association state, but have been idle longer than the Delete Age configuration, are treated as a new connection and do not automatically go to the same application server.</p> <p>Load Balance Algorithm: Hash or Least Load options.</p> <p>Note: 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.</p> <p>Note: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.</p> <p>Execute the following command if Hash Load Balance Algorithm was selected above. We recommend you cut and paste to prevent errors.</p> <p>Establish an SSH session to the SOAM VIP, login as admusr.</p> <pre>\$ sudo iset -fvalue="50" DpiOption where "name='MpEngIngressMpsPercentile'" === changed 1 records ===</pre>
-------------------------------	---	---

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

<p>5</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Configuration of IPFE target sets, Part 3 (target set configuration)</p>	<p>Navigate to Main Menu -> IPFE -> Configuration -> Target Sets.</p> <p>(Optional): If you have selected the Least Load algorithm, you may configure the following fields to adjust the algorithm's behavior.</p> <p>MPS Factor – Messages per Second (MPS) is one component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). It is recommended that IPFE connections have Reserved Ingress MPS set to something other than the default, which is 0.</p> <p>To configure Reserved Ingress MPS, navigate 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.</p> <p>Connection Count Factor – This is the other component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern.</p> <p>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.</p>
--	--	---

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

6 <input type="checkbox"/>	SOAM VIP GUI: Configuration of IPFE Target sets-Part 4 (Target Set Configuration)	<p>Primary Public IP Address: IP address for the target set</p> <p>Note: This address must reside on the XSI (External Signaling Interface) network because it is used by the application clients to reach the application servers. This address MUST NOT be a real interface address (that is, must not be associated with a network interface card).</p> <p>Active IPFE: IPFE to handle the traffic for the target set address.</p> <p>Secondary Public IP Address: If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a secondary IP address.</p> <p>Note: A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections will not be multi-homed.</p> <p>Note: If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure that SCTP failover functions as designed.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Click Add to add more application servers (up to 16).</p> <p>Click Apply.</p>
-------------------------------	---	---

Procedure 26. Procedure 26: IP Front End (IPFE) Configuration

7	<input type="checkbox"/> SOAM VIP GUI: Repeat for additional configuration of IPFE target sets.	Repeat steps 3-6 for each target set (up to 16). At least one target set must be configured.
---	--	--

4.5 SNMP Configuration

Procedure 27. Configure SNMP Trap Receiver(s)

S	This procedure configures forwarding of SNMP Traps from each individual server.	
T	Note: If SNMP configuration is not required, skip to step 6.	
E	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
P		
#	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
1	<input type="checkbox"/> 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: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>http://<Primary_NOAM_VIP_IP_Address></code> </div> Login as the guiadmin user.

Procedure 27. Configure SNMP Trap Receiver(s)

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Configure system-wide SNMP trap receiver(s)</p>	<p>Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping.</p> <p>Select the Server Group tab for SNMP trap configuration:</p> <p>Type 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.</p> <p>Continue to type additional secondary, tertiary, etc., manager IPs in the corresponding slots if desired.</p> <p>Check Traps Enabled checkboxes for the manager servers being configured:</p> <p>Enter the SNMP Community Name.</p> <p>Leave all other fields at their default values. Click OK.</p>
--	---	---

Procedure 27. Configure SNMP Trap Receiver(s)

4	PMAC GUI: Login	Open web browser, navigate to the PMAC GUI, and enter a URL of: <div data-bbox="422 279 1279 327" style="border: 1px solid black; padding: 2px;"><code>http://<pmac_network_Network_IP_Address></code></div> Login as the guiadmin user.
---	---------------------------	---

Procedure 27. Configure SNMP Trap Receiver(s)

<p>6</p> <p><input type="checkbox"/></p>	<p>(Workaround)</p> <p>NOAM VIP</p> <p>GUI: Login</p>	<p>Note: Perform this workaround step only in the following cases:</p> <ul style="list-style-type: none"> • If SNMP is not configured (i.e., if above steps 1-6 are skipped). • If SNMP is already configured and SNMPv3 is selected as enabled version. <p>Note: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3.</p> <p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>7</p> <p><input type="checkbox"/></p>	<p>NOAM VIP</p> <p>GUI:</p> <p>Configure system-wide SNMP trap receiver(s)</p>	<p>Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping.</p> <p>Select the Server Group tab for SNMP trap configuration:</p>

Procedure 27. Configure SNMP Trap Receiver(s)

8 <input type="checkbox"/>	PMAC GUI: Login	Open web browser, navigate to the PMAC GUI, and enter a URL of: <div data-bbox="443 279 1299 327" style="border: 1px solid black; padding: 2px;"><code>http://<pmac_network_Network_IP_Address></code></div> Login as the guiadmin user.
-------------------------------	---------------------------	---

4.6.1 IDIH Installation

The installation procedure uses the **fast deployment** utility (fdconfig) bundled with the PMAC server to install and configure IDIH.

Procedure 28. IDIH Configuration

S T E P #	This procedure installs and configures IDIH. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
1 <input type="checkbox"/>	TVOE Host: Load application ISO	Add the Application ISO images (mediation, application, and oracleGuest) to the PMAC, this can be done in one of three ways: <ol style="list-style-type: none"> 1. Insert the Application CD required by the application 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) 4. Using sftp, connect to the PMAC server <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ sftp pmacftpusr@<pmac_management_network_ip> \$ put <image>.iso</pre> </div> 5. After the image transfer is 100% complete, close the connection: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ quit</pre> </div> <p>Note: If there is insufficient disk space with the PMAC repository as pmacftpuser, please follow the “Configure PMAC Application Guest isoimages Virtual Disk” section in [12] Platform 7.2 Configuration Procedure, E64363 to increase it.</p>

Procedure 28. IDIH Configuration

2 <input type="checkbox"/>	PMAC GUI: Login	Open web browser, navigate to the PMAC GUI, and enter a URL of: <div data-bbox="456 279 1398 327" style="border: 1px solid black; padding: 2px;"><code>http://<pmac_network_Network_IP_Address></code></div> Login as the guiadmin user.
-------------------------------	---------------------------	---

Procedure 28. IDIH Configuration

<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Attach the software image to the PMAC guest</p>	<p>If the image is on a CD or USB device, continue with this step. 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.</p> <p>In the PMAC GUI, navigate to Main Menu -> VM Management. Select the PMAC guest from the VM Entities list. On the resulting View VM Guest page, select the Media tab.</p> <p>Under the Media tab, find the ISO image in the Available Media list, and click its Attach button. After a pause, the image displays in the Attached Media list.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Add application image</p>	<p>Navigate to Main Menu -> Software -> Manage Software Images.</p> <p>Click Add Image. Select the image from the list.</p> <p>If the image was supplied on a CD or a USB drive, it displays as a virtual device (device://...). These devices are assigned in numerical order as CD and USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally 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.</p> <p>If in step 1 the image was transferred to PMAC via sftp, it displays in the list as a local file /var/TKLC/...</p> <p>Select the appropriate path and click Add New Image.</p> <p>You may check the progress using the Task Monitoring link. Observe the green bar indicating success.</p> <p>Once the green bar is displayed, remove the DSR application Media from the optical drive of the management server.</p>

Procedure 28. IDIH Configuration

5 <input type="checkbox"/>	PMAC: Establish terminal session	Establish an SSH session to the PMAC and login as admusr .
6 <input type="checkbox"/>	PMAC: Reset create guest default timeout and other timeout parameters	<p>Reset the create guest default timeout.</p> <p>Execute the following commands:</p> <pre data-bbox="456 464 1419 709">\$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=3000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"; \$ sudo pmacadm setParam --paramName=defaultTpdProvTimeout --paramValue=120 \$ sudo pmacadm setParam --paramName=guestDiskDeployTimeout --paramValue=50</pre> <p>To verify whether the above values are set correctly, run the below commands.</p> <pre data-bbox="456 772 1419 947">\$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'select name, value from params where name like "%TIMEOUT%"; \$ sudo pmacadm getParam --paramName=defaultTpdProvTimeout \$ sudo pmacadm getParam --paramName=guestDiskDeployTimeout</pre>
7 <input type="checkbox"/>	PMAC: Copy the fdc.cfg file to the guest-dropin directory	<p>Copy the fdc.cfg file to the pmac guest-dropin directory.</p> <p>Execute the following command:</p> <pre data-bbox="456 1052 1419 1121">\$ sudo cp /usr/TKLC/smac/html/TPD/mediation-*/fdc.cfg /var/TKLC/smac/guest-dropin</pre>
8 <input type="checkbox"/>	PMAC: Configure the fdc.cfg file	<p>Configure the fdc.cfg file. See Appendix I: IDIH Fast Deployment Configuration for a breakdown of the parameters.</p> <p>Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.</p>

Procedure 28. IDIH Configuration

9 <input type="checkbox"/>	PMAC: Run the FDC creation script <code>idihFdc.sh</code>	<p>Rename the <code>fdc.cfg</code> file to your preference; also note that two files are generated by the <code>fdc</code> shell script. One is for the Installation procedure and the other file is used for the upgrade procedure. The upgrade FDC is named <code>upgrade</code>.</p> <p>Example: <code>hostname.cfg</code></p> <p>Note: The following hostname for guests has been reserved for internal use. Please try to avoid them:</p> <ul style="list-style-type: none"> • oracle • mediation • appserver <p>Here are the suggested hostname for guests:</p> <ul style="list-style-type: none"> • <code><server hostname>-ora</code> example, <code>thunderbolt-ora</code> • <code><server hostname>-med</code> example, <code>thunderbolt-med</code> • <code><server hostname>-app</code> example, <code>thunderbolt-app</code> <p>Run the FDC creation script <code>fdc.sh</code>.</p> <p>Execute the following commands:</p> <pre style="border: 1px solid black; padding: 5px;">\$cd /var/TKLC/smac/guest-dropin/ \$sudo /usr/TKLC/smac/html/TPD/mediation-8.0.0.0_80.x.x-x86_64/fdc.sh fdc.cfg</pre> <p>Note: Verify the values in the xml generated from the <code>fdc.sh</code> script match those of the values entered in <code>fdc.cfg</code>.</p>
10 <input type="checkbox"/>	TVOE Host: Verify/Remove external devices	<p>Establish an SSH session to the TVOE host that hosts the IDIH and login as <code>admusr</code>.</p> <p>Before IDIH has ever been installed, or after the external disk removal procedure has been successfully completed:</p> <p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ ls /dev/sd*</pre> <p>Verify you only have <code>sda*</code> devices (e.g., <code>sda1</code>, <code>sda2</code>, etc.)</p> <p>Expected output:</p> <pre style="border: 1px solid black; padding: 5px;">\$ ls /dev/sd* /dev/sda /dev/sda1 /dev/sda2 /dev/sda3</pre> <p>Note: If any other devices are listed (e.g. <code>sdb*</code>, <code>sdc*</code>, <code>sdd*</code>, etc...) Stop. You must first remove the extra device(s) in your system (e.g., <code>sdb*</code>, <code>sdc*</code>, <code>sdd*</code>, etc.). Refer to Appendix J: IDIH External Drive Removal. Reboot the <code>tvoe</code> and verify the extra device(s) are still removed (<code>> ls /dev/sd*</code>)</p>

Procedure 29. Configure DSR Reference Data Synchronization for IDIH

script.	<pre> corsair-app:/usr/TKLC/xIH_apps/trda-config.sh dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace- refdata-ad Please enter DSR oam server IP address: 10.240.39.175 SQL*Plus: Release 12.1.0.2.0 Production on Thu Oct 1 15:04:40 2015 Copyright (c) 1982, 2014, Oracle. All rights reserved. Last Successful login time: Thu Oct 01 2015 13:27:57 -04:00 Connected to: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options SQL> SQL> 2 3 4 5 1 row merged. SQL> Commit complete. SQL> Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Produ With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options Buildfile: /usr/TKLC/xIH/apps/trace-refdata- adapter/build.xml app.disable: common.weblogic.stop: [echo] [echo] [echo] ===== [echo] application: xihtra [echo] date: 2015-10-01 15:04:41 [echo] ===== [echo] === stop application EAR [echo] date: 2015-10-01 15:04:41 [java] weblogic.Deployer invoked with options: - adminurl t3://appserver:7001 - userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop [java] <Oct 1, 2015 3:05:08 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating [java] Task 24 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adap [java] Task 24 completed: [Deployer:149026]stop </pre>
---------	---

Procedure 29. Configure DSR Reference Data Synchronization for IDIH

		<pre> application xIH Trace Reference Data Adap [java] Target state: stop completed on Server nsp [java] BUILD SUCCESSFUL Total time: 29 seconds Buildfile: /usr/TKLC/xIH/apps/trace-refdata- adapter/build.xml app.enable: common.weblogic.start: [echo] [echo] [echo] ===== [echo] application: xihtra [echo] date: 2015-10-01 15:05:10 [echo] ===== [echo] == start application EAR [echo] date: 2015-10-01 15:05:10 [java] weblogic.Deployer invoked with options: - adminurl t3://appserver:7001 - userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start [java] <Oct 1, 2015 3:05:56 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating [java] Task 25 initiated: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Task 25 completed: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Target state: start completed on Server nsp [java] BUILD SUCCESSFUL Total time: 1 minute 17 seconds </pre> <p>For prompt Please enter DSR SOAM server IP address, enter the VIP of the DSR SOAM and click Enter.</p> <p>Note: If the address entered is unreachable the script exits with an Unable to connect to <ip-address>! error.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>IDIH App Server: Monitor completion</p>	<p>Monitor the log file located at:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>/var/TKLC/xIH/log/apps/weblogic/apps/application.log</p> </div> <p>Examine the log file for entries containing text Trace Reference Data Adapter.</p>

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

<p>S This procedure configures SSO domain for IDIH.</p> <p>T Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>E</p> <p>P If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p> <p>#</p>		
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

2 <input type="checkbox"/>	NOAM VIP GUI: Configure DNS	Navigate to Main Menu -> Administration -> Remote Servers -> DNS Configuration. Select the NOAM tab: Configure values for the following fields: <ul style="list-style-type: none">• Domain Name• Name Server• Search Domain 1 If values have already been configured, click Cancel ; otherwise configure the above values and click OK .
-------------------------------	---	---

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Establish SSO local zone</p>	<p>Navigate to Main Menu -> Access Control -> Certification Management.</p> <p>Click Establish SSO Zone.</p> <p>Enter a value for Zone Name:</p> <p>Click OK.</p> <p>Information for the new Certificate type of SSO Local is now displayed.</p> <p>Click Report.</p> <p>The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access.</p> <p>Example of Certificate report:</p> <pre> -----BEGIN CERTIFICATE----- MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV BAYTA1VTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwG T3JhY2x1MQswCQYDVQQQLDAJQVjEQMA4GA1UEAwwHTG1iZXJ0eTETMBEGCSqGSIb3 DQEJARYEdGVzdDAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ BgNVBAYTA1VTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UE CgwGT3JhY2x1MQswCQYDVQQQLDAJQVjEQMA4GA1UEAwwHTG1iZXJ0eTETMBEGCSqG SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQCZ/MpkhlvMP/iJ s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAf BgNVHSMEGDAWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAMBgNVHRMEBTADAQH/MA0G CSqGSIb3DQEBCwUAA0EAOWIqBMEQyvfvvt38r/yfgIx3w5dn8SBwHjHC5TpJrHV6U zFlg5dfzoLz7ditjGohWJ919VRw39LQ81KFp7SMXwA== -----END CERTIFICATE----- </pre>
--	--	--

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

4 <input type="checkbox"/>	IDIH Application Server GUI: Login	Establish a GUI session on the IDIH application server: Login as the idihadmin user:
5 <input type="checkbox"/>	IDIH Application Server GUI: Launch the OAM portal	Navigate to the OAM portal icon to Launch the OAM web application:

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

6 <input type="checkbox"/>	IDIH Application Server GUI: Configure the SSO domain	<p>Navigate to System -> Single Sign On.</p> <p>Select the SSO Parameters tab.</p> <p>Click the Edit Value icon.</p> <p>Enter a value for the Domain Name.</p> <p>Note: This should be the same domain name assigned in the DSR NOAM DNS configuration (step 2).</p> <p>Click the Save icon.</p> <p>Click the Refresh icon to display data saved for the remote zone.</p>
-------------------------------	---	---

Procedure 30. IDIH Configuration: Configuring the SSO Domain (Optional)

7 <input type="checkbox"/>	IDIH Application Server GUI: Configure the SSO remote zone	<p>Navigate to System -> Single Sign On.</p> <p>Select the SSO Zones tab.</p> <p>Click the Add icon.</p> <p>Enter a value for field Remote Name.</p> <p>For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.</p> <p>Click the Save icon.</p> <p>Click the Refresh icon to display the data saved for remote zone.</p>
-------------------------------	--	---

Procedure 31. IDIH Configuration: Configure IDIH in the DSR

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure completes the IDIH integration on the DSR.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 31. IDIH Configuration: Configure IDIH in the DSR

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Configure ComAgent connection</p>	<p>Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers.</p> <p>Click Insert.</p> <p>Add the IDIH mediation server.</p> <p>For the remote server IP address field, type the IMI IP address of the IDIH Mediation Server.</p> <p>For the IP address preference field, type the IP protocol preference (if IPv6 and IPv4 are configured).</p> <p>Set the Remote Server Mode to Server.</p> <p>Select the DA-MP server group from the Available Local Server Groups column.</p> <p>Click the >> button to move the DA-MP server group to the Assigned Local Server Groups column.</p> <p>Click OK.</p>
--	---	--

Procedure 31. IDIH Configuration: Configure IDIH in the DSR

3 <input type="checkbox"/>	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: <div data-bbox="446 310 1299 357" style="border: 1px solid black; padding: 2px;"><code>http://<Primary_SOAM_VIP_IP_Address></code></div> Login as the guiadmin user.
-------------------------------	----------------------------	---

Procedure 32. IDIH Configuration: Configure Mail Server (Optional)

2 <input type="checkbox"/>	IDIH Application Server: Configure the authenticated mail server	Enter the platcfg menu, execute the following command: <pre>\$ sudo su - platcfg</pre> Select Application Server Configuration . Select SMTP Configuration . Click Edit . Enter the following parameters: <ol style="list-style-type: none">1. Mail Server IP Address2. User3. Password4. Email Address (From)5. Mail smtp timeout6. Mail smtp connectiontimeout7. SNMP over SSL used? Click OK . Click Exit to exit the platcfg menu.
-------------------------------	--	--

Procedure 34. IDIH Configuration: Change Network Interface (Optional)

<p>S T E P #</p>	<p>This procedure changes the default network interface.</p> <p>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.</p> <p>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'.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>IDIH Mediation Server: Login</p>	<p>Establish an SSH session to the IDIH mediation server. Login as user admusr.</p> <p>Issue the following commands to login as tekelec user.</p> <pre>\$ sudo su - tekelec</pre>
<p>2 <input type="checkbox"/></p>	<p>IDIH Mediation Server: Execute the change interface script</p>	<p>Execute the change interface script with the following command:</p> <pre>\$ chgIntf.sh</pre> <p>Answer the following questions during execution of the script:</p> <pre>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...</pre>

Procedure 35. IDIH Configuration: Backup the Upgrade and Disaster Recovery FDC File (Optional)

<p>S T E P #</p>	<p>This procedure generates a disaster recovery fdc file.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Identify backup server</p>	<p>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:</p> <ul style="list-style-type: none"> • TVOE • PMAC • DSR NOAM • DSR SOAM
<p>2 <input type="checkbox"/></p>	<p>PMAC: Establish terminal session</p>	<p>Establish an SSH session to the PMAC. Login as admusr.</p>
<p>3 <input type="checkbox"/></p>	<p>PMAC: Verify Upgrade fdc file exists</p>	<p>Execute the following commands to verify the upgrade FDC file for IDIH exists:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /var/TKLC/smac/guest-dropin \$ ls -l *.xml</pre> <p>The following output is expected:</p> <pre style="border: 1px solid black; padding: 5px;">-rw-r----- 1 root smac 9542 May 11 09:43 <idih_install>.xml -rw-r----- 1 root smac 5107 May 11 09:43 <idih_upgrade>.xml</pre> <p>Note: The <idih_upgrade>.xml file is the same file used for upgrade and disaster recovery procedures.</p>
<p>4 <input type="checkbox"/></p>	<p>PMAC: Transfer the FDC file to a remote server</p>	<p>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.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/guest-dropin/<idih_upgrade.xml> /path/to/destination/</pre> <p>When prompted, enter the admusr user password and click Enter.</p> <p>If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system.</p>

Procedure 35. IDIH Configuration: Backup the Upgrade and Disaster Recovery FDC File (Optional)

5	<input type="checkbox"/> PMAC Server: Backup FDC file	Transfer the fdc file to the fdc directory so that the file can be backed up with PMAC backups. Issue the following command to ensure the directory where the backups are stored exists: <pre style="border: 1px solid black; padding: 5px;">\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/fdc</pre> If you receive an error such as the following: <pre style="border: 1px solid black; padding: 5px;">-bash: ls: /usr/TKLC/smac/etc/fdc: No such file or directory</pre> Create the directory by issuing the following command: <pre style="border: 1px solid black; padding: 5px;">\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc</pre> Issue the following command to copy the fdc files to the fdc backup directory: <pre style="border: 1px solid black; padding: 5px;">\$ sudo cp /var/TKLC/smac/etc/<idih_upgrade.xml> /usr/TKLC/smac/etc/fdc/</pre>
---	---	--

Procedure 36. IDIH Configuration: Change Alarm Ignore List (Optional)

S T E P #	This procedure changes the alarm severity and/or identifiers to ignore on the mediation server. Note: Initially the default is to ignore alarms with severity 4 (informational) Note: A script is provided to manage the settings so that the operator does not need to know the details required to apply the settings. There are two settings 'ignore.event' and 'ignore.severity' 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 P: My Oracle Support (MOS) and ask for assistance.	
1	<input type="checkbox"/> IDIH Mediation Server: Login	Establish an SSH session to the IDIH mediation server. Login as user admusr . Issue the following commands to login as tekelec user. <pre style="border: 1px solid black; padding: 5px;">\$ sudo su - tekelec</pre>

Procedure 36. IDIH Configuration: Change Alarm Ignore List (Optional)

<p>2</p> <p><input type="checkbox"/></p> <p>IDIH Mediation Server: Execute the CHANGE INTERFACE SCRIPT</p>	<p>Execute the change alarms script with the following command:</p> <pre>\$ chgAlms.sh</pre> <p>Answer the following questions during execution of the script:</p> <p>This script is used to change ignore list for mediation alarms.</p> <p>There are two lists, one for Severity where the list contains the severity values (no spaces, comma separated). Severity default list = '4'</p> <p>Possible severity values are:</p> <ul style="list-style-type: none"> 1 Critical error 2 Major error 3 Minor error 4 Information only; no error 5 Cleared <p>The other is the event list which contains the (comcol) event numbers (no spaces, comma separated).</p> <p>Please answer the following questions or enter CTRL-C to exit out of the script.</p> <p>Current setting are: ignore.event= ignore.severity=4</p> <p>Enter new ignore list for alarm severity (comma separated list) or '0' to keep current [4]: 0</p> <p>Enter new ignore list for alarm events (comma separated list) or '0' to keep current []: 0</p> <p>Updating configuration properties file with 'ignore.severity=4' and 'ignore.event='</p> <p>Backing-up configuration properties with 'ignore.severity=4' and 'ignore.event='</p> <p>Restarting ImpAlarms process ...</p> <p>Done!</p>
---	---

4.7 Post-Install Activities

4.7.1 Activate Optional Features

Procedure 37. Activate Optional Features

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure installs DSR optional components once regular installation is complete.</p> <p>Prerequisite: All previous DSR installation steps have been completed.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Refer to Activation Guides for optional features</p>	<p>Refer to 3.4 Optional Features for a list of feature activation documents whose procedures are to be executed at this moment.</p>

4.7.2 Configure ComAgent Connections (DSR + SDS)

Procedure 38. Configure ComAgent Connections (DSR + SDS)

S T E P #	<p>This procedure configures ComAgent connections on DSR/SDS for use in the FABR application.</p> <p>Prerequisite: FABR application is activated.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>SDS NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the SDS NOAM by using the XMI VIP address. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_SDS_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 38. Configure ComAgent Connections (DSR + SDS)

2 <input type="checkbox"/>	SDS NOAM VIP GUI: Configure remote server IP address	Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers. Click Insert.
-------------------------------	---	--

Procedure 38. Configure ComAgent Connections (DSR + SDS)

<p>3</p> <p><input type="checkbox"/></p>	<p>SDS NOAM VIP GUI: Configure remote server IP address</p>	<p>Type the Remote Server Name for the DSR MP server:</p> <p>Type the Remote Server IMI IP Address.</p> <p>Note: This should be the IMI IP address of the DAMP server. Select Client for the Remote Server Mode from the list.</p> <p>Select IP Address Preference (ComAgent Network Preference, IPv4 Preferred, or IPv6 Preferred) from the list.</p> <p>Select the Local Server Group for the SDS DP server group and click >>.</p> <p>Click Apply.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>SDS NOAM VIP GUI: Repeat</p>	<p>Repeat steps 2-3 for each remote MP in the same SOAM NE.</p>

Procedure 38. Configure ComAgent Connections (DSR + SDS)

<p>5</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Login</p>	<p>Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="412 310 1268 359" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_DSR_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Configure remote server IP address</p>	<p>Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers.</p> <p>Click Insert.</p>

Procedure 38. Configure ComAgent Connections (DSR + SDS)

<p>7 <input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Configure remote server IP address</p>	<p>Type the Remote Server Name for the SDS DP server:</p> <p>Type the Remote Server IMI IP Address.</p> <p>Note: This should be the IMI IP address of the DP server. Select Server for the Remote Server Mode from the list.</p> <p>Select IP Address Preference (ComAgent Network Preference, IPv4 Preferred, or IPv6 Preferred) from the list.</p> <p>Select the Local Server Group for the DSR MP server group, click >>.</p> <p>Click Apply.</p>
<p>8 <input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Repeat</p>	<p>Repeat steps 6-7 for each remote DP in the same SOAM NE.</p>

Procedure 38. Configure ComAgent Connections (DSR + SDS)

<p>9</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Configure Connection Groups</p>	<p>Navigate to Main Menu -> Communication Agent -> Configuration -> Connection Groups.</p>												
<p>10</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Edit connection groups</p>	<p>Select the DPSvcGroup Connection Group.</p>  <p>Click Edit.</p> <p>Select the desired DP servers from the Available Servers in Network Element.</p> <p>Editing existing Connection Groups</p> <table border="1" data-bbox="412 835 1325 1020"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Connection Group Name *</td> <td>DPSvcGroup</td> <td>Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]</td> </tr> </tbody> </table> <div data-bbox="412 1020 1325 1230"> <p>Available Servers in Network Element: [SDSDP1] Assigned Servers in Connection Group: []</p> <p>>> <<</p> </div> <p>Click >>.</p> <p>Editing existing Connection Groups</p> <table border="1" data-bbox="412 1373 1325 1558"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Connection Group Name *</td> <td>DPSvcGroup</td> <td>Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]</td> </tr> </tbody> </table> <div data-bbox="412 1558 1325 1768"> <p>Available Servers in Network Element: [] Assigned Servers in Connection Group: [SDSDP1]</p> <p>>> <<</p> </div> <p>Ok Apply Cancel</p> <p>Click OK.</p>	Field	Value	Description	Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]	Field	Value	Description	Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]
Field	Value	Description												
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]												
Field	Value	Description												
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]												

Procedure 38. Configure ComAgent Connections (DSR + SDS)

11	DSR NOAM VIP GUI: Verify correct number of servers in group	Verify correct number of servers are in the connection group.
----	---	---

4.7.3 Shared Secret Encryption Key Revocation (RADIUS ONLY)

Procedure 39. Shared Secret Encryption Key Revocation (RADIUS Only)

S	This procedure changes shared secret encryption key on DSR RADIUS setup.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1	<input type="checkbox"/> Revoke RADIUS shared secret encryption key	Refer to RADIUS Shared Secret Key revocation MOP to change the encryption key on the DSR installed setup. Refer [11] DSR RADIUS Shared secret encryption key revocation MOP MO008572. Note: This is highly recommended to change the key after installation due to security reasons.

4.7.4 Backup TVOE Configuration

Procedure 40. Backup TVOE Configuration

S	This procedure backs up each TVOE rack mount server or blade server after a successful installation.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1	<input type="checkbox"/> 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: <ul style="list-style-type: none"> • TVOE • PMAC • DSR NOAM • DSR SOAM
2	<input type="checkbox"/> TVOE Server: Login	Establish an SSH session to the TVOE host server and login as admusr .

Procedure 40. Backup TVOE Configuration

3 <input type="checkbox"/>	TVOE Server: Build ISO backup file	<p>Execute the following command from the TVOE server:</p> <pre>\$ sudo su - platcfg</pre> <p>Navigate to Maintenance -> Backup and Restore -> Backup Platform (CD/DVD).</p> <p>The Backup TekServer Menu screen displays.</p> <p>Note: If no cdrom device is found by TPD, the No disk device available. This is normal on systems without a cdrom device message displays. Press Enter.</p> <p>Build the backup ISO image by selecting Build ISO file only.</p> <p>Note: Creating the ISO image may happen so quickly that this screen may only display for an instant.</p> <p>After the ISO is created, platcfg returns to the Backup TekServer menu. The ISO has now been created and is located in the <code>/var/TKLC/bkp/</code> directory. An example filename of a backup file that was created is: hostname1307466752-plat-app-201104171705.iso</p> <p>Exit out of platcfg by selecting Exit.</p>
-------------------------------	---	---

Procedure 40. Backup TVOE Configuration

<p>4</p> <p><input type="checkbox"/></p>	<p>Backup Server: Transfer TVOE files to backup server</p>	<p>Log into 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.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/</pre> <p>When prompted, type the tvoexfer user password and press Enter.</p> <p>If the customer system is a Windows system, refer to [7] DSR Hardware and Software Installation Part 1, E76180 using WinSCP to copy the backup image to the customer system.</p> <p>The TVOE backup file has now been successfully placed on the backup server.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>Repeat for additional TVOE servers</p>	<p>Repeat steps 3-4 for additional TVOE servers.</p>

4.7.5 Backup PMAC Application

Procedure 41. Backup PMAC Application

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure backs up each PMAC application installed in this procedure.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Identify backup server</p>	<p>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:</p> <ul style="list-style-type: none"> • TVOE • PMAC • DSR NOAM • DSR SOAM
<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC Server: Login</p>	<p>Establish an SSH session to the PMAC server and login as admusr.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC Server: Build backup file</p>	<p>Execute the following command from the PMAC server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/pmacadm backup PM&C backup been successfully initiated as task ID 7</pre> <p>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 <code>sudo pmaccli getBgTasks</code>. The result should eventually be PMAC Backup successful and the background task should indicate COMPLETE.</p>

Procedure 41. Backup PMAC Application

<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser, navigate to the PMAC GUI, and enter a URL of:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>http://<pmac_network_Network_IP_Address></pre> </div> <p>Login as the guiadmin user.</p>  <p>The screenshot shows the Oracle System Login interface. At the top is the Oracle logo. Below it, the text 'Oracle System Login' is followed by the date and time 'Mon Jul 11 13:59:37 2016 EDT'. A central box titled 'Log In' contains the instruction 'Enter your username and password to log in'. It features two input fields for 'Username:' and 'Password:', a checkbox for 'Change password', and a 'Log In' button. At the bottom of the box, it says 'Welcome to the Oracle System Login.'</p>										
<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC Server GUI: Monitor/Verify backup task completion</p>	<p>Navigate to Main Menu -> Task Monitoring.</p>  <p>The screenshot shows the 'Main Menu' with several options: 'Status and Manage', 'Task Monitoring' (highlighted), 'Help', 'Legal Notices', and 'Logout'.</p> <p>Monitor the Backup PMAC task.</p> <p>Main Menu: Task Monitoring</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p>Filter* ▾</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>1458</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> </tr> </tbody> </table> </div> <p>Note: Alternatively, you can monitor the Backup task by executing the following command:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ sudo pmaccli getBgTasks</pre> </div>	ID	Task	Target	Status	State	1458	Backup PM&C		PM&C Backup successful	COMPLETE
ID	Task	Target	Status	State								
1458	Backup PM&C		PM&C Backup successful	COMPLETE								

Procedure 41. Backup PMAC Application

6	<input type="checkbox"/> <p>Backup Server: Transfer PMAC file to backup server</p>	<p>Log into 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.</p> <pre style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;">\$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/</pre> <p>When asked, type the admusr user password and click Enter.</p> <p>If the customer system is a Windows system, refer to reference [7] DSR Hardware and Software Installation Part 1, E76180 using WinSCP to copy the backup image to the customer system.</p>
---	---	---

4.7.6 Backup NOAM Database

Procedure 42. NOAM Database Backup

S	This procedure backs up the NOAM database.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1	<input type="checkbox"/> <p>Identify backup server</p>	<p>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:</p> <ul style="list-style-type: none"> • TVOE • PMAC • DSR NOAM • DSR SOAM

Procedure 42. NOAM Database Backup

2 <input type="checkbox"/>	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: <div data-bbox="393 310 1250 357" style="border: 1px solid black; padding: 2px;"><code>http://<Primary_NOAM_VIP_IP_Address></code></div> Login as the guiadmin user.
-------------------------------	-----------------------------------	---

Procedure 42. NOAM Database Backup

6 <input type="checkbox"/>	Backup Server: Transfer file to backup server	<p>Log into the backup server identified in step 1 and copy backup image and key file (RADIUS Only) to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/</pre> <p>Execute following command to encrypt the key file before sending to filemgmt area:</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$./sharedKrevo -encr</pre> <p>Copy key file to customer server :</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/DpiKf.bin.encr /path/to/destination/</pre> <p>When asked, type the admusr user password and press Enter.</p> <p>If the customer system is a Windows system, refer to reference [7] DSR Hardware and Software Installation Part 1, E76180 using WinSCP to copy the backup image to the customer system.</p>
-------------------------------	---	---

4.7.7 Backup SOAM Database

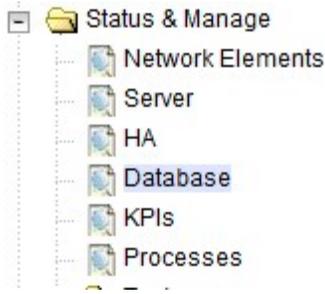
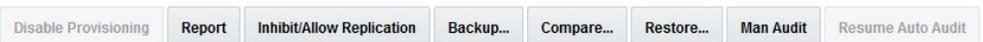
Procedure 43. SOAM Database Backup

S	This procedure backs up the SOAM database.	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	Identify backup server	<p>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:</p> <ul style="list-style-type: none"> • TVOE • PMAC • DSR NOAM • DSR SOAM

Procedure 43. SOAM Database Backup

2 <input type="checkbox"/>	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: <div data-bbox="425 310 1281 359" style="border: 1px solid black; padding: 2px;"><code>http://<Primary_SOAM_VIP_IP_Address></code></div> Login as the guiadmin user.
-------------------------------	----------------------------	---

Procedure 43. SOAM Database Backup

4	<p>SOAM VIP</p> <p>GUI: Perform database backup</p>	<p>Navigate to Main Menu -> Status & Manage -> Database.</p>  <p>Select the Active SOAM.</p> <p>Click Backup.</p>  <p>Select the desired file compression method.</p> <p>Database Backup</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Field</th> <th style="width: 40%;">Value</th> <th style="width: 30%;">Descrip</th> </tr> </thead> <tbody> <tr> <td colspan="3">Server: ZombieSOAM1</td> </tr> <tr> <td>Select data for backup</td> <td> <input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration </td> <td>Select th</td> </tr> <tr> <td>Compression *</td> <td> <input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none </td> <td> Select th The follo • .t • .t • .t [A value </td> </tr> <tr> <td>Archive Name *</td> <td>Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M</td> <td>Modify ai</td> </tr> <tr> <td>Comment</td> <td><input type="text"/></td> <td>May not</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Ok"/> <input type="button" value="Cancel"/> </p> <p>Set the archive file name, if needed.</p> <p>Click OK.</p>	Field	Value	Descrip	Server: ZombieSOAM1			Select data for backup	<input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration	Select th	Compression *	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none	Select th The follo • .t • .t • .t [A value	Archive Name *	Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M	Modify ai	Comment	<input type="text"/>	May not
Field	Value	Descrip																		
Server: ZombieSOAM1																				
Select data for backup	<input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration	Select th																		
Compression *	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none	Select th The follo • .t • .t • .t [A value																		
Archive Name *	Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M	Modify ai																		
Comment	<input type="text"/>	May not																		

Procedure 43. SOAM Database Backup

6	<input type="checkbox"/> Backup Server: Transfer SOAM file to backup server	<p>Log into 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.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/</pre> <p>When asked, enter the admusr user password and press Enter.</p> <p>If the Customer System is a Windows system, refer to [7] DSR Hardware and Software Installation Part 1, E76180 using WinSCP to copy the backup image to the customer system.</p>
6	<input type="checkbox"/> Repeat for additional TVOE servers	<p>Repeat steps 2-4 for additional DSR SOAM sites.</p>

4.7.8 Enable/Disable DTLS (SCTP Diameter Connections Only)

Procedure 44. Enable/Disable DTLS (SCTP Diameter Connections Only)

S T E P #	Important	
	<p>This procedure prepares clients before configuring SCTP diameter connections.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1	<input type="checkbox"/> Enable/Disable DTLS (SCTP diameter connections only)	<p>Oracle's SCTP Datagram Transport Layer Security (DTLS) has SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers installing DSR should prepare clients before the DSR connections are established after installation. This ensures the DSR to Client SCTP connection establishes with SCTP AUTH extensions enabled. See RFC 6083. If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices DO NOT establish after the DSR is installed.</p> <p>https://access.redhat.com/security/cve/CVE-2015-1421</p> <p>https://access.redhat.com/security/cve/CVE-2014-5077</p> <p>Execute procedures in [10] DSR DTLS Feature Activation Procedure, E78942 to disable/enable the DTLS feature.</p>

Appendix A: Sample Network Element and Hardware Profiles

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.

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

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

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

Note: In Figure 5. Example Network Element XML File, IP values are network ID IPs and not host IPs.

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

Figure 5. Example Network Element XML File

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

The server hardware information is needed to configure the Ethernet interfaces on the servers. This server hardware profile data XML file is used for DSR deployments using HP c-Class blade servers and HP c-Class rack-mount servers. It is supplied to the NOAM server so that the information can be pulled in and presented to the user in the GUI during server configuration. The following is an example of a server hardware profile XML file.

```

<profile>
<serverType>HP c-Class Blade</serverType>
<available>
<device>bond0</device>
</available>
<devices>
<device>
<name>bond0</name>
<type>BONDING</type>
<createBond>>true</createBond>
<slaves>
<slave>eth01</slave>
<slave>eth02</slave>
</slaves>
<option>
<monitoring>mii</monitoring>
<interval>100</interval>
<upstream_delay>200</upstream_delay>
<downstream_delay>200</downstream_delay>
</option>
</device>
</devices>
</profile>

```

Figure 6. Example Server Hardware Profile XML-HP c-Class Blade

```

<profile>
<serverType>TVOE Guest</serverType>
<available>
<device>Management</device>
<device>Control</device>
<device>xmi</device>
<device>imi</device>
<device>xsi</device>
</available>
<devices>
<device>
<name>management</name>
<type>ETHERNET</type>
</device>
<device>
<name>control</name>
<type>ETHERNET</type>
</device>

```

```

<device>
<name>xmi</name>
<type>ETHERNET</type>
</device>
<device>
<name>imi</name>
<type>ETHERNET</type>
</device>
<device>
<name>xsi</name>
<type>ETHERNET</type>
</device>
</devices>
</profile>
    
```

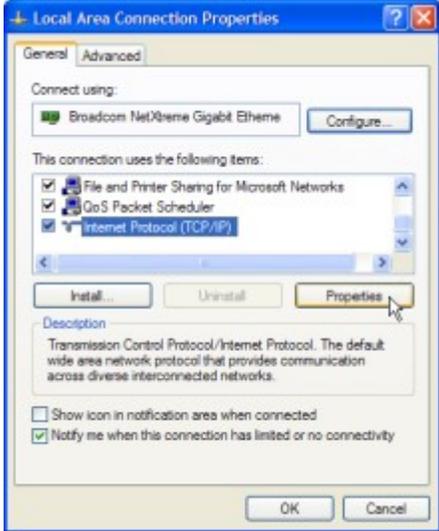
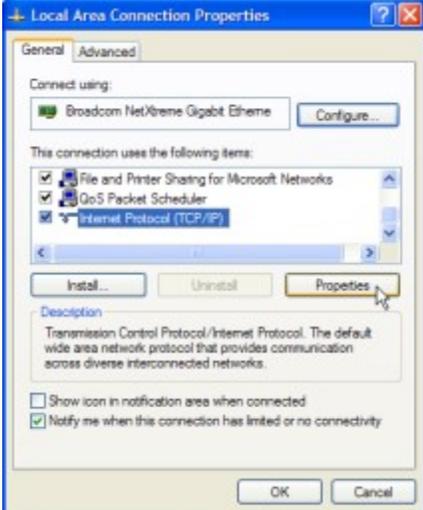
Figure 7. Example Server Hardware Profile XML- Virtual Guest on TVOE

Appendix B: Configure for TVOE iLO Access

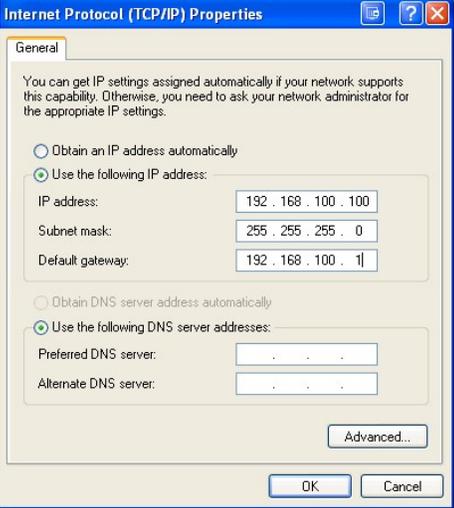
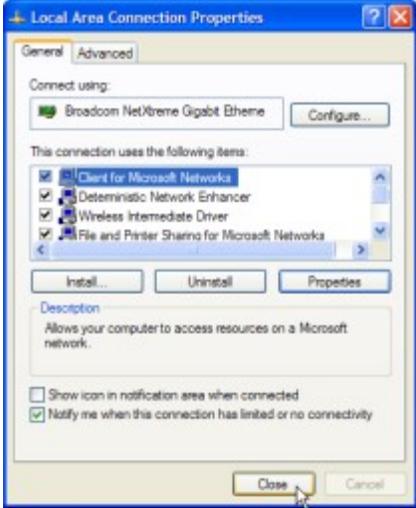
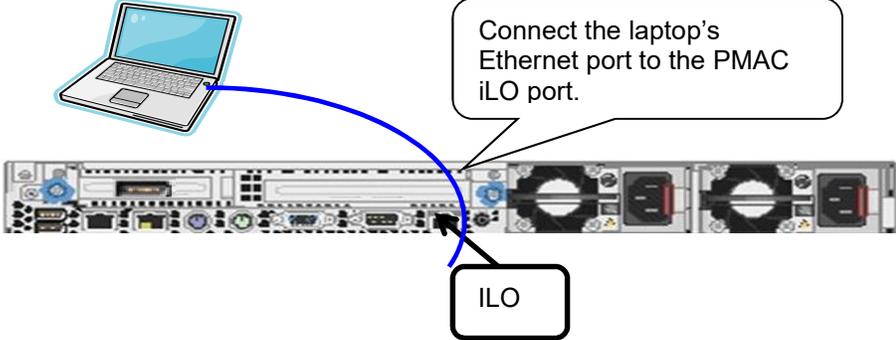
Procedure 45. Connect to the TVOE iLO

S	This procedure connects a laptop to the TVOE iLO via a directly cabled ethernet connection.		
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.		
E			
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.		
#			
1	Access the laptop	Windows XP	Windows 7

Procedure 45. Connect to the TVOE iLO

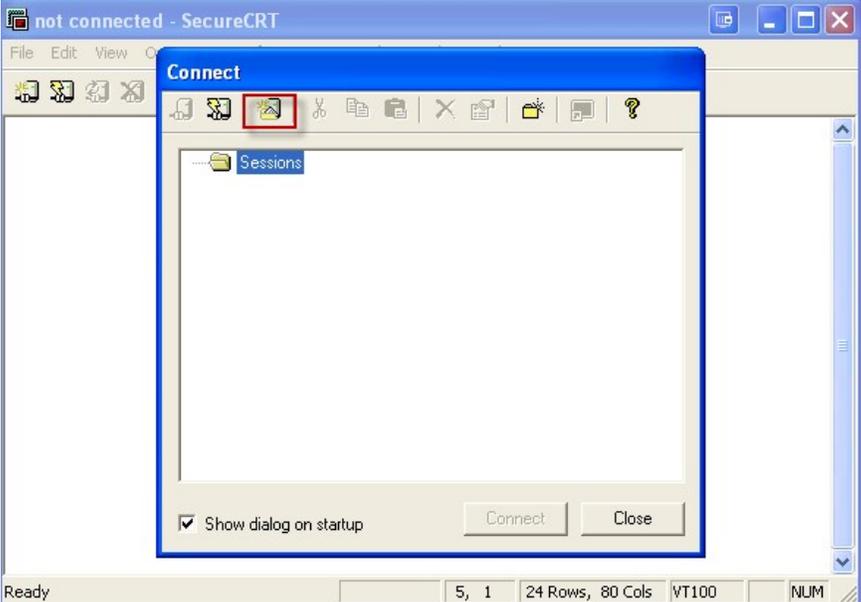
<p><input type="checkbox"/> network interface cards TCP/IP Properties screen.</p> <p>Note: For this step, follow the instructions specific to the laptop's OS (Windows XP or Windows 7)</p>	<p>Go to Control Panel.</p> <p>Double-click on Network Connections.</p> <p>Right-click the wired Ethernet Interface icon and select Properties.</p> <p>Click Internet Protocol (TCP/IP).</p> <p>Click Properties.</p> 	<p>Go to Control Panel.</p> <p>Double-click on Network and Sharing Center.</p> <p>Click Change Adapter Settings (left menu).</p> <p>Right-click the Local Area Connection icon and click Properties.</p> <p>Click Internet Protocol Version 4 (TCP/IPv4).</p> 
---	--	---

Procedure 45. Connect to the TVOE iLO

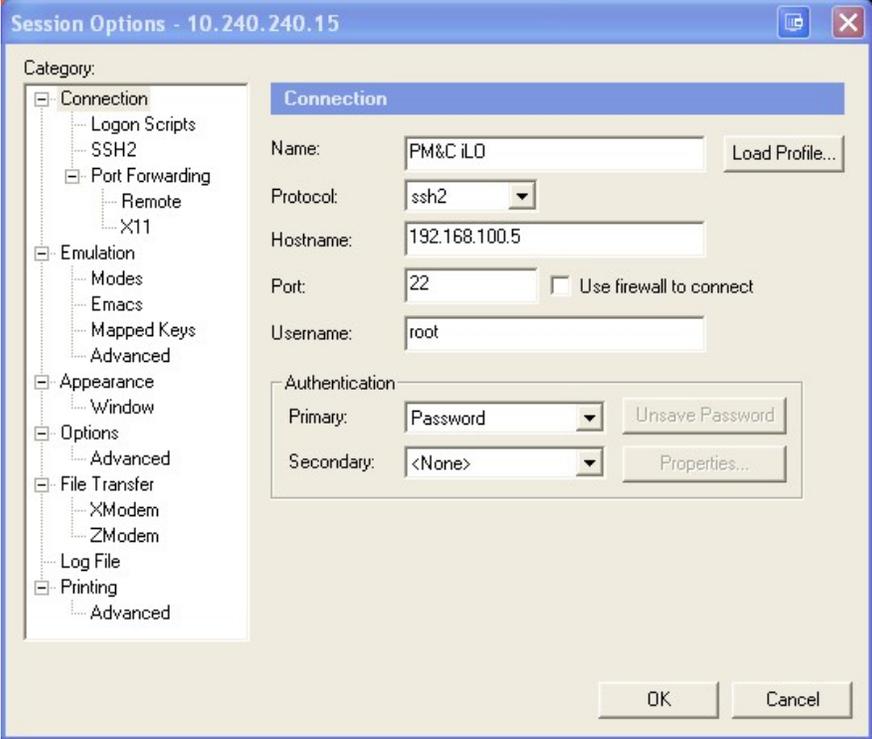
<p>2</p> <p><input type="checkbox"/></p>	<p>Configure IP address</p>	<p>Click Use the following IP address.</p> <p>Set the IP address to 192.168.100.100.</p> <p>Set the Subnet mask to 255.255.255.0.</p> <p>Set the Default gateway to 192.168.100.1.</p> <p>Select OK.</p> <p>Click Close from the network interface card's main Properties screen.</p> <div style="display: flex; justify-content: space-around;">   </div>
<p>3</p> <p><input type="checkbox"/></p>	<p>Connect ports</p>	<p>Connect the laptop's Ethernet port directly to the TVOE iLO port using a standard Cat-5 cross-over cable.</p> <div style="text-align: center;">  </div>

Appendix C: TVOE iLO Access

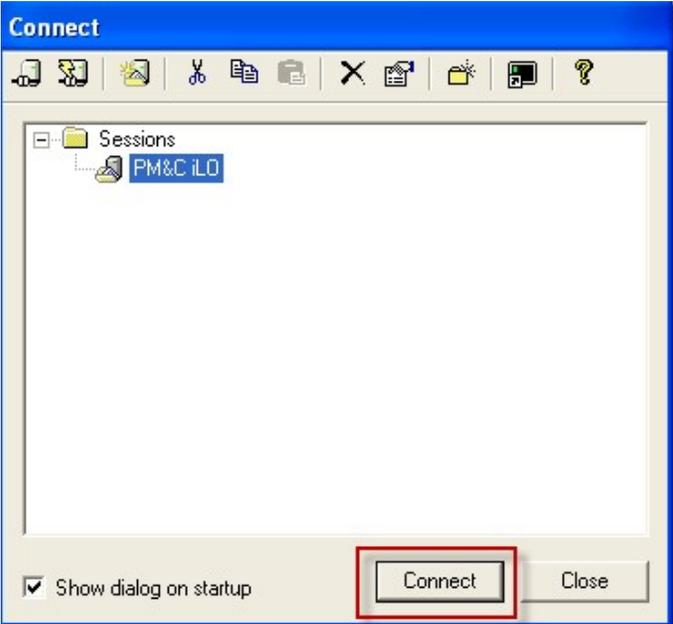
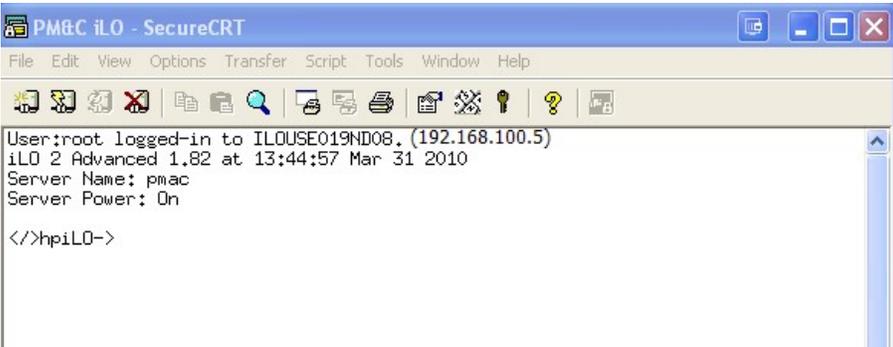
Procedure 46. Access the TVOE iLO

<p>S T E P #</p>	<p>This procedure contains the steps to access the TVOE iLO.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Launch terminal emulator</p>	<p>Launch a terminal emulator, e.g., Putty, Secure CRT.</p> <p>Navigate to File -> Connect.</p> <p>Click the New Session icon.</p> <p>Note: This example demonstrates Secure CRT.</p> 

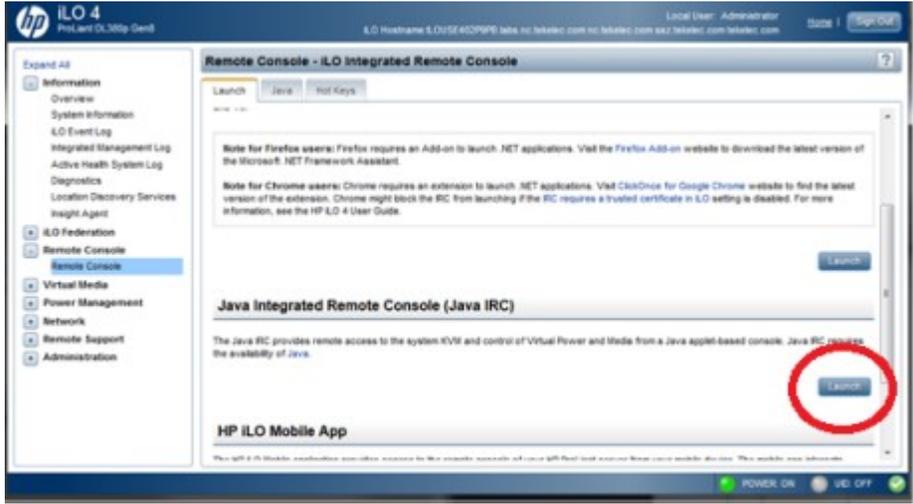
Procedure 46. Access the TVOE iLO

2	Configure TVO ILO <input type="checkbox"/>	<p>Name: Type TVOE iLO</p> <p>Hostname: 192.168.100.5 (Manufacturing default) or customer IP set during installation</p> <p>Username: Enter admusr</p> <p>Click OK.</p> <p>Note: See Appendix B: Configure for TVOE iLO Access to configure your system network to access the TVOE iLO.</p>
		

Procedure 46. Access the TVOE iLO

<p>3</p> <p><input type="checkbox"/></p>	<p>Connect to TVO iLOE</p>	<p>Navigate File -> Connect to open the Connect window.</p> <p>Highlight the session you created and click Connect.</p> 
<p>4</p> <p><input type="checkbox"/></p>	<p>Log into TVO iLOE</p>	<p>Login to the TVOE iLO using the appropriate password.</p>  <p>The TVOE iLO displays.</p> 

Procedure 47. TVOE iLO4 GUI Access

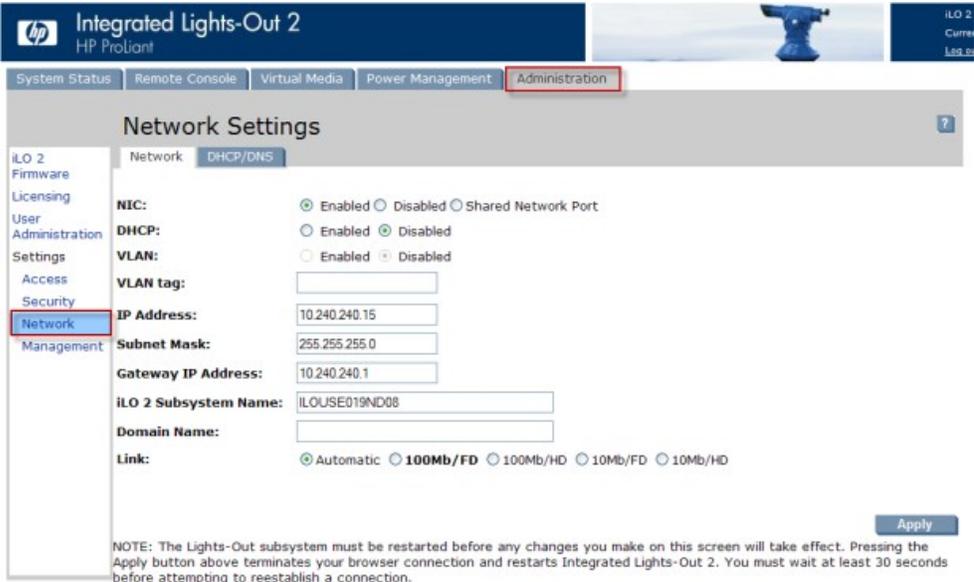
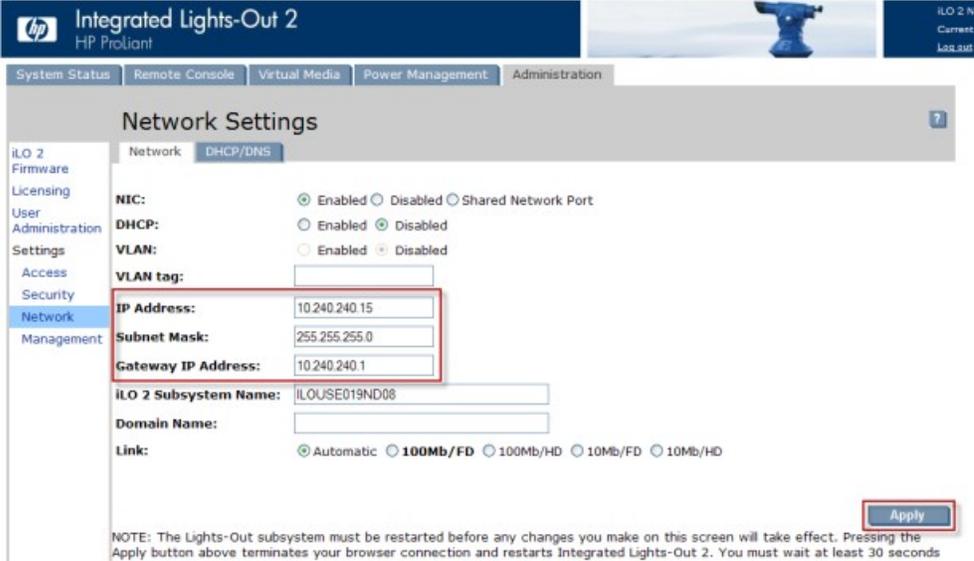
<p>3</p> <p><input type="checkbox"/></p>	<p>Launch the PMAC iLO4 CLI</p>	<p>Click Launch to start the PMAC iLO4 CLI.</p>  <p>The screenshot shows the HP iLO4 Remote Console interface. The left sidebar contains a navigation menu with 'Remote Console' selected. The main content area has a 'Launch' button circled in red. The interface also displays information about the Java Integrated Remote Console (Java IRC) and the HP iLO Mobile App.</p>
--	---------------------------------	--

Appendix E: Change the TVOE iLO Address

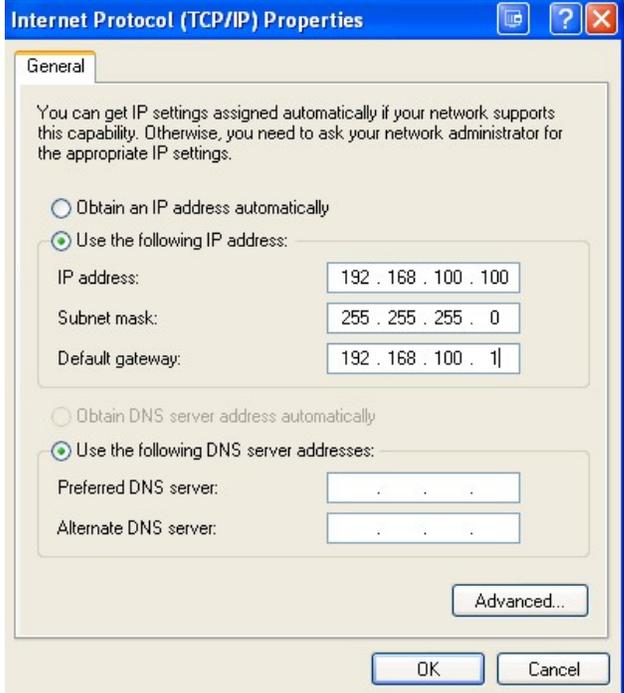
Procedure 48. Change the TVOE iLO Address

<p>S T E P #</p>	<p>This procedure sets the IP address of the TVOE iLO to the customer's network so it can be accessed by Oracle support.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<p>Connect to the TVOE iLO GUI</p> <p>Using the instructions in Appendix D: TVOE iLO4 GUI Access, connect to TVOE iLO GUI.</p>  <p>The screenshot shows the HP Integrated Lights-Out 2 GUI. The 'Status Summary' page is displayed, showing various system details for the server 'pmac: ProLiant DL360 G6'. The IP address is listed as 192.168.100.5. The interface includes a navigation menu and a 'Launch' button for the Remote Console.</p>

Procedure 48. Change the TVOE iLO Address

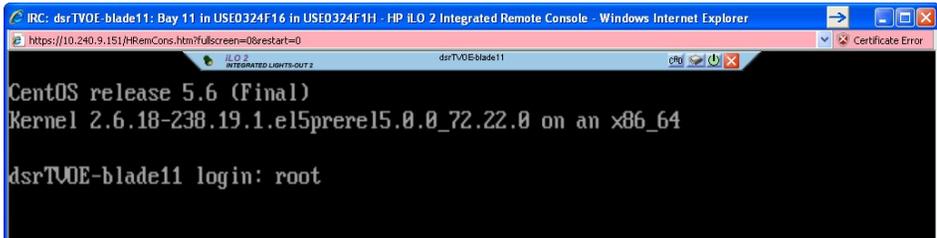
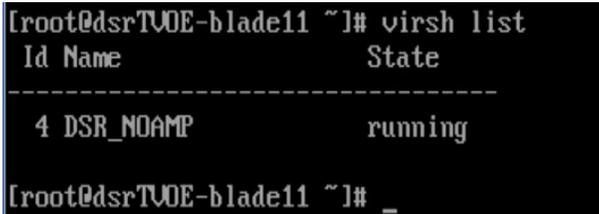
<p>2</p> <p><input type="checkbox"/></p>	<p>ILO GUI: Navigate to the network menu</p>	<p>Click the Administration tab. Under Settings in the left column, click Network.</p> 
<p>3</p> <p><input type="checkbox"/></p>	<p>ILO GUI: Configure TVOE iLOE Note: You lose access after you click Apply.</p>	<p>Change the IP Address, Subnet Mask, and Gateway IP Address to the values supplied in the IP site survey for the TVOE iLO. Click Apply.</p> 

Procedure 48. Change the TVOE iLO Address

<p>4</p> <p><input type="checkbox"/></p>	<p>Local Machine: Reset PC's network connection</p>	<p>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.</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>Local Machine: Connect to the TVOE iLO GUI</p>	<p>Connect to the TVOE iLO GUI using the instructions in Appendix D: TVOE iLO4 GUI Access.</p> <p>Note: Use the IP address entered in step 3.</p> 

Appendix F: PMAC/NOAM/SOAM Console iLO Access

Procedure 49. PMAC/NOAM/SOAM Console iLO Access

<p>S T E P #</p>	<p>This procedure logs into the PMAC/NOAM/SOAM console from ILO.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Log into TVOE</p>	<p>Login as admusr on the TVOE server hosting the NOAM using either ILO or SSH to the TVOE server's XMI or Mgmt. address.</p> 
<p>2 <input type="checkbox"/></p>	<p>Locate VM</p>	<p>On the TVOE host, execute the following command:</p> <pre style="border: 1px solid black; padding: 5px; width: fit-content;">\$sudo virsh list</pre> <p>This produces a listing of currently running virtual machines.</p>  <p>Find the VM name for your DSR NOAM and note its ID number in the first column.</p> <p>Note: If the VM state is not listed as running or you do not find a VM you configured for your NOAM at all, then halt this procedure and contact Oracle Customer Support.</p>

Procedure 49. PMAC/NOAM/SOAM Console iLO Access

3	<p>Connect to console of the VM using the VM number obtained in step 2.</p>	<p>On the TVOE host, execute:</p> <pre style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;">\$sudo virsh console <DSRNOAM-VMID></pre> <p>Where DSRNOAM-VMID is the VM ID you obtained in step 2.</p> <pre style="background-color: black; color: white; padding: 10px; width: fit-content; margin: 10px auto;">Connected to domain DSR_NOAMP Escape character is ^] CentOS release 5.6 (Final) Kernel 2.6.18-238.19.1.el5prere15.0.0_72.22.0 on an x86_64 hostname1322840832 login: _</pre> <p>You are now connected to the DSR NOAMs console.</p> <p>If you wish to return to the TVOE host, you can exit the session by pressing CTRL +].</p>
---	---	---

Appendix G: List of Frequently Used Time Zones

This table lists several valid timezone strings that can be used for the time zone setting in a CSV file, or as the time zone parameter when manually setting a DSR blade timezone. For an exhaustive list of **ALL** timezones, log into the PMAC server console and view the text file: `/usr/share/zoneinfo/zone.tab`.

Table 3. List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico City	Central Time — most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01
Asia/Hong Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01

Time Zone Value	Description	Universal Time Code (UTC) Offset
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time — west British Columbia	UTC-08
America/Edmonton	Mountain Time — Alberta, east British Columbia & west Saskatchewan	UTC-07
America/Toronto	Eastern Time — Ontario — most locations	UTC-05
America/Montreal	Eastern Time — Quebec — most locations	UTC-05
America/Sao Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia — most locations	UTC+08
Australia/Sydney	New South Wales — most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto Rico		UTC-04
Europe/Moscow	Moscow+00 — west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

Appendix H: Application NetBackup Client Installation Procedures

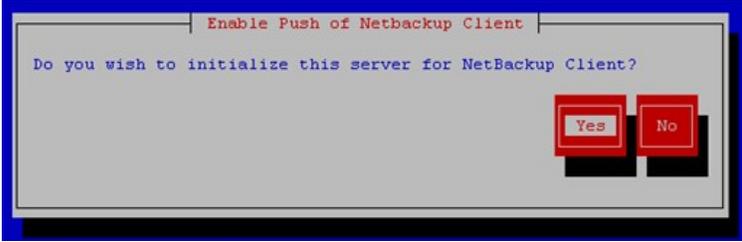
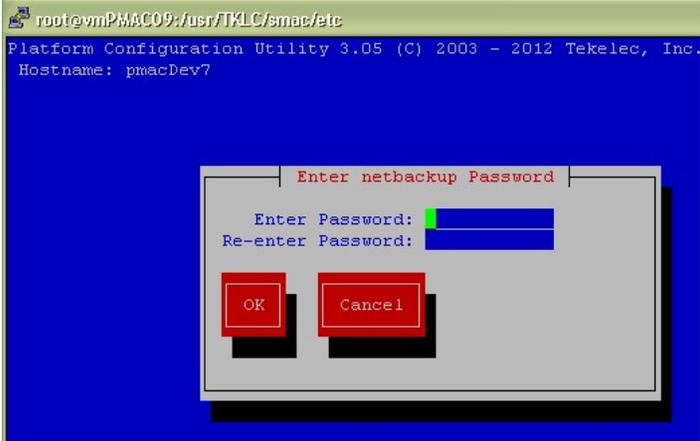
NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite supports disaster recovery at the customer site. The following procedures install and configure the NetBackup client software on an application server in two different ways: first, using platcfg, and second, using nbAutoInstall (push configuration).

Appendix H.1: NETBACKUP Client Installation Using PLATCFG

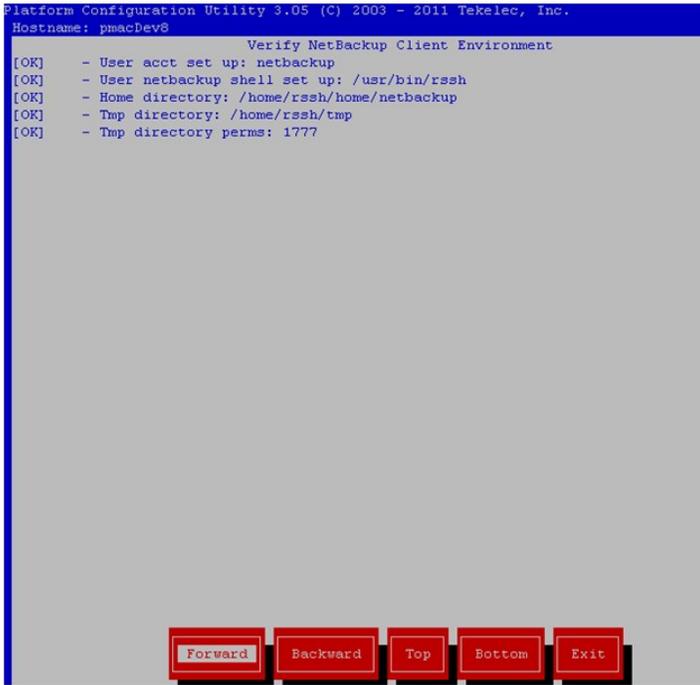
Procedure 50. Application NetBackup Client Installation (Using Platcfg)

S T E P #	<p>This procedure explains the Netbackup installation using platcfg.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • 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. • Execute Appendix A.3 of [7] <p>Note: Execute the following procedure to switch/migrate to having netBackup installed via platcfg instead of using NBAutoInstall (Push Configuration)</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
	1 <input type="checkbox"/>	<p>Application Server iLO: Login</p>
2 <input type="checkbox"/>	<p>Application Server iLO: Navigate to NetBackup configuration</p>	<p>Configure NetBackup Client on application server.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ sudo su - platcfg</pre> </div> <p>Navigate to NetBackup -> Configuration.</p>

Procedure 50. Application NetBackup Client Installation (Using Platcfg)

<p>3</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Enable push of NetBackup client</p>	<p>Navigate to NetBackup Configuration -> Enable Push of NetBackup Client.</p> 
<p>4</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Enter NetBackup password</p>	<p>Enter the NetBackup password.</p>  <p>Click OK.</p> <p>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.</p>

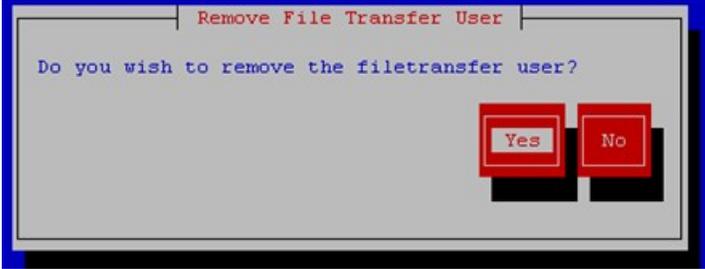
Procedure 50. Application NetBackup Client Installation (Using Platcfg)

<p>5</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Verify NetBackup client software push is enabled</p>	<p>Navigate to NetBackup Configuration -> Verify NetBackup Client Push.</p>  <p>Verify list entries indicate OK for NetBackup client software environment. Click Exit to return to NetBackup Configuration menu.</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>NetBackup Server: Push appropriate NetBackup client software to application server</p>	<p>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.</p> <p>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.</p> <p>Log into the NetBackup server using password provided by customer: Navigate to the appropriate NetBackup Client software path:</p> <p>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)</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/opencv/NetBackup/client/Linux/7.5</pre> <p>Execute the sftp_to client NetBackup utility using the application IP address and application NetBackup user:</p>

Procedure 50. Application NetBackup Client Installation (Using Platcfg)

<p>7</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Install NetBackup client software on application server</p>	<p>Execute the command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo chmod 555 /var/TKLC/home/rssh/tmp/client_config</pre> <p>Where NETBACKUP_BIN is the temporary directory where the NetBackup client install programs were copied in step 5. The directory should look similar to /tmp/bp.XXXX/.</p> <p>Navigate to NetBackup Configuration -> Install NetBackup Client.</p>  <p>Verify list entries indicate OK for NetBackup client software installation.</p> <p>Click Exit to return to NetBackup Configuration menu.</p>
<p>8</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Verify NetBackup client software installation on the application server</p>	<p>Navigate to NetBackup Configuration -> Verify NetBackup Client Installation.</p>  <p>Verify list entries indicate OK for NetBackup Client software installation.</p> <p>Click Exit to return to NetBackup Configuration menu.</p>

Procedure 50. Application NetBackup Client Installation (Using Platcfg)

<p>9</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Disable NetBackup client software transfer to the application server</p>	<p>Navigate to NetBackup Configuration -> Remove File Transfer User.</p>  <p>Click Yes to remove the NetBackup file transfer user from the application server.</p>
<p>10</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Exit platform configuration utility (platcfg)</p>	<p>Exit platform configuration utility (platcfg).</p>
<p>11</p> <p><input type="checkbox"/></p>	<p>Application Server iLO: Verify server bp.conf file</p>	<p>Verify the server has been added to the /usr/opensv/NetBackup/bp.conf file.</p> <p>Issue the following command:</p> <pre data-bbox="456 919 1409 1056">\$ sudo cat /usr/opensv/NetBackup/bp.conf CLIENT_NAME = 10.240.34.10 SERVER = NB71server</pre>

Procedure 50. Application NetBackup Client Installation (Using Platcfg)

12



Application Server iLO:
Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias

Note: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup `/usr/opensv/NetBackup/bp.conf` file, identified by the **Server** configuration parameter.

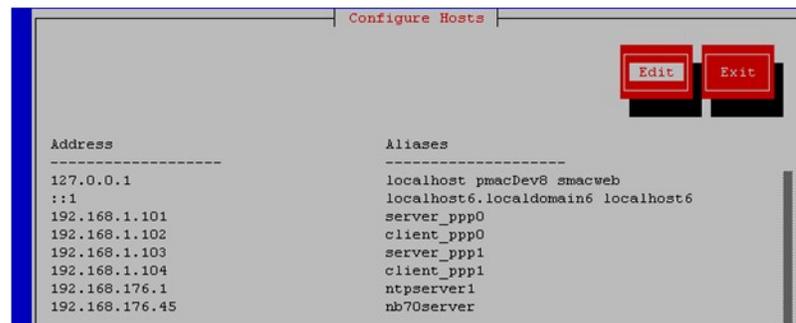
The NetBackup server hostname and IP address must be added to the application server's host's file. List NetBackup servers hostname:

```
$ sudo cat /usr/opensv/NetBackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

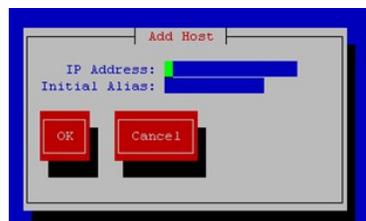
Navigate to **Network Configuration -> Modify Hosts File.**



Select **Edit**. The **Host Action Menu** displays.



Select **Add Host** and enter the appropriate data.



Select **OK**, confirm the host alias added, and exit Platform Configuration Utility.

Procedure 50. Application NetBackup Client Installation (Using Platcfg)

13 <input type="checkbox"/>	Application Server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.	Copy the notify scripts from appropriate path on application server for given application: <pre style="border: 1px solid black; padding: 5px;">\$ sudo ln -s <path>/bpstart_notify /usr/opensv/NetBackup/bin/bpstart_notify \$ sudo ln -s <path>/bpend_notify /usr/opensv/NetBackup/bin/bpend_notify</pre> <p>An example of <path> is "/usr/TKLC/appworks/sbin"</p>
--------------------------------	---	--

Appendix H.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 enables TPD to detect when a NetBackup Client is installed automatically and completes TPD related tasks 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.

Procedure 51. Application NetBackup Client Installation (NBAutoInstall)

S T E P	<p>This procedure installs NetBackup with NBAutoInstall.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • 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. <p>Note: If the customer does not have a way to push and install NetBackup Client, then use NetBackup Client Install/Upgrade with platcfg.</p> <p>Note: It is required that this procedure is executed before the customer does the NetBackup Client install.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p># If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Application Server iLO: Login	Login and launch the integrated remote console. ssh to the application server (PMAC or NOAM) as admusr using the management network for the PMAC or XMI network for the NOAM.
2 <input type="checkbox"/>	Application Server iLO: Enable nbAutoInstall	Execute the following command: <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable</pre>

Procedure 51. Application NetBackup Client Installation (NBAutoInstall)

3 <input type="checkbox"/>	Application Server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them	<p>Execute the following commands:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo mkdir -p /usr/opensv/NetBackup/bin/ \$ sudo ln -s <path>/bpstart_notify /usr/opensv/NetBackup/bin/bpstart_notify \$ sudo ln -s <path>/bpend_notify /usr/opensv/NetBackup/bin/bpend_notify</pre> <p>Note: An example of <path> is “/usr/TKLC/plat/sbin”</p>
4 <input type="checkbox"/>	Application Server iLO: Verify NetBackup configuration file	<p>Open /usr/opensv/NetBackup/bp.conf and make sure it points to the NetBackup Server using the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo vi /usr/opensv/NetBackup/bp.conf SERVER = nb75server CLIENT_NAME = 10.240.10.185 CONNECT_OPTIONS = localhost 1 0 2</pre> <p>Note: Verify the server name matches the NetBackup Server, and the CLIENT_NAME matches the hostname or IP of the local client machine. If they do not, update them as necessary.</p> <p>Edit /etc/hosts using the following command and add the NetBackup server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo vi /etc/hosts e.g.: 192.168.176.45 nb75server</pre> <p>Note: The server periodically checks to see if a new version of NetBackup Client has been installed and performs necessary TPD configuration accordingly.</p> <p>At any time, the customer may push and install a new version of NetBackup client.</p>

Appendix H.3: Create NetBackup Client Configuration File

Procedure 52. Create NetBackup Client Configuration File

S T E P #	<p>This procedure copies a NetBackup Client configuration file into the appropriate location on the TPD based application server. This configuration file allows a customer to install previously unsupported versions of the NetBackup client by providing necessary information to TPD.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Application Server iLO: Create NetBackup configuration file</p>	<p>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:</p> <p><code>NB\$ver.conf</code></p> <p>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:</p> <p><code>/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf</code></p> <p>Note: The config files must start with NB and must have a suffix of .conf.</p> <p>The server is now capable of installing the corresponding NetBackup Client.</p>
2 <input type="checkbox"/>	<p>Application Server iLO: Create NetBackup configuration script</p>	<p>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.</p> <p>As an example for the NetBackup 7.5 client, the following is applicable:</p> <p>NetBackup Client config: <code>/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf</code></p> <p>NetBackup Client config script: <code>/usr/TKLC/plat/etc/NetBackup/scripts/NB75</code></p>

Appendix H.4: Open Ports for NetBackup Client Software

Procedure 53. Open Ports for NetBackup Client Software

S T E P #	<p>This procedure uses iptables and ip6tables (if applicable) to open the applicable ports for the NetBackup client to communicate to the NetBackup server.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Active NOAM Server: Login</p>	<p>Establish an SSH session to the active NOAM server and login as admusr.</p>

Procedure 53. Open Ports for NetBackup Client Software

<p>2</p> <p><input type="checkbox"/></p>	<p>Active NOAM Server: Open ports for NetBackup client software</p>	<p>Change directories to /usr/TKLC/plat/etc/iptables.</p> <pre>\$ cd /usr/TKLC/plat/etc/iptables</pre> <p>Using vi, create a file named 60netbackup.ipt.</p> <pre>\$ sudo vi 60netbackup.ipt</pre> <p>Insert the following contents into the file:</p> <pre># NetBackup ports. # *filter -A INPUT -m state --state NEW -m tcp -p tcp --dport 1556 -j ACCEPT -A INPUT -m state --state NEW -m tcp -p tcp --dport 13724 -j ACCEPT -A INPUT -m state --state NEW -m tcp -p tcp --dport 13782 -j ACCEPT</pre> <p>Now save and close the file using ':wq'</p> <p>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 /usr/TKLC/plat/etc/ip6tables directory.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>Standby NOAM: Open ports for NetBackup client software</p>	<p>Repeat steps 1-2 for the standby NOAM to open ports for NetBackup client software.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Open ports for NetBackup client software</p>	<p>Repeat steps 1-2 for the active SOAM to open ports for NetBackup client software.</p>
<p><input type="checkbox"/></p>	<p>Standby SOAM: Open ports for NetBackup client software</p>	<p>Repeat steps 1-2 for the standby SOAM to open ports for NetBackup client software.</p>

Appendix I: IDIH Fast Deployment Configuration

The `fdc.cfg` file contains 8 sections. The following is a list of those sections with a short description:

Section	Description
Software Images	A list of the TVOE, TPD, and iDIH application versions.
TVOE Blade	Contains the enclosure ID, OA addresses, location, name and hardware type of an HP blade.
TVOE RMS	Includes hardware type and ILO address of the rack mount server.
Type	Management or Standalone
TVOE Configuration	Contains all IP addresses, hostname and network devices for the TVOE host.

Section	Description
Guest Configurations (3)	The guest sections contain network and hostname configuration for the Oracle, Mediation and Application guests.

Software Images

Be sure to update the software images section based on software versions you intend to install. The following table outlines typical installation failures caused by incorrect software versions. Use the **fdconfig dumpsteps -file=** command to produce output of a fast deployment session.

Software Image	Element	Command Text
TVOE ISO	mgmtsrvrtvoe	IPM server
TPD ISO	Oracle,tpd Mediation,tpd Application,tpd	IPM server
iDIH Mediation ISO	Mgmtsrvrtvoe,configExt	Transfer file
iDIH Oracle ISO iDIH Mediation ISO iDIH Application ISO	Oracle,ora Mediation,med Application,app	Upgrade server

Note: For installation, oracleGuest-8.0.0.0.0_80.x.x-x86_64.iso is to be used.

TVOE Blade

The TVOE Blade section should be commented out if you intend to install a rack mount server. Be sure to fill in the sections properly. Enclosure ID, OA IP addresses and the Bay must be correct or the PMAC cannot discover the blade. Hardware profiles are different for Gen8 and Gen6. Gen6 blades profiles have fewer CPU's and Ram allocated to the Guest.

TVOE RMS

The TVOE RMS section should be commented out if you intend to install a TVOE Blade. It contains the ILO IP address and hardware profile. If the ILO IP address is incorrect, the PMAC cannot discover the rack mount server. Server discovery must occur before the installation can begin.

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 sets up a management network instead of an XMI network and it removes the software stanza inside of the TVOE server stanza. If you are setting up a standalone IDIH, then comment out **Type=Management**, which sets up 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.

Execute **cat hw_id** or **hardwareInfo** command on TVOE host to get the hardware ID for the **Hw=** parameter.

Note: For Gen9 (Hardware ID ProLiantDL380Gen9), please use Gen8's Hardware ID (ProLiantDL380pGen8).

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:

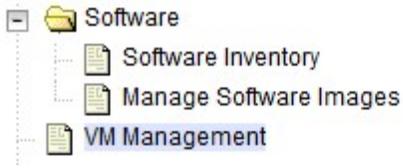
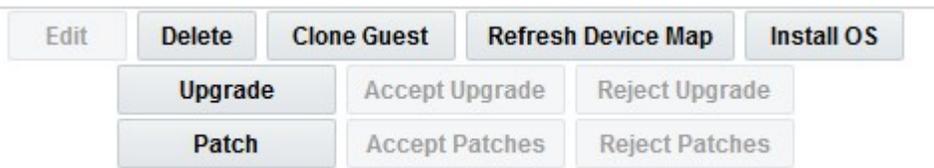
```
# Software Images
TvoeIso="TVOE-3.0.1.0.0_86.20.0-x86_64"
TpdIso="TPD.install-7.0.1.0.0_86.20.0-OracleLinux6.6-x86_64"
OraIso="oracleGuest-8.0.0.0.0_80.25.0-x86_64"
MedIso="mediation-8.0.0.0.0_80.25.0-x86_64"
AppIso="apps-8.0.0.0.0_80.25.0-x86_64"
# Tvoe Blade OA IP and Bay uncomment if this server 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="SUNNETRAX4270M3"
# 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="10.250.32.10"
TvoeIp6="2607:f0d0:1002:51::4/64"
TvoeIp6Gw="fe80::0"
# xmibond
XmiDev="bond0"
XmiEth="eth01,eth02"
# imibond
ImiDev="bond1"
ImiEth="eth03,eth04"
# xmi/management
MgmtInt="bond0.3"
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="$TvoeIp6Gw"
# Mediation Guest Config
MedName="thunderbolt-med"
MedIp="10.250.51.10"
MedMask=$Mask
MedGw=$Gateway
ImiIp="192.168.32.11"
ImiMask="255.255.255.224"
MedIp6="2607:f0d0:1002:51::6/64"
MedIp6Gw="$TvoeIp6Gw"
ImiIp6="2608:f0d0:1002:51::6/64"
# Application Guest Config
AppName="thunderbolt-app"
AppIp="10.250.51.11"
AppMask=$Mask
AppGw=$Gateway
AppIp6="2607:f0d0:1002:51::7/64"
AppIp6Gw="$TvoeIp6Gw"
```

Appendix J: IDIH External Drive Removal

This procedure should only be run if the user intends to do a fresh installation on an existing IDIH.

Procedure 54. IDIH External Drive Removal

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure destroys all of the data in the Oracle database.</p> <p>Warning: Do not perform this procedure on an IDIH system unless you intend to do a fresh TVOE installation.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser and enter:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="https://<PMAC_Mgmt_Network_IP>">https://<PMAC_Mgmt_Network_IP></p> </div> <p>Login as guiadmin user:</p>
<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Delete VMs, if needed</p>	<p>Before a re-installation can be performed, the IDIH VMs must be removed first.</p> <p>Navigate to Main Menu -> VM Management.</p> <div style="margin: 5px 0;">  </div> <p>Select each of the IDIH VMs and click Delete.</p> <div style="margin: 5px 0;">  </div>

Procedure 54. IDIH External Drive Removal

<p>3 <input type="checkbox"/></p>	<p>IDIH TVOE Host: Login</p>	<p>Establish an ssh session to the TVOE host and login as admusr.</p>
<p>4 <input type="checkbox"/></p>	<p>IDIH TVOE Host: Verify external drive exists for HP BL460 Blade</p>	<p>Execute the following command to verify the external drive exists for HP BL460 Blade:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo hpssacli ctrl slot=3 ld all show</pre> <p>The following information displays:</p> <pre style="border: 1px solid black; padding: 5px;">Smart Array P410i in Slot 3 array A logicaldrive 1 (3.3 TB, RAID 1+0, OK)</pre>
<p>5 <input type="checkbox"/></p>	<p>IDIH TVOE Host: Verify external drive exists for HP DL380 Gen8 RMS</p>	<p>Execute the following command to verify the external drive exists for HP DL380 Gen8 RMS:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo hpssacli ctrl slot=2 ld all show</pre> <p>The following information displays:</p> <pre style="border: 1px solid black; padding: 5px;">Smart Array P420 in Slot 2 array A logicaldrive 1 (1.1 TB, RAID 1+0, OK)</pre>
<p>6 <input type="checkbox"/></p>	<p>IDIH TVOE Host: Verify external drive exists for Netra X3</p>	<p>Execute the following command to verify the external drive exists for Netra X3:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo storcli -ldinfo -l1 -a0 head</pre> <p>The following information displays:</p> <pre style="border: 1px solid black; padding: 5px;">Adapter 0 -- Virtual Drive Information: Virtual Drive: 1 (Target Id: 1) Name : RAID Level : Primary-1, Secondary-0, RAID Level Qualifier-0 Size : 1.633 TB Mirror Data : 1.633 TB State : Optimal Strip Size : 64 KB</pre>

Procedure 54. IDIH External Drive Removal

7 <input type="checkbox"/>	IDIH TVOE Host: Verify external drive exists for HP DL380 Gen9 RMS	Execute the following command to verify the external drive exists for HP DL380 Gen9 RMS : <pre>\$ sudo hpssacli ctrl slot=0 ld all show</pre> The following information displays: <pre>Smart Array P440ar in Slot 0 (Embedded) array A logicaldrive 1 (838.3 GB, RAID 1, OK) array B logicaldrive 2 (838.3 GB, RAID 1, OK) array C logicaldrive 3 (838.3 GB, RAID 1, OK)</pre>
8 <input type="checkbox"/>	IDIH TVOE Host: Remove the external drive and volume group for HP BL460 Blade	Execute the following command to remove the external drive and volume group for HP BL460 Blade : <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=3</pre> The following information displays: <pre>Called with options: hpdisk --slot=3 WARNING: This destroys all application data on the server! Continue? [Y/N]</pre>
9 <input type="checkbox"/>	IDIH TVOE Host: Remove the external drive and volume group for HP DL380 Gen8 RMS	Execute the following command to remove the external drive and volume group for HP DL380 Gen8 RMS : <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2</pre> The following information displays: <pre>Called with options: hpdisk --slot=2 WARNING: This destroys all application data on the server! Continue? [Y/N]</pre>
10 <input type="checkbox"/>	IDIH TVOE Host: Remove the external drive and volume Group for Netra X3 with one external disk	Execute the following command to remove the external drive and volume group for Netra X3 with one external disk : <pre>\$ sudo vgs VG #PV #LV #SN Attr VSize VFree external 1 1 0 wz--n- 1.63t 73.58g vgguests 1 6 0 wz--n- 538.56g 138.56g vgroot 1 6 0 wz--n- 19.00g 4.25g</pre> <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean pool \ --poolName=external --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean lvm \ --vgName=external --level=scrub \$ sudo megacli -cfglddel -l1 -a0</pre>

Procedure 54. IDIH External Drive Removal

11 <input type="checkbox"/>	IDIH TVOE HOST: Remove the external drive and volume group for Netra X3 with three external disks	<p>Execute the following command to remove the external drive and volume group for Netra X3 with three external disks:</p> <pre>\$ sudo vgs VG #PV #LV #SN Attr VSize VFree external1 1 1 0 wz--n- 557.86g 24.86g external2 1 1 0 wz--n- 557.86g 24.86g external3 1 1 0 wz--n- 557.86g 24.86g vgguests 1 6 0 wz--n- 538.56g 138.56g vgroot 1 6 0 wz--n- 19.00g 4.25g</pre> <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean pool \ --poolName=external3 --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean pool \ --poolName=external2 --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean pool \ --poolName=external1 --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean lvm \ --vgName=external3 --level=scrub \$ sudo /usr/TKLC/plat/sbin/storageClean lvm \ --vgName=external2 --level=scrub \$ sudo /usr/TKLC/plat/sbin/storageClean lvm \ --vgName=external1 --level=scrub [root@hellcat ~]# sudo storcli -cflgddel -l3 -a0 [root@hellcat ~]# sudo storcli -cflgddel -l2 -a0 [root@hellcat ~]# sudo storcli -cflgddel -l1 -a0</pre>
12 <input type="checkbox"/>	IDIH TVOE HOST: Remove the External Drive and Volume Group for HP DL380 Gen9 RMS	<p>Execute the following command to remove the external drive and volume group for HP DL380 Gen9 RMS:</p> <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean pool -- \ poolName=external2 --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean pool -- \ poolName=external1 --level=pv \$ sudo /usr/TKLC/plat/sbin/storageClean lvm -- \ vgName=external2 --level=scrub \$ sudo /usr/TKLC/plat/sbin/storageClean lvm -- \ vgName=external1 --level=scrub \$ sudo hpssacli ctrl slot=0 ld 3 delete \$ sudo hpssacli ctrl slot=0 ld 2 delete</pre>

Appendix K: DSR Fast Deployment Configuration

The following table contains the variables the NOAM DSR fast deployment asks for during NOAM deployment.

Fast Deployment Variable	Description	Value
Cabinet ID of this Enclosure? (NOAM Blade Deployment Only)	This value should match the value entered from Section “Enclosure and Blades Setup” from reference [7] DSR Hardware and Software Installation Part 1, E76180.	
Enclosure ID? (NOAM Blade Deployment Only)	This value should match the value entered from Section “Enclosure and Blades Setup” from reference [7].	
Bay number of the First NOAM TVOE Host (NOAM Blade Deployment Only)	This value will be the blade number of the first NOAM server. Note: ‘F’ MUST append the bay number (example: 8F)	
Bay number of the Second NOAM TVOE Host (NOAM Blade Deployment Only)	This value will be the blade number of the second NOAM server. Note: ‘F’ MUST append the bay number (example: 16F).	
iLO/iLOM IP address of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM IP address of the First rack mount server. Note: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure “Add Rack Mount Server to the PMAC System Inventory” from reference [7].	
iLO/iLOM IP address of the Second Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM IP address of the First rack mount server.	
iLO/iLOM username of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM username of the first rack mount server. Note: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure “Add Rack Mount Server to the PMAC System Inventory” from reference [7].	
iLO/iLOM username of the Second Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM username of the second rack mount server.	

Fast Deployment Variable	Description	Value
iLO/iLOM password of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM password of the first rack mount server. Note: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure "Add Rack Mount Server to the PMAC System Inventory" from reference [7].	
iLO/iLOM password of the Second Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM password of the second rack mount server.	
Hostname for the First TVOE Host	This value will be the hostname of the first TVOE host.	
Hostname for the Second TVOE Host	This value will be the hostname of the second TVOE host.	
XMI IP address of the First TVOE Host (NOAM Blade Deployment Only)	This value will be the XMI IP address of the first TVOE host.	
XMI IP address of the Second TVOE Host (NOAM Blade Deployment Only)	This value will be the XMI IP address of the second TVOE host.	
PMAC VM Name of the First NOAM	This value will be the VM name (visible from Main Menu -> VM Management on the PMAC).	
PMAC VM Name of the Second NOAM	This value will be the VM name (visible from Main Menu -> VM Management on the PMAC).	
First NOAM Hostname	This value will be the first NOAM hostname.	
Second NOAM Hostname	This value will be the second NOAM hostname.	
XMI IP address of the First NOAM	This value will be the XMI IP address of the first NOAM. Note: this value will be used to access the NOAM GUI for configuration.	
Customer Provided NTP Server #1 Customer Provided NTP Server #2 Customer Provided NTP Server #3	Customer provided NTP source. Refer to Figure 2 of [7].	NTP Server #1: NTP Server #2: NTP Server #3:
XMI bond interface	This value will be the XMI bond interface. Example: bond0.3	
XMI VLAN ID	This value will be the XMI VLAN ID. Example: 3	
IMI bond interface	This value will be the IMI bond interface. Example: bond0.4	

Fast Deployment Variable	Description	Value
IMI VLAN ID	This value will be the IMI VLAN ID. Example: 4.	
Management bond interface (NOAM Rack Mount Server Deployments Only)	This value will be the Management bond interface. Example: bond0.2 Note: If NOAMs are located on the same TVOE host as the PMAC, this value MUST match what was configured in Section “TVOE Network Configuration” of reference [7].	
Management VLAN ID (NOAM Rack Mount Server Deployments Only)	This value will be the Management VLAN ID. Example: 2. Note: If NOAMs are located on the same TVOE host as the PMAC, this value MUST match what was configured in Section “TVOE Network Configuration” of reference [7].	
xmi Network IP Subnet Mask	This value will be the xmi IP network subnet mask.	
Management Network IP subnet mask	This value will be the management IP network subnet mask.	
xmi Network IP default gateway	This value will be the default gateway of the xmi network.	
Management Network IP default gateway	This value will be the default gateway of the management network.	

Appendix L: Growth/De-Growth

For scenarios where growth or de-growth is required, it may be necessary to delete or re-shuffle VM guests, SDS, and DSR servers. Appendix L.1 explains how to add individual VMs and add various DSR/SDS servers. Appendix L.2 explains how to delete individual VMs and move or remove various DSR/SDS servers.

Appendix L.1: Growth

For growth scenarios where it is necessary to add DSR servers, the following sequence of steps should be followed:

Step	Procedure(s)
Perform backups	Procedure 55. Perform Backups
Perform system health check	Procedure 56. Perform Health Check
Identify servers which are affected by the growth: <ul style="list-style-type: none"> • DR-NOAM • SOAM Spares • MP (SBR, SS7MP, IPFE) 	

Step	Procedure(s)
Add new servers Create and Configure the VMs on new servers (SOAM spare and DR-NOAMs only)	Procedure 57. Add a New Server/VMs
Configure servers in new VM locations	NOAM/DR-NOAM: Procedure 58. Growth: DR-NOAM SOAM: Procedure 59. Growth: SOAM spare (PCA Only) MP: Procedure 60. Growth: MP
Post growth health check	Procedure 61. Post Growth Health Check
Post growth backups	Procedure 62. Post Growth Backups

Procedure 55. Perform Backups

S T E P #	This procedure backs up all necessary items before a growth scenario.	
	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
1 <input type="checkbox"/>	Backup TVOE	Backup all TVOE host configurations by executing Procedure 40. Backup TVOE Configuration.
2 <input type="checkbox"/>	Backup PMAC	Backup the PMAC application by executing Procedure 41. Backup PMAC Application.
3 <input type="checkbox"/>	Backup NOAM/SOAM databases	Backup the NOAM and SOAM databases by executing Procedure 42. NOAM Database Backup and Procedure 43. SOAM Database Backup.

Procedure 56. Perform Health Check

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure verifies system status and log all alarms.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login \</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 56. Perform Health Check

<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Log current alarms</p>	<p>Navigate to Main Menu -> Alarms & Events -> View Active.</p> <p>Click Report.</p> <p>Save or Print this report, keep copies for future reference.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Repeat for SOAM</p>	<p>Repeat steps 1-4 for the SOAM</p>

Procedure 57. Add a New Server/VMs

<p>S</p> <p>T</p> <p>E</p> <p>P</p> <p>#</p>	<p>This procedure adds a new rack mount server.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Add/Configure additional servers</p>	<p>Follow the sections below to install and configure additional servers:</p> <p>DR-NOAMs: Section 4.2.1 Execute DSR Fast Deployment for DR-NOAMs</p> <p>Spare SOAMs: Procedure 11. Configure SOAM TVOE Server Blades</p> <p>MPs: Insert blade in desired location.</p>
<p>2</p> <p><input type="checkbox"/></p>	<p>Add/Configure new VMs</p>	<ol style="list-style-type: none"> 1. Create new virtual Machines for the Spare SOAMs by following Procedure 12. Create SOAM Guest VMs. 2. Install TPD and DSR Software by following Procedure 13. IPM Blades and VMs.

Procedure 58. Growth: DR-NOAM

S T E P #	<p>This procedure configures a DR-NOAM on the new virtual machine for VM growth scenarios.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> NEW Virtual Machine Created TPD/DSR software installed <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	NOAM VIP GUI: Configure the DR-NOAM	<p>Configure the DR-NOAM by executing the steps referenced in the following procedures:</p> <p>DSR DR-NOAM: Section 4.2.2 Pair DR-NOAMs (Section 4.2.3 Install NetBackup Client (Optional))</p>
2 <input type="checkbox"/>	DR-NOAM: Activate optional features (DSR only)	<p>If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to Section 3.4 Optional Features</p>
3 <input type="checkbox"/>	NOAM VIP: Execute the key revocation script on the active NOAM (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new NOAM server created:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_NOAM_hostname></pre> <p>Note: Key transfer successful output should be given.</p>

Procedure 59. Growth: SOAM spare (PCA Only)

S T E P #	<p>This procedure configures an SOAM spare on the new virtual machine for VM growth scenarios.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> NEW Virtual Machine Created TPD/DSR software installed <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	NOAM VIP GUI: Configure the SOAM spare	<p>Configure the SOAM spare by executing the steps referenced in the following procedures:</p> <p>DSR SOAM spare:</p> <ul style="list-style-type: none"> Procedure 15. Configure SOAM NE Procedure 16. Configure the SOAM Servers Procedure 17. Configure the SOAM Server Group (steps 1, 4, 6, and 9)

Procedure 59. Growth: SOAM spare (PCA Only)

2 <input type="checkbox"/>	NOAM GUI: Activate optional features	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to Section 3.3 Optional Features.
3 <input type="checkbox"/>	NOAM VIP: Execute the key revocation script on the active NOAM (RADIUS)	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new SOAM server created:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_SOAM_hostname></pre> <p>Note: Key transfer successful output should be given.</p>

Procedure 60. Growth: MP

S	This procedure configures an MP on the new virtual machine for growth scenarios.	
T	Prerequisites: TPD/DSR software installed	
E	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	NOAM VIP GUI: Configure the MP	<p>Configure the MP/DP by executing the steps referenced in the following procedures:</p> <p>DSR MP: Procedure 20. Configure MP Blade Servers (steps 1-2, 7-14, 15-17 (Optional))</p>
2 <input type="checkbox"/>	NOAM VIP: Execute the key revocation script on the active NOAM (RADIUS)	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new MP server created:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_MP_hostname></pre> <p>Note: Key transfer successful output should be given.</p>

Procedure 61. Post Growth Health Check

<p>S T E P #</p>	<p>This procedure verifies system status and logs all alarms after growth.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div data-bbox="480 541 1333 590" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>
<p>2 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify server status</p>	<p>Navigate to Main Menu -> Status & Manage -> Server.</p> <p>Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).</p>

Appendix L.2: De-Growth

For De-growth scenarios where it is necessary to remove/delete DSR/SDS MP(SBR, SS7, IPFE) servers, the following sequence of steps should be followed:

Step	Procedure(s)
Perform backups	Procedure 63. Perform Backups
Perform system health check	Procedure 64. Perform Health Check
Identify servers affected by the de-growth: DSR MP (SBR, SS7MP, IPFE)	
Remove identified servers from server group	Procedure 65. Remove Server from Server Group
Shutdown and remove the identified server's VM	
Post de-growth health check	Procedure 66. Post Growth Health Check
Post de-growth backups	Procedure 67. Post Growth Backups

Procedure 63. Perform Backups

S T E P #	This procedure backs up all necessary items before a growth scenario.	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
1 <input type="checkbox"/>	Backup TVOE	Backup all TVOE host configurations by executing Procedure 40. Backup TVOE Configuration.
2 <input type="checkbox"/>	Backup PMAC	Backup the PMAC application by executing Procedure 41. Backup PMAC Application.
3 <input type="checkbox"/>	Backup NOAM/SOAM databases	Backup the NOAM and SOAM databases by executing Procedure 42. NOAM Database Backup and Procedure 43. SOAM Database Backup.

Procedure 64. Perform Health Check

<p>S T E P #</p>	<p>This procedure verifies system status and logs all alarms.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div data-bbox="480 541 1333 590" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 64. Perform Health Check

<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Log current alarms</p>	<p>Navigate to Main Menu -> Alarms & Events -> View Active.</p> <p>Click Report.</p> <p>Save or Print this report and keep copies for future reference.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Repeat for SOAM</p>	<p>Repeat steps 1-4 for the SOAM.</p>

Procedure 65. Remove Server from Server Group

<p>S T E P #</p>	<p>Once the server's that will be deleted have been identified, the server first needs to be removed from its server group.</p> <p>The following procedure removes a server from a server group.</p> <p>Warning: It is recommended that no more than one server from each server group be removed from a server group at a time.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>SOAM VIP GUI: Login</p>	<p>Execute this step if removing SS7MP, otherwise skip to step 11.</p> <p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_SOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 65. Remove Server from Server Group

10 <input type="checkbox"/>	SOAM VIP GUI: Delete SS7-MP transports	Execute this step if Removing SS7MP, otherwise skip to step 11. Navigate to Main Menu -> Transport Manager -> Maintenance -> Transport. Delete the associated transports from the identified SS7-MP.
11 <input type="checkbox"/>	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: <div data-bbox="444 764 1299 814" style="border: 1px solid black; padding: 2px;"><code>http://<Primary_NOAM_VIP_IP_Address></code></div> Login as the guiadmin user.

Procedure 65. Remove Server from Server Group

12 <input type="checkbox"/>	NOAM VIP GUI: Set server to OOS	Navigate to Main Menu -> Status & Manage -> HA. Click Edit. Set the server's Max Allowed HA Role to OOS. Click OK.
--------------------------------	---	---

Procedure 66. Post Growth Health Check

<p>S T E P #</p>	<p>This procedure verifies system status and logs all alarms after growth.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div data-bbox="480 541 1334 592" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user.</p>

Procedure 67. Post Growth Backups

S	This procedure backs up all necessary items after a growth scenario.	
T	Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		
P	If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.	
#		
1 <input type="checkbox"/>	Backup TVOE	Backup all TVOE host configurations by executing Procedure 40. Backup TVOE Configuration.
2 <input type="checkbox"/>	Backup PMAC	Backup the PMAC application by executing Procedure 41. Backup PMAC Application.
3 <input type="checkbox"/>	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Procedure 42. NOAM Database Backup and Procedure 43. SOAM Database Backup.

Appendix O: Restore SNMP Configuration to SNMPv3 (Optional)

<p>S T E P #</p>	<p>This procedure restores SNMP configuration to SNMPv3 for forwarding of SNMP traps from each individual server.</p> <p>Note: If SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a work around step (section 4.5, steps 6-9) and the SNMPv3 is required to be configured.</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix P: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>(Workaround)</p> <p>Primary NOAM VIP GUI: Login</p>	<p>Note: This workaround step should be performed only in the following case if SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a workaround step (section 4.5, steps 6-9) and the SNMPv3 is required to be configured.</p> <p>Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<NOAM_XMI_VIP_IP_Address>">http://<NOAM_XMI_VIP_IP_Address></p> </div> <p>Login as the guiadmin user.</p>

2	NOAM VIP GUI: <input type="checkbox"/> Configure system-wide SNMP Trap receiver(s)	<p>Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping.</p> <p>Select the Server Group tab for SNMP trap configuration. The server group that is configured for SNMPv2c & SNMPv3 as a workaround:</p> <p>Click Edit.</p> <div style="display: flex; justify-content: center; gap: 10px;"> Insert Edit Delete Suspend Resume </div> <p>Update the Enabled Versions as SNMPv3:</p> <p>Enabled Versions <input style="width: 150px;" type="text" value="SNMPv3"/></p> <p>Click OK.</p>
---	--	--

Appendix P: My Oracle Support (MOS)

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

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

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

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