Oracle® Communications

Diameter Signaling Router 7.2/7.3

C-Class Software Installation and Configuration

Procedure 2/2

E69409 Revision 02

July 2016

ORACLE®

Oracle ® Communication Diameter Signaling Router DSR C-Class Software Installation and Configuration Procedure 2/2 Release 7.2/7.3

CAUTION:

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

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

See more information on MOS in the Appendix section.

Note: This document represents the 2nd part of the DSR 7.2/7.3 Installation Process. Prior to executing this document, make sure that the 1st part was fully executed:

- **DSR 7.2/7.3 Installs:** Use document [7] as Part 1

Table of Contents

List of Procedures

Tables and Figures

1.0 INTRODUCTION

1.1 Purpose and Scope

This document describes the application-related installation procedures for an HP C-class Diameter Signaling Router 7.2/7.3 system.

This document assumes that platform-related configuration has already been done. Before executing this document, please ensure that all procedures from [7] 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 N**: Growth/De-Growth.

1.2 References

[1] DSR Meta Administration Feature Activation Procedure, E58661
[2] DSR Full Address Based Resolution (FABR) Feature Activation Procedure, E58664
[3] DSR Range Based Address Resolution (RBAR) Feature Activation Procedure, E58664
[4] SDS SW Installation and Configuration Guide, E57487
[5] MAP-Diameter IWF Feature Activation Procedure. E58666
[6] DSR IPv6 Migration Guide, E57517
[7] DSR 7.2/7.3 Base Hardware and Software Installation, E53488
[8] DSR GLA Feature Activation Procedure, E58659
[9] DSR 7.2/7.3 PCA Activation and Configuration, E67989
[10] DSR DTLS Feature Activation Procedure, E67867
[11] DSR 7.2/7.3 Radius Shared secret encryption key revocation MOP MO008572
[12] Platform 7.0 Configuration Procedure, E54386

1.3 Acronyms

An alphabetized list of acronyms used in the document

Table 1 Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
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
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

1.4 Terminology

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

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

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

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

5 ☐	**ServerX:** Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. **`$ cu -l /dev/ttyS7`**

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

Table 2 Terminology

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 PM&C) and to serve other configuration purposes.
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.
Site	Applicable for various applications, a Site is type of "Place". A Place is configured object that allows servers to be associated with a physical location. A Site place allows servers to be associated with a physical site. For example, Sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one Site when the server is configured. For the Policy & Charging DRA application, when configuring a Site only put DA-MPs and SBR MP servers in the site. Do not add NOAM, SOAM or IPFE MPs to a Site
Place Association	Applicable for various applications, a "Place Association" is a configured object that allows Places to be grouped together. A Place can be a member of more than one Place Association. The Policy & Charging DRA application defines two Place Association Types: Policy Binding Region and Policy & Charging Mated Sites.
Two Site Redundancy	Two Site Redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy & Charging Mated Sites Place Association containing two sites. Two Site Redundancy is a feature provided by Server Group configuration. This feature provides geographic redundancy. Some Server Groups can be configured with servers located in two geographically separate Sites(locations). This feature will ensure that there is always a functioning Active server in a Server Group even if all the servers in a single site fail.

Three Site Redundancy	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 & Charging Mated Sites Place Association containing three sites. 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 will ensure that there is always a functioning Active server in a Server Group even if all the servers in two sites fail.
Policy & Charging SBR Server Group Redundancy	The Policy and Charging application will use SBR Server Groups to store the application data. The SBR Server Groups will support both Two and Three Site Redundancy. The Server Group Function name is “Policy & Charging SBR”.
Server Group Primary Site	A Server Group Primary Site is a term used to represent the principle location within a SOAM or SBR Server Group. SOAM and SBR Server groups are intended to span several Sites(Places). For the Policy & Charging DRA application, these Sites(Places) are all configured within a single “Policy and Charging Mated Sites” Place Association. The Primary Site may be in a different Site(Place) for each configured SOAM or SBR Server Group . A Primary Site is described as the location in which the Active and Standby servers to reside, however there cannot be any Preferred Spare servers within this location. All SOAM and SBR Server Groups will have a Primary Site.
Server Group Secondary Site	A Server Group Secondary Site is a term used to represent location in addition to the Primary Site within a SOAM or SBR Server Group. SOAM and SBR Server groups are intended to span several Sites(Places). For the Policy & Charging DRA application, these Sites(Places) are all configured within a single “Policy and Charging Mated Sites” Place Association. 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.

Server Group Tertiary Site	A Server Group Tertiary Site is a term used to represent location in addition to the Primary & 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. The Tertiary Site may be in a different Site(Place) for each configured SOAM or SBR Server Group . 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.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

2.0 GENERAL DESCRIPTION

This document defines the steps to execute the initial installation of the Diameter Signaling Router (DSR) 7.2/7.3 application on new HP C-Class Hardware.

DSR 7.2/7.3 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.

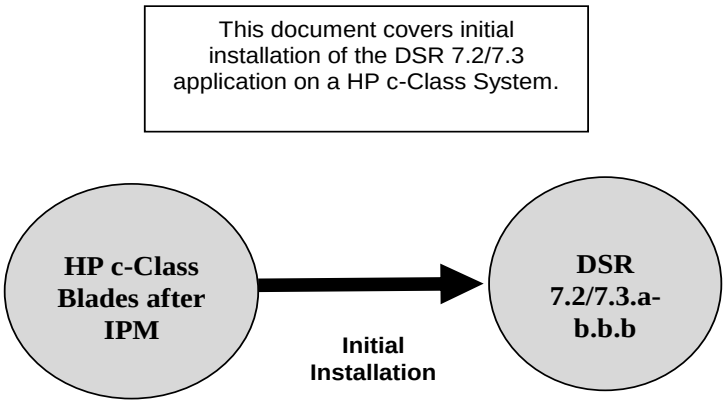


Figure 2 Example of Initial Application Installation Path

3.0 INSTALL OVERVIEW

This section provides a brief overview of the recommended method for installing DSR software that is on an HP c-Class system. The basic install process and approximate time required is outlined in **Figure 4**.

3.1 Required Materials

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

3.2 Installation Overview

This section describes the overall strategy to be employed for a single or multi-site DSR 7.2/7.3 installation. It also lists the procedures required for installation with estimated times. **Section 3.2.1 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. **3.2.3 Installation Procedures)** lists the steps required to install a DSR 7.2/7.3 system. These latter sections expand on the information from the matrix and provide a general timeline for the installation.

3.2.1 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 will executed at each site.

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

1) An overall installation requirement is decided upon. Among the data that should be collected:
    - The total number of 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 will 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 will execute the procedures in document [7] to set up the PMAC, HP enclosures, and switches. Then, using the procedures in this document, all servers will be IPM-ed with the proper TPD and DSR application ISO image. **Figure 4** details the exact procedures that are to be executed for the 2nd part of this install. When this is complete, all non-NOAM sites will be reachable through the network and ready for further installation when the primary NOAM site is brought up.
4) The installer will then move to the "main" site that will contain the primary NOAM. Again, [7] will be executed for this site. Then, moving on to the procedures in this document, **Figure 4** is consulted to determine the procedure list. During this install, the user will "bring up" the other sub-sites (if they exist) that were 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] and this document, then full DSR installation is complete.

    Note: An alternative install strategy will swap steps 3 & 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.

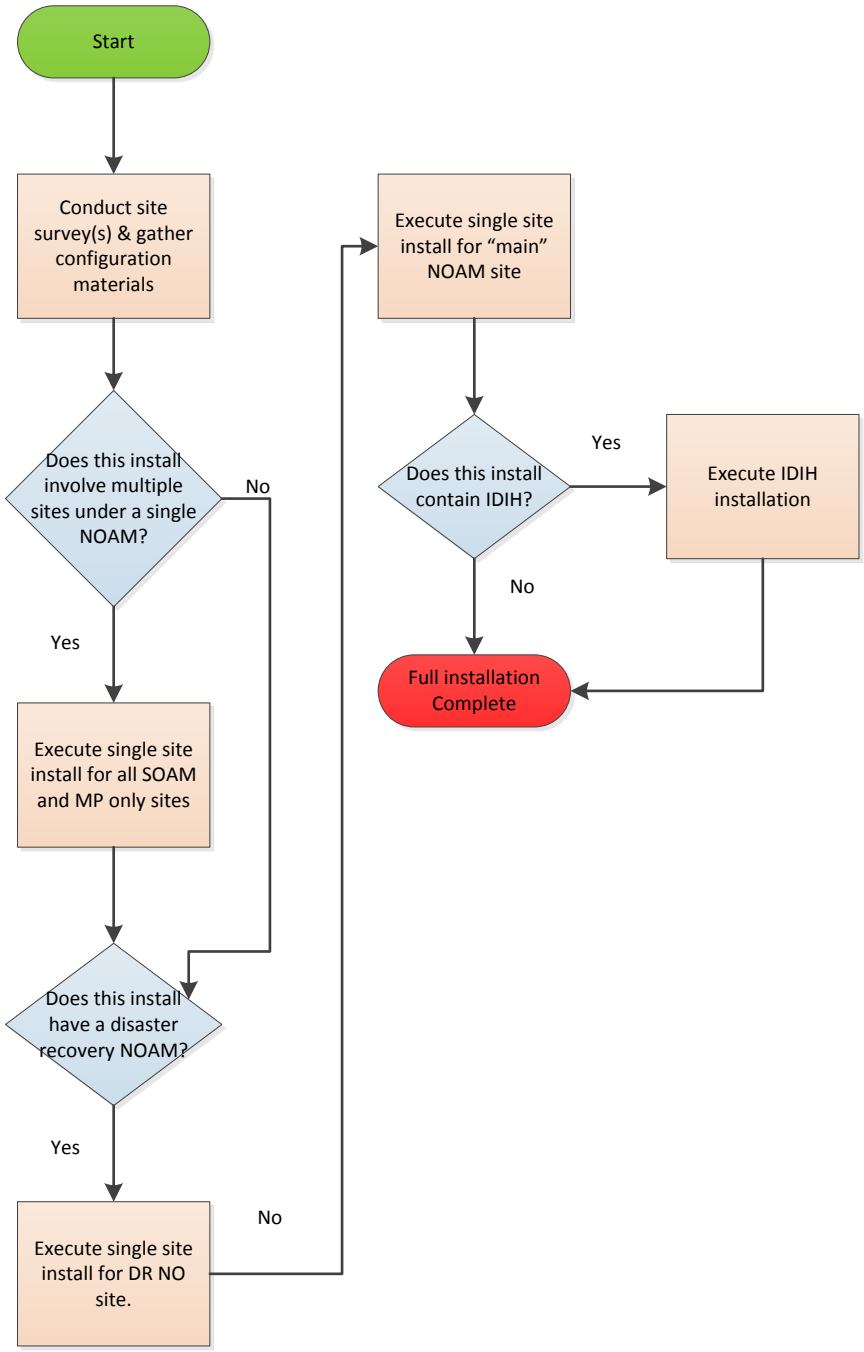


Figure 3 DSR Installation: High Level Sequence

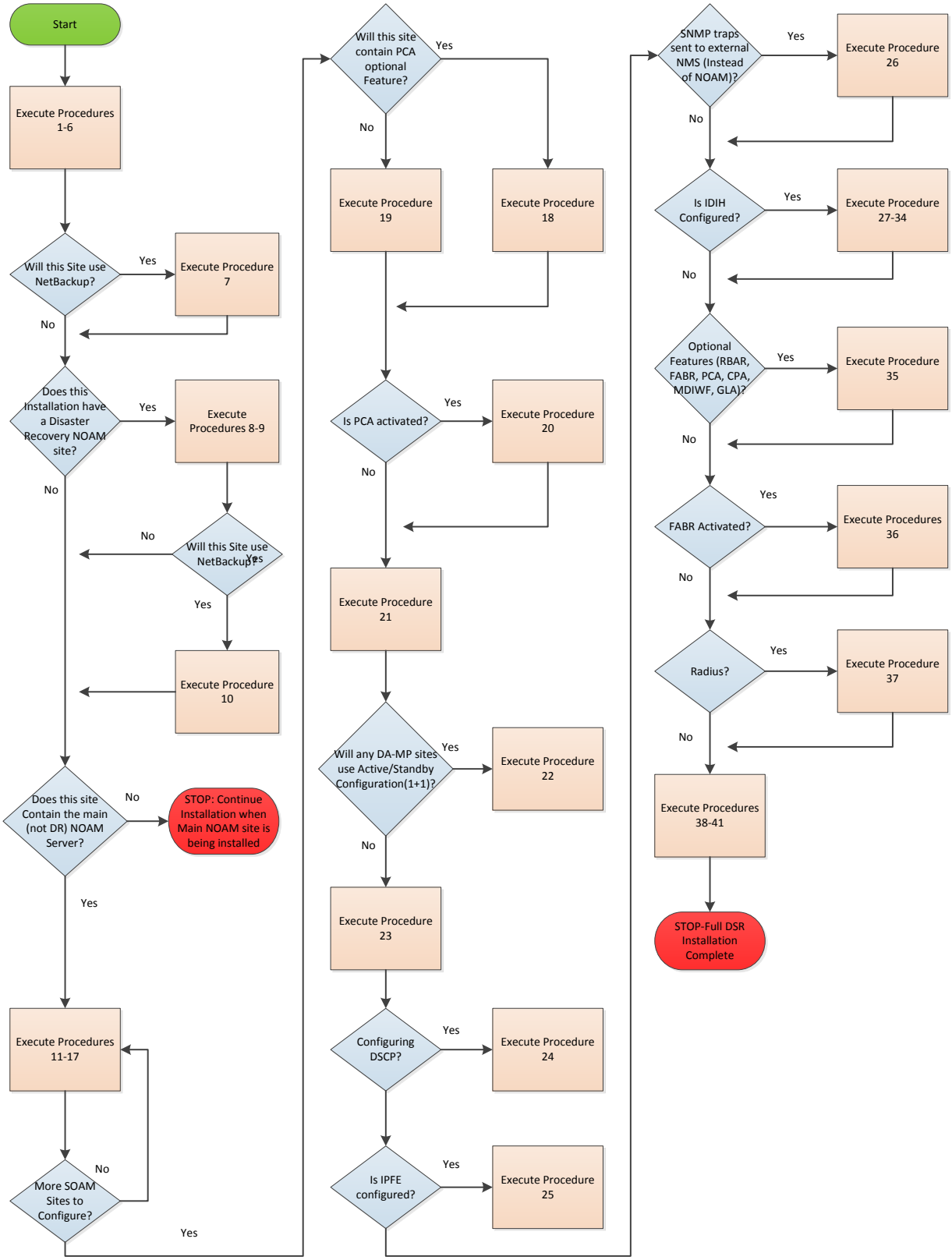


Figure 4 DSR Single Site Installation Procedure Map

3.2.2 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 will terminate at the NOAM and be 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 will be seen at the SOAM AND/OR NOAM as alarms AND they will be 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

3.2.3 Installation Procedures

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

TABLE 2 INSTALLATION OVERVIEW

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 1	Load Application and TPD ISO onto PMAC Server	15	15
Procedure 2	Configure NOAM Servers	25	40
Procedure 3	Configure the First NOAM NE and Server	10	50
Procedure 4	Configure the NOAM Server Group	5	55
Procedure 5	Configure the Second NOAM Server	10	65
Procedure 6	Complete NOAM Server Group Configuration	5	70
Procedure 7	Install NetBackup Client*	15	85
Procedure 8	NOAM Configuration for DR Site*	25	110
Procedure 9	Pairing for DR-NOAM site*	15	125
Procedure 10	Install NetBackup Client*	15	140
Procedure 11	Configure SOAM TVOE Server Blades	15	165
Procedure 12	Create SOAM Guest VMs	5	170
Procedure 13	IPM Blades and VMs	20	190
Procedure 14	Install the Application Software	15	215
Procedure 15	Configure SOAM NE	5	220
Procedure 16	Configure the SOAM Servers	20	240
Procedure 17	Configure the SOAM Server Group	10	250
Procedure 18	Configure MP Blade Servers	25	275
Procedure 19	Activate PCA (PCA Only)*	10	285
Procedure 20	Configure Places and Assign MP Servers to Places (PCA ONLY)*	10	295
Procedure 21	Configure the MP Server Group(s) and Profile(s)	10	305
Procedure 22	Add VIP for Signaling networks (Active/Standby Configurations Only)*	5	310
Procedure 23	Configure the Signaling Network Routes	10	320
Procedure 24	Configure DSCP Values for Outgoing Traffic*	10	330
Procedure 25	IP Front End (IPFE) Configuration*	15	345
Procedure 26	Configure SNMP Trap Receiver(s)*	10	355
Procedure 27	IDIH Configuration*	90	445
Procedure 28	Configure DSR Reference Data Synchronization for IDIH*	15	460
Procedure 29	IDIH Configuration: Configuring the SSO Domain*	30	490
Procedure 30	IDIH Configuration: Configure IDIH in the DSR*	20	510
Procedure 31	IDIH Configuration: Configure Mail Server*	20	530
Procedure 32	IDIH Configuration: Configure SNMP Management Server*	20	550
Procedure 33	IDIH Configuration: Change Network Interface*	20	570

Procedure 34	IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File*	10	580
Procedure 35	Activate Optional Features*	30	610
Procedure 36	Configure ComAgent Connections (DSR + SDS)	20	630
Procedure 37	Shared secret encryption key revocation (Radius Only)*	20	650
Procedure 38	Backup TVOE Configuration	10	660
Procedure 39	Backup PMAC Application	10	670
Procedure 40	NOAM Database Backup	10	680
Procedure 41	SOAM Database Backup	10	690

* denotes Optional Steps

3.2 Optional Features

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

TABLE 3 OPTIONAL FEATURES

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure, E58661
Charging Proxy Application (CPA)	DSR CPA Feature Activation Procedure, E58663
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E58664
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure, E58665
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure, E58666
Policy and Charging Application (PCA)	DSR 7.0 PCA Activation and Configuration Procedure, E58667 DSR 7.1/7.2/7.3 PCA Activation and Configuration Procedure, E63560
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure, E58659

4.0 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] for instructions on how to accomplish this IPv6 migration.

4.1 Install and Configure NOAM Servers

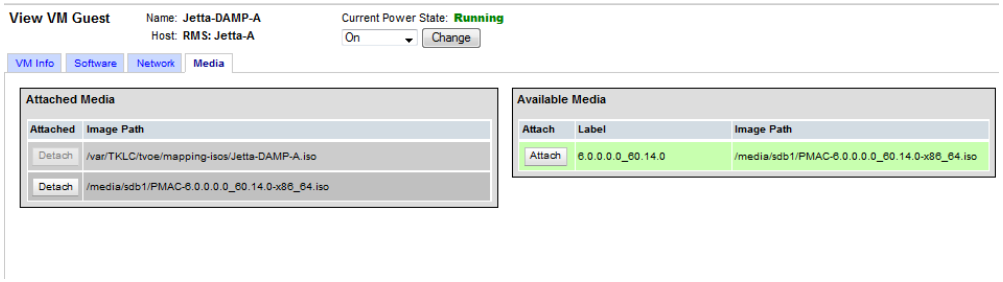
4.1.1 Load Application and TPD ISO onto the PMAC Server

Procedure 1: Load Application and TPD ISO onto PMAC Server

S T E P #	This procedure will load the DSR Application and TPD ISO into the PMAC Server **Needed material:** - Application Media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O:** My Oracle Support (MOS), and ask for assistance.	

1
☐
	TVOE Host: Load Application ISO	Add the Application ISO image to the PM&C, this can be done in one of three ways:
		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 PM&C server into the **"/var/TKLC/smac/image/isoimages/home/smacftpus**r/" directory as pmacftpusr user:
		cd into the directory where your ISO image is located on the **TVOE Host** (*not on the PM&C server*)
		Using sftp, connect to the PM&C server
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		After the image transfer is 100% complete, close the connection:
		`$ quit`

Procedure 1: Load Application and TPD ISO onto PMAC Server

2 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 
3 ☐	**PMAC GUI:** Attach the software Image to the PMAC Guest	If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, navigate to **Main Menu -> VM Management.** Select the PMAC guest. On the resulting *"**View VM Guest**"* page, select the **Media** tab. Under the **Media** tab, find the ISO image in the *"**Available Media**"* list, and click its **Attach** button. After a pause, the image will appear in the *"**Attached Media**"* list. 

Procedure 1: Load Application and TPD ISO onto PMAC Server

4
☐
	PMAC GUI:
	Add Application Image
		Navigate to **Main Menu -> Software -> Manage Software Images**
		
		Press **Add Image** button. Use the drop down to select the image.
		
		Add Image Edit Image Delete Selected
		
		If the image was supplied on a CD or a USB drive, it will appear as a virtual device ***("device://…").*** These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, ***"device://dev/sr1".*** If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.
		If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file ***"/var/TKLC/...".***
		
		Add Software Image
		
		Images may be added from any of these sources:
		• Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
		• USB media attached to the PM&C's host (Refer to Note)
		• External mounts. Prefix the directory with "extfile://".
		• These local search paths:
		  ○ /var/TKLC/upgrade/*.iso
		  ○ /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso
		
		Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM
		
		Path: /var/TKLC/upgrade/DSR-7.2.0.0.0_72.9.0-x86_64.iso
		Description:
		
		Add New Image
		
		Select the appropriate path and Press **Add New Image** button.
		
		You may check the progress using the **Task Monitoring** link. Observe the green bar indicating success.
		
		Once the green bar is displayed, remove the DSR application Media from the optical drive of the management server.

Procedure 1: Load Application and TPD ISO onto PMAC Server

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

4.1.2 Execute DSR Fast Deployment for NOAMs

Procedure 2: Configure NOAM Servers

S T E P #	This procedure will extend 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. **Prerequisite:** TVOE and PMAC (virtualized) have been installed on the First RMS Server as described in [7] 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 O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**PMAC Server:** Login	Establish an SSH session to the PMAC server, login as ***admusr***.

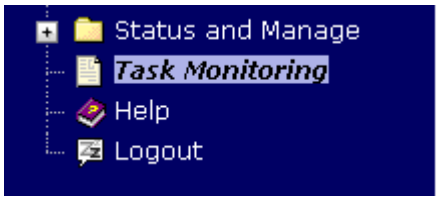
Procedure 2: Configure NOAM Servers

2
☐
	PMAC Server: Update the DSR Fast Deployment template	Perform the following command to navigate to the directory containing the DSR fast deployment template:
		
		`$ cd /usr/TKLC/smac/etc`
		
		DSR Fast Deployment Template Names:
		
		NOAM on Rack Mount Servers: DSR_NOAM_FD_RMS.xml
		NOAM on Blade Servers: DSR_NOAM_FD_Blade.xml
		
		Note: If the fast deployment template is not present, then please re-execute section "Setup PM&C" step 10, sub step C from [7].
		
		Update the following items within the Fast deployment xml:
		
		TPD and DSR ISO:
		
		<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-7.2/7.3.0.0.0_72.8.0-x86_64</name>
		</image>
		</software>
		
		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:
		
		`$ ls /var/TKLC/smac/image/repository`
		
		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.
		
		<!--
		<tpdinterface id="bond1">
		<device>bond1</device>
		<type>Bonding</type>
		<bonddata>
		<bondinterfaces>eth03,eth04</bondinterfaces>
		<bondopts>mode=active-backup,miimon=100</bondopts>
		</bonddata>
		<onboot>yes</onboot>
		<bootproto>none</bootproto>
		</tpdinterface>
		-->

Procedure 2: Configure NOAM Servers

3
☐
	PMAC Server: Validate and Run the Fast Deployment File	Validate/Create the fast deployment file by executing the following command:
		
		For NOAMs deployed on rack mount servers:
		
		`$ sudo fdconfig validate --file=DSR_NOAM_FD_RMS.xml`
		
		For NOAMs deployed on blade servers:
		
		`$ sudo fdconfig validate --file=DSR_NOAM_FD_Blade.xml`
		
		Note: Refer to **Appendix M**: DSR Fast Deployment Configuration for information of the variables that must be input during execution of NOAM fast deployment.
		
		If there were errors during validation, correct the errors within the xml file and re-run the validation.
		
		After successful validation, a new Fast deployment xml file is created:
		
		`---  NOTICE  ---`
		`Config Data saved as a new file: "./DSR_NOAM_FD_Blade_20151217T102402.xml"`
		`---  NOTICE  ---`
		
		`Configuration file validation successful.`
		`Validation complete`
		`[admusr@GuestPMACeco upgrade]$`
		
		Execute the following commands to run the fast deployment file:
		
		`$ screen`
		
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`
		
		Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “screen -dr” to resume the screen session in the event of a terminal timeout etc.

Procedure 2: Configure NOAM Servers

4 ☐	**PMAC GUI:** Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the DSR NOAM TVOE configuration to completion:

	110	Tpd ServerAction: File Transfer	RMS: Oahu-TVOE-2	File transfer success	COMPLETE	0:00:14	2015-11-24 07:42:35	100%
	109	Tpd ServerAction: File Transfer	RMS: Oahu-TVOE-1	File transfer success	COMPLETE	0:00:03	2015-11-24 07:42:35	100%
	108	Accept Upgrade	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Success	COMPLETE	0:01:02	2015-11-24 07:41:08	100%
	107	Accept Upgrade	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Success	COMPLETE	0:01:03	2015-11-24 07:34:30	100%
	106	Upgrade	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Success	COMPLETE	0:12:57	2015-11-24 07:26:05	100%
	105	Upgrade	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Success	COMPLETE	0:07:17	2015-11-24 07:26:00	100%
	104	Install OS	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Done: TPD.install-7.0.2.0.0_86.34.0-OracleLinux6.6-x86_64	COMPLETE	0:11:21	2015-11-24 07:11:07	100%
	103	Install OS	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Done: TPD.install-7.0.2.0.0_86.34.0-OracleLinux6.6-x86_64	COMPLETE	0:11:26	2015-11-24 07:11:02	100%
	102	VirtAction: Create	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Guest creation completed (Oahu-DSR-NOAM-2)	COMPLETE	0:00:10	2015-11-24 07:10:52	100%
	101	VirtAction: Create	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Guest creation completed (Oahu-DSR-NOAM-1)	COMPLETE	0:00:05	2015-11-24 07:10:52	100%

4.1.3 Configure NOAMs

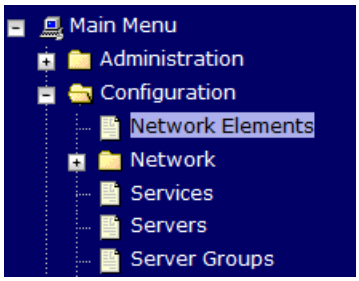
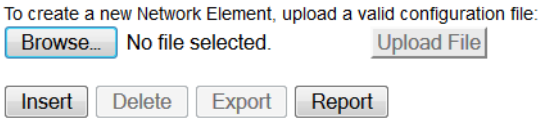
Procedure 3: Configure the First NOAM NE and Server

S T E P #	This procedure will provide the steps to configure the First NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Save the NOAM Network Data to an XML file**	Using a text editor, create a NOAM Network Element file that describes the networking of the target install environment of your first NOAM server. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is ***"Appname_NEname_NetworkElement.XML"***, so for example a DSR2 NOAM network element XML file would have a filename ***"DSR2_NOAM_NetworkElement.xml"***. Alternatively, you can update the sample DSR 7.2/7.3 Network Element file. It can be found on the management server at: `/usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml` A sample XML file can also be found in **Appendix A**: Sample Network Element and Hardware Profiles. **Note:** The following limitations apply when specifying a Network Element name: A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.

Procedure 3: Configure the First NOAM NE and Server

2 ☐	**NOAM GUI:** Login	Using the xmi IP address configured in **procedure 2** ($NOAM1_xmi_IP_address) Login to the NOAM GUI as the ***guiadmin*** user: 

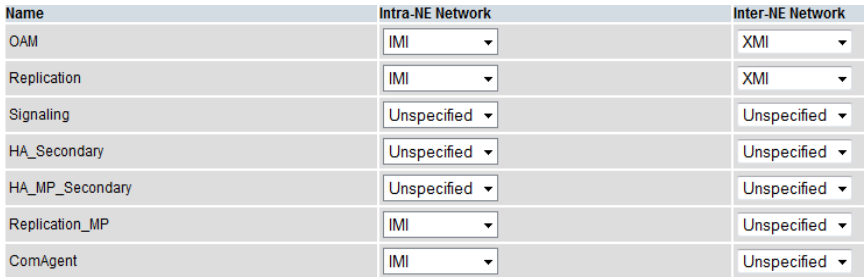
Procedure 3: Configure the First NOAM NE and Server

3 ☐	**Create the NOAM Network Element using the XML File**	Navigate to **Main Menu->Configuration->Network Elements**  Select the **Browse/ChooseFile** button, and enter the pathname of the NOAM network XML file. Select the **Upload File** button to upload the XML file and configure the NOAM Network Element.  Once the data has been uploaded, you should see a folder appear with the name of your network element. Click on this folder and you will get a drop-down which describes the individual networks that are now configured: Network Element NO_9006005 Network Name / Network Address / Netmask / VLAN ID / Gateway IP Address INTERNALXMI / 10.240.10.32 / 255.255.255.224 / 3 / 10.240.10.35 INTERNALIMI / 10.240.10.0 / 255.255.255.224 / 4 / 10.240.10.3

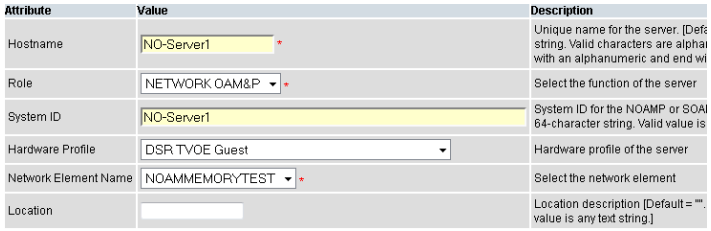
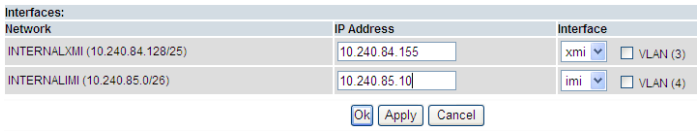
Procedure 3: Configure the First NOAM NE and Server

4 ☐	**Map Services to Networks**	Navigate to **Main Menu ->Configuration-> Services.** Select the **Edit** button and set the Services as shown in the table below: (see table below) For example, if your IMI network is named **IMI** and your XMI network is named ***XMI,*** then your services should config should look like the following: (see screenshot below) Select the **Ok** button to apply the Service-to-Network selections. Press **Ok** for the following prompt to restart all servers. (see screenshot below)

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



Procedure 3: Configure the First NOAM NE and Server

5 ☐	**Insert the 1st NOAM server**	Navigate to **Main Menu -> Configuration -> Servers.** Select the **Insert** button to insert the new NOAM server into servers table (the first or server).  Attribute / Value / Description Hostname: NO-Server1 * — Unique name for the server. [Defa string. Valid characters are alpha with an alphanumeric and end wi Role: NETWORK OAM&P * — Select the function of the server System ID: NO-Server1 — System ID for the NOAMP or SOA 64-character string. Valid value is Hardware Profile: DSR TVOE Guest — Hardware profile of the server Network Element Name: NOAMMEMORYTEST * — Select the network element Location: — Location description [Default = "". value is any text string.] Fill in the fields as follows: **Hostname: <Hostname>** **Role: NETWORK OAM&P** **System ID: <Site System ID>** **Hardware Profile: DSR TVOE Guest** **Network Element Name: [Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Interfaces: Network / IP Address / Interface INTERNALXMI (10.240.84.128/25) — 10.240.84.155 — xmi — VLAN (3) INTERNALIMI (10.240.85.0/26) — 10.240.85.10 — imi — VLAN (4) Ok Apply Cancel Fill in 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 '$NOAM1_xmi_IP_address' configured in Procedure 2 Fill in the server IP addresses for the IMI network. Select **imi** for the interface. **Leave the "VLAN" checkbox unchecked**. **Note:** The imi server IP must match '$NOAM1_imi_IP_address' configured in Procedure 2 Next, add the following NTP servers: **NTP Server** — **Preferred?** ***<TVOE_XMI_IP_Address(NO1)/ TVOE_Mgmt_IP_Address(NO1)>*** — Yes Select the **Ok** button when you have completed entering all the server data.

Procedure 3: Configure the First NOAM NE and Server

6 ☐	**Export the Initial Configuration**	Navigate to **Main Menu -> Configuration -> Servers.** From the GUI screen, select the NOAM server and then select **Export** to generate the initial configuration data for that server. Insert Edit Delete Export Report
7 ☐	**NOAM:** Copy Configuration File to 1st NOAM Server	Establish an SSH session to the 1st NOAM server, logging in as the **admusr** user. Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the /var/tmp directory. The configuration file will have a filename like TKLCConfigData.<***hostname***>.sh. The following is an example: `$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.blade01.sh /var/tmp/TKLCConfigData.sh`
8 ☐	**NOAM:** Wait for Configuration to Complete	The automatic configuration daemon will look for the file named ***"TKLCConfigData.sh"*** in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server, but **DO NOT** reboot the server, it will be rebooted later on in this procedure. **Note**: Ignore the warning about removing the USB key, since no USB key is present. .

9
☐
	NOAM: Set the Time zone and Reboot the Server	From the command line prompt, execute ***set_ini_tz.pl***. This will set the system time zone The following command example uses the America/New_York time zone.
		
		Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see **Appendix I**: List of Frequently used Time Zones.
		
		`$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1`
		
		`$ sudo init 6`

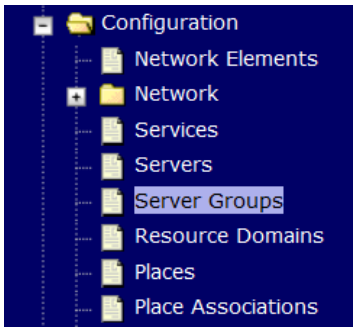
Procedure 3: Configure the First NOAM NE and Server

10 ☐	**1st NOAM:** Configure Networking for Dedicated NetBackup Interface (Optional)	**Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup. Obtain a terminal window to the 1st NOAM server, logging in as the ***admusr*** user. **$ sudo /usr/TKLC/plat/bin/netAdm set --device=NetBackup** **--type=Ethernet --onboot=yes** **--address=<NO1_NetBackup_IP_Adress>** **--netmask=<NO1_NetBackup_NetMask>** **$ sudo /usr/TKLC/plat/bin/netAdm add --route=net** **--device=netbackup --address=<NO1_NetBackup_Network_ID>** **--netmask=<NO1_NetBackup_NetMask>** **--gateway=<NO1_NetBackup_Gateway_IP_Address>**
11 ☐	**1st NOAM Server:** Verify Server Health	Execute the following command on the 1st NOAM server and make sure that no errors are returned: **$ sudo syscheck** Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log

Procedure 4: Configure the NOAM Server Group

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

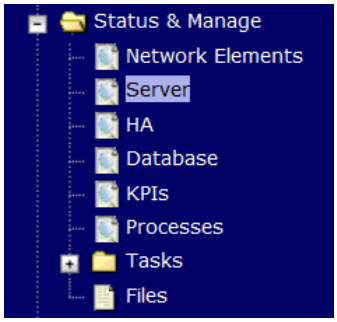
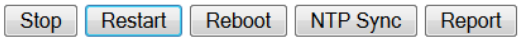
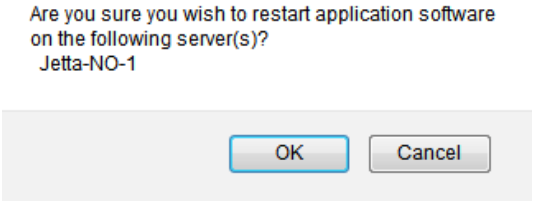
Procedure 4: Configure the NOAM Server Group

2 ☐	**NOAM GUI:** Enter NOAM Server Group Data	Navigate to **Main Menu** -> **Configuration** -> **Server Groups**  Select **Insert** and fill the following fields: Insert Edit Delete Report • **Server Group Name: <Enter Server Group Name>** • **Level: A** • **Parent : None** • **Function: DSR (Active/Standby Pair)** • **WAN Replication Connection Count: Use Default Value** Select **OK** when all fields are filled in.
3 ☐	**NOAM GUI:** Edit the NOAM Server Group	From the GUI **Main Menu -> Configuration -> Server Groups**. Select the new server group, and then select **Edit** Insert Edit Delete Report Select the Network Element that represents the NOAM. NO_900060103 Server | SG Inclusion | Preferred HA Role HPC6NO | ☑ Include in SG | ☐ Preferred Spare In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Click the **Include in SG** checkbox. Leave other boxes blank. Press **OK**

Procedure 4: Configure the NOAM Server Group

4 ☐	**NOAM:** Verify NOAM blade server role	From terminal window to the iLO of the first NOAM server, execute the following command: `$ha.mystate` Verify that the **DbReplication** and **VIP** item under the **resourceId** column has a value of **Active** under the **role** column. You might have to wait a few minutes for it to become in that state. Example: [admusr@Jetta-NO-1 ~]$ ha.mystate resourceId role node subResources lastUpdate DbReplication Active A1027.209 0 0316:161158.499 VIP Active A1027.209 0 0316:161158.501 pSbrBBaseRepl OOS A1027.209 0 0316:155546.074 pSbrBindingRes OOS A1027.209 0 0316:155546.074 pSbrSBaseRepl OOS A1027.209 0 0316:155546.075 pSbrSessionRes OOS A1027.209 0 0316:155546.075 PSBR_B_Proc OOS A1027.209 0 0316:155546.074 PSBR_S_Proc OOS A1027.209 0 0316:155546.075 CacdProcessRes Active A1027.209 0 0316:161158.501 DA_MP_Leader OOS A1027.209 0 0316:155546.071 DSR_SLDB OOS A1027.209 0-63 0316:155546.071 VIP_DA_MP OOS A1027.209 0-63 0316:155546.072 EXGSTACK_Process OOS A1027.209 0-63 0316:155546.072 DSR_Process OOS A1027.209 0-63 0316:155546.072 CAPM_HELP_Proc OOS A1027.209 0 0316:155546.070 DSROAM_Proc Active A1027.209 0 0316:161158.497 CAPM_PSFS_Proc OOS A1027.209 0 0316:155546.070 SS7_MP_Process_HA_Proc OOS A1027.209 0-63 0316:155546.073 SS7_MP_Process OOS A1027.209 0-63 0316:155546.074

Procedure 4: Configure the NOAM Server Group

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

Procedure 5: Configure the Second NOAM Server

S T E P #	This procedure will provide the steps to configure the Second NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**NOAM GUI:** Login	If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of: `https://<NO1_XMI_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 5: Configure the Second NOAM Server

2 ☐	**NOAM GUI:** Insert the 2nd NOAM server	Navigate to **Main Menu -> Configuration -> Servers.** Select the **Insert** button to insert the 2nd NOAM server into servers table (the first or server). Adding a new server **Attribute** / **Value** Hostname: NO-Server2 * Role: NETWORK OAM&P * System ID: NO-Server2 Hardware Profile: DSR TVOE Guest Network Element Name: JETTA * Location: Fill in the fields as follows: **Hostname: <Hostname>** **Role: NETWORK OAM&P** **System ID: <Site System ID>** **Hardware Profile: DSR TVOE Guest** **Network Element Name: [Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element Interfaces: **Network** / **IP Address** / **Interface** INTERNALXMI (10.240.84.128/25) / 10.240.84.155 / xmi / ☐ VLAN (3) INTERNALIMI (10.240.85.0/26) / 10.240.85.10 / imi / ☐ VLAN (4) Ok Apply Cancel Fill in 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 '$NOAM2_xmi_IP_address' configured in Procedure 2 Fill in the server IP addresses for the IMI network. Select **imi** for the interface. **Leave the "VLAN" checkbox unchecked**. **Note:** The imi server IP must match '$NOAM1_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 Select the **Ok** button when you have completed entering all the server data.

Procedure 5: Configure the Second NOAM Server

3 ☐	**NOAM GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.** From the GUI screen, select the NOAM server and then select **Export** to generate the initial configuration data for that server. Insert Edit Delete Export Report
4 ☐	**1st NOAM Server:** Copy Configuration File to 2nd NOAM Server	Obtain a terminal session to the 1st NOAM as the ***admusr*** user. Execute the following command to configure the 2nd NOAM server: **$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>.sh admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData.sh**
5 ☐	**2nd NOAM Server:** Verify configuration was called and Reboot the Server	Establish an SSH session to the 2nd NOAM server (NOAM2_xmi_IP_address) Login as the ***admusr*** user. The automatic configuration daemon will look for the file named ***"TKLCConfigData.sh"*** in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify awpushcfg was called by checking the following file **$ sudo cat /var/TKLC/appw/logs/Process/install.log** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Now Reboot the Server: **$ sudo init 6** Wait for the server to reboot

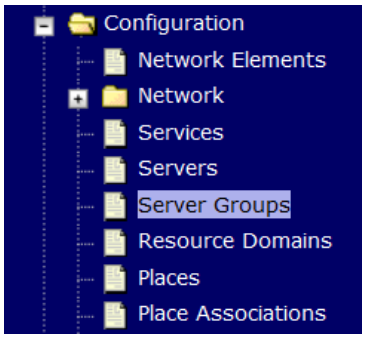
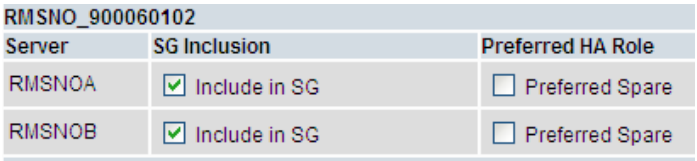
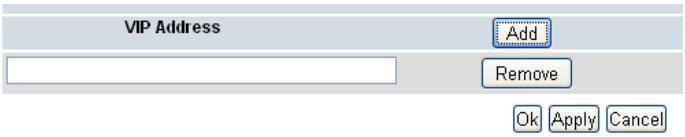
Procedure 5: Configure the Second NOAM Server

6 ☐	**2nd NOAM Server:** Configure Networking for Dedicated NetBackup Interface (Optional)	**Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup. Obtain a terminal window to the 2nd NOAM server, logging in as the ***admusr*** user. **$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup** **--type=Ethernet --onboot=yes** **--address=<NO2_NetBackup_IP_Adress>** **--netmask=<NO2_NetBackup_NetMask>** **$ sudo /usr/TKLC/plat/bin/netAdm add --route=net** **--device=netbackup --address=<NO1_NetBackup_Network_ID>** **--netmask=<NO2_NetBackup_NetMask>** **--gateway=<NO2_NetBackup_Gateway_IP_Address>**
7 ☐	**2nd NOAM Server:** Verify Server Health	Execute the following command on the 2nd NOAM server and make sure that no errors are returned: **$ sudo syscheck** Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log

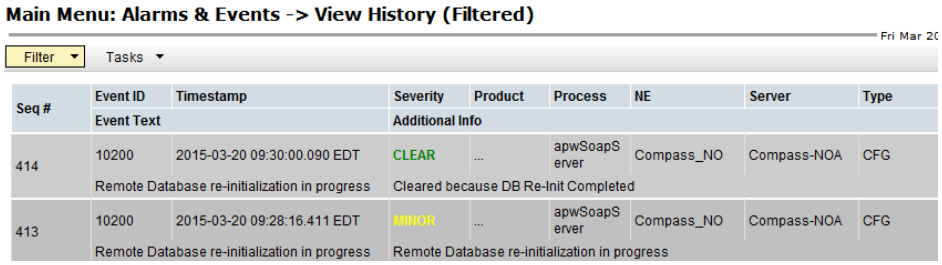
Procedure 6: Complete NOAM Server Group Configuration

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

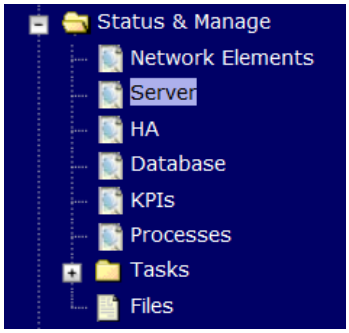
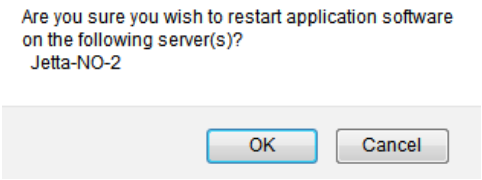
Procedure 6: Complete NOAM Server Group Configuration

2 ☐	**NOAM GUI:** Edit the NOAM Server Group Data	Navigate to **Main Menu->Configuration->Server Groups.**  Select the NOAM Server group and click on **Edit**  Add the 2nd NOAM server to the Server Group by clicking the ***Include in SG*** checkbox for the 2nd NOAM server.  Click **Apply.** Add a NOAM VIP by click on **Add.** Fill in the VIP Address and press **Ok** as shown below 

Procedure 6: Complete NOAM Server Group Configuration

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

Procedure 6: Complete NOAM Server Group Configuration

5 ☐	**NOAM GUI:** Restart 1st NOAM Server	From the NOAM GUI, select the **Main menu** -> **Status & Manage** -> **Server** menu.  Select the 2nd NOAM server. Select the **Restart** button.  Answer **OK** to the confirmation popup.  Wait for restart to complete. Wait approximately 3-5 minutes before proceeding.

4.1.4 Install NetBackup Client (Optional)

Procedure 7: Install NetBackup Client

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

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

S T E P #	This procedure will extend the TVOE networking configuration on the First DR-NOAM RMS server (if necessary), configure the networking on additional rack mount servers, create the DR-NOAM VMs, and deploy the DSR and TPD images. **Prerequisite:** TVOE and PMAC (virtualized) have been installed on the First DR-NOAM RMS Server as described in [7] 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 O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**PMAC Server:** Login	Establish an SSH session to the PMAC server, login as ***admusr***.

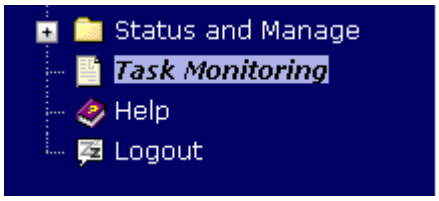
Procedure 8: NOAM Configuration for DR Site

2
☐
	PMAC Server: Update the DSR Fast Deployment template	Perform the following command to navigate to the directory containing the DSR fast deployment template:
		
		`$ cd /usr/TKLC/smac/etc`
		
		DSR Fast Deployment Template Names:
		
		NOAM on Rack Mount Servers: DSR_NOAM_FD_RMS.xml
		NOAM on Blade Servers: DSR_NOAM_FD_Blade.xml
		
		Note: If the fast deployment template is not present, then please re-execute section "Setup PM&C" step 10, sub step C from [7].
		
		Update the following items within the Fast deployment xml:
		
		TPD and DSR ISO:
		
		<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-7.2/7.3.0.0.0_72.8.0-x86_64</name>
		</image>
		</software>
		
		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:
		
		`$ ls /var/TKLC/smac/image/repository`
		
		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.
		
		<!--
		<tpdinterface id="bond1">
		<device>bond1</device>
		<type>Bonding</type>
		<bonddata>
		<bondinterfaces>eth03,eth04</bondinterfaces>
		<bondopts>mode=active-backup,miimon=100</bondopts>
		</bonddata>
		<onboot>yes</onboot>
		<bootproto>none</bootproto>
		</tpdinterface>
		-->

Procedure 8: NOAM Configuration for DR Site

3
☐
	PMAC Server: Validate and Run the Fast Deployment File	Validate/Create the fast deployment file by executing the following command:
		
		For NOAMs deployed on rack mount servers:
		
		`$ sudo fdconfig validate --file=DSR_NOAM_FD_RMS.xml`
		
		For NOAMs deployed on blade servers:
		
		`$ sudo fdconfig validate --file=DSR_NOAM_FD_Blade.xml`
		
		Note: Refer to **Appendix M**: DSR Fast Deployment Configuration for information of the variables that must be input during execution of the NOAM fast deployment.
		
		If there were errors during validation, correct the errors within the xml file and re-run the validation.
		
		After successful validation, a new Fast deployment xml file is created:
		
		`---  NOTICE  ---`
		`Config Data saved as a new file: "./DSR_NOAM_FD_Blade_20151217T102402.xml"`
		`---  NOTICE  ---`
		
		`Configuration file validation successful.`
		`Validation complete`
		`[admusr@GuestPMACeco upgrade]$`
		
		Execute the following commands to run the fast deployment file:
		
		`$ screen`
		
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`
		
		Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “screen -dr” to resume the screen session in the event of a terminal timeout etc.

Procedure 8: NOAM Configuration for DR Site

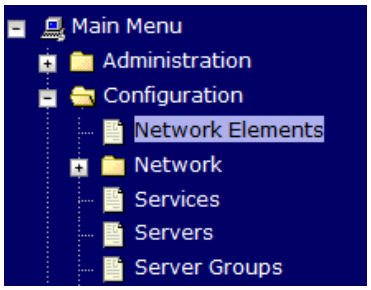
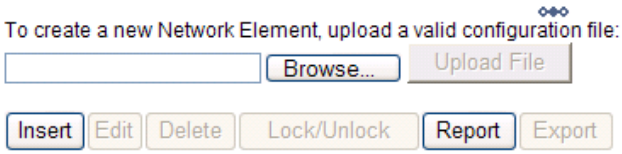
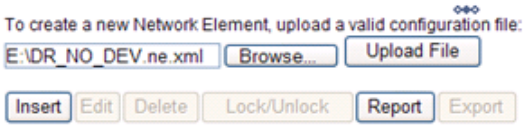
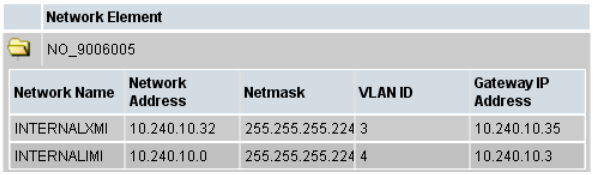
4 ☐	**PMAC GUI:** Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the DSR NOAM TVOE configuration to completion:

110	Tpd ServerAction: File Transfer	RMS: Oahu-TVOE-2	File transfer success	COMPLETE	0:00:14	2015-11-24 07:42:35	100%
109	Tpd ServerAction: File Transfer	RMS: Oahu-TVOE-1	File transfer success	COMPLETE	0:00:03	2015-11-24 07:42:35	100%
108	Accept Upgrade	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Success	COMPLETE	0:01:02	2015-11-24 07:41:08	100%
107	Accept Upgrade	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Success	COMPLETE	0:01:03	2015-11-24 07:34:30	100%
106	Upgrade	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Success	COMPLETE	0:12:57	2015-11-24 07:26:05	100%
105	Upgrade	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Success	COMPLETE	0:07:17	2015-11-24 07:26:00	100%
104	Install OS	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Done: TPD.install-7.0.2.0.0_86.34.0-OracleLinux6.6-x86_64	COMPLETE	0:11:21	2015-11-24 07:11:07	100%
103	Install OS	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Done: TPD.install-7.0.2.0.0_86.34.0-OracleLinux6.6-x86_64	COMPLETE	0:11:26	2015-11-24 07:11:02	100%
102	VirtAction: Create	RMS: Oahu-TVOE-2 Guest: Oahu-DSR-NOAM-2	Guest creation completed (Oahu-DSR-NOAM-2)	COMPLETE	0:00:10	2015-11-24 07:10:52	100%
101	VirtAction: Create	RMS: Oahu-TVOE-1 Guest: Oahu-DSR-NOAM-1	Guest creation completed (Oahu-DSR-NOAM-1)	COMPLETE	0:00:05	2015-11-24 07:10:52	100%

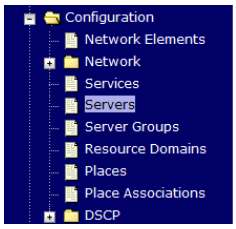
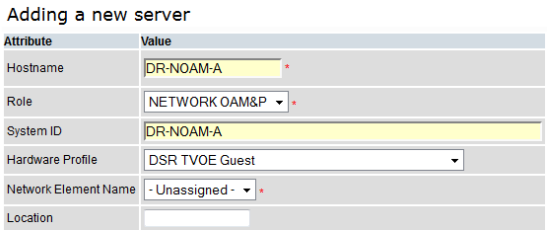
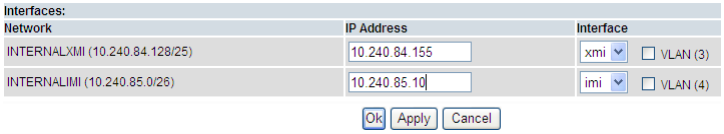
Procedure 8: NOAM Configuration for DR Site

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

Procedure 8: NOAM Configuration for DR Site

6 ☐	**PRIMARY NOAM VIP GUI:** Insert the DR NOAM Network Element	Navigate to **Main Menu->Configuration->Network Elements**  The **Network Elements** screen will display select the **Browse** (scroll to bottom left corner of screen).  A dialogue will pop up, browse to the location of the DSR DR NOAM Site Element XML File and click the **Open** button. Then click **Upload File** as shown below  Once the data has been uploaded, you should see a folder appear with the name of your network element. Click on this folder and you will get a drop-down which describes the individual networks that are now configured:  Network Element NO_9006005 Network Name / Network Address / Netmask / VLAN ID / Gateway IP Address INTERNALXMI / 10.240.10.32 / 255.255.255.224 / 3 / 10.240.10.35 INTERNALIMI / 10.240.10.0 / 255.255.255.224 / 4 / 10.240.10.3

Procedure 8: NOAM Configuration for DR Site

7 ☐	**PRIMARY NOAM VIP GUI:** Insert the 1st DR-NOAM server	Navigate to **Main Menu -> Configuration -> Servers.**  Select the **Insert** button to insert the new DR-NOAM server into servers table.  Fill in the fields as follows: **Hostname: <Hostname>** **Role: NETWORK OAM&P** **System ID: <Site System ID>** **Hardware Profile: DSR TVOE Guest** **Network Element Name: [Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Fill in the server IP addresses for the XMI network. Select **xmi** for the interface. **Leave the "VLAN" checkbox unchecked**. **Note:** The xmi server IP must match '$DR-NOAM_xmi_IP_address' configured in step 2 Fill in the server IP addresses for the IMI network. Select **imi** for the interface. **Leave the "VLAN" checkbox unchecked**. **Note:** The imi server IP must match '$DR-NOAM_xmi_IP_address' configured in Step 2 Next, add the following NTP servers: **NTP Server** | **Preferred?** **<TVOE_XMI_IP_Address(DR-NO1)/ TVOE_Mgmt_IP_Address(DR-NO1)>** | Yes Select the **Ok** button when you have completed entering all the server data.

Procedure 8: NOAM Configuration for DR Site

8 ☐	**PRIMARY NOAM VIP GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.** From the GUI screen, select the DR-NOAM server and then select **Export** to generate the initial configuration data for that server. Insert Edit Delete Export Report
9 ☐	**1st NOAM Server:** Copy Configuration File to DR-NOAM NOAM Server	Obtain a terminal session to the primary NOAM as the ***admusr*** user. Execute the following command to configure the DR-NOAM server: **$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DR-NOAM_Hostname>.sh admusr@<DR-NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh**
10 ☐	**1st DR-NOAM Server:** Verify configuration was called and Reboot the Server	Establish an SSH session to the DR-NOAM server (DR-NOAM_xmi_IP_address) Login as the ***admusr*** user. The automatic configuration daemon will look for the file named ***"TKLCConfigData.sh"*** in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify awpushcfg was called by checking the following file **$ sudo cat /var/TKLC/appw/logs/Process/install.log** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Now Reboot the Server: **$ sudo init 6** Wait for the server to reboot

Procedure 8: NOAM Configuration for DR Site

<table>
<tr><td>11
☐</td><td>1st DR-NOAM: Configure Networking for Dedicated NetBackup Interface (Optional)</td><td>

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

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

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup
--type=Ethernet --onboot=yes
--address=<NO1_NetBackup_IP_Adress>
--netmask=<NO1_NetBackup_NetMask>
```

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

</td></tr>
<tr><td>12
☐</td><td>1st DR-NOAM Server: Verify Server Health</td><td>

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

```
$ sudo syscheck
Running modules in class hardware...OK
Running modules in class disk...OK
Running modules in class net...OK
Running modules in class system...OK
Running modules in class proc...OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

</td></tr>
<tr><td>13
☐</td><td>Repeat for 2nd DR NOAM Server</td><td>

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:

<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><TVOE_XMI_IP_Address(DR-NO2)/ TVOE_Mgmt_IP_Address(DR-NO2)></td><td>Yes</td></tr>
</table>

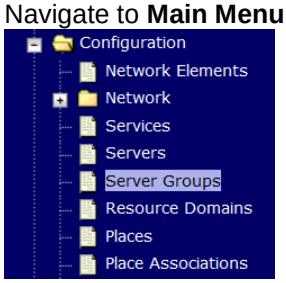
</td></tr>
</table>

4.2.2 Configure DR-NOAMs

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

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

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

2 ☐	**Primary NOAM VIP GUI**: Enter DR-NOAM Server Group Data	Navigate to **Main Menu** -> **Configuration** -> **Server Groups**  Select **Insert** and fill the following fields:  • **Server Group Name: <Enter Server Group Name>** • **Level: A** • **Parent : None** • **Function: DSR (Active/Standby Pair)** • **WAN Replication Connection Count: Use Default Value** Select **OK** when all fields are filled in.
3 ☐	**Primary NOAM VIP GUI**: Update Server Group	Select the **Server Group** that was created in the previous step, and click on **Edit**.  The user will be presented with the **Server Groups [Edit]** screen Check the checkbox labeled **Include in SG** for **both** DR-NOAM Servers as shown below and click on **Apply** deaDR_CSLAB_ATT Server: deaNO-ChaNC-A; SG Inclusion: ☑ Include in SG; Preferred HA Role: ☐ Preferred Spare Server: deaNO-ChaNC-B; SG Inclusion: ☑ Include in SG; Preferred HA Role: ☐ Preferred Spare
4 ☐	**Primary NOAM VIP GUI**: Add DR-NOAM VIP	Click the **Add** dialogue button for the VIP Address and enter an IP Address for the VIP as shown below  Then click the **Apply** dialogue button. Verify that the banner information message states **Data committed**. 

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

5 ☐	**Primary NOAM VIP GUI**: Wait for Remote Database Alarm to Clear	Wait for the alarm **Remote Database re-initialization in progress** to be cleared before proceeding. Navigate to **Main menu->Alarms & Events->View Active** **Main Menu: Alarms & Events -> View History (Filtered)** Fri Mar 2(Filter Tasks Seq # | Event ID | Timestamp | Severity | Product | Process | NE | Server | Type Event Text | Additional Info 414 | 10200 | 2015-03-20 09:30:00.090 EDT | CLEAR | ... | apwSoapServer | Compass_NO | Compass-NOA | CFG Remote Database re-initialization in progress | Cleared because DB Re-Init Completed 413 | 10200 | 2015-03-20 09:28:16.411 EDT | MINOR | ... | apwSoapServer | Compass_NO | Compass-NOA | CFG Remote Database re-initialization in progress | Remote Database re-initialization in progress
6 ☐	**Primary NOAM VIP GUI**: Restart 1st DR-NOAM Server	From the NOAM GUI, select the **Main menu** -> **Status & Manage** -> **Server** menu. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the 1st DR-NOAM server. Select the **Restart** button. Stop Restart Reboot NTP Sync Report Answer **OK** to the confirmation popup. Are you sure you wish to restart application software on the following server(s)? Jetta-NO-2 OK Cancel Wait for restart to complete. Wait approximately 3-5 minutes before proceeding.
7 ☐	**Primary NOAM VIP GUI** :Restart the application on the 2nd DR-NOAM Server	Repeat Step 6, but this time selecting 2nd DR-NOAM Server.

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

8
☐
	Primary NOAM:
	Modify DSR OAM process
		Establish an SSH session to the primary NOAM, login as ***admusr***.
		Execute the following commands:
		Retrieve the cluster ID of the DR-NOAM:
		$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"
		`Server_ID NodeID ClusterID`
		`1 Oahu-DSR-DR-NOAM-2 A1055`
		Execute the following command to start the DSR OAM process on the DR-NOAM:
		$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -fcluster –fresource -foptional HaClusterResourceCfg

4.2.3 Install NetBackup Client (Optional)

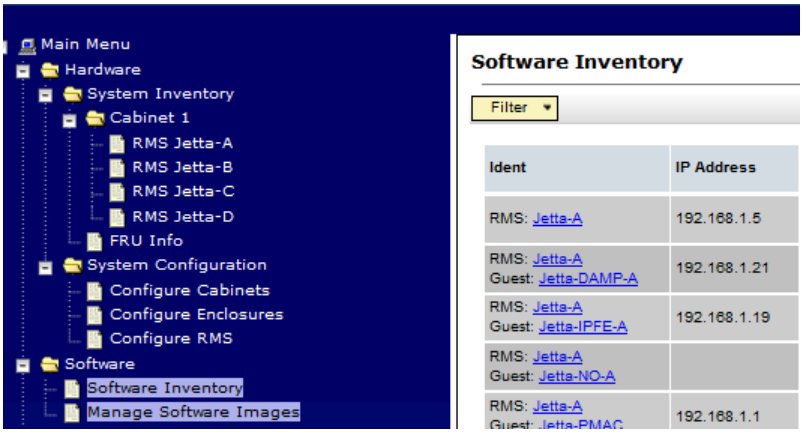
Procedure 10: Install NetBackup Client

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

4.3 Install and Configure SOAM Servers

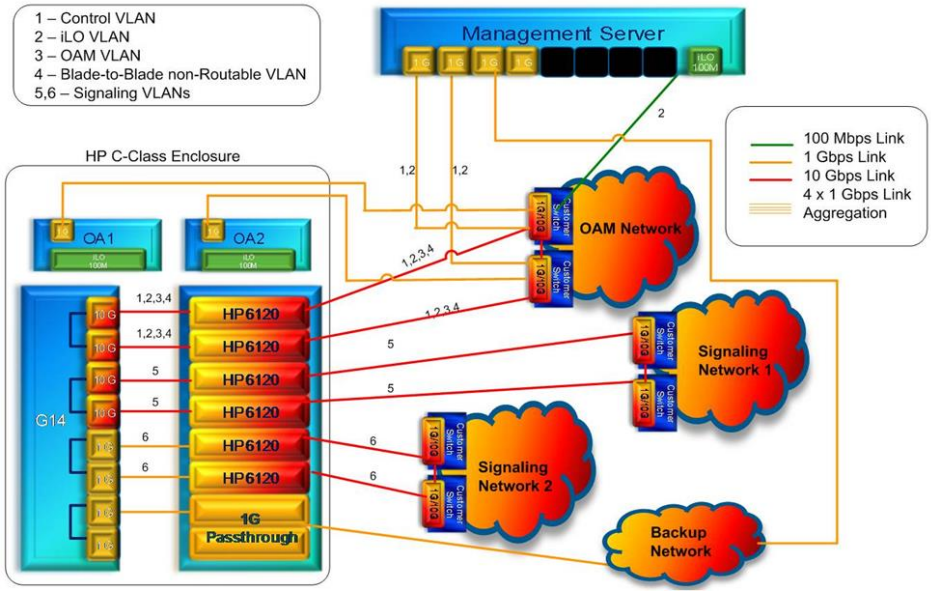
4.3.1 Configure SOAM TVOE Server Blades

Procedure 11: Configure SOAM TVOE Server Blades

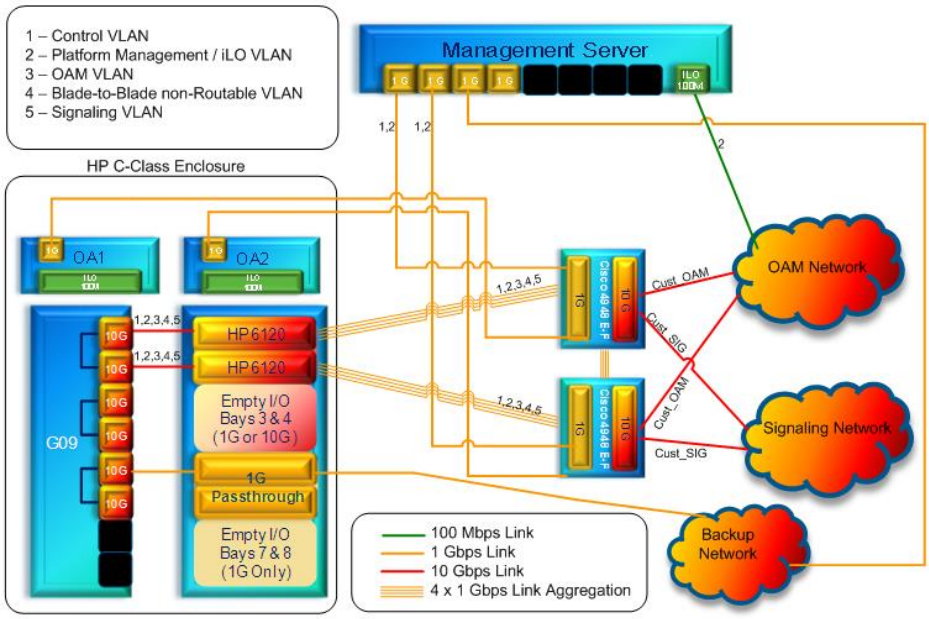
S T E P #	This procedure will configure TVOE on the server blades that will host DSR SOAM VMs. It details the configuration for a single server blade and should be repeated for every TVOE blade that was IPM-ed for this install. **NOTE:** TVOE should only be installed on Blade servers that will run as DSR SOAMs. They should NOT be installed on Blade servers intended to run as DSR MPs. **Prerequisite**: TVOE OS has been installed on the target server blades as per instructions in [7] 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 O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**PMAC Server:** Exchange SSH keys between PMAC and TVOE server	Use the PMAC GUI to determine the Control Network IP address of TVOE server. From the PMAC GUI, navigate to **Main Menu -> Software -> Software Inventory**.  Note the IP address TVOE server. 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 prompted for the password, enter the password for the TVOE server. `$ keyexchange admusr@<TVOE_Control_Blade_IP_address>`

Procedure 11: Configure SOAM TVOE Server Blades

2 ☐	**TVOE Server:** Login and Copy Configuration Scripts from PMAC	Login as **admusr** on the TVOE server using the ILO facility.
		
		Execute the following commands:
		
		`$ sudo scp admusr@<Mgmt_Server_Control_IP_address>:/usr/TKLC/smac/etc/TVOE* /usr/TKLC/`
		
		`$ sudo chmod 777 /usr/TKLC/TVOE*`
		
		Note: If no TVOE configuration scripts are found here, then please re-execute section 4.2.2, Step #13 of [7]

3 ☐	**TVOE Server:** Mezzanine card/ segregated OAM/XMI network configuration	If your TVOE server blade DOES have mezzanine cards AND you will be running OAM/XMI traffic on a separate physical network (*example below*). If you do not have mezzanine cards, **skip this step.**  Execute the following command: `$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID> mezz`

Procedure 11: Configure SOAM TVOE Server Blades

4 ☐	**TVOE Server:** No Mezzanine card/ No segregated OAM/XMI network configuration	If your TVOE server blade **DOES NOT** have mezzanine cards AND/OR you will NOT be running OAM/XMI traffic over a separate physical network (example below).  Execute the following command: `$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID>`

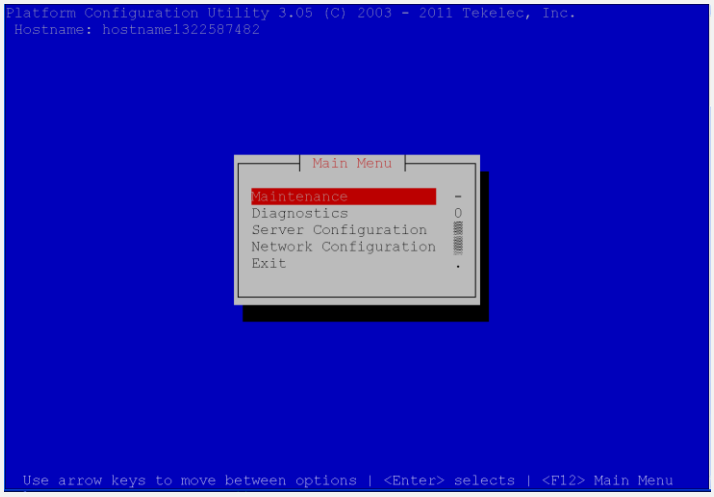
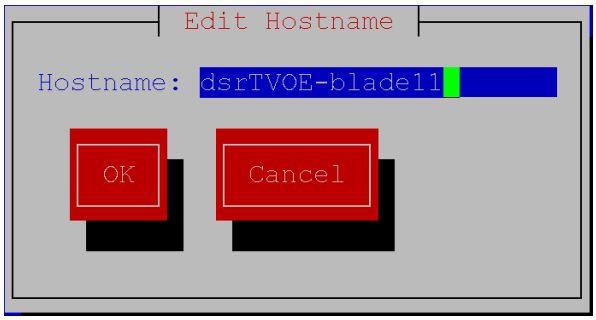
Procedure 11: Configure SOAM TVOE Server Blades

5
☐
	TVOE Server:
	Verify TVOE configuration
		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 will be the values of the “INTERNAL-IMI” and “INTERNAL-XMI” VLAN ids, respectively. For layer-2 only deployments, the IMI and XMI VLAN ids will be obtained from the customer.
		
		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):
		
		`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!`
		
		The prompt will return.
		
		Note: If for any reason, you ran the wrong version of the TVOEcfg.sh command, you can execute the following command to reset the networking configuration so you can repeat either steps 3 or 4:
		
		`Sudo ./usr/TKLC/TVOEclean.sh`

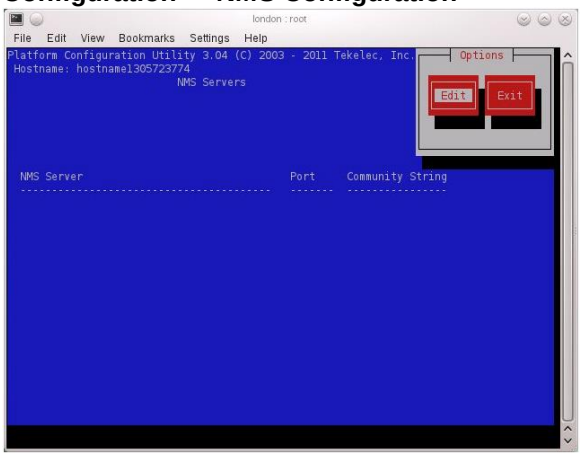
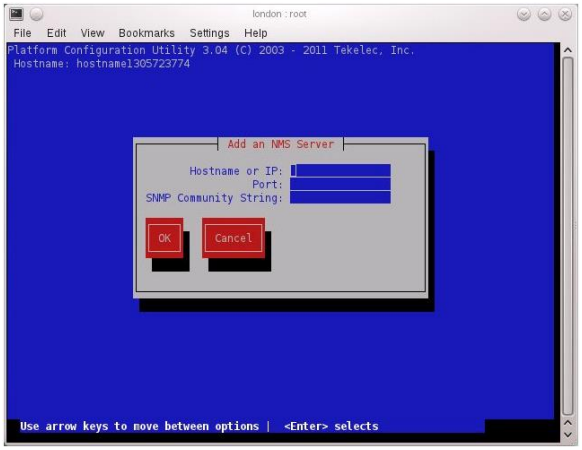
Procedure 11: Configure SOAM TVOE Server Blades

6 ☐	**TVOE Server:** Configure XMI IP and Default Route	Configure IP address on the XMI network: **$ 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. Restart network services: **$ sudo service network restart** [wait for the prompt to return] Set the default route: **$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=xmi --gateway=<TVOE_XMI_Gateway_IP_Address>** Route to xmi added.
7 ☐	**TVOE Server:** Configure NetBackup Dedicated Interface and Bridge (Optional)	In these examples, <interface> should be replaced with the actual Ethernet interface that will be used as the dedicated NetBackup port. For instance, ***"eth01"*** or ***"eth22"***. Un-bonded Ethernet Interface: **$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Ethernet interface> --slave=no --onboot=yes** **[OPTIONAL]** If this installation is using jumbo frames, set the Ethernet interface MTU to the desired jumbo frame size: **$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Ethernet interface> --MTU=<NetBackup_MTU_size>** Create NetBackup VM Bridge Interface: **$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=netbackup --bridgeInterfaces=<Ethernet interface> --onboot=yes**

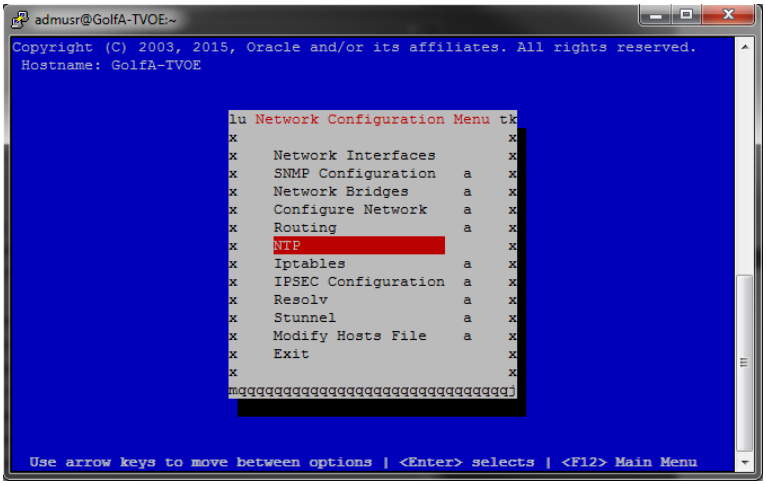
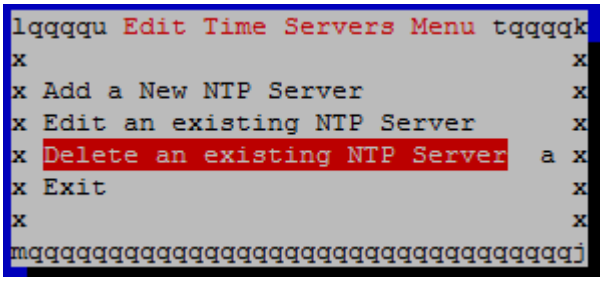
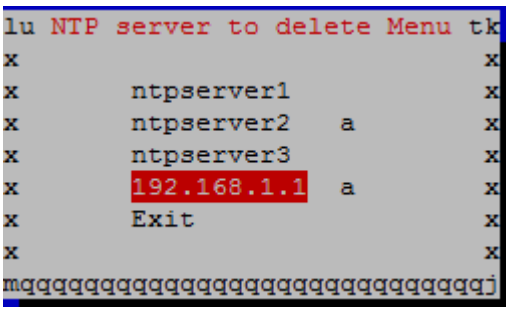
Procedure 11: Configure SOAM TVOE Server Blades

8 ☐	**TVOE Server:** Set Hostname	**$ sudo su – platcfg**  Navigate to **Server Configuration->Hostname-> Edit** and enter a new hostname for your server:  Press **OK** and select and continue to press Exit until you are at the platcfg main menu again. **Note:** Although the new hostname has been properly configured and committed at this point, it will not appear on your command prompt unless you log out and log back in again.

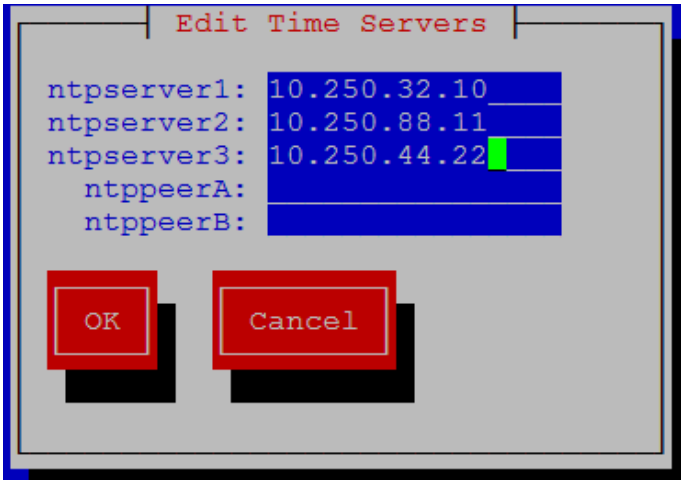
Procedure 11: Configure SOAM TVOE Server Blades

9 ☐	**TVOE Server:** Configure SNMP	From the platcfg main menu, navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**  Press **Edit**. Choose **Add a New NMS Server**  Enter the following NMS servers, pressing **OK** after each one and then selecting the **Add NMS** option again: 1. 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. 2. 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 Press **Exit**. Select **Yes** when prompted to restart the Alarm Routing Service. Once Done, press **Exit** to quit to the platcfg main menu.

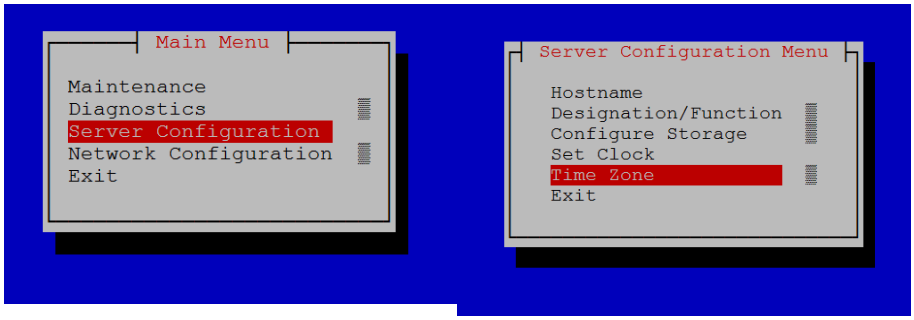
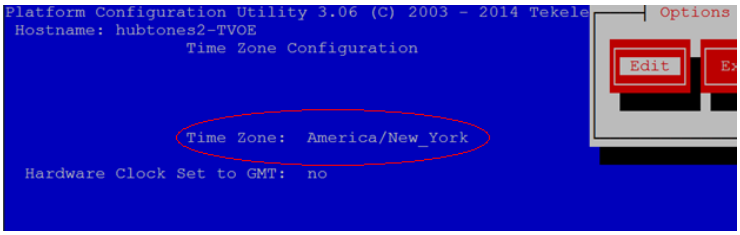
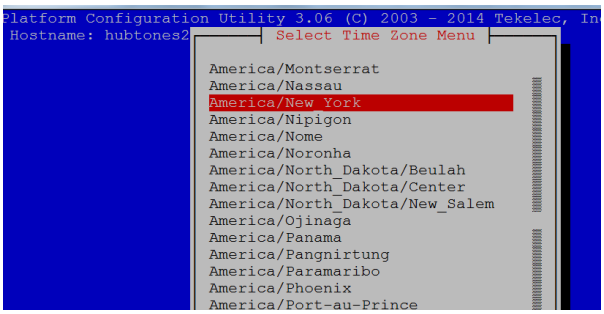
Procedure 11: Configure SOAM TVOE Server Blades

10 ☐	**RMS iLO/iLOM:** Delete PMAC VM as NTP Source on RMS	Navigate to **Network Configuration ->NTP**.  Select **Delete an existing NTP Server**  Select the PMAC VM Control IP, Click **[Enter]**  You will be returned to the **NTP Menu**

Procedure 11: Configure SOAM TVOE Server Blades

11 ☐	**TVOE Server:** Configure NTP	Click **Edit**  • ntpserver1: Enter customer provided NTP server #1 IP address. • ntpserver2: Enter customer provided NTP server #2 IP address. • ntpserver3: Enter customer provided NTP server #3 IP address. Press **OK** Press **Exit** to return to the platcfg menu.

Procedure 11: Configure SOAM TVOE Server Blades

12 ☐	**TVOE Server:** Configure Time Zone	`$ sudo su - platcfg` Navigate to **Server Configuration->Time Zone**   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. Click **Edit**  Select the desired time zone from the list and press **Enter** Continue pressing **Exit** until you are out of the platcfg program.
13 ☐	**TVOE Server:** Reboot	Reboot the server by executing the following command: `$ sudo init 6`

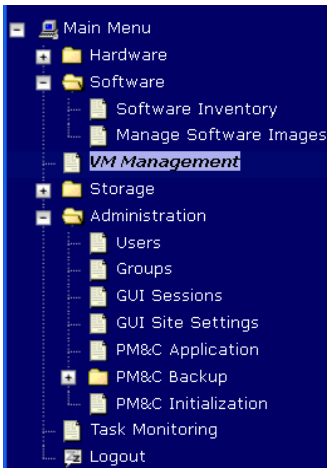
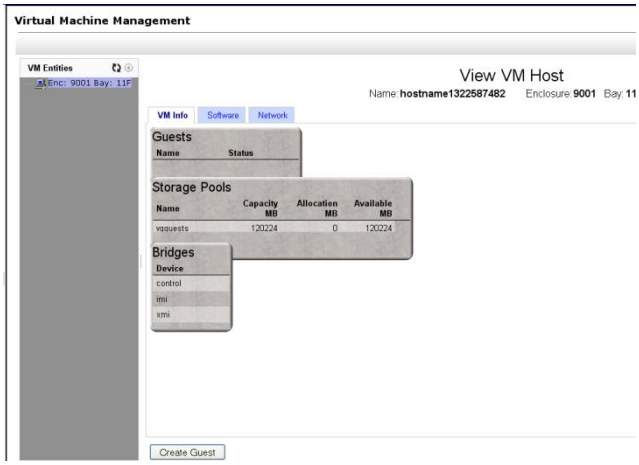
Procedure 11: Configure SOAM TVOE Server Blades

14 ☐	**TVOE server:** Repeat Procedure for other TVOE blades.	Configuration of this TVOE server blade is complete. Repeat this procedure from the beginning for other TVOE hosts that need to be configured.
15 ☐	**Install SDS (Optional)**	If this deployment contains SDS, SDS can now be installed. Refer to document referenced in [4].

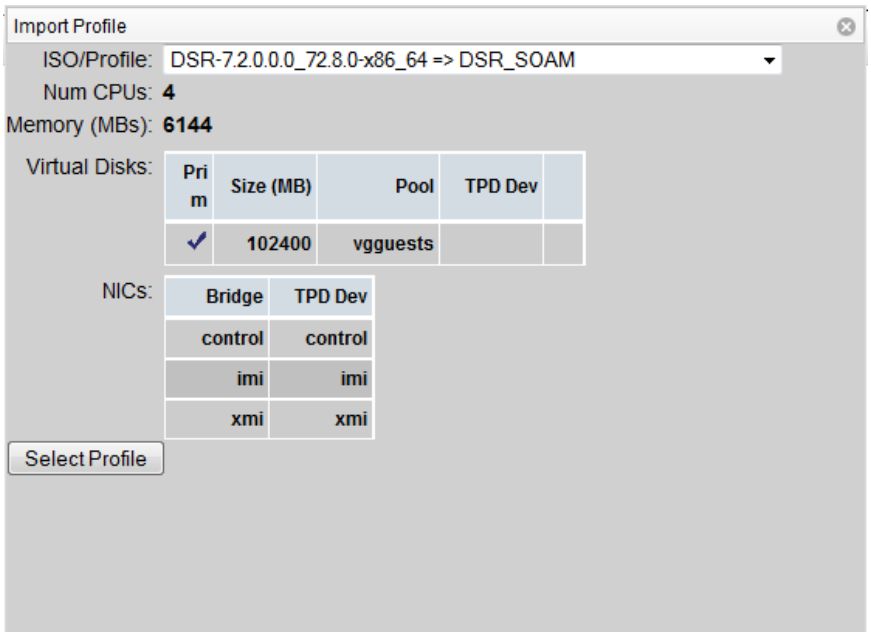
Procedure 12: Create SOAM Guest VMs

S T E P #	This procedure will provide the steps needed to create a DSR SOAM virtual machine (referred to as a "guest") on a TVOE server blade. It must be repeated for every SOAM server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target blade server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O:** My Oracle Support (MOS), and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

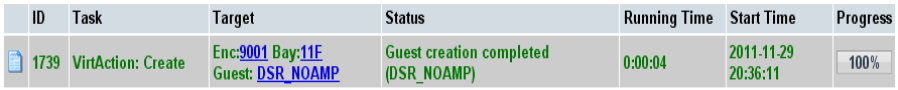
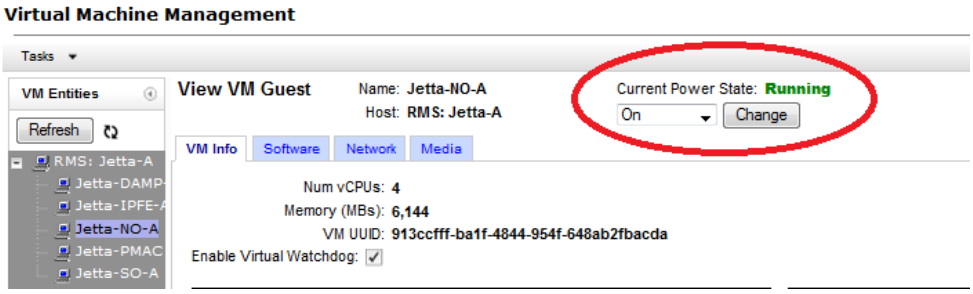
Procedure 12: Create SOAM Guest VMs

2 ☐	**PMAC GUI:** Navigate to VM Management of the Target Server Blade	Navigate to **Main Menu -> VM Management**  Select the TVOE server blade or rack mounted server from the ***VM Entities*** listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.  Click **Create Guest** 

Procedure 12: Create SOAM Guest VMs

3 ☐	**PMAC GUI:** Configure VM Guest Parameters	Select **Import Profile**  From the ***"ISO/Profile"*** drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running on and your preference for NetBackup interfaces: **SOAM VM TVOE Hardware Type(s)** / **Dedicated Netbackup Interface?** / **Choose Profile (<Application ISO NAME>)➔** HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade / No / **DSR_SOAM** HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade / Yes / **DSR_SOAM_NBD** Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM Press **Select Profile**. You can edit the name, if you wish. For instance: ***"DSR_SOAM_A,"*** or ***DSR_SOAM_B".*** *(This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)* Press **Create** 

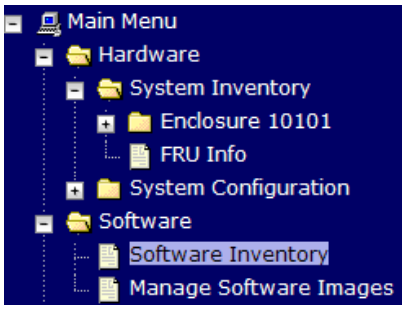
Procedure 12: Create SOAM Guest VMs

4 ☐	**PMAC GUI:** Wait for Guest Creation to Complete	Navigate to **Main Menu -> Task Monitoring** to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched. Wait or refresh the screen until you see that the guest creation task has completed successfully.  ID: 1739 Task: VirtAction: Create Target: Enc:9001 Bay:11F Guest: DSR_NOAMP Status: Guest creation completed (DSR_NOAMP) Running Time: 0:00:04 Start Time: 2011-11-29 20:36:11 Progress: 100%
5 ☐	**PMAC GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the TVOE server blade on which the guest machine was just created. 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".***  VM Creation for this guest is complete. Repeat from **Step 2** for any remaining NOAM VMs (*for instance, the standby SOAM*) that must be created.

Procedure 13: IPM Blades and VMs

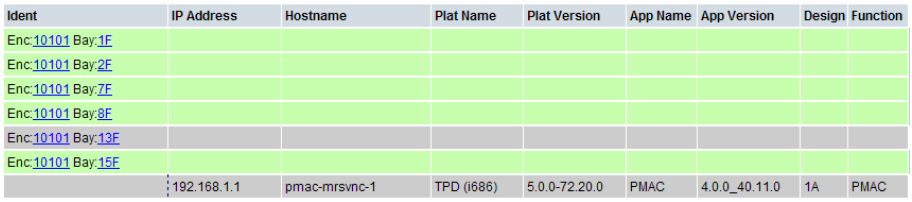
S T E P #	This procedure will provide the steps to install TPD on Blade servers and Blade server guest VMs **Prerequisite**: Enclosures containing the blade servers targeted for IPM that have been configured. **Prerequisite**: TVOE has been installed and configured on Blade servers that will host DSR NOAM VMs. **Prerequisite**: DSR NOAM and SOAM Guest VMs have been created successfully. **Needed material:** - TPD Media (64-bits) 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

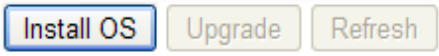
Procedure 13: IPM Blades and VMs

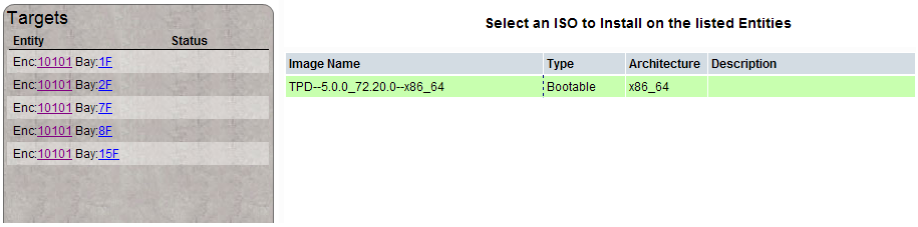
<table>
<tr>
<td>2
☐</td>
<td>PMAC GUI:
Select Servers for OS install</td>
<td>
Navigate to Software -> Software Inventory.


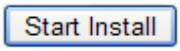
Select the servers (VMs, IPFEs, MPs, Etc.) you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.

Note: VM's will have the text "Guest: <VM_GUEST_NAME>" underneath the physical blade or RMS that hosts them.



Click on Install OS


</td>
</tr>
<tr>
<td>3
☐</td>
<td>PMAC GUI:
Initiate OS Install</td>
<td>
The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.


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


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

Procedure 13: IPM Blades and VMs

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

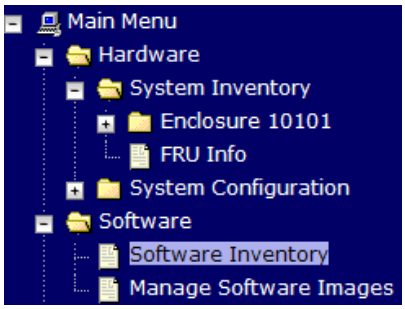
ID	Task	Target	Status	Running Time	Start Time	Progress
14	Install OS	Enc:10101 Bay:15F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
13	Install OS	Enc:10101 Bay:8F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
12	Install OS	Enc:10101 Bay:7F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
11	Install OS	Enc:10101 Bay:2F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
10	Install OS	Enc:10101 Bay:1F	Boot install image	0:00:02	2011-09-20 11:12:01	50%
9	Add Image		Done: TPD.install-5.0.0_72.20.0-CentOS5.6-x86_64	0:00:09	2011-09-20 11:01:50	100%

Procedure 14: Install the Application Software

S T E P #	This procedure will provide the steps to install Diameter Signaling Router on the Blade servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

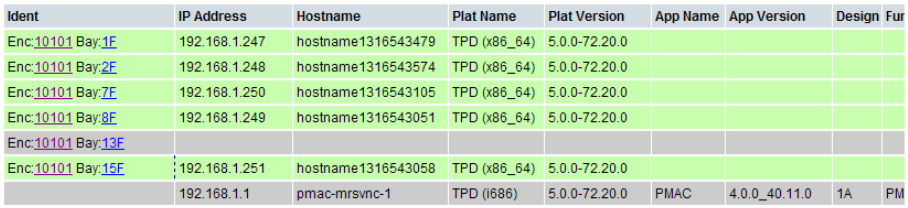
Procedure 14: Install the Application Software

<table>
<tr>
<td>2
☐</td>
<td>PMAC GUI:
Select Servers for Application install</td>
<td>
Navigate to Software -> Software Inventory.



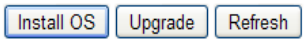
Select the servers on which the application is to be installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.

Note: VM's will have the text "Guest: <VM_GUEST_NAME>" underneath the physical blade that hosts them.

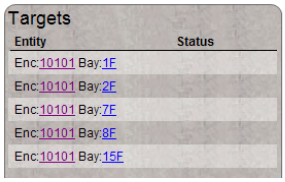


Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Design	Fur
Enc:10101 Bay:1F	192.168.1.247	hostname1316543479	TPD (x86_64)	5.0.0-72.20.0				
Enc:10101 Bay:2F	192.168.1.248	hostname1316543574	TPD (x86_64)	5.0.0-72.20.0				
Enc:10101 Bay:7F	192.168.1.250	hostname1316543105	TPD (x86_64)	5.0.0-72.20.0				
Enc:10101 Bay:8F	192.168.1.249	hostname1316543051	TPD (x86_64)	5.0.0-72.20.0				
Enc:10101 Bay:13F								
Enc:10101 Bay:15F	192.168.1.251	hostname1316543058	TPD (x86_64)	5.0.0-72.20.0				
	192.168.1.1	pmac-mrsvnc-1	TPD (i686)	5.0.0-72.20.0	PMAC	4.0.0_40.11.0	1A	PM

Click on **Upgrade**

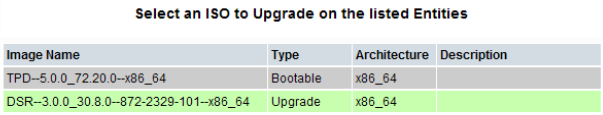


</td>
</tr>
<tr>
<td>3
☐</td>
<td>PMAC GUI:
Initiate Application Install</td>
<td>
The left side of this screen shows the servers to be affected by this application installation. From the list of available bootable images on the right side of the screen, select one application image to install to all of the selected servers.



Targets

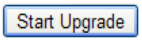
Entity	Status
Enc:10101 Bay:1F	
Enc:10101 Bay:2F	
Enc:10101 Bay:7F	
Enc:10101 Bay:8F	
Enc:10101 Bay:15F	



Select an ISO to Upgrade on the listed Entities

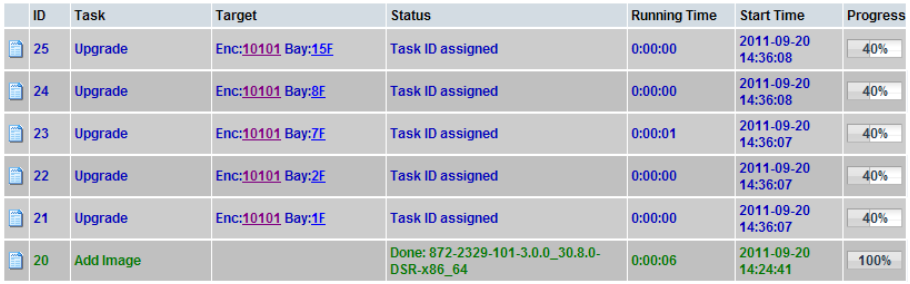
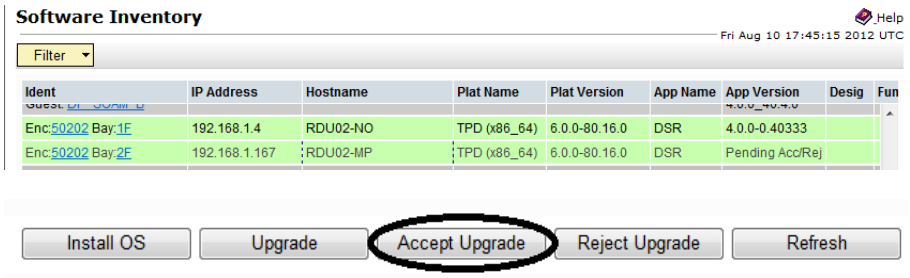
Image Name	Type	Architecture	Description
TPD--5.0.0_72.20.0--x86_64	Bootable	x86_64	
DSR--3.0.0_30.8.0--872-2329-101--x86_64	Upgrade	x86_64	

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



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

Procedure 14: Install the Application Software

4 ☐	**PMAC GUI:** Monitor the installation status	Navigate to **Main Menu -> Task Monitoring** to monitor the progress of the Application Installation task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".
5 ☐	**PMAC GUI:** Accept/Reject Upgrade	Navigate to **Software -> Software Inventory** to accept the software installation. Select all the servers on which the application has been installed in the previous steps and click on **Accept Upgrade** as shown below.  **Note:** Once the upgrade has been accepted, the App version will change from ***"Pending Acc/Rej"*** to the version number of the application.

ID	Task	Target	Status	Running Time	Start Time	Progress
25	Upgrade	Enc:10101 Bay:15F	Task ID assigned	0:00:00	2011-09-20 14:36:08	40%
24	Upgrade	Enc:10101 Bay:8F	Task ID assigned	0:00:00	2011-09-20 14:36:08	40%
23	Upgrade	Enc:10101 Bay:7F	Task ID assigned	0:00:01	2011-09-20 14:36:07	40%
22	Upgrade	Enc:10101 Bay:2F	Task ID assigned	0:00:00	2011-09-20 14:36:07	40%
21	Upgrade	Enc:10101 Bay:1F	Task ID assigned	0:00:00	2011-09-20 14:36:07	40%
20	Add Image		Done: 872-2329-101-3.0.0_30.8.0-DSR-x86_64	0:00:06	2011-09-20 14:24:41	100%

Software Inventory

Help

Fri Aug 10 17:45:15 2012 UTC

Filter

Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Desig	Fun
Enc:50202 Bay:1F	192.168.1.4	RDU02-NO	TPD (x86_64)	6.0.0-80.16.0	DSR	4.0.0-0.40333		
Enc:50202 Bay:2F	192.168.1.167	RDU02-MP	TPD (x86_64)	6.0.0-80.16.0	DSR	Pending Acc/Rej		

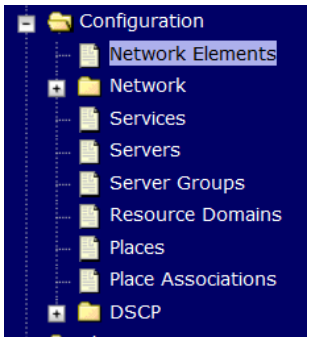
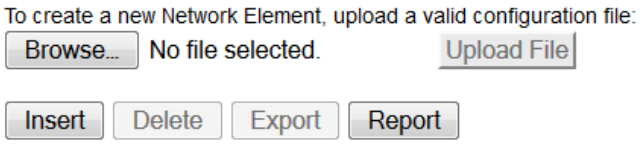
Install OS | Upgrade | Accept Upgrade | Reject Upgrade | Refresh

4.3.2 Configure SOAMs

Procedure 15: Configure SOAM NE

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

Procedure 15: Configure SOAM NE

2 ☐	**NOAM VIP GUI:** Create the SOAM Network Element using an XML File	Make sure to have an SOAM Network Element XML file available on the PC that is running the web browser. The SOAM Network Element XML file is similar to what was created and used in **Procedure 3**, but defines the SOAM "Network Element". Refer to **Appendix A**: Sample Network Element and Hardware Profiles for a sample Network Element xml file Navigate to **Main Menu->Configuration->Network Elements**  Select the **Browse** button, and enter the path and name of the SOAM network XML file. Select the **Upload** File button to upload the XML file and configure the SOAM Network Element. 

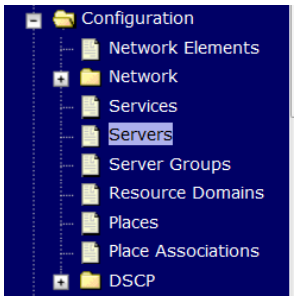
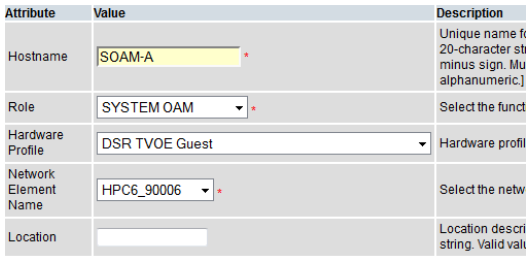
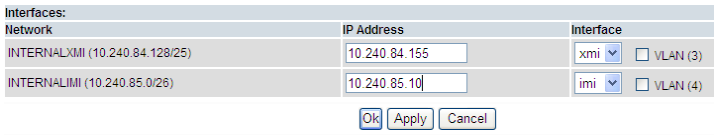
Procedure 16: Configure the SOAM Servers

S T E P #	This procedure will provide the steps to configure the SOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Exchange SSH keys between SOAM site's local PMAC and the SOAM Server**	Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From the PMAC GUI, navigate to **Main Menu -> Software -> Software Inventory.** Enc:9102 Bay:1F Guest: DSR_SOAM_A | 192.168.1.246 | Compass-SOA | TPD (x86_64) | 7.0.0.0.0-86.14.0 | DSR Note the IP address for the SOAM server. Login to the PMAC terminal as the ***admusr*.** From a terminal window connection on the PMAC as the ***admusr*** user, exchange SSH keys for ***admusr*** between the PMAC and the SOAM server using the keyexchange utility, using the Control network IP address for the SOAM server. When prompted for the password, enter the password for the ***admusr*** user of the NOAM server. `$ keyexchange admusr@<SO1_Control_IP Address>`
2 ☐	**Exchange SSH keys between NOAM and PMAC at the SOAM site (If necessary)**	**Note**: If this SOAM shares the same PMAC as the NOAM, then you can skip this step. From a terminal window connection on the NOAM VIP, as the ***admusr,*** exchange SSH keys for admusr between the NOAM and the PMAC for this SOAM site using the keyexchange utility. When prompted for the password, enter the admusr password for the PMAC server. `$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address>`

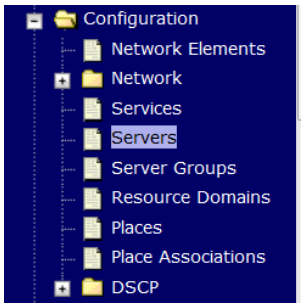
Procedure 16: Configure the SOAM Servers

3 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 16: Configure the SOAM Servers

4 ☐	**NOAM VIP GUI:** Insert the 1st SOAM server	Navigate to **Main Menu -> Configuration -> Servers.**  Select the **Insert** button to insert the 1st SOAM server into servers table (the first or server).  Attribute / Value / Description Hostname: SOAM-A Role: SYSTEM OAM Hardware Profile: DSR TVOE Guest Network Element Name: HPC6_90006 Location Fill in the fields as follows: **Hostname: <Hostname>** **Role: SYSTEM OAM** **System ID: <Site System ID>** **Hardware Profile: DSR TVOE Guest** **Network Element Name: [Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Interfaces: Network / IP Address / Interface INTERNALXMI (10.240.84.128/25) 10.240.84.155 xmi VLAN (3) INTERNALIMI (10.240.85.0/26) 10.240.85.10 imi VLAN (4) Ok Apply Cancel Fill in the server IP addresses for the XMI network. Select **xmi** for the interface. **Leave the "VLAN" checkbox unchecked**. Fill in the server IP addresses for the IMI network. Select **imi** for the interface. **Leave the "VLAN" checkbox unchecked**. Next, add the following NTP servers: **NTP Server** / **Preferred?** **<TVOE_XMI_IP_Address(SO1)>** / Yes Select the **Ok** button when you have completed entering all the server data.

Procedure 16: Configure the SOAM Servers

5 ☐	**NOAM VIP GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.**  From the GUI screen, select the NOAM server and then select **Export** to generate the initial configuration data for that server. 
6 ☐	**NOAM VIP:** Copy Configuration File to 1st SOAM Server	Obtain a terminal session to the NOAM VIP as the ***admusr*** user. Use the **awpushcfg** utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the 1st SOAM server, using the Control network IP address for the 1st SOAM server. The configuration file will have a filename like "TKLCConfigData.<***hostname***>.sh". `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user will be prompted for the following: • IP address of the local PMAC server: Use the 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 3**

Procedure 16: Configure the SOAM Servers

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

8
☐
	1st SOAM Server: Verify Server Health	Execute the following command on the 1st SOAM server and make sure that no errors are returned:
		
		$ sudo syscheck
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules in class system...OK`
		`Running modules in class proc...OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

9 ☐	**Insert and Configure the 2nd SOAM server**	Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so: **NTP Server** — **Preferred?** **<TVOE_XMI_IP_Address(SO2)>** — Yes 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.

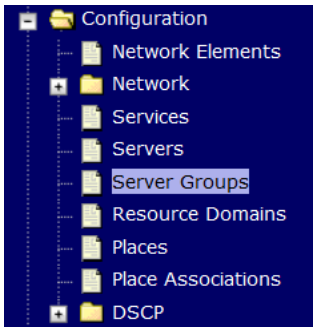
Procedure 16: Configure the SOAM Servers

10 ☐	**Install Netbackup Client Software on SOAMs (Optional)**	If you are using NetBackup at this site, then execute **Procedure 13** again to install the NetBackup Client on all SOAM servers.

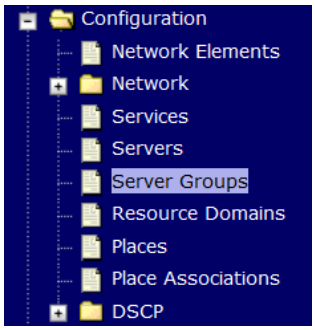
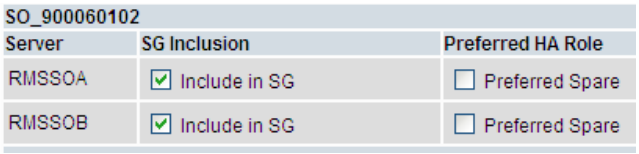
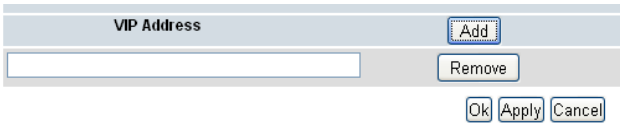
Procedure 17: Configure the SOAM Server Group

S T E P #	This procedure will provide the steps to configure the SOAM Server Group Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 17: Configure the SOAM Server Group

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

Procedure 17: Configure the SOAM Server Group

3 ☐	**NOAM VIP GUI:** Edit the SOAM Server Group and add VIP	From the GUI **Main Menu->Configuration->Server Groups**  Select the new SOAM server group, and then select **Edit.**  Add both SOAM servers to the Server Group Primary Site by clicking the **Include in SG** checkbox. Do not check any of the **Preferred Spare** checkboxes.  SO_900060102 Server | SG Inclusion | Preferred HA Role RMSSOA | ☑ Include in SG | ☐ Preferred Spare RMSSOB | ☑ Include in SG | ☐ Preferred Spare Click **Apply.** Add a SOAM VIP by click on **Add**. Fill in the ***VIP Address*** and press **Ok** as shown below: 

Procedure 17: Configure the SOAM Server Group

<table>
<tr><td>4
☐</td><td>NOAM VIP GUI: Edit the SOAM Server Group and add Preferred Spares for Site Redundancy (Optional)</td><td>If the Two Site Redundancy feature is wanted for the SOAM Server Group, add a SOAM server that is located in its Server Group Secondary Site by clicking the Include in SG checkbox. Also check the Preferred Spare checkbox.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>LabF123SOsp1</td><td>☑ Include in SG</td><td>☑ Preferred Spare</td></tr>
</table>

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 clicking the Include in SG checkbox. Also check the Preferred Spare checkbox.

Note: The Preferred Spare servers must be Server Group Secondary & Tertiary Sites. There should be servers from three separate sites (locations).

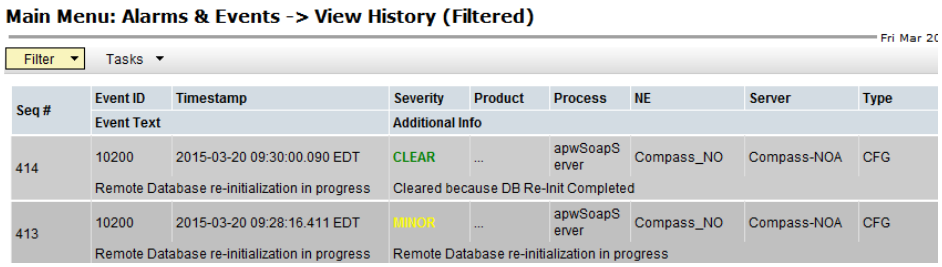
<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>LabF123SOsp1</td><td>☑ Include in SG</td><td>☑ Preferred Spare</td></tr>
<tr><td>LabF123SOsp2</td><td>☑ Include in SG</td><td>☑ Preferred Spare</td></tr>
</table>

For more information about Server Group Secondary Site, Tertiary Site or Site Redundancy, see the 1.4 Terminology section.</td></tr>
<tr><td>5
☐</td><td>NOAM VIP GUI: Edit the SOAM Server Group and add additional SOAM VIPs (Optional)</td><td>Add additional SOAM VIPs by click on Add. Fill in the “VIP Address” and press Ok as shown below.

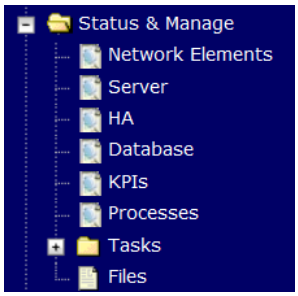
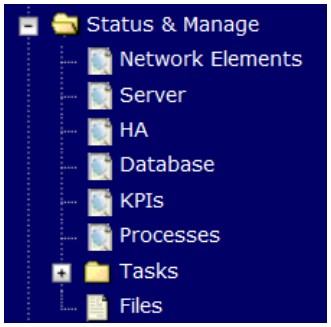
Note: Additional SOAM VIPs only apply to SOAM Server Groups with Preferred Spare SOAMs.


</td></tr>
<tr><td>6
☐</td><td>NOAM VIP GUI: Wait for Remote Database Alarm to Clear</td><td>Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.

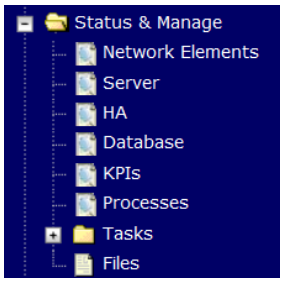
Navigate to Main menu->Alarms & Events->View Active


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

Procedure 17: Configure the SOAM Server Group

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

Procedure 17: Configure the SOAM Server Group

9 ☐	**NOAM VIP GUI**: Restart all Preferred Spare SOAM Servers	If additional Preferred Spare servers are not configured for *Secondary or Tertiary Sites*, this step can be skipped. If additional Preferred Spare servers are configured for *Secondary and/or Tertiary Sites*, continuing in the **Main menu->Status & Manage->Server**  Select the all **Preferred Spare** SOAM servers. Select the **Restart** button. Answer **OK** to the confirmation popup. 

Procedure 18: Activate PCA (PCA Only)

S T E P #	This procedure will provide the steps to activate PCA Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**(PCA Only) Activate PCA Feature**	If you are installing PCA, execute procedures (Added SOAM site activation or complete system activation) within **Appendix A** of the PCA activation and configuration guide [9] to activate PCA. **Note:** If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.

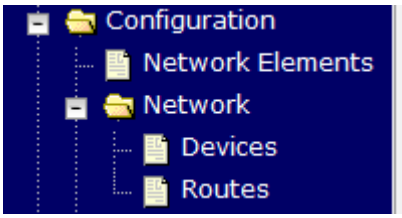
4.4 Configure MP Servers

4.4.1 Configure MP Servers

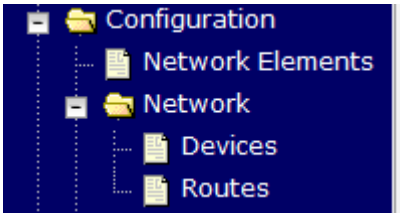
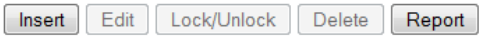
Procedure 19: Configure MP Blade Servers

S T E P #	This procedure will provide the steps to configure an MP Blade Servers (IPFE, SBR, SS7-MP, DA-MP) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 19: Configure MP Blade Servers

2 ☐	**NOAM VIP GUI:** Navigate to Signaling Network Configuration Screen	Navigate to **Main Menu -> Configuration -> Network**  Click on **Insert** in the lower left corner. 
3 ☐	**NOAMP VIP:** Add Signaling Networks	You will see the following screen: Insert Network Field / Value / Description Network Name: XSI1 * — The name of this network. [Default = N/A. Range = Alpha Network Element: - Unassigned - * — The network element this network is a part of. If not spec VLAN ID: 5 * — The VLAN ID to use for this network. [Default = N/A. Rang Network Address: 10.71.88.0 * — The network address of this network. [Default = N/A. Ran colon hex (IPv6) format.] Netmask: 255.255.255.0 * — Subnetting to apply to servers within this network. [Defau IPv6) or dotted decimal (IPv4) format.] Router IP: 10.71.88.3 — The IP address of a router on this network. If this is a def route on servers with interfaces on this network. If custor monitored. Default Network: Yes / No — A selection indicating whether this is the network with a c Routable: Yes / No — Whether or not this network is routable outside its netwo be possibly present in all network elements. Ok Apply Cancel Enter the **Network Name**, **VLAN ID**, **Network Address**, **Netmask**, and **Router IP** that matches the Signaling network **Note:** Even if the network does not use VLAN Tagging, you should enter the correct VLAN ID here as indicated by the NAPD • **IMPORTANT:** Leave the Network Element field as **Unassigned**. • Select **No** for Default Network • Select **Yes** for Routable. Press **OK.** if you are finished adding signaling networks ***-OR-*** Press **Apply** to save this signaling network and repeat this step to enter additional signaling networks.

Procedure 19: Configure MP Blade Servers

4 ☐	**NOAM VIP GUI:** [PCA Only]:Navigate to Signaling Network Configuration Screen	**Note:** Execute this step only if you are defining a separate, dedicated network for SBR Replication. Navigate to **Main Menu -> Configuration -> Network**  Click on **Insert** in the lower left corner. 

Procedure 19: Configure MP Blade Servers

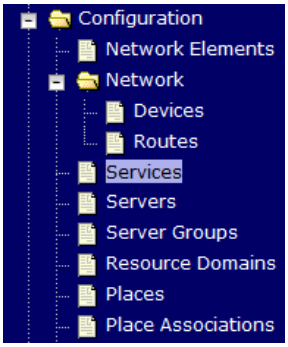
5 ☐	**NOAM VIP GUI:** [PCA Only]: Define SBR DB Replication Network	**Note:** Execute this step only if you are defining a separate, dedicated network for SBR Replication. **Main Menu: Configuration -> Network [Insert]** Info Insert Network Field / Value / Description Network Name: Replicaiton * — The name of this network. [Default = N/A. Range = Alphanumer Network Element: - Unassigned - — The network element this network is a part of. If not specified, t VLAN ID: 8 * — The VLAN ID to use for this network. [Default = N/A. Range = 1- Network Address: 10.71.88.0 * — The network address of this network. [Default = N/A. Range = V format.] Netmask: 255.255.255.0 * — Subnetting to apply to servers within this network. [Default = N/ decimal (IPv4) format.] Router IP: 10.71.88.3 — The IP address of a router on this network. If this is a default ne with interfaces on this network. If customer router monitoring is Default Network: Yes / No — A selection indicating whether this is the network with a default Routable: Yes / No — Whether or not this network is routable outside its network ele present in all network elements. Ok Apply Cancel Enter the **Network Name**, **VLAN ID, Network Address**, **Netmask**, and **Router IP** that matches the SBR DB Replication network **Note:** Even if the network does not use VLAN Tagging, you should enter the correct VLAN ID here as indicated by the NAPD • **IMPORTANT:** Leave the Network Element field as **Unassigned**. • Select **No** for Default Network • Select **Yes** for Routable. Press **Ok.** if you are finished adding signaling networks ***-OR-*** Press **Apply** to save this signaling network and repeat this step to enter additional signaling networks.

Procedure 19: Configure MP Blade Servers

<table>
<tr>
<td>6
☐</td>
<td>NOAM VIP GUI: [PCA Only]: Perform Additional Service to Networks Mapping</td>
<td>

Note: Execute this step only if you are defining a separate, dedicated network for SBR Replication.

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



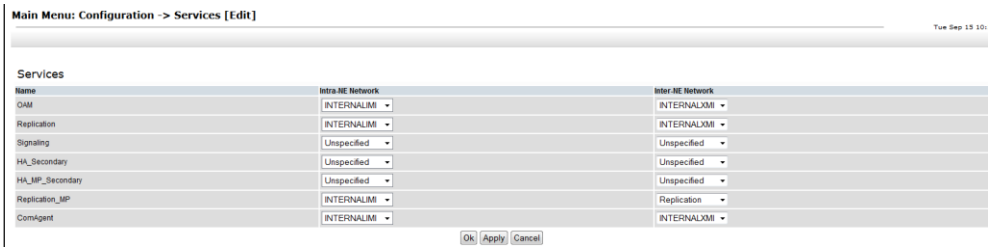
Select the **Edit** button

Set the Services as shown in the table below:

<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>Replication_MP</td><td><IMI Network></td><td><SBR DB Replication Network>*</td></tr>
<tr><td>ComAgent</td><td><IMI Network></td><td><SBR DB Replication Network>*</td></tr>
<tr><td>HA_MP_Secondary</td><td><IMI Network></td><td><SBR DB Replication Network>*</td></tr>
</table>

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.

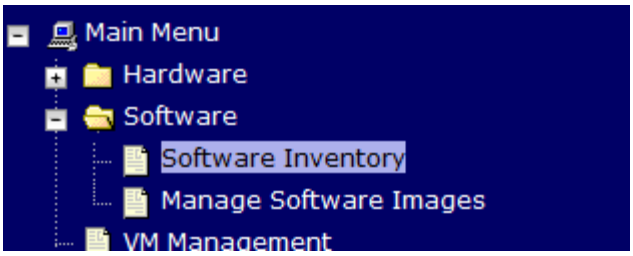
Note: For **HA_MP_Secondary** it is recommended the **Inter-NE Network** be set as the PCA replication network-Optional (configured in **Step 5**) or the XMI network and **Intra-NE Network** be set as the IMI network.



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

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

Procedure 19: Configure MP Blade Servers

7 ☐	**PMAC:** Exchange SSH keys between MP site's local PMAC and the MP server	Use the MP site's PMAC GUI to determine the Control Network IP address of the blade server that is to be an MP server. From the MP site's PMAC GUI, navigate to **Main Menu** -> **Software** -> **Software Inventory**.  Enc:9102 Bay:3F | 192.168.1.239 | Compass-DAMP-03 Note the IP address for an MP server. Login to the MP site's PMAC terminal as the ***admusr.*** From a terminal window connection on the MP site's PMAC as the **admusr**. Exchange SSH keys for ***admusr*** *between* the PMAC and the MP blade server using the keyexchange utility, using the Control network IP address for the MP blade server. `$ keyexchange admusr@<MP_Control_Blade_IP Address>` When prompted for the password, enter the password for the ***admusr*** user of the MP server.

Procedure 19: Configure MP Blade Servers

<table>
<tr>
<td>8
☐</td>
<td>NOAM VIP GUI: Insert the MP server (Part 1)</td>
<td>
Before creating the MP blade server, first identify the hardware profile

Hardware Profile: In the following step, you will select the profile that matches your MP physical hardware and enclosure networking environment.

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.

<table>
<tr><th>Profile Name</th><th>Number of Enclosure Switches (Pairs)?</th><th>Bonded Signaling Interfaces?</th></tr>
<tr><td>1-Pair</td><td>1</td><td>Yes</td></tr>
<tr><td>2-Pair</td><td>2</td><td>Yes</td></tr>
<tr><td>3-Pair-bonded</td><td>3</td><td>Yes</td></tr>
<tr><td>3-Pair-un-bonded</td><td>3</td><td>No</td></tr>
</table>

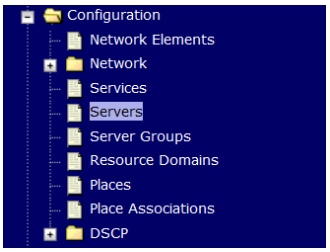
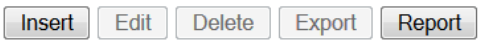
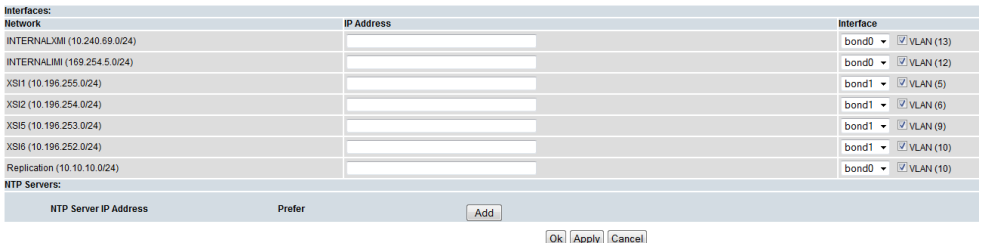
Note: If none of the above profiles properly describe your MP server blade, then you will have to create your own in a text editor (See Figure 7 of Appendix A: Sample Network Element and Hardware Profiles) and copy it into the /var/TKLC/appworks/profiles/ directory of the active NOAM server, the standby NOAM server, and both the DR NOAM servers (if applicable).

Note: After transferring the above file, set the proper file permission by executing the following command:

<pre>$ sudo chmod 777 /var/TKLC/appworks/profiles/<profile name></pre>

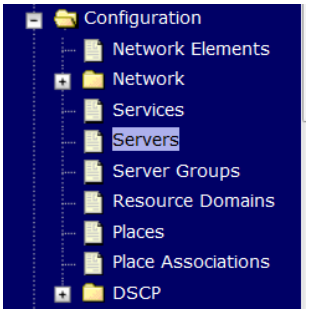
Make note of the profile used here, as it will be used in server creation in the following step.
</td>
</tr>
</table>

Procedure 19: Configure MP Blade Servers

9 ☐	**NOAM VIP GUI:** Insert the MP server (Part 2)	Navigate to **Main Menu**->**Configuration**->**Servers**  Select the **Insert** button to insert the new MP server into servers table.  Fill out the following values: **Hostname**:**<Hostname>** **Role**: **MP** **Network Element**: **[Choose Network Element]** **Hardware Profile**: Select the profile that matches your MP physical hardware and enclosure networking environment from **step 3**. **Location: <enter an optional location description>** The interface configuration form will now appear.  Interfaces: Network / IP Address / Interface INTERNALXMI (10.240.69.0/24) — bond0 — VLAN (13) INTERNALIMI (169.254.5.0/24) — bond0 — VLAN (12) XSI1 (10.196.255.0/24) — bond1 — VLAN (5) XSI2 (10.196.254.0/24) — bond1 — VLAN (6) XSI5 (10.196.253.0/24) — bond1 — VLAN (9) XSI6 (10.196.252.0/24) — bond1 — VLAN (10) Replication (10.10.10.0/24) — bond0 — VLAN (10) NTP Servers: NTP Server IP Address / Prefer / Add Ok Apply Cancel Enter the IP addresses for all networks. Select the correct bond or interface. Ensure the correct bond and VLAN tagging (if required) is selected. For the IMI network, enter the MP's IMI IP address. Select the proper bond or interface, and **select the VLAN checkbox.** **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.**

Procedure 19: Configure MP Blade Servers

<table>
<tr><td>10
☐</td><td>NOAM VIP GUI: Insert the MP server (Part 3)</td><td>Next, add the following NTP servers:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<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>
</table>
Note: For multiple enclosure deployments, prefer the SOAM TVOE Host that is located in the same enclosure as the MP Server.

Select OK when all fields are filled in to finish MP server insertion.</td></tr>
<tr><td>11
☐</td><td>NOAM VIP GUI: Export the Configuration</td><td>Navigate to Main Menu -> Configuration -> Servers.
 

From the GUI screen, select the MP server and then select Export to generate the initial configuration data for that server.
Insert | Edit | Delete | Export | Report</td></tr>
<tr><td>12
☐</td><td>NOAM VIP: Copy Configuration File to MP Server</td><td>Obtain a terminal session to the NOAM VIP as the admusr user.

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

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

<pre>$ sudo awpushcfg</pre>
The awpushcfg utility is interactive, so the user will be prompted for the following:

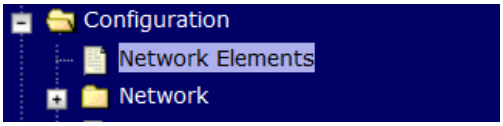
• IP address of the local PMAC server: Use the management network address from the PMAC.
• Username: Use admusr
• Control network IP address for the target server: In this case, enter the control IP for the MP server).
• Hostname of the target server: Enter the server name configured in step 1</td></tr>
</table>

Procedure 19: Configure MP Blade Servers

13 ☐	**MP Server:** Verify awpushcfg was called and Reboot the Configured Server	Obtain a terminal window connection on the MP server console by establishing an ssh session from the NOAM VIP terminal console. **$ ssh admusr@<MP_Control_IP>** Login as the ***admusr*** user. Verify awpushcfg was called by checking the following file: **$ sudo cat /var/TKLC/appw/logs/Process/install.log** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Reboot the server: **$ sudo init 6** Proceed to the next step once the Server finished rebooting, The server is done rebooting once the login prompt is displayed.

14 ☐	**MP Server:** Verify Server Health	After the reboot, login as ***admusr.***
		
		Execute the following command as super-user on the server and make sure that no errors are returned:
		
		$ sudo syscheck
		`Running modules in class hardware…OK`
		`Running modules in class disk…OK`
		`Running modules in class net…OK`
		`Running modules in class system…OK`
		`Running modules in class proc…OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

Procedure 19: Configure MP Blade Servers

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

Procedure 19: Configure MP Blade Servers

16 ☐	**MP Server:** Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network-Part2 (Optional)	After gathering the network information from step 15, proceed with modifying the default routes on the MP server. Establish a connection to the MP server, login as ***admusr.*** Create network routes to the NO's XMI(OAM) network: **Note:** If your NOAM XMI network is exactly the same as your MP XMI network, then you should skip this command and only configure the DR NO route. **$ sudo /usr/TKLC/plat/bin/netAdm add –route=net** **--address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask>** **--gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>** Route to <MP_XMI_Interface> added. Create network routes to the DR NO's XMI(OAM) network: **$ sudo /usr/TKLC/plat/bin/netAdm add –route=net** **--address=<DR-NO_Site_Network_ID> --netmask=<<DR-NO_Site_Network_Netmask>** **--gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>** Route to <MP_XMI_Interface> added. Create network routes to the Management Server TVOE XMI(OAM) network for NTP: **$ sudo /usr/TKLC/plat/bin/netAdm add –route=net** **--address=<TVOE_Mgmt_XMI_Network_Address>** **--netmask=<TVOE_Mgmt_XMI_Network_Netmask>** **--gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>** Route to <MP_XMI_Interface> added. **(Optional)** If Sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network: **$ sudo /usr/TKLC/plat/bin/netAdm add –route=host** **--address=<Customer_NMS_IP> --gateway=<MP_XMI_Gateway_IP_Address>** **--device=<MP_XMI_Interface>** Route to <MP_XMI_Interface> added. (Repeat for any existing customer NMS stations) Delete the existing default route: **$ sudo /usr/TKLC/plat/bin/netAdm delete –route=default** **--gateway=<MP_XMI_Gateway_IP> --device=<MP_XMI_Interface>** Route to <MP_XMI_Interface> removed.

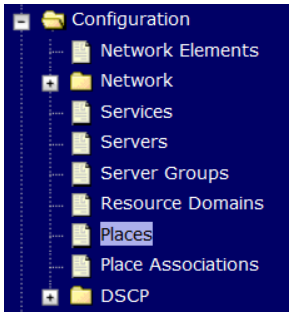
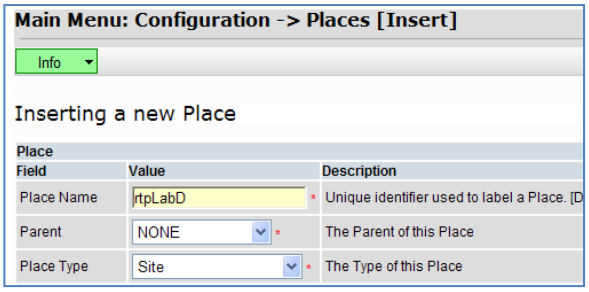
Procedure 19: Configure MP Blade Servers

17 ☐	**MP Server:** Verify connectivity	After steps 16 and 17 have been executed, verify network connectivity. Establish a connection to the MP server, login as ***admusr.*** Ping active NO XMI IP address to verify connectivity: **$ 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 **(Optional)** Ping Customer NMS Station(s): **$ ping <Customer_NMS_IP>** PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data. 64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support.
18 ☐	**Repeat for remaining MP at all sites**	**Repeat** this entire procedure for all remaining MP blades.

Procedure 20: Configure Places and Assign MP Servers to Places (PCA ONLY)

S T E P #	This procedure will provide the steps/reference to add “Places” in the POLICY AND CHARGING DRA Network. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 20: Configure Places and Assign MP Servers to Places (PCA ONLY)

2 ☐	**NOAM VIP GUI:** Configure Places	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user ***guiadmin***. Navigate to **Main Menu -> Configuration -> Places**  Select the **Insert** button   **Place Name: <Site Name>** **Parent: NONE** **Place Type: Site** Repeat this step for each of the *PCA Places (Sites)* in the network. See the 1.4 Terminology section for more information on Sites & Places.

Procedure 20: Configure Places and Assign MP Servers to Places (PCA ONLY)

3 ☐	**NOAM VIP GUI:** Assign MP Servers To Places	Select the place configured in step 2, press the edit button. Insert Edit Delete Report For each place you have defined, choose the set of MP servers that will be assigned to those places. **Place** **Field** **Value** Place Name rtpLabC * Parent NONE * Place Type Site * **Servers** LABCSONE ☐ labCe1b04pdra1 Check all the check boxes for **PCA DA-MP** and **SBR** servers that will be assigned to this place. Repeat this step for all other DA-MP or SBR servers you wish to assign to places. **Note**: All **PCA DA-MPs, SS7MPs** and **SBR MPs** must be added to the *Site Place* that corresponds to the physical location of the server. See the **1.4** Terminology section for more information on *Sites*.

Procedure 21: Configure the MP Server Group(s) and Profile(s)

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

Procedure 21: Configure the MP Server Group(s) and Profile(s)

<table>
<tr>
<td>2
☐</td>
<td>NOAM VIP GUI:
Determine Server Group Function</td>
<td>
Determine what server group function will be configured, make note the following configuration decisions.
<table>
<tr><th>Server Group Function</th><th>MPs Will Run</th><th>Redundancy Model</th></tr>
<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>Policy & Charging 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>
</table>
For the CPA application:
At least one MP Server Group with the “Session Binding Repository” function.

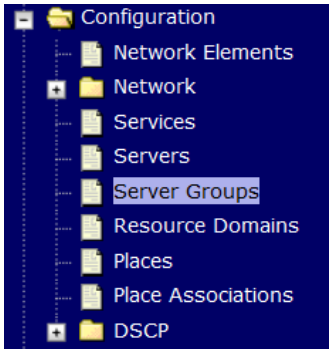
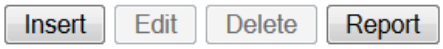
For PCA application:
- Online Charging function (only)
  ○ At least one MP Server Group with the “Policy and Charging SBR” function must be configured
  ○ At least one MP Server Group with the “DSR (multi-active cluster)” function must be configured
  ○ MP Server Groups with the “IP Load Balancer” function (IPFE) are optional.
- Policy DRA function
  ○ At least two MP Server Groups with the “Policy and Charging SBR” function must be configured. One will store Session data and one will store 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.

WAN Replication Connection Count:
• For non-Policy and Charging SBR Server Groups: Default Value
• For Policy and Charging Server Groups: 8

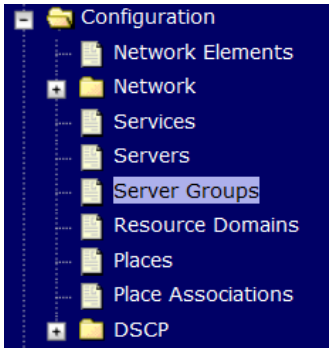
For the PCA application, the following types of MP Server Groups must be configured:

- DA-MP (Function: DSR (multi-active cluster))
- SBR (Function: Policy and Charging SBR)
- IPFE (Function: IP Load Balancer) – Optional)
</td>
</tr>
</table>

Procedure 21: Configure the MP Server Group(s) and Profile(s)

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

Procedure 21: Configure the MP Server Group(s) and Profile(s)

5 ☐	**NOAM VIP GUI:** Edit the MP Server Groups to include MP blades.	From the GUI, navigate to **Main Menu**->**Configuration**->**Server Groups**  Select a server group that you just created and then select **Edit.** Select the Network Element that represents the MP server group you wish to edit. Click the **Include in SG** box for every MP server that you wish to include in *this* server group. Leave other checkboxes blank. **HPC6_90006** **Server** / **SG Inclusion** / **Preferred HA Role** MP-1 / ☑ Include in SG / ☐ Preferred Spare MP-2 / ☑ Include in SG / ☐ Preferred Spare **Note:** Each IPFE and SS7MP server should be in its own server group. Select **OK.**

Procedure 21: Configure the MP Server Group(s) and Profile(s)

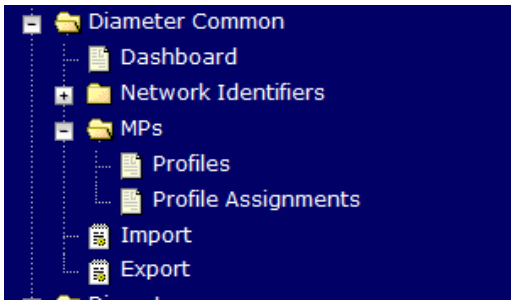
6 ☐	**NOAM VIP GUI:** [PCA ONLY] Edit the MP Server Group and add Preferred Spares for Site Redundancy (Optional)	If Two Site Redundancy for the Policy and Charging SBR Server Group is wanted, add a MP server that is physically located in a separate site (location) to the Server Group by clicking the **Include in SG** checkbox and also check the **Preferred Spare** checkbox. Server | SG Inclusion | Preferred HA Role LabF123SBRsp1 | ☑ Include in SG | ☑ Preferred Spare 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 clicking the **Include in SG** checkbox and also check the **Preferred Spare** checkbox for both servers. **Note:** The **Preferred Spare** servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations). Server | SG Inclusion | Preferred HA Role LabF123SBRsp1 | ☑ Include in SG | ☑ Preferred Spare LabF123SBRsp2 | ☑ Include in SG | ☑ Preferred Spare For more information about Site Redundancy for Policy and Charging SBR Server Groups, see the **1.4** Terminology section. Select **OK** to save
7 ☐	**NOAM VIP GUI:** Repeat For Additional Server Groups	Repeat Steps 5- 6 for any remaining MP server groups you need to edit.
8 ☐	**NOAM VIP GUI:** Wait for Remote Database Alarm to Clear	Wait for the alarm **Remote Database re-initialization in progress** to be cleared before proceeding. Navigate to **Main menu->Alarms & Events->View Active** **Main Menu: Alarms & Events -> View History (Filtered)** Fri Mar 20 Filter Tasks Seq # | Event ID | Timestamp | Severity | Product | Process | NE | Server | Type Event Text | Additional Info 414 | 10200 | 2015-03-20 09:30:00.090 EDT | CLEAR | ... | apwSoapServer | Compass_NO | Compass-NOA | CFG Remote Database re-initialization in progress | Cleared because DB Re-Init Completed 413 | 10200 | 2015-03-20 09:28:16.411 EDT | MINOR | ... | apwSoapServer | Compass_NO | Compass-NOA | CFG Remote Database re-initialization in progress | Remote Database re-initialization in progress

Procedure 21: Configure the MP Server Group(s) and Profile(s)

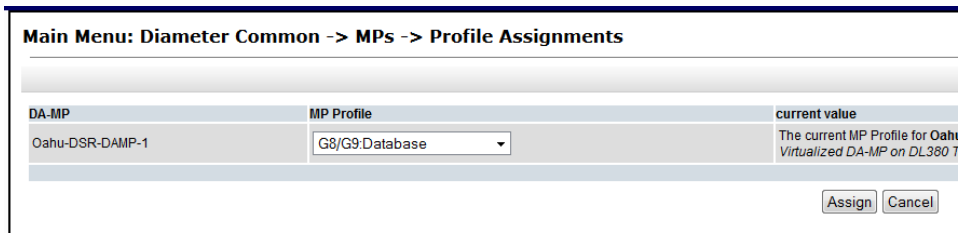
9 ☐	**SOAM VIP GUI:** Login	If not already done, establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login to the SOAM GUI as the ***guiadmin*** user: 

Procedure 21: Configure the MP Server Group(s) and Profile(s)

<table>
<tr>
<td>10
☐</td>
<td>SOAM VIP GUI: Assign Profiles to DA-MPs from SOAM GUI.</td>
<td>
Navigate to Main Menu -> Diameter Common ->MPs -> Profile Assignments



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



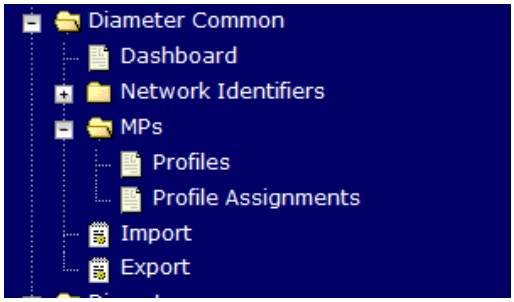
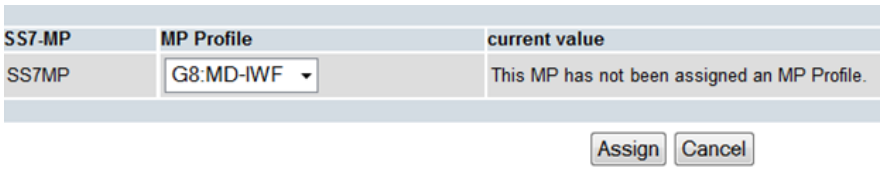
For each MP, select the proper profile assignment based on the MP's hardware type and the function it will serve:

<table>
<tr><th>Profile Name</th><th>Description</th></tr>
<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>
</table>

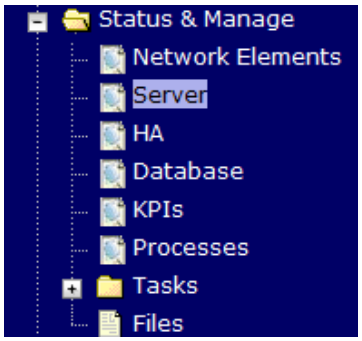
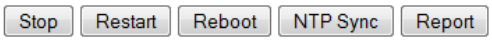
Note: If the DA-MPs at this site are configured for *Active/Standby* then there will be a single selection box visible that assigns profiles for all MPs.

When finished, press the **Assign** button
</td>
</tr>
</table>

Procedure 21: Configure the MP Server Group(s) and Profile(s)

11 ☐	**SOAM VIP GUI:** Assign Profiles to SS7-MPs.	Navigate to **Main Menu->Diameter->Configuration->MPs->Profiles Assignments**  Refer to the **SS7-MP** section. (If the site has both DSR and MAP-IWF server groups, you will see both a DA-MP section and an SS7-MP section)  For each SS7 MP, select the proper profile assignment based on the SS7 MP's hardware type and the function it will serve: <table><tr><th>Profile Name</th><th>Description</th></tr><tr><td>**G8:MD-IWF**</td><td>HP BL460 Gen8/9 Running MAP-IWF fucntions</td></tr></table> When finished, press the **Assign** button

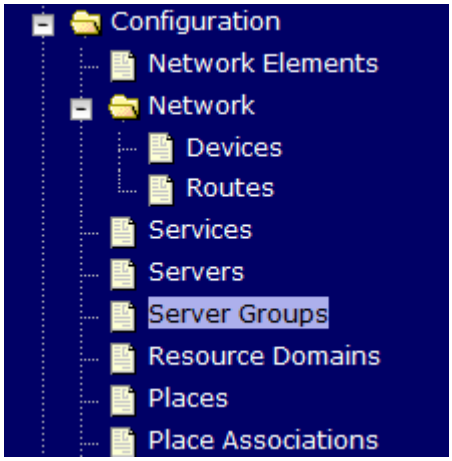
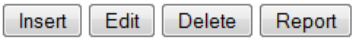
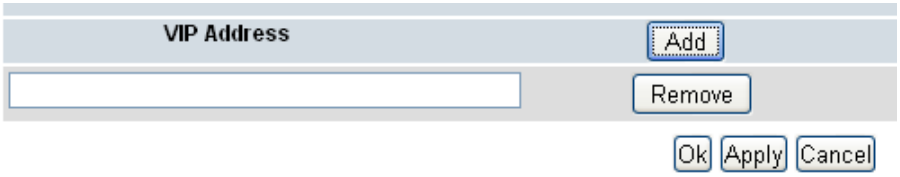
Procedure 21: Configure the MP Server Group(s) and Profile(s)

12 ☐	**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: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 
13 ☐	**NOAM VIP GUI:** Restart MP blade servers	Navigate to **Main menu**->**Status & Manage**->**Server**  For each MP server: • Select the MP server. • Select the **Restart** button. • Answer **OK** to the confirmation popup. Wait for the message which tells you that the restart was successful.  **Note**: POLICY AND CHARGING DRA INSTALLATIONS: You may continue to see alarms related to ComAgent until you complete PCA installatio

Procedure 22: Add VIP for Signaling networks (Active/Standby Configurations Only)

S T E P #	This procedure will provide the steps to configure the VIPs for the signaling networks on the MPs. 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 22: Add VIP for Signaling networks (Active/Standby Configurations Only)

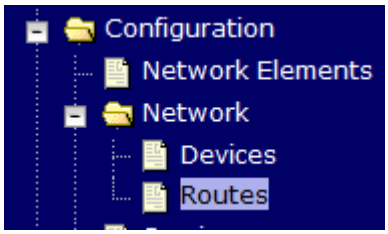
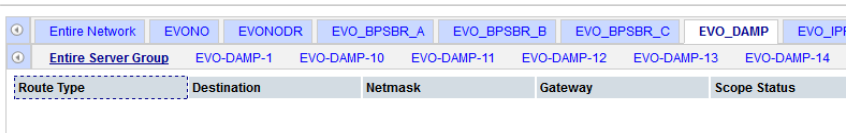
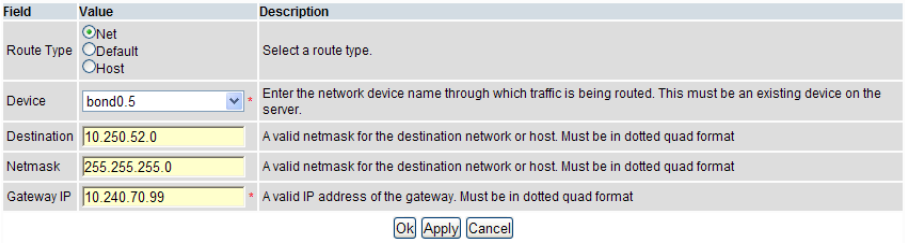
2 ☐	**NOAM VIP GUI:** Edit the MP Server Group and add VIPs (ONLY FOR 1+1)	**IF YOUR MPs ARE IN A DSR MULTI-ACTIVE CLUSTER SERVER GROUP CONFIGURATION (N+0), THEN SKIP THIS STEP** From **Main Menu->Configuration->Server Groups**  Select the MP server group, and then select **Edit**  Click on **Add** to add the VIP for XSI1 Enter the VIP of int-XSI-1 and click on **Apply** Click on **Add** again to add the VIP for XSI2 Enter the VIP of int-XSI-2 and click on **Apply** If more Signaling networks exist, add their corresponding VIP addresses. Finally Click on **OK.** 

4.4.2 Configure Signaling Network Routes

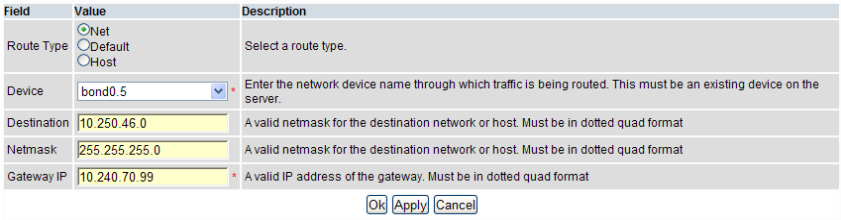
Procedure 23: Configure the Signaling Network Routes

S T E P #	This procedure will provide the steps to configure Signaling Network Routes on MP-type servers (DA-MP, IPFE,SS7-MP, etc.) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 23: Configure the Signaling Network Routes

2 ☐	**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, then verify the **Entire Server Group** link is selected, if not, select the link. 
3 ☐	**NOAM VIP GUI:** Add Route	Click on **Insert** at the bottom of the screen to add additional routes. Insert Edit Delete Report Report All
4 ☐	**NOAM VIP GUI:** Add Default Route for MPs Going Through Signaling Network Gateway (Optional)	**OPTIONAL -** Only execute this step if you performed **Procedure 19: Step 10**: which removed the XMI gateway default route on MPs If your MP servers no longer have a default route, then you can now insert a default route here which uses one of the signaling network gateways.  Field / Value / Description Route Type: Net, Default, Host — Select a route type. Device: bond0.5 — Enter the network device name through which traffic is being routed. This must be an existing device on the server. Destination: 10.250.52.0 — A valid netmask for the destination network or host. Must be in dotted quad format Netmask: 255.255.255.0 — A valid netmask for the destination network or host. Must be in dotted quad format Gateway IP: 10.240.70.99 — A valid IP address of the gateway. Must be in dotted quad format Ok Apply Cancel **Route Type: Default** **Device: Select the signaling device that is directly attached to the network where the XSI default gateway resides.** **Gateway IP: The XSI gateway you wish to use for default signaling network access**. Select **OK** Ok Apply Cancel

Procedure 23: Configure the Signaling Network Routes

5
☐
	NOAM VIP GUI: Add Network Routes for Diameter Peers	Use this step to add IP and/or IPv6 routes to *diameter* peer destination networks. The goal here is to ensure that diameter traffic uses the gateway(s) on the signaling networks.
		
		 
		Route Type: **Net, Default, Host**
		
		Device: Select the appropriate signaling interface that will be used to connect to that network
		
		Destination: Enter the Network ID of Network to which the peer node is connected to.
		
		Netmask: Enter the corresponding Netmask (if configuring Net or Default 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.
		
		If you have more routes to enter, Press **Apply** to save the current route entry and repeat this step to enter more routes
		
		If you are finished entering routes, Press **OK** to save the latest route and leave this screen.
		
		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 will vary) :
		
		Add routes (IPv4 & IPv6):
		
		`$ sudo netConfig –device=switch1A addRoute network=10.10.10.0 mask=25.255.255.0 nexhop=10.50.76.81`
		`$ sudo netConfig –device=switch1A addRoute network6=2001::/64 nexthop=fd0f::1`
		
		Delete routes (IPv4 & IPv6):
		
		`$ sudo netConfig –device=switch1A deleteRoute network=10.10.10.0 mask=25.255.255.0 nexhop=10.50.76.81`
		`$ sudo netConfig –device=switch1A deleteRoute network6=2001::/64 nexthop=fd0f::1`

Field	Value	Description
Route Type	⦿Net ○Default ○Host	Select a route type.
Device	bond0.5 *	Enter the network device name through which traffic is being routed. This must be an existing device on the server.
Destination	10.250.46.0	A valid netmask for the destination network or host. Must be in dotted quad format
Netmask	255.255.255.0	A valid netmask for the destination network or host. Must be in dotted quad format
Gateway IP	10.240.70.99 *	A valid IP address of the gateway. Must be in dotted quad format

Ok Apply Cancel

Procedure 23: Configure the Signaling Network Routes

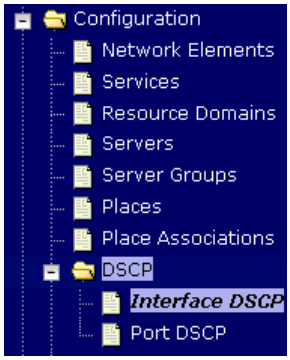
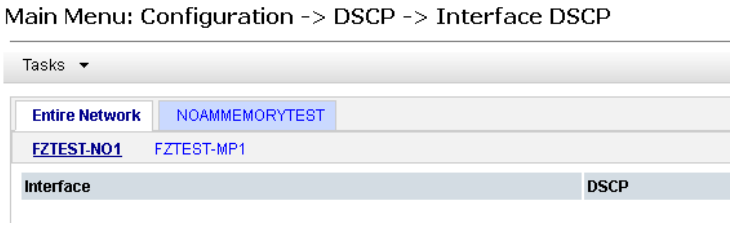
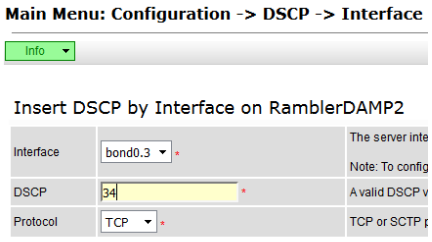
6 ☐	**Local PMAC:** Perform a netConfig Backup	After the routes are added to the aggregation switches via netconfig, a **netconfig backup** should be taken so that the new routes are retained in the backup. Execute the following command: `$ netConfig backupConfiguration --device=<Switch Hostname service=<ssh_Service> filename=<Backup Filename>`
7 ☐	**NOAM VIP GUI:** Repeat for all other MP server groups.	The routes entered in this procedure should now be configured on all MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from **step 2**, but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups. This includes DAMP, IPFE, and SS7MP servers. **Note:** IPFE and DAMP servers must have the same routes configured.

4.4.3 Configure DSCP (Optional)

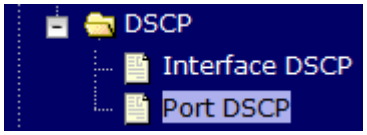
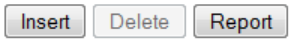
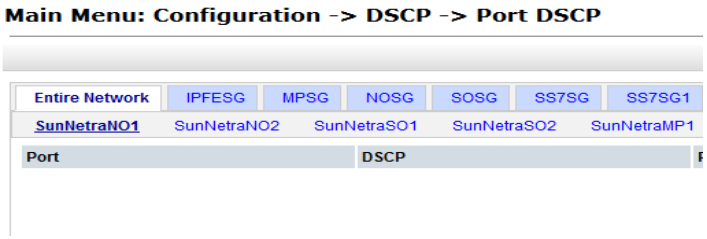
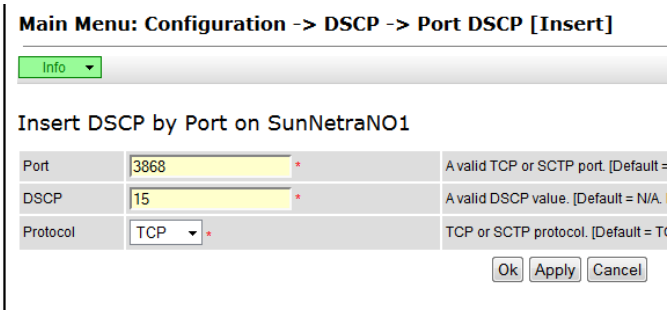
Procedure 24: Configure DSCP Values for Outgoing Traffic

S T E P #	This procedure will provide the steps to configure the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network will utilize packet DSCP markings for Quality-of-Service purposes. **Note:** If your enclosure switches already have DSCP configuration for the signaling VLANs, then the switch configuration will override the settings in this procedure. It is strongly recommended, however, that you configure DSCP here at the application level where you have the most knowledge about outgoing traffic patterns and qualities. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 24: Configure DSCP Values for Outgoing Traffic

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

Procedure 24: Configure DSCP Values for Outgoing Traffic

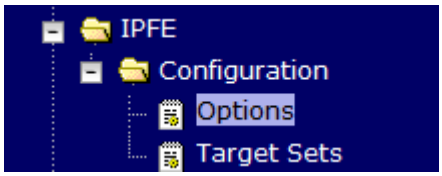
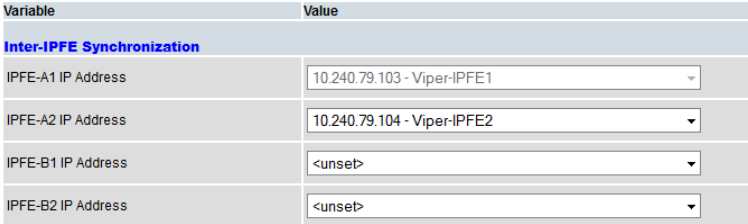
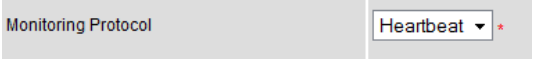
3 ☐	**NOAM VIP GUI:** Option 2: Configure Port DSCP	**Note:** The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to **Main Menu -> Configuration -> DSCP -> Port DSCP**  Select the server you wish to configure from the list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

4.4.4 Configure IP Front End Servers (Optional)

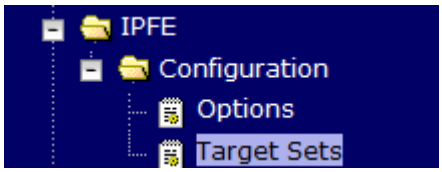
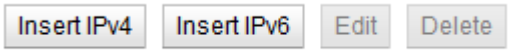
Procedure 25: IP Front End (IPFE) Configuration

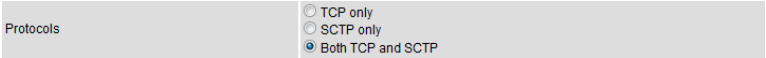
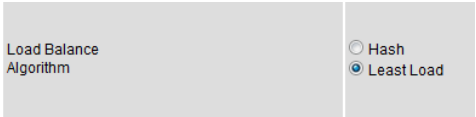
S T E P #	This procedure will provide the steps to configure IP Front End (IPFE), and optimize performance. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for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

Procedure 25: IP Front End (IPFE) Configuration

2 ☐	**SOAM VIP GUI:** Configuration of replication IPFE association data.	Select **Main Menu -> IPFE -> Configuration -> Options**  Enter the IP address of the 1st IPFE in the IPFE-A1 IP Address field and the IP address of the 2nd IPFE in the IPFE-A2 IP Address field If applicable, enter the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields.  **Note:** It is recommended that the address reside on the IMI (Internal Management Interface) network. **Note:** IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2. **Note:** In order for the IPFE to provide Least Load distribution, Monitoring Protocol must be set to ***Heartbeat*** so that the application servers can provide the load information the IPFE uses to select the ***least-loaded*** server for connections.  **Note:** The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios. If Hash load balance algorithm is desired, select None for Monitoring Protocol:  Click **Ok**

Procedure 25: IP Front End (IPFE) Configuration

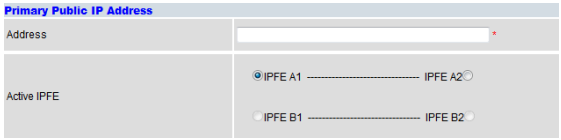
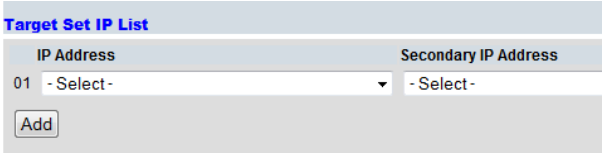
3 ☐	**SOAM VIP GUI:** Configuration of IPFE Target sets-Part 1 (Insert Target Set)	Select **Main Menu -> IPFE -> Configuration -> Target Sets**  Select either **Insert IPv4** or **Insert IPv6** button, depending on the IP version of the target set you plan to use. 

4
☐
	SOAM VIP GUI: Configuration of IPFE Target sets-Part 2 (Target Set Configuration)	Continued from the previous step, the following are configurable:
		Protocols: protocols the target set will support.
		 
		
		Delete Age: Specifies when the IPFE should remove its association data for a connection. Any packets presenting a source IP address/port combination that had been previously stored as association state but have been idle longer than the **Delete Age** configuration will be treated as a new connection and will not automatically go to the same application server.
		 
		
		Load Balance Algorithm: ***Hash*** or ***Least Load*** options
		 
		
		Establish an SSH session to the SOAM VIP, login as ***admusr***.
		Execute the following command (advise cut and paste to prevent errors):
		`$ sudo iset -fvalue="50" DpiOption where "name='MpEngIngressMpsPercentile'"`
		`=== changed 1 records ===`

Procedure 25: IP Front End (IPFE) Configuration

5 ☐	**SOAM VIP GUI:** Configuration of IPFE Target sets-Part 3 (Target Set Configuration)	**(Optional):** If you have selected the **Least Load algorithm**, you may configure the following fields to adjust the algorithm's behavior: **MPS Factor** – Messages per Second (MPS) is one component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). It is recommended that IPFE connections have Reserved Ingress MPS set to something other than the default, which is 0. MPS Factor 50 * Connection Count Factor 50 * To configure **Reserved Ingress MPS**, go to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> Capacity Configuration Sets**. If you choose not to use **Reserved Ingress MPS**, set **MPS Factor** to 0 and **Connection Count Factor**, described below, to 100. **Connection Count Factor** – This is the other component of the **least load** algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern. **Allowed Deviation** - Percentage within which two application server's load calculation results are considered to be equal. If very short, intense connection bursts are expected to occur, increase the value to smooth out the distribution. Allowed Deviation 5 *

Procedure 25: IP Front End (IPFE) Configuration

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

Procedure 25: IP Front End (IPFE) Configuration

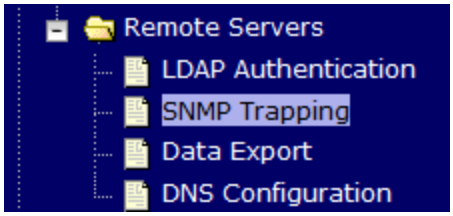
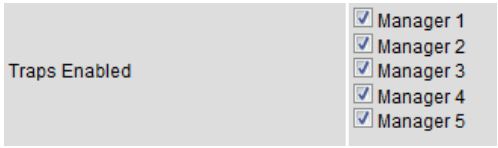
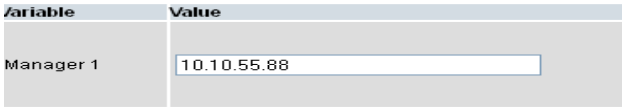
7 ☐	**SOAM VIP GUI:** Repeat for additional Configuration of IPFE Target sets.	Repeat for **steps 3-6** for each target set (Up to 16). At least one target set must be configured.

4.5 SNMP Configuration (Optional)

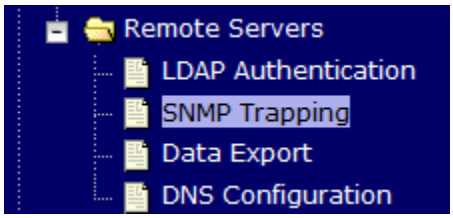
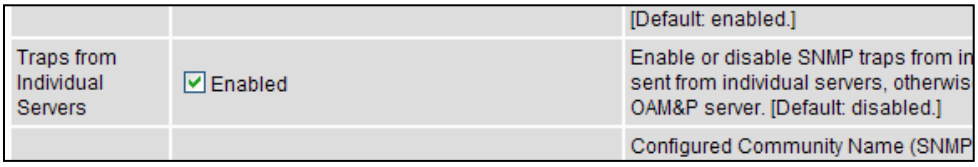
Procedure 26: Configure SNMP Trap Receiver(s)

S T E P #	This procedure will provide the steps to configure forwarding of SNMP Traps from each individual server. 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login to the NOAM GUI as the ***guiadmin*** user: 

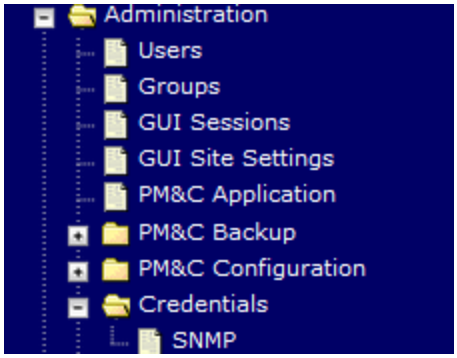
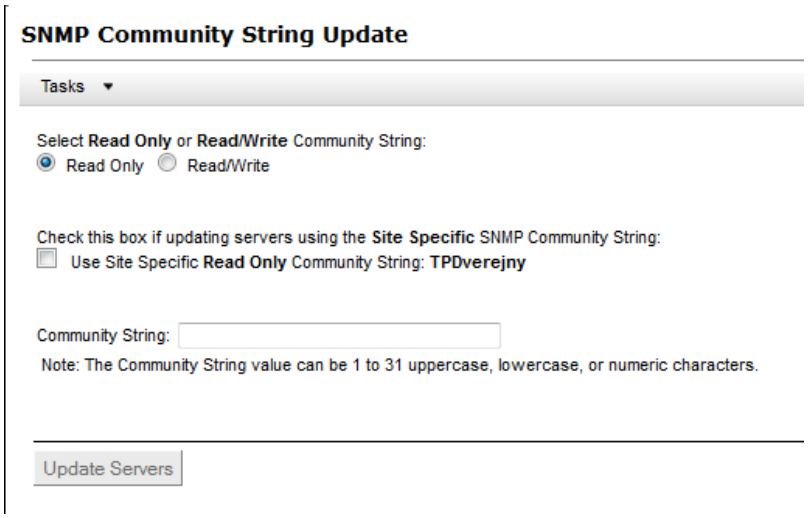
Procedure 26: Configure SNMP Trap Receiver(s)

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

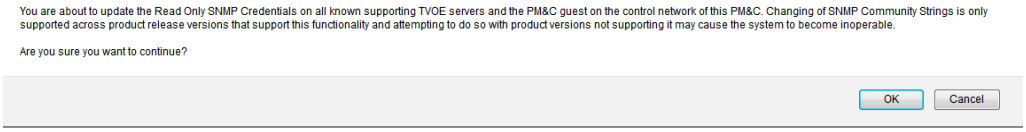
Procedure 26: Configure SNMP Trap Receiver(s)

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

Procedure 26: Configure SNMP Trap Receiver(s)

5 ☐	**PMAC GUI:** Update the TVOE Host SNMP Community String	Navigate to **Main Menu -> Administration -> Credentials -> SNMP**  Select the **Read Only** or **ReadWrite** button depending on which SNMP community string is to be updated.  **Note:** If this the first time the SNMP Community Strings has been updated for this PMAC, perform the following: 1. Leave the Use Site Specific checkbox (*TPDverejny*) unchecked. 2. Enter the community string configured in step 2 of this procedure.

Procedure 26: Configure SNMP Trap Receiver(s)

6 ☐	**PMAC GUI:** Update the TVOE Host SNMP Community String	Continued from the previous step, enter the new Community String into the Community string textbox. Click the **Update Servers** button  The following warning will be displayed:  Select **OK** **Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be up dated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.

4.6 IDIH Installation and Configuration (Optional)

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

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

4.6.1 IDIH Installation

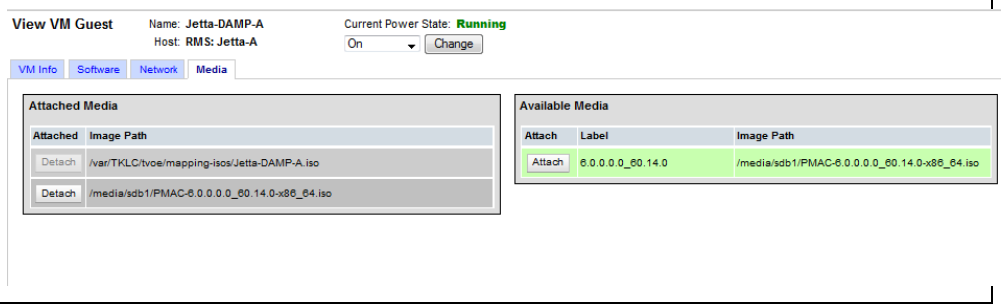
The installation procedure uses the "fast deployment" utility (fdconfig) bundled with the PMAC server to install and configure IDIH.

Procedure 27: IDIH Configuration

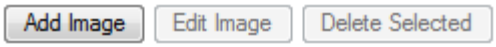
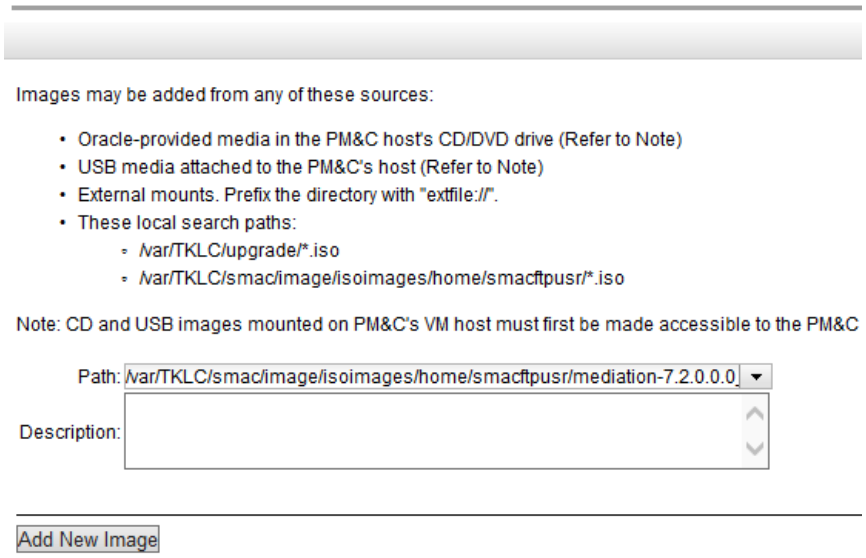
STEP #	This procedure will provide the steps to install and configure IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	

1
☐
	TVOE Host:
	Load Application ISO
		Add the Application ISO images (**Mediation, application, and Oracle**) to the PM&C, this can be done in one of three ways:
		1. Insert the 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 PM&C 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 PM&C server*)
		Using sftp, connect to the PM&C server
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		After the image transfer is 100% complete, close the connection:
		`$ quit`
		
		Note: If there is insufficient disk space with the PMAC repository as pmacftpuser, please follow section "Configure PM&C Application Guest isoimages Virtual Disk" of [12] to increase it.

Procedure 27: IDIH Configuration

2 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 
3 ☐	**PMAC GUI:** Attach the software Image to the PMAC Guest	If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, navigate to **Main Menu -> VM Management.** In the *"**VM Entities**"* list, select the PM&C guest. On the resulting *"**View VM Guest**"* page, select the **Media** tab. Under the **Media** tab, find the ISO image in the *"**Available Media**"* list, and click its **Attach** button. After a pause, the image will appear in the *"**Attached Media**"* list. 

Procedure 27: IDIH Configuration

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

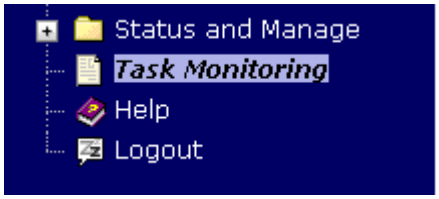
Procedure 27: IDIH Configuration

6 ☐	**PMAC:** Copy the fdc.cfg file to the guest-dropin Directory	Copy the fdc.cfg file to the pmac guest-dropin directory. Execute the following command: `$ sudo cp  /usr/TKLC/smac/html/TPD/mediation-*/fdc.cfg /var/TKLC/smac/guest-dropin`
7 ☐	**PMAC:** Configure the fdc.cfg file	Configure the fdc.cfg file. See **Appendix** K: IDIH Fast Deployment Configuration for a breakdown of the parameters. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.

8
☐
	PMAC: Run the FDC creation script idihFdc.sh	Rename the fdc.cfg file to your preference; also note that two files are generated by the fdc shell script. One is for the Installation procedure and the other file is used for the upgrade procedure. The upgrade FDC is named upgrade.
		
		Example: hostname.cfg
		
		Note: The following hostname for guests has been reserved for internal use. Please try to avoid them:
		• oracle
		• mediation
		• appserver
		
		Here are the suggested hostname for guests:
		• <server hostname>-ora example, thunderbolt-ora
		• <server hostname>-med example, thunderbolt-med
		• <server hostname>-app example, thunderbolt-app
		
		Run the FDC creation script **fdc.sh**.
		
		Execute the following commands:
		
		`$cd /var/TKLC/smac/guest-dropin/`
		
		`$sudo /usr/TKLC/smac/html/TPD/mediation-7.1.0.0.0_71.x.x-x86_64/fdc.sh fdc.cfg`
		
		Note: Verify the values in the xml generated from the fdc.sh script match those of the values entered in fdc.cfg.

Procedure 27: IDIH Configuration

9
☐
	TVOE Host: Verify/Remove External Devices	Establish an SSH session to the TVOE Host which will host the IDIH, login as ***admusr***.
		
		On the TVOE host which will host the IDIH, before IDIH has ever been installed, or, after the external disk removal procedure has been successfully completed:
		
		Execute the following command:
		
		`$ ls /dev/sd*`
		
		Verify you only have sda* devices (e.g. sda1, sda2, etc…)
		Expected output:
		
		`$ ls /dev/sd*`
		`/dev/sda  /dev/sda1  /dev/sda2  /dev/sda3`
		
		Note: If any other devices are listed (e.g. sdb*, sdc*, sdd*, etc…) Stop. You must first remove the extra device(s) in your system (e.g. sdb*, sdc*, sdd*, etc…). Refer to **Appendix L: IDIH External Drive Removal**. Reboot the tvoe and verify the extra device(s) are still removed (> ls /dev/sd*)

10 ☐	**PMAC:** Run the fdconfig.	Run the fdconfig configuration. Execute the following commands: **`$ screen`** **`$sudo fdconfig config --file=hostname_xx-xx-xx.xml`** Example: `$sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml` **Note:** This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a *"screen -dr"* to resume the screen session in the event of a terminal timeout etc.
11 ☐	**PMAC GUI:** Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the IDIH configuration to completion.

4.6.2 Post IDIH Installation Configuration

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

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

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

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

Procedure 28: Configure DSR Reference Data Synchronization for IDIH

STEP #	This procedure will provide the steps to configure DSR reference data syncornization for IDIH Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**IDIH Application Server:** Login	Establish an SSH session to the IDIH Application Server. Login as user ***admusr.*** Issue the following commands to login as ***tekelec*** user. `$ sudo su – tekelec`

Procedure 28: Configure DSR Reference Data Synchronization for IDIH

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

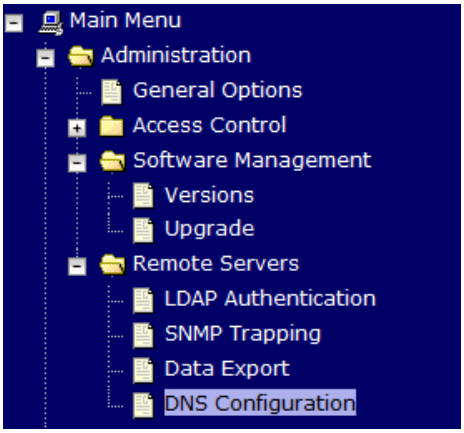
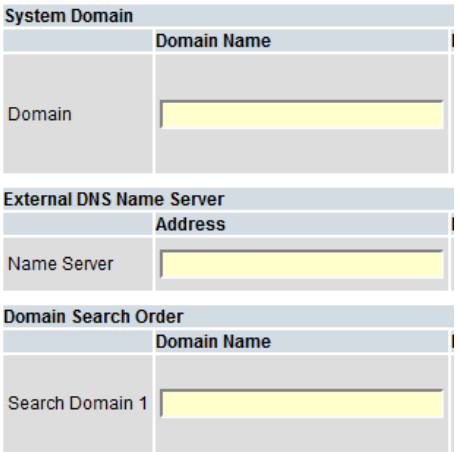
Procedure 28: Configure DSR Reference Data Synchronization for IDIH

3 ☐	**IDIH App Server:** Monitor Completion	Monitor the log file located at: `/var/TKLC/xIH/log/apps/weblogic/apps/application.log` Examine the log file for entries containing text **"Trace Reference Data Adapter"**

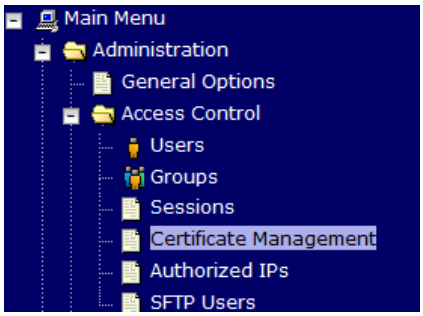
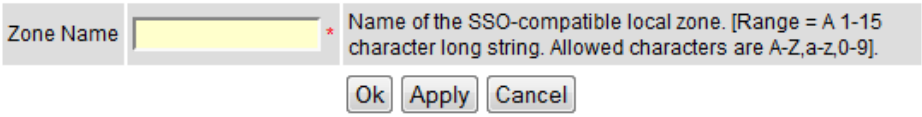
Procedure 29: IDIH Configuration: Configuring the SSO Domain

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

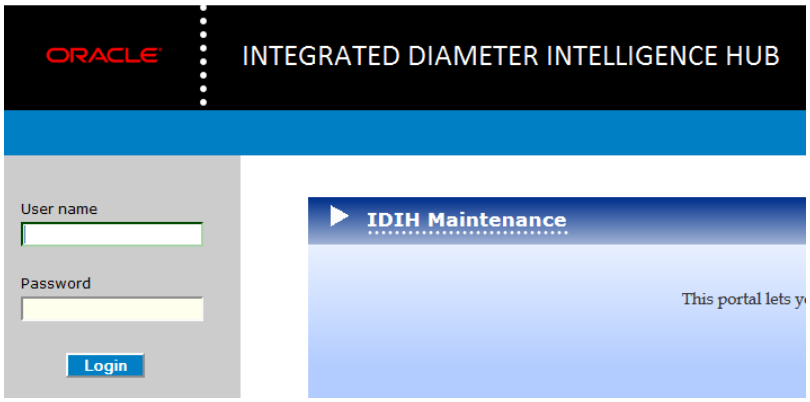
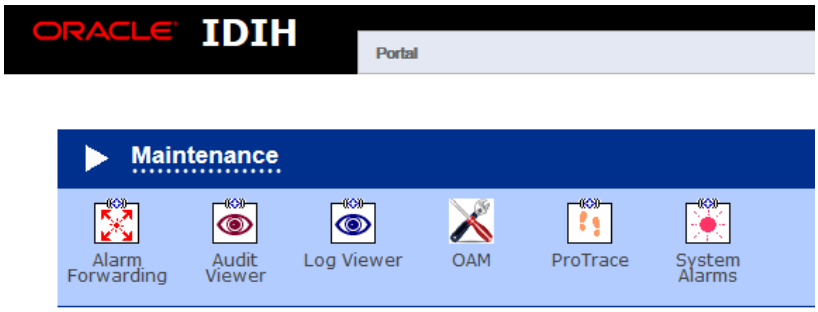
Procedure 29: IDIH Configuration: Configuring the SSO Domain

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

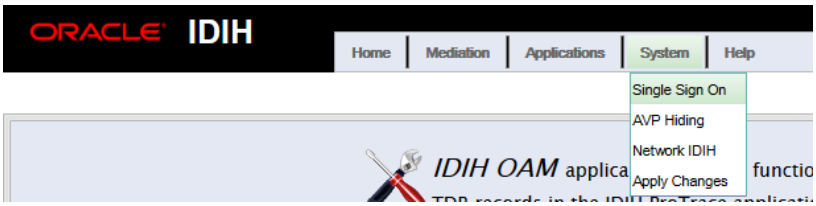
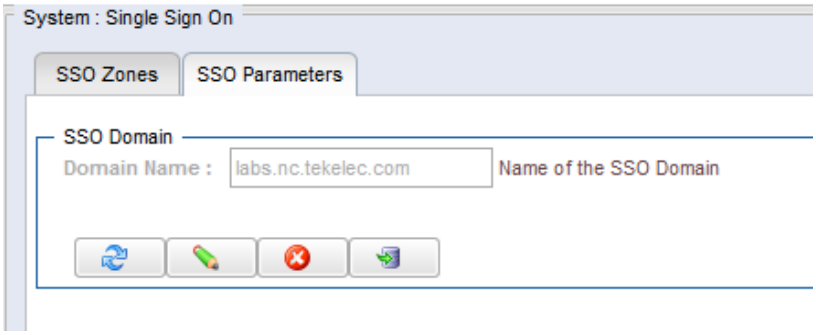
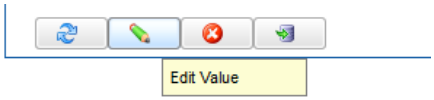
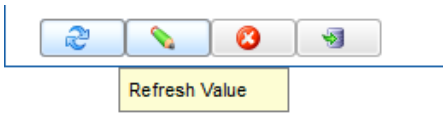
Procedure 29: IDIH Configuration: Configuring the SSO Domain

3 ☐	**NOAM VIP GUI:** Establish SSO Local Zone	Navigate to **Main Menu -> Access Control -> Certification Management**  Select the **Establish SSO Zone** button  Enter a value for Zone Name:  Select the **Ok** button. Information for the new Certifcate type of SSO Local is now displayed. Select the **Report** button.  The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access. Example of Certiciate report: -----BEGIN CERTIFICATE----- MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV BAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwG T3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqGSIb3 DQEJARYEdGVzdDAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ BgNVBAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UE CgwGT3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqG SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZ/MpkhlvMP/iJ s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAf BgNVHSMEGDAWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAMBgNVHRMEBTADAQH/MA0G CSqGSIb3DQEBCwUAA0EAOwIqBMEQyvfvt38r/yfgIx3w5dN8SBwHjHC5TpJrHV6U zFlg5dfzoLz7ditjGOhWJ9l9VRw39LQ8lKFp7SMXwA== -----END CERTIFICATE-----

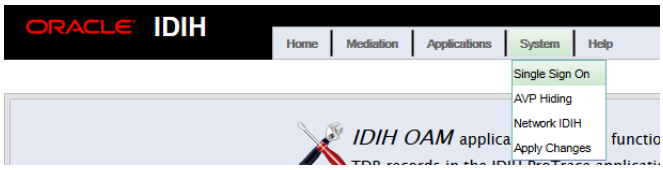
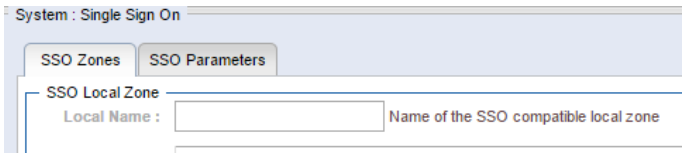
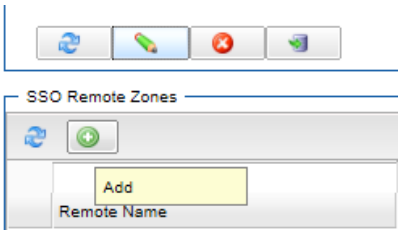
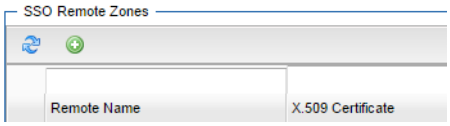
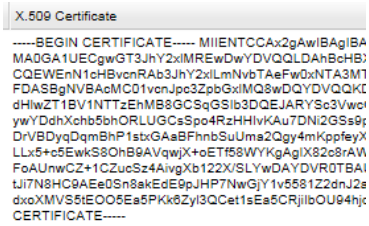
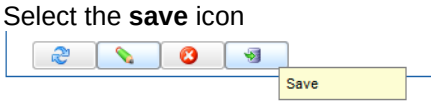
Procedure 29: IDIH Configuration: Configuring the SSO Domain

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

Procedure 29: IDIH Configuration: Configuring the SSO Domain

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

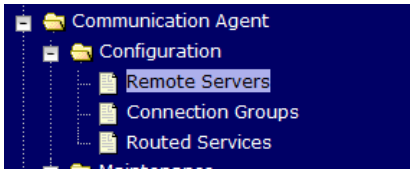
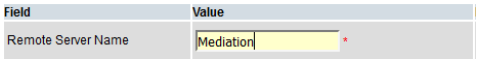
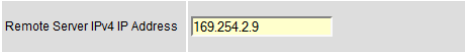
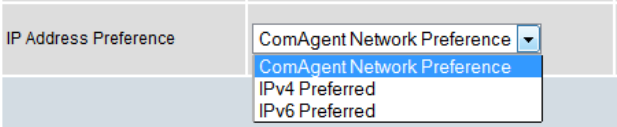
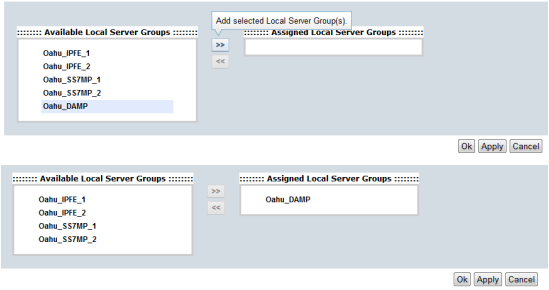
Procedure 29: IDIH Configuration: Configuring the SSO Domain

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

Procedure 30: IDIH Configuration: Configure IDIH in the DSR

S T E P #	This procedure will provide the steps to complete the IDIH integration on the DSR. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: **https://<Primary_NOAM_VIP_IP_Address>** Login as the ***guiadmin*** user: 

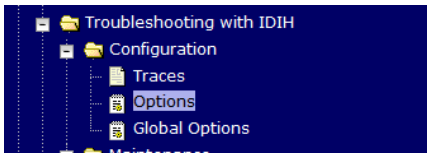
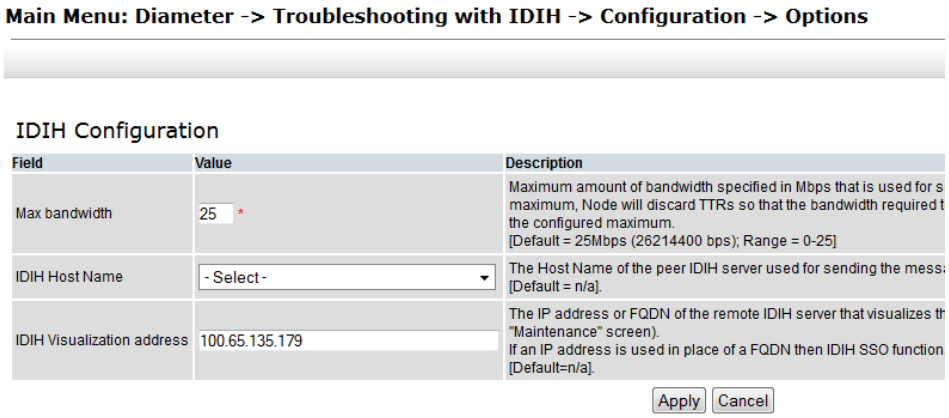
Procedure 30: IDIH Configuration: Configure IDIH in the DSR

2 ☐	**NOAM VIP GUI:** Configure CommAgent Connection	Navigate to **Main Menu -> Communcation Agent -> Configuration -> Remote Servers**  Select the **Insert** button  Add the IDIH Mediation Server For the Remote Server IP address field, enter the IMI IP address of the IDIH Mediation Server.  For the Remote Server IP address field, enter the IMI IP address of the IDIH Mediation Server.  **Note:** This should be the IMI IP address of the DP Server. Select **Server** for the Remote Server Mode from the pull down menu:  Select the IP Address Preference:  Select the Local Server Group for the DSR MP server group:  Click **Apply**

Procedure 30: IDIH Configuration: Configure IDIH in the DSR

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

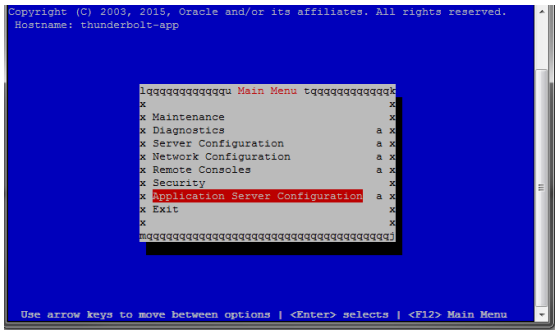
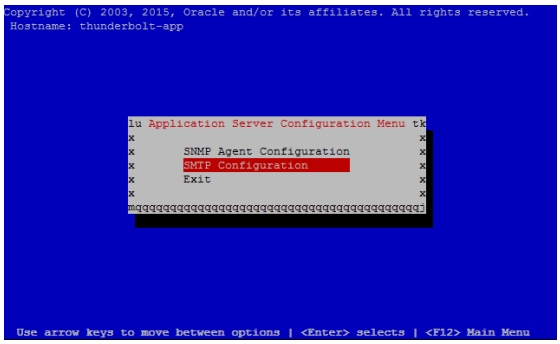
Procedure 30: IDIH Configuration: Configure IDIH in the DSR

4 ☐	**SOAM VIP GUI:** Configure IDIH Hostname	Navigate to **Main Menu -> Diameter -> Troubleshooting with IDIH -> Configuration -> Options**  Enter the fully qualified IDIH host name in the I**DIH Visualization Address field**:  Click the **Apply** button

Procedure 31: IDIH Configuration: Configure Mail Server (Optional)

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

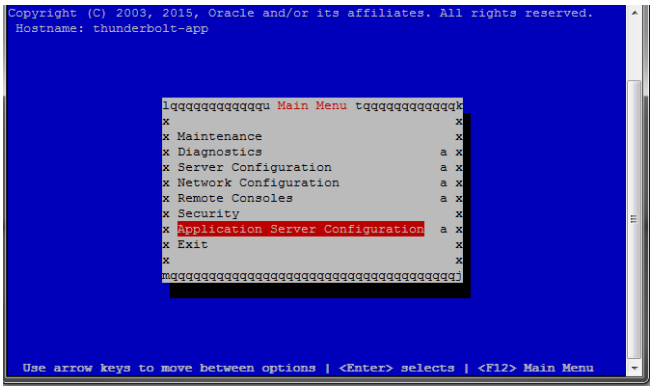
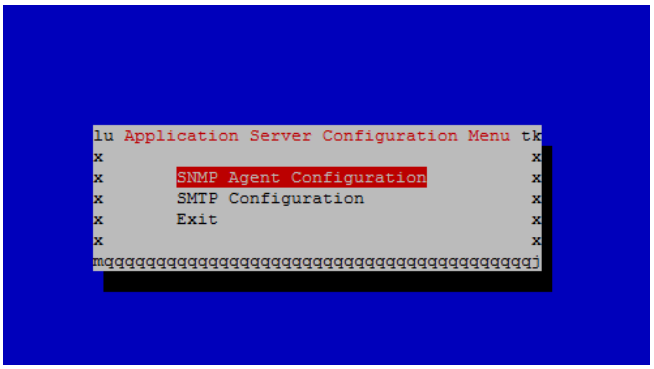
Procedure 31: IDIH Configuration: Configure Mail Server (Optional)

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

Procedure 32: IDIH Configuration: Configure SNMP Management Server (Optional)

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

Procedure 32: IDIH Configuration: Configure SNMP Management Server (Optional)

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

Procedure 33: IDIH Configuration: Change Network Interface (Optional)

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

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

Procedure 34: IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File (Optional)

S T E P #	This procedure will provide the steps to generate a disaster recovery fdc file. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Identify Backup Server**	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM
2 ☐	**PMAC:** Establish Terminal Session	Establish an SSH session to the PMAC. Login as ***admusr***.
3 ☐	**PMAC:** Verify Upgrade fdc file exists	Execute the following commands to verify the upgrade FDC file for IDIH exists: **$ cd /var/TKLC/smac/guest-dropin** **$ ls –l *.xml** The following output is expected: -rw-r----- 1 root smac 9542 May 11 09:43 <idih_install>.xml -rw-r----- 1 root smac 5107 May 11 09:43 <idih_upgrade>.xml **Note:** The <idih_upgrade>.xml file is the same file used for upgrade and disaster recovery procedures.
4 ☐	**PMAC:** Transfer the FDC file to a remote server.	Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. **$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/guest-dropin/<idih_upgrade.xml> /path/to/destination/** When prompted, enter the admusr user password and press **Enter.** If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system.

Procedure 35: IDIH Configuration: Change Alarm Ignore List (Optional)

S T E P #	This procedure will provide the steps to change 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**IDIH Mediation Server:** Login	Establish an SSH session to the IDIH Mediation Server. Login as user ***admusr.*** Issue the following commands to login as tekelec user. `$ sudo su - tekelec`

Procedure 35: IDIH Configuration: Change Alarm Ignore List (Optional)

2
☐
	IDIH Mediation Server: Execute the Change Interface Script	Execute the change alarms script with the following command:
		
		`$ chgAlms.sh`
		
		Answer the following questions during execution of the script:
		
		`This script is used to change ignore list for mediation alarms.`
		`There are two lists, one for Severity where the list contains the severity values (no spaces, comma separated).`
		`Severity default list = '4'`
		`Possible severity values are:`
		`  1  Critical error`
		`  2  Major error`
		`  3  Minor error`
		`  4  Information only; no error`
		`  5  Cleared`
		
		`The other is the event list which contains the (comcol) event numbers (no spaces, comma separated).`
		`Please answer the following questions or enter CTLR-C to exit out of the script.`
		
		`Current setting are: ignore.event= ignore.severity=4`
		
		`Enter new ignore list for alarm severity (comma separated list) or '0' to keep current [4]: 0`
		
		`Enter new ignore list for alarm events (comma separated list) or '0' to keep current []: 0`
		
		`Updating configuration properties file with 'ignore.severity=4' and 'ignore.event='`
		
		`Backing-up configuration properties with 'ignore.severity=4' and 'ignore.event='`
		
		`Restarting ImpAlarms process ...`
		
		`Done!`

4.7 Post-Install Activities

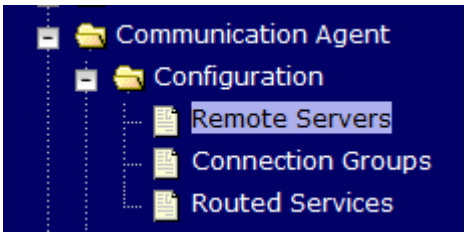
Procedure 36: Activate Optional Features

S T E P #	This procedure will provide instruction on how to install DSR optional components once regular installation is complete. **Prerequisite:** All previous DSR installation steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Refer to Activation Guides for Optional Features**	Refer to 3.2 Optional Features for a list of feature activation documents whose procedures are to be executed at this moment.

Procedure 37: Configure ComAgent Connections (DSR + SDS)

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

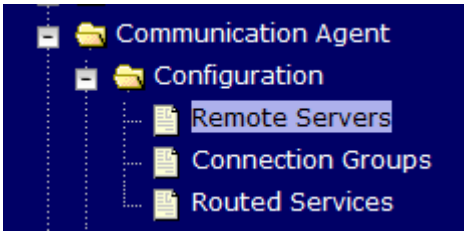
Procedure 37: Configure ComAgent Connections (DSR + SDS)

2 ☐	**SDS NOAM VIP GUI:** Configure Remote Server IP Address	Navigate to **Main Menu -> Communication Agent -> Configuration -> Remote Servers**  Click **Insert** 

Procedure 37: Configure ComAgent Connections (DSR + SDS)

3 ☐	**SDS NOAM VIP GUI:** Configure Remote Server IP Address	Enter the Remote Server Name for the DSR MP Server: **Field** / **Value** / **Description** Remote Server Name / RDU08MP1 * / Unique identifier used to label a Remote Server. [Default: n/a; Range: A 32-character string. Valid underscore. Must contain at least one alpha and Enter the Remote Server IMI IP address: Remote Server IP Address / 169.254.2.6 * / This is the IP address of the Remote Server. Default: n/a; Range: A valid IPv4 address. **Note:** This should be the IMI IP address of the MP server. Select **Client** for the Remote Server Mode from the pull down menu: Remote Server Mode / Client * Select the Local Server Group for the SDS DP server group: ::::::: Available Local Server Groups ::::::: DP_rlghnc_1_grp DP_drhmnc_1_grp Add selected Local Server Group(s). ::::::: Assigned Local Server Groups ::::::: Ok Apply Cancel Click **Apply** ::::::: Available Local Server Groups ::::::: ::::::: Assigned Local Server Groups ::::::: DP_rlghnc_1_grp DP_drhmnc_1_grp Ok Apply Cancel
4 ☐	**SDS NOAM VIP GUI:** Repeat	Repeat steps 2-3 for each remote MP in the same SOAM NE.

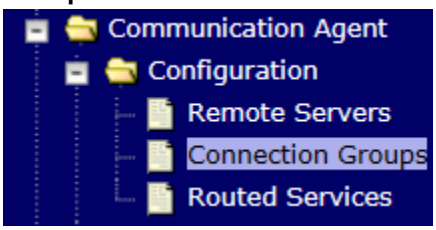
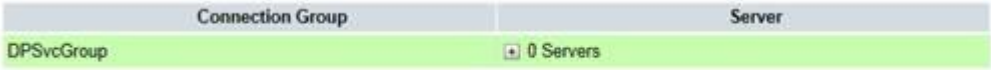
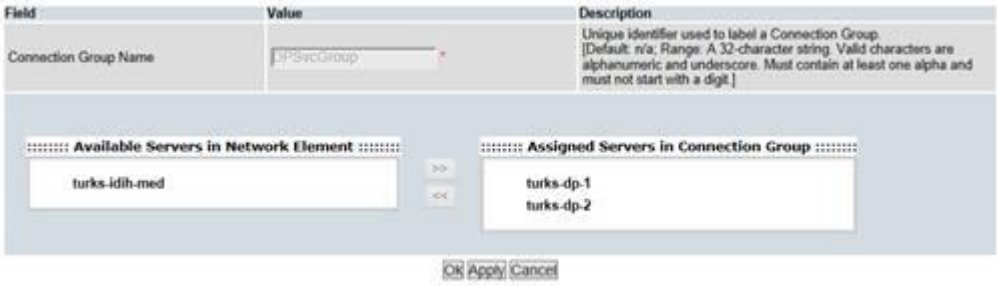
Procedure 37: Configure ComAgent Connections (DSR + SDS)

5 ☐	**DSR NOAM VIP GUI:** Login	Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_DSR_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
6 ☐	**DSR NOAM VIP GUI:** Configure Remote Server IP Address	Navigate to **Main Menu -> Communication Agent -> Configuration -> Remote Servers**  Click **Insert** 

Procedure 37: Configure ComAgent Connections (DSR + SDS)

7 ☐	**DSR NOAM VIP GUI:** Configure Remote Server IP Address	Enter the Remote Server Name for the SDS DP Server: **Field** / **Value** Remote Server Name: RDU08SDSDP1 * Enter the Remote Server IMI IP address: Remote Server IPv4 IP Address: 169.254.2.9 **Note:** This should be the IMI IP address of the DP Server. Select **Server** for the Remote Server Mode from the pull down menu: Remote Server Mode: Server * Select the IP Address Preference: IP Address Preference: ComAgent Network Preference ComAgent Network Preference IPv4 Preferred IPv6 Preferred Select the Local Server Group for the DSR MP server group: ::::::: Available Local Server Groups ::::::: Oahu_IPFE_1 Oahu_IPFE_2 Oahu_SS7MP_1 Oahu_SS7MP_2 Oahu_DAMP Add selected Local Server Group(s). >> << ::::::: Assigned Local Server Groups ::::::: Ok Apply Cancel ::::::: Available Local Server Groups ::::::: Oahu_IPFE_1 Oahu_IPFE_2 Oahu_SS7MP_1 Oahu_SS7MP_2 >> << ::::::: Assigned Local Server Groups ::::::: Oahu_DAMP Ok Apply Cancel Click **Apply**
8 ☐	**DSR NOAM VIP GUI:** Repeat	Repeat steps 6-7 for each remote DP in the same SOAM NE.

Procedure 37: Configure ComAgent Connections (DSR + SDS)

9 ☐	**DSR NOAM VIP GUI:** Configure Connection Groups	Navigate to **Main Menu -> Communication Agent -> Configuration -> Connection Groups** 
10 ☐	**DSR NOAM VIP GUI:** Edit Connection Groups	Select the DPSvcGroup Connection Group  Click **Edit**  Select the desired DP servers from the Available Servers in Network Element:   Click **Ok**

Procedure 37: 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. 

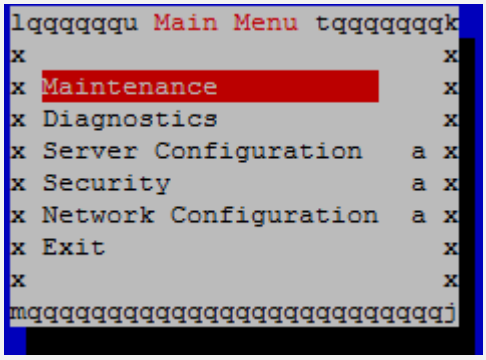
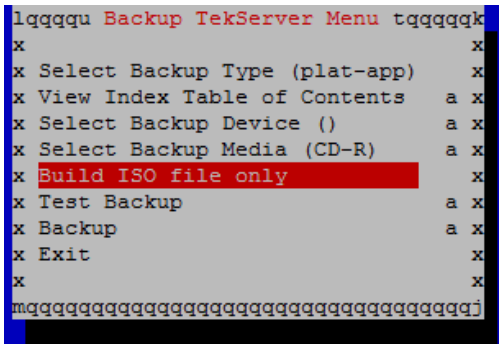
Procedure 38: Shared secret encryption key revocation (RADIUS Only)

STEP #	This procedure will provide instruction on how to change shared secret encryption key on DSR 7.2/7.3 radius setup. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Revoke RADIUS shared secret encryption key**	Refer to RADIUS Shared Secret Key revocation MOP to change the encryption key on the DSR installed setup. Refer [11] **Note:** This is highly recommended to change the key after installation due to security reasons.

Procedure 39: Backup TVOE Configuration

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

Procedure 39: Backup TVOE Configuration

3 ☐	**TVOE Server:** Build ISO backup file	Execute the following command from the TVOE server: `$ sudo su - platcfg`  Select the following menu options sequentially: **Maintenance -> Backup and Restore ->Backup Platform (CD/DVD)**. The ***"Backup TekServer Menu"*** page will now be shown. Build the backup ISO image by selecting: Build ISO file only  **Note:** Creating the ISO image may happen so quickly that this screen may only appear for an instant. After the ISO is created, platcfg will return to the Backup TekServer Menu. The ISO has now been created and is located in the /var/TKLC/bkp/ directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso" Exit out of platcfg by selecting **Exit**.

Procedure 39: Backup TVOE Configuration

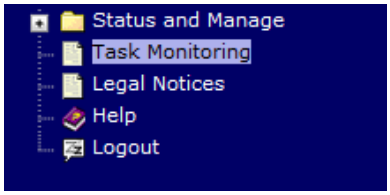
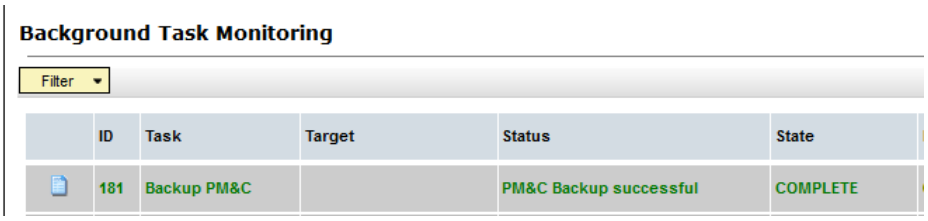
4 ☐	**Backup Server:** Transfer TVOE Files to Backup Server	Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/` When prompted, enter the tvoexfer user password and press **Enter.** If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system. The TVOE backup file has now been successfully placed on the backup server.
5 ☐	**Repeat for Additional TVOE Servers**	Repeat steps **3-4** for additional TVOE servers

Procedure 40: Backup PMAC Application

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

3
☐
	PMAC Server: Build backup File	Execute the following command from the PMAC server:
		
		`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		
		`PM&C backup been successfully initiated as task ID 7`
		
		Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor page:
		
		or issue the command "**pmaccli getBgTasks** ". The result should eventually be "PMAC Backup successful" and the background task should indicate "COMPLETE".

Procedure 40: Backup PMAC Application

4 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 
5 ☐	**PMAC Server GUI:** Monitor/Verify Backup Task Completion	Navigate to **Main Menu -> Task Monitoring**  Monitor the Backup PM&C Task:  **Note:** Alternatively, you can monitor the Backup task by executing the following command: `$ sudo pmaccli getBgTasks`

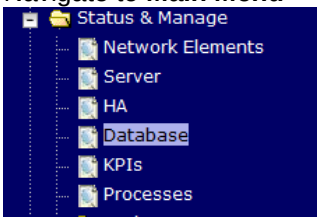
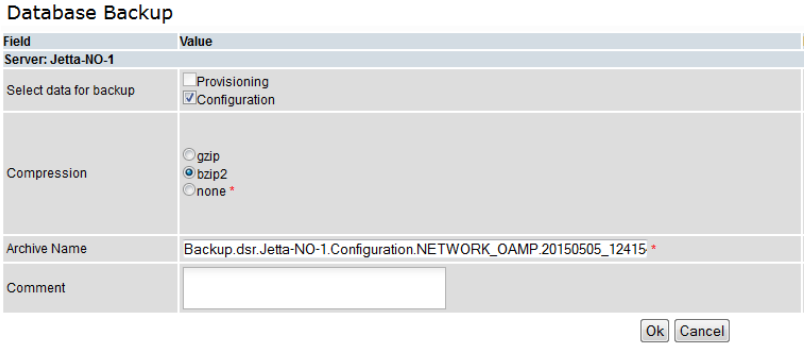
Procedure 40: Backup PMAC Application

6 ☐	**Backup Server:** Transfer PMAC File to Backup Server	Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/` When prompted, enter the admusr user password and press **Enter.** If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system.

Procedure 41: NOAM Database Backup

S T E P #	This procedure will provide instruction on how to back up the NOAM Database. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Identify Backup Server**	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM
2 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Procedure 41: NOAM Database Backup

4 ☐	**NOAM VIP GUI:** Perform Database Backup	Navigate to **Main Menu -> Status & Manage -> Database**  Select the Active NOAM Select the **Backup** Button:  Select the desired file compression method  Set the archive file name if needed. Select **OK**

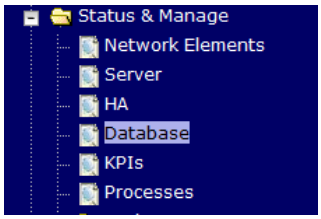
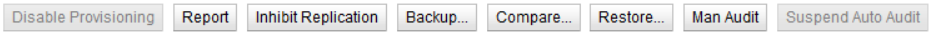
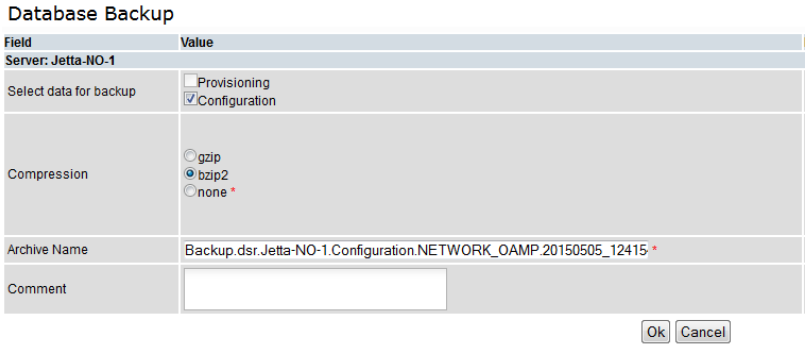
Procedure 41: NOAM Database Backup

6 ☐	**Backup Server:** Transfer File to Backup Server	Login to the backup server identified in **step 1** and copy backup image and key file (RADIUS Only) to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. **$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/** Execute following command to encrypt the key file before sending to filemgmt area : **$ ./sharedKrevo –encr** Copy key file to customer server : **$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/DpiKf.bin.encr /path/to/destination /** When prompted, enter the admusr user password and press **Enter.** If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system.

Procedure 42: SOAM Database Backup

S T E P #	This procedure will provide instruction on how to back up the SOAM Database. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Identify Backup Server**	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM
2 ☐	**SOAM VIP GUI:** Login	Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Procedure 42: SOAM Database Backup

4 ☐	**SOAM VIP GUI:** Perform Database Backup	Navigate to **Main Menu -> Status & Manage -> Database**  Select the Active SOAM Select the **Backup** Button:  Select the desired file compression method  Set the archive file name if needed. Select **OK**
6 ☐	**Backup Server:** Transfer PMAC File to Backup Server	Login to the backup server identified in **step 1** and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/` When prompted, enter the admusr user password and press **Enter.** If the Customer System is a Windows system please refer to reference [7] Using WinSCP to copy the backup image to the customer system.
6 ☐	**Repeat for Additional TVOE Servers**	Repeat **steps 2-6** for additional SOAM Sites

Procedure 43: Enable/Disable DTLS (SCTP Diameter Connections Only)

S T E P #	This procedure will provide instructions on how to prepare clients before configuring SCTP diameter connections. **Important** Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐		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 7.1/7.1.1 should prepare clients before the DSR connections are established after installation. This will ensure the DSR to Client SCTP connection will establish with SCTP AUTH extensions enabled. See RFC 6083. If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices WILL NOT establish after the DSR is installed. https://access.redhat.com/security/cve/CVE-2015-1421 https://access.redhat.com/security/cve/CVE-2014-5077 Execute procedures in [10] to disable/enable the DTLS feature.

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.

It is expected that the maintainer/creator of this file has networking knowledge of this product and the customer site at which it is being installed. This network element XML file is used for DSR deployments using Cisco 4948 switches and HP c-Class blade servers. The following is an example of a Network Element XML file.

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

Figure 5 Example Network Element XML File

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

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

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.

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

```
<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 7 Example Server Hardware Profile XML- Virtual Guest on TVOE

```
<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>
```

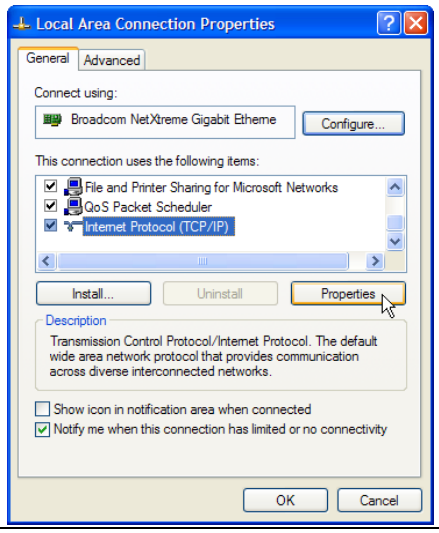
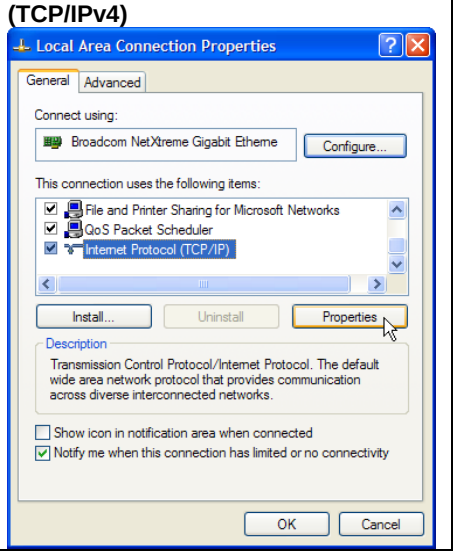
Appendix B: Configuring for TVOE iLO Access

Appendix B 1: Connecting to the TVOE iLO

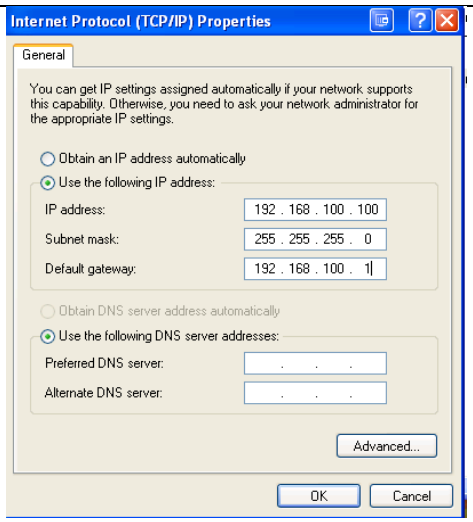
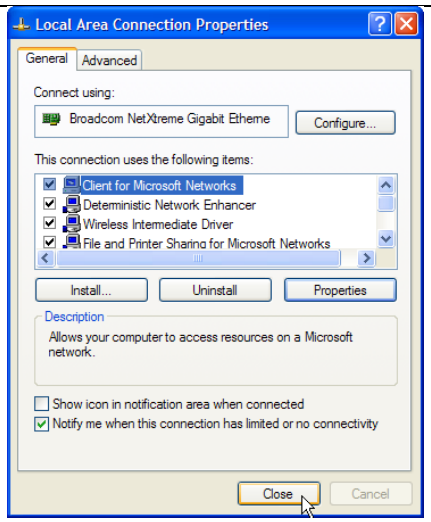
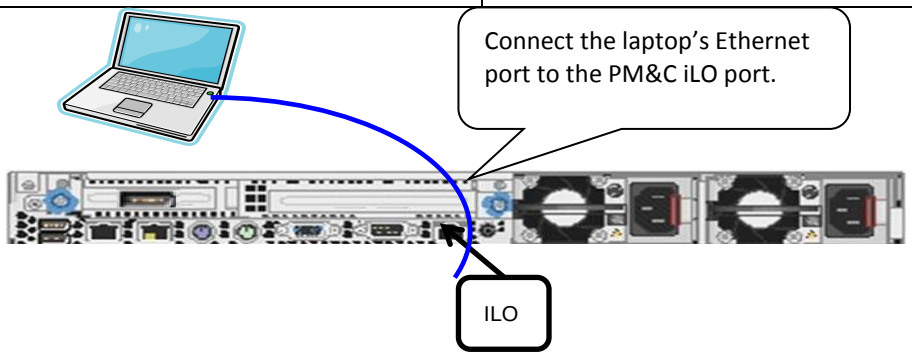
This procedure contains the steps to connect a laptop to the TVOE iLO via a directly cabled Ethernet connection.

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

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

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

Appendix B 1: Connecting to the TVOE iLO

2 ☐	Click **Use the following IP address** Set the **IP address** to 192.168.100.100 Set the **Subnet mask** to 255.255.255.0 Set the **Default gateway** to 192.168.100.1 Select **OK**. Select **Close** from the network interface card's main **Properties** screen.		
3 ☐	Connect the laptop's Ethernet port directly to the TVOE iLO port using a standard Cat-5 cross-over cable.		

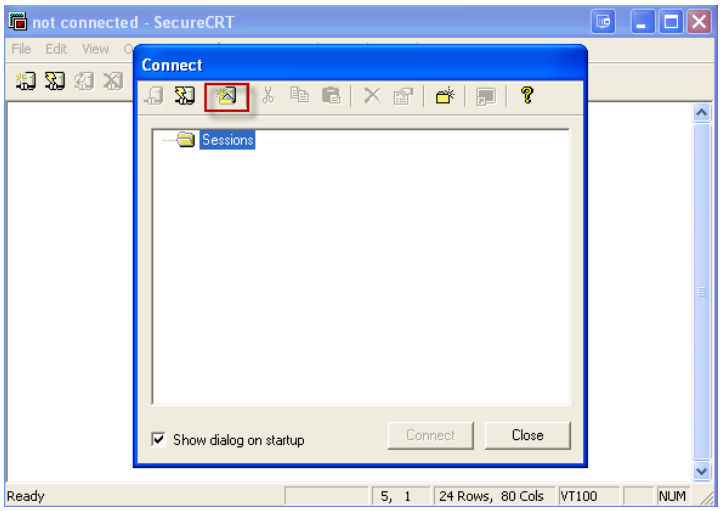
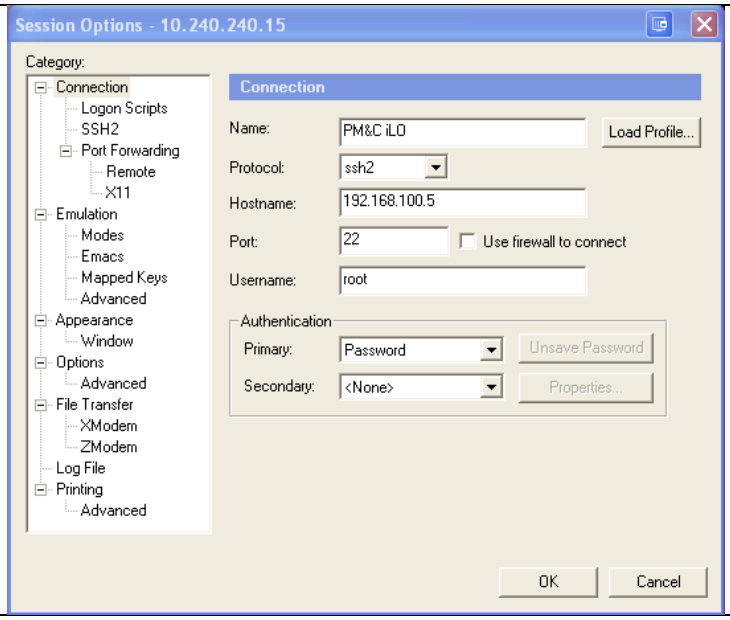
Appendix C: TVOE iLO Access

Appendix C 1: Accessing the TVOE iLO

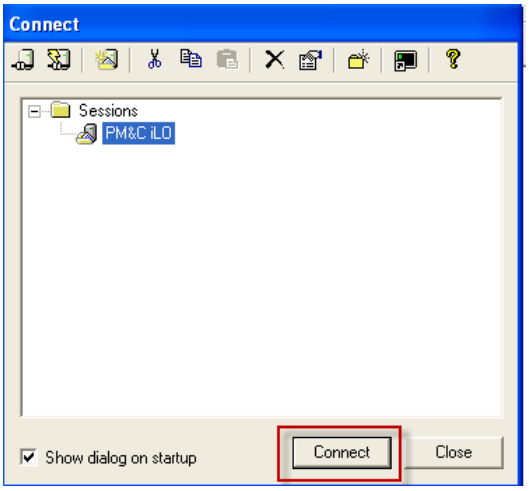
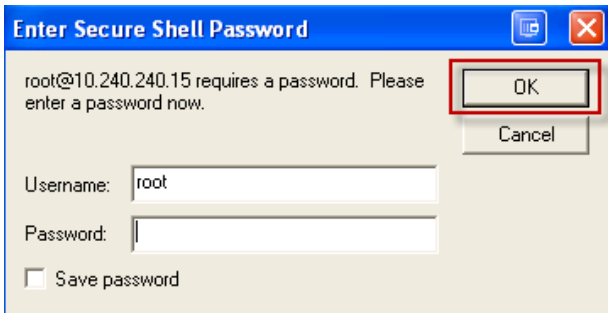
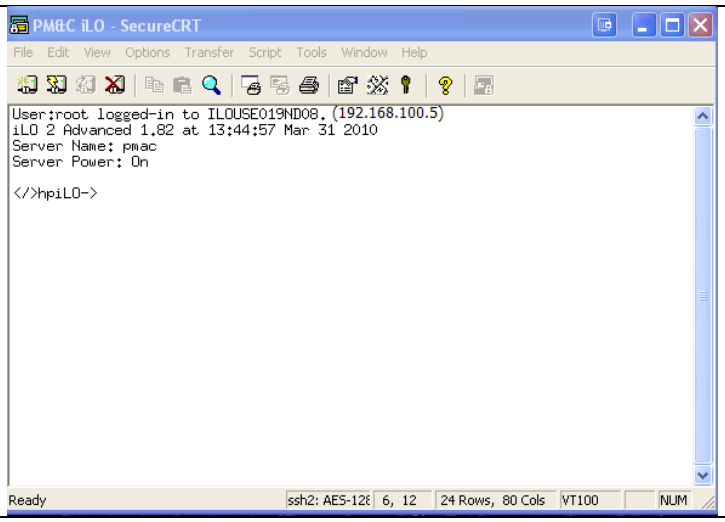
This procedure contains the steps to access the TVOE iLO.

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 O: My Oracle Support** (MOS), and ask for assistance.

STEP #	Procedure	Result
1 ☐	Launch a terminal emulator, e.g. Putty, Secure CRT. Navigate to **File -> Connect** Click on the **New Session** icon. **Note:** This example demonstrates Secure CRT.	
2 ☐	Enter TVOE iLO for **Name** 192.168.100.5(Manufacturing default) or customer IP set during installation for **Hostname.** Enter admusr for **Username.** Click **OK** **Note:** See **Appendix B**: Configuring for TVOE iLO Access to configure your system network to access the TVOE iLO.	

Appendix C 1: Accessing the TVOE iLO

3 ☐	Navigate **File -> Connect** to open the Connect window. Highlight the session you created and click **Connect.**	
4 ☐	**Login** to the TVOE iLO using the appropriate password.	
5 ☐	The TVOE iLO is displayed.	

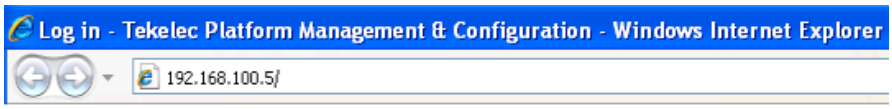
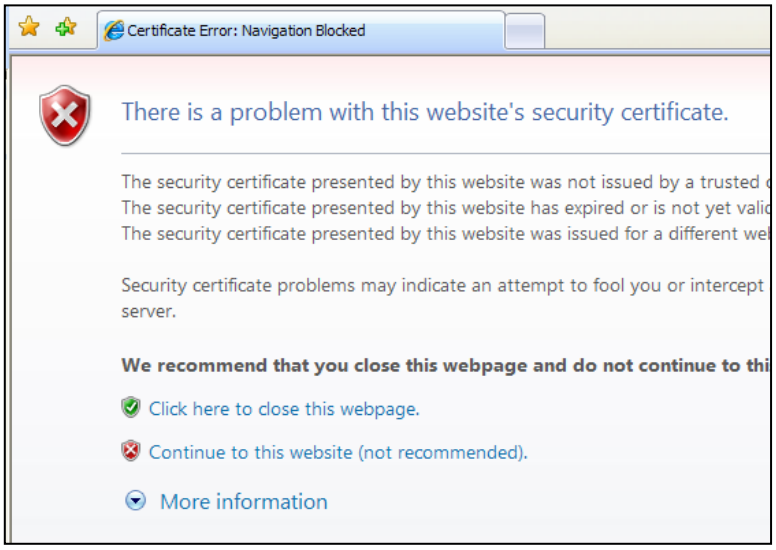
Appendix D: TVOE iLO4 Access

Appendix D 1: TVOE iLO4 GUI Access

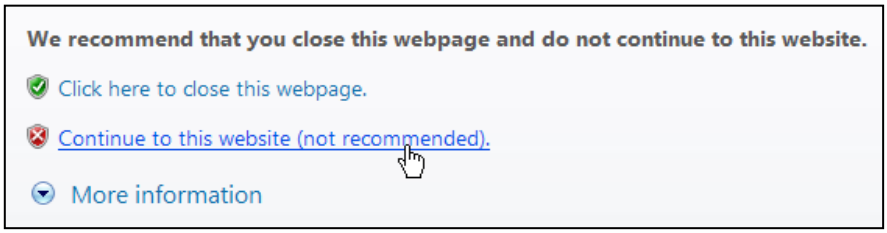
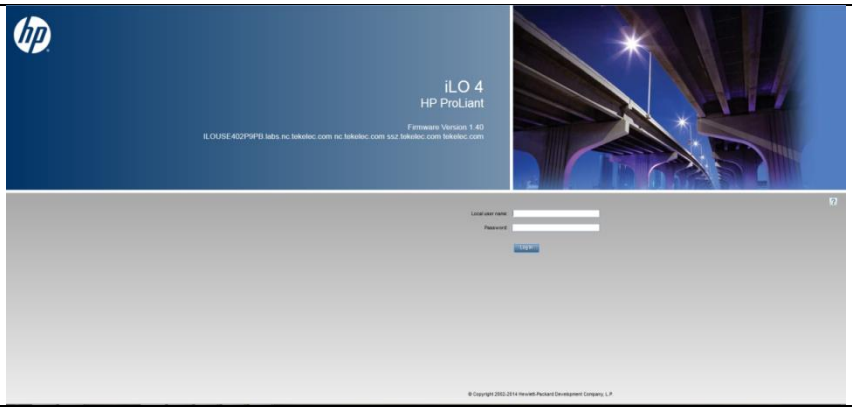
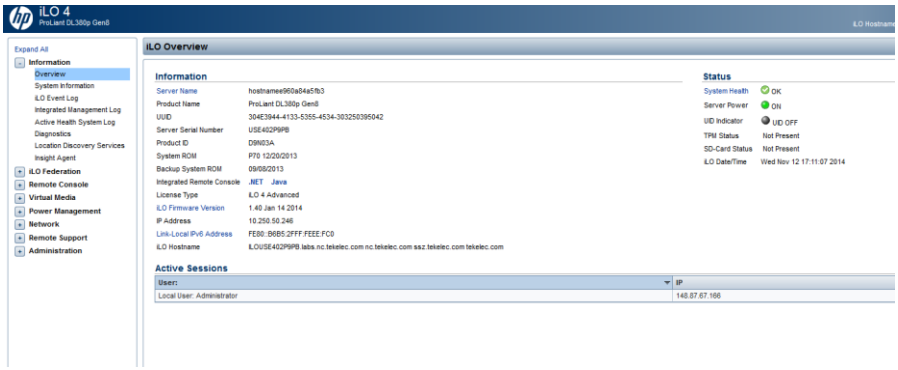
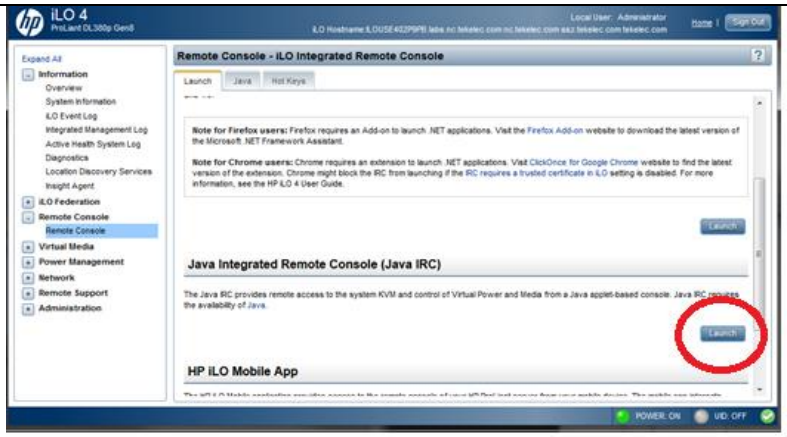
This procedure contains the steps to access the TVOE iLO4 GUI.

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

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

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

Appendix D 1: TVOE iLO4 GUI Access

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

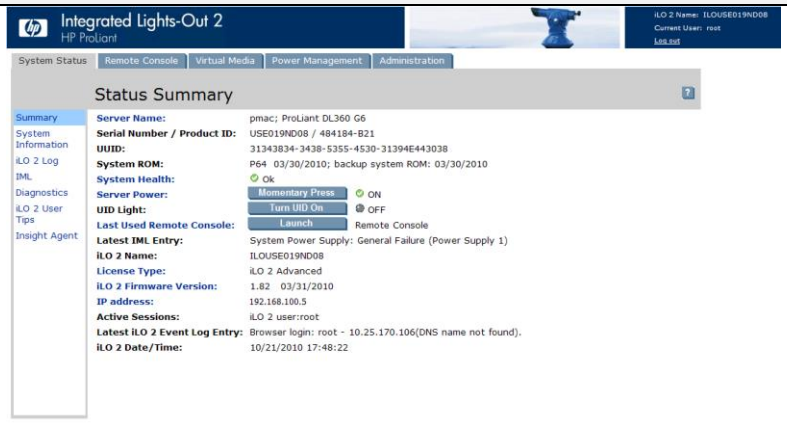
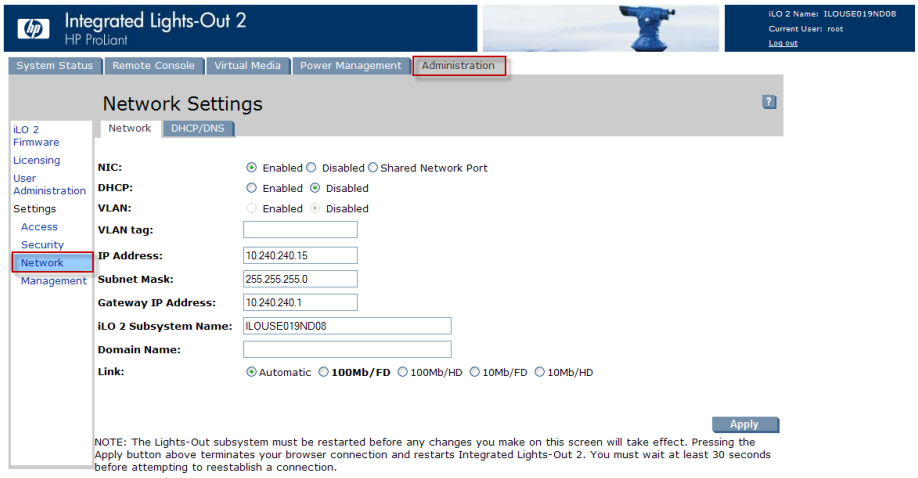
Appendix E: Changing the TVOE iLO Address

Appendix E 1: Changing the TVOE iLO Address

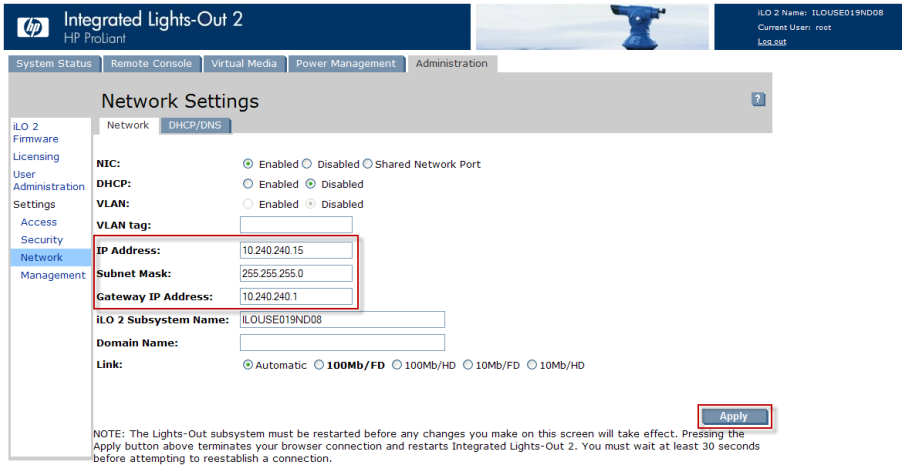
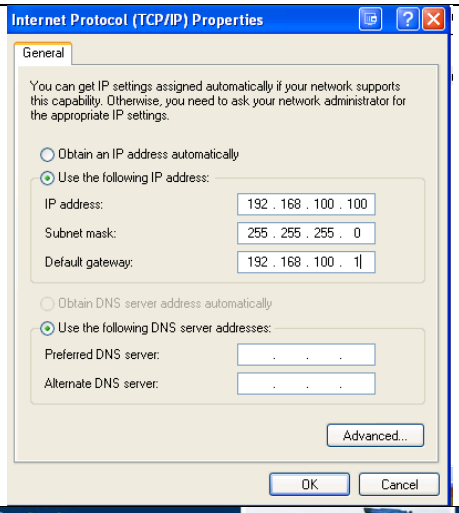
This procedure will set the IP address of the TVOE iLO to the customer's network so that it can be accessed by Oracle support.

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

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

STEP #	Procedure	Result
1 ☐	Connect to the TVOE iLO GUI using the instructions in **Appendix D**: TVOE iLO4 Access	
2 ☐	Click the **Administration** tab. Under **Settings** in the left column click on **Network**.	

Appendix E 1: Changing the TVOE iLO Address

3 ☐	Change the **IP Address, Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey for the TVOE iLO. Select **Apply**. **Note:** You will lose access after you hit the **Apply** button.	
4 ☐	Reset the PC's network connection replacing the ***Subnet Mask*** and ***Gateway*** with those just used for the TVOE iLO. Use an appropriate **IP address** for this subnet.	
5 ☐	Connect to the TVOE iLO GUI using the instructions in **Appendix D**: TVOE iLO4 Access **Note**: Use the IP address entered in **Step 3**	

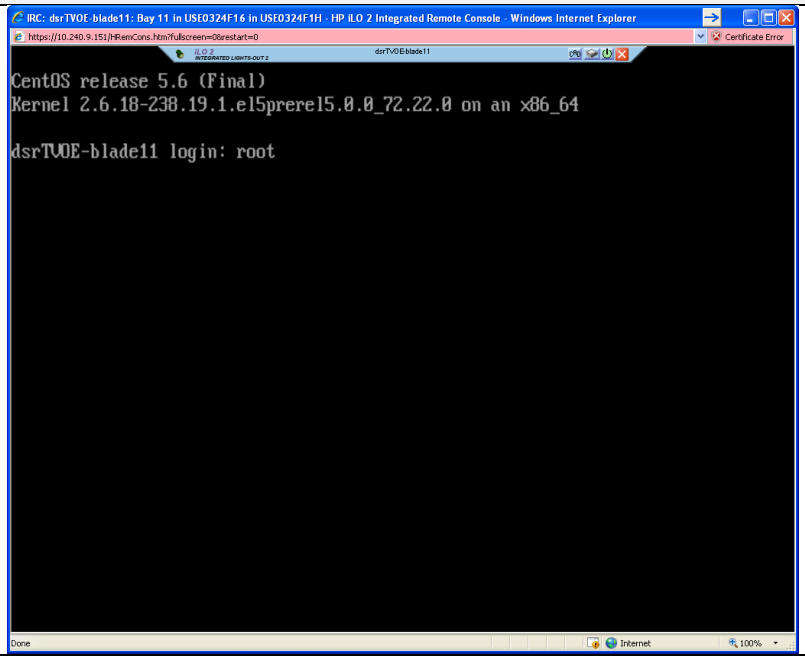
Appendix F: PMAC/NOAM/SOAM Console iLO Access

Appendix F 1: PMAC/NOAM/SOAM Console iLO Access

This procedure describes how to log into the PMAC/NOAM/SOAM console from ILO.

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 O: My Oracle Support** (MOS), and ask for assistance.

STEP #	Procedure	Result
1 ☐	Log in as ***admusr*** on the TVOE server hosting the NOAM using either ILO or SSH to the TVOE server's XMI or Mgmt. address	

Appendix F 1: PMAC/NOAM/SOAM Console iLO Access

2
☐
		On the TVOE host, execute the following command:
		
		`$sudo virsh list`
		
		This will produce a listing of currently running virtual machines.
		
		`[root@dsrTVOE-blade11 ~]# virsh list`
		`Id Name State`
		`----------`
		`4 DSR_NOAMP running`
		
		`[root@dsrTVOE-blade11 ~]# _`
		
		Find the VM name for your DSR NOAM and note its ID number in the first column.
		
		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.

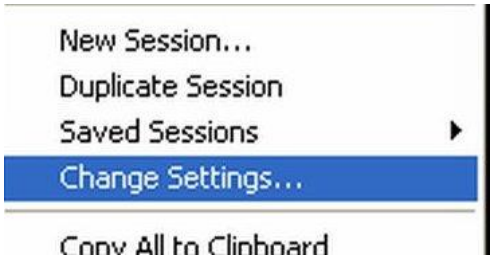
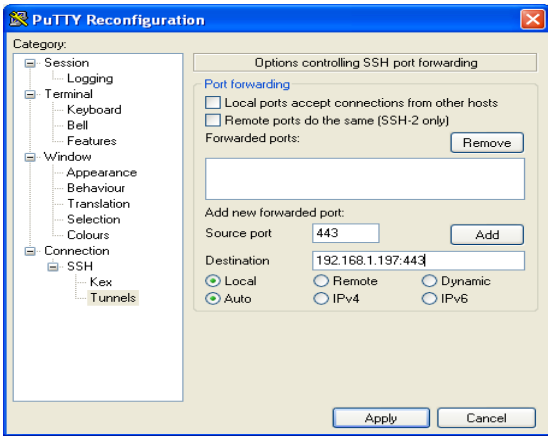
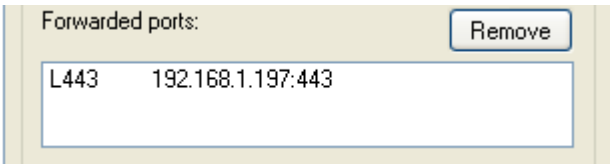
3
☐
	Connect to console of the VM using the VM number obtained in Step 2.	On the TVOE host, execute:.
		
		`$sudo virsh console <DSRNOAM-VMID>`
		
		Where **DSRNOAM-VMID** is the VM ID you obtained in **Step 2**:
		
		`Connected to domain DSR_NOAMP`
		`Escape character is ^]`
		
		`CentOS release 5.6 (Final)`
		`Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.22.0 on an x86_64`
		
		`hostname1322840832 login: _`
		
		You are now connected to the DSR NOAMs console.
		
		If you wish to return to the TVOE host, you can exit the session by pressing **CTRL +]**

Appendix G: Accessing the NOAM GUI using SSH Tunneling with Putty

Appendix G 1: Accessing the NOAM GUI using SSH Tunneling with Putty

STEP #	**Note**: This procedure assumes that the NOAM server you wish to create a tunnel to has been IPM'd with the DSR application ISO **Note**: This procedure assumes that you have exchanged SSH keys between the PMAC and the first NOAM server. **Note:** This procedure assumes that you have obtained the control network IP address for the first NOAM server. You can get this from the PMAC GUI's Software Inventory screen. That variable will be referred to as <NOAM-Control-IP> in these instructions. **Note:** It is recommended that you only use this procedure if you are using Windows XP. There are known issues with putty and Windows 7 that may cause unpredictable results when viewing GUI screens through SSH tunnels. 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	Log in to PMAC Server using PuTTY	Launch the PuTTY application from your station and open a session to the PMAC's management address. Login as ***admusr***

Appendix G 1: Accessing the NOAM GUI using SSH Tunneling with Putty

2 ☐	**Create** SSH Tunnel through the PMAC in PuTTY	 Click the icon in the upper left hand corner of the PuTTY window to bring down the **main menu.** Select **Change Settings** Select **Connections -> SSH -> Tunnels**  Verify that the ***"Local"*** and ***"Auto"*** buttons are selected. Leave other fields blank In **Source Port,** enter **443** In **Destination,** enter **<NOAM-Control-IP>:443** Click **Add**  You should now see a display similar to the following in the text box at the center of this dialog. Click **Apply** Now establish the SSH session to the PMAC, login as **admusr**

Appendix G 1: Accessing the NOAM GUI using SSH Tunneling with Putty

3 ☐	Use Local Web Browser to **Connect** to GUI	Using your web browser, navigate to the following URL: `https://localhost/`  You should arrive at the login screen for the NOAM GUI. **Note:** If using windows 7 and a blank screen is displayed, enable **Compatibility Mode** in IE, or use a different browser (Firefox or Chrome)

Appendix H: Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

Appendix H 1: Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

STEP #		
	Note: This procedure assumes that the NOAMP server you wish to create a tunnel to has been IPM'd with the DSR application ISO **Note:** This procedure assumes that you have exchanged SSH keys between the PMAC and the first NOAMP server. **Note:** This procedure assumes that you have obtained the control network IP address for the first NOAMP server. You can get this from the PMAC GUI's Software Inventory screen. That variable will be referred to as <NOAM-Control-IP> in these instructions. **Note:** This is the recommended tunneling method if you are using Windows 7. 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 O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	If Needed, Download and Install **OpenSSH** for Windows	Download **OpenSSH for Windows** from here. Extract the installer from the ZIP file, then run the installer**.openssh** is now installed on your PC.
2 ☐	**Create** SSH Tunnel Through the PMAC	Open up a Command Prompt shell Within the command shell, enter the following to create the SSH tunnel to the 1st NO, through the PMAC: **> ssh -L 443:<1st_NO_Control_IP_Address>:443 admusr@<PMAC_Management_IP_Address>** (Answer **Yes** if it asks if you want to continue connecting) C:\>ssh -L 443:192.168.1.14:443 root@10.240.9.132 The authenticity of host '10.240.9.132 (10.240.9.132)' can't be established. RSA key fingerprint is e0:f5:2c:bf:70:d9:a6:fd:42:74:83:09:a0:7a:da:0c. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '10.240.9.132' (RSA) to the list of known hosts. root@10.240.9.132's password: Last login: Sat Mar 23 09:28:00 2013 from 10.26.15.162 [root@pmac-90006 ~]# _ The tunnel to the 1st NOAM is now established.

Appendix H 1: Accessing the NOAM GUI using SSH Tunneling with OpenSSH for Windows

3 ☐	Use Local Web Browser to Connect to GUI	Using your web browser, navigate to the following URL: `https://localhost/`  You should arrive at the login screen for the NOAM GUI.

Appendix I: List of Frequently used Time Zones

Table 4 Time Zones

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

Appendix J: Application NetBackup Client Installation Procedures

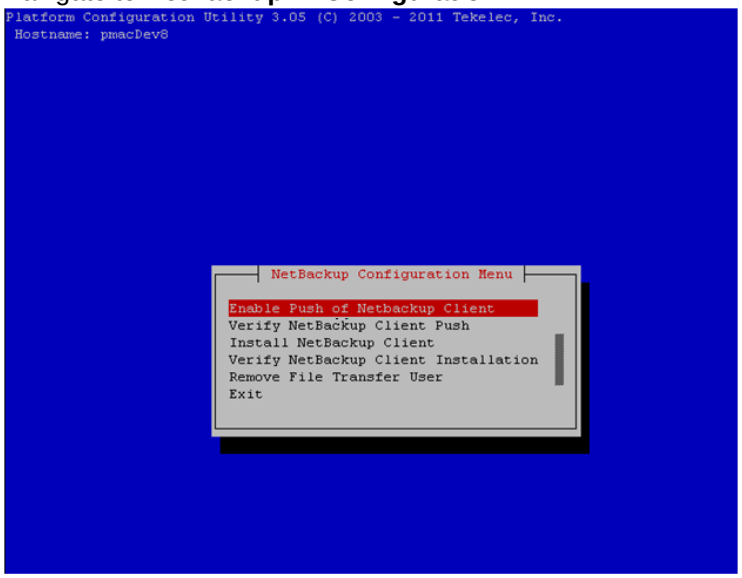
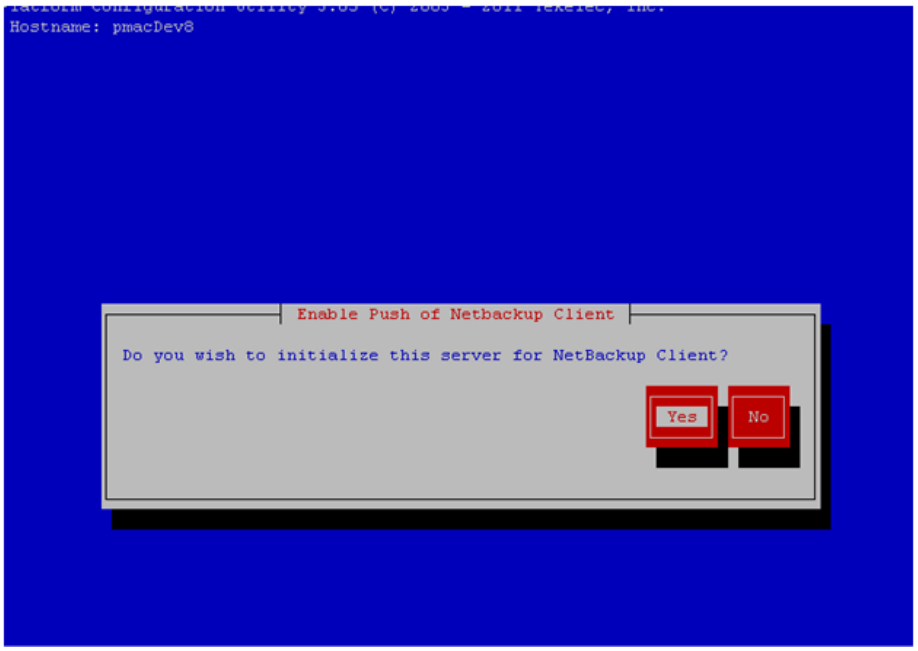
NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. The following procedures provides instructions for installing and configuring the NetBackup client software on an application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

NETBACKUP CLIENT INSTALL USING PLATCFG

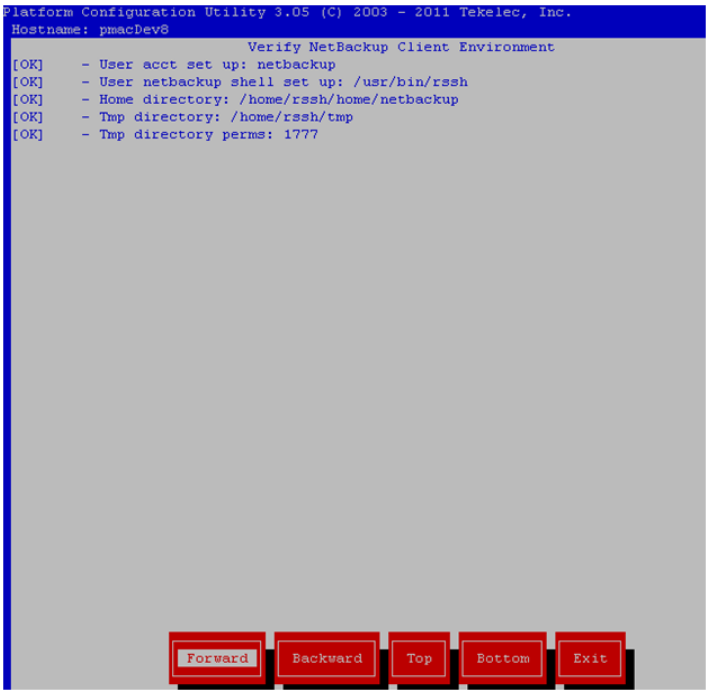
Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

STEP #	This procedure explains the Netbackup installation using platcfg **Prerequisites:** • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. • Execute Appendix A.3 of [7] **Note:** Execute the following procedure to switch/migrate to having netBackup installed via platcfg instead of using NBAutoInstall *(Push Configuration)* Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Application server iLO:** Login	Login and launch the integrated remote console SSH to the application Server (PMAC or NOAM) as ***admusr*** using the management network for the PMAC or XMI network for the NOAM.

Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

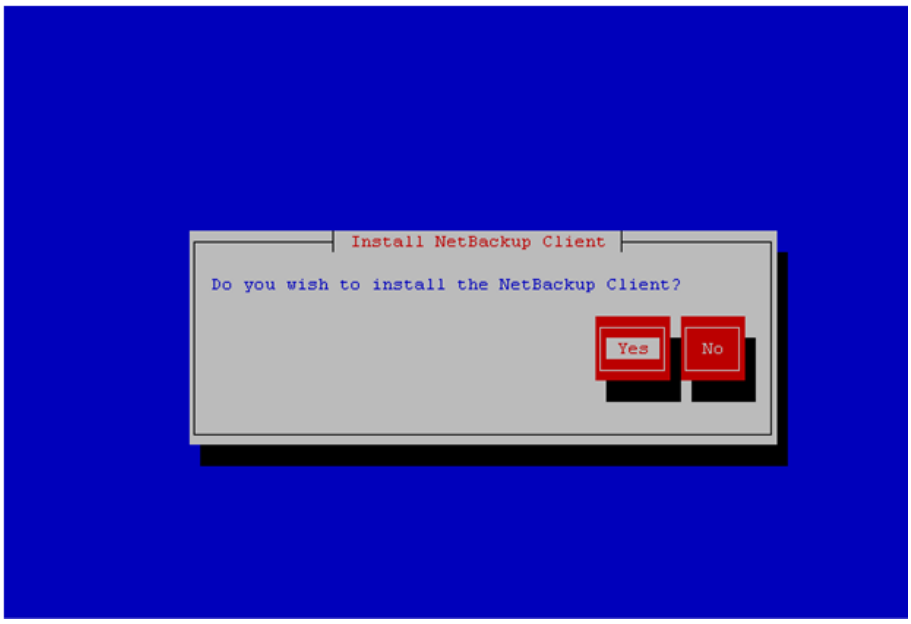
2 ☐	**Application server iLO:** Navigate to NetBackup Configuration	Configure NetBackup Client on application server `$ sudo su - platcfg` Navigate to **NetBackup -> Configuration** 
3 ☐	**Application server iLO:** Enable Push of NetBackup Client	Navigate to **NetBackup Configuration -> Enable Push of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

Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

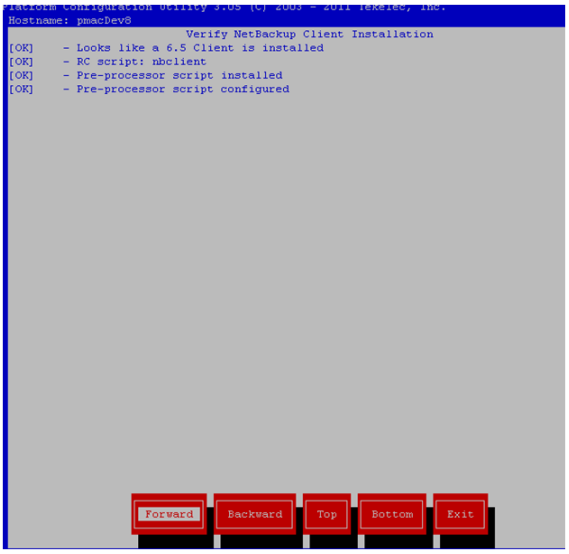
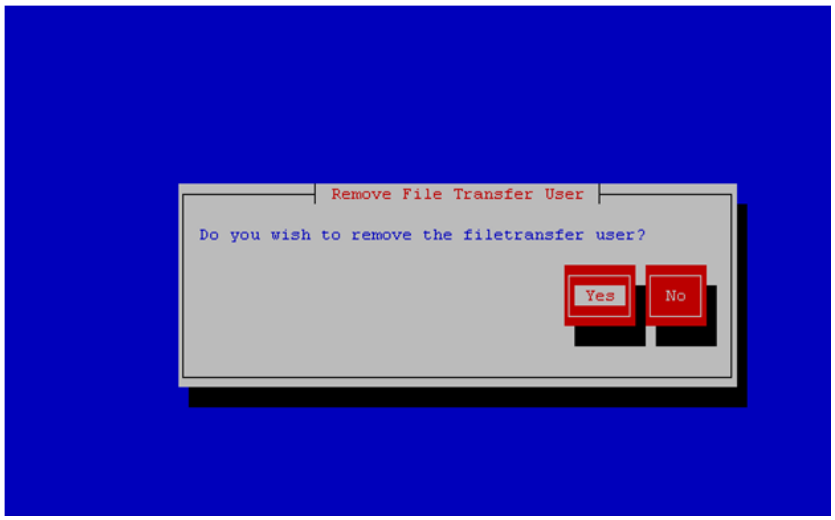
4 ☐	**Application server iLO:** Verify NetBackup Client software push is enabled.	Navigate to **NetBackup Configuration -> Verify NetBackup Client Push**  Verify list entries indicate **OK** for NetBackup client software environment. Select **Exit** to return to NetBackup Configuration menu.

5 ☐	**NetBackup server:** Push appropriate NetBackup Client software to application server	**Note:** The NetBackup server is not an application asset. Access to the NetBackup server and location path of the NetBackup Client software is under the control of the customer. Below are the steps that are required on the NetBackup server to push the NetBackup Client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment. **Note:** The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider that is being used at this site. **Login** to the NetBackup server using password provided by customer: Navigate to the appropriate NetBackup Client software path: **Note:** The input below is only used as an example. (7.5 in the path below refer to the NetBackup version. If installed a different version (e.g. 7.1 or 7.6), replace 7.5 with 7.1 or 7.6) **$ cd /usr/openv/netbackup/client/Linux/7.5** **Execute** the sftp_to client NetBackup utility using the application IP address and application netbackup user: **$ ./sftp_to_client <application IP> netbackup** Connecting to 192.168.176.31 netbackup@192.168.176.31's password: **Enter application server netbackup user password; the following NetBackup software output is expected, observe the sftp completed successfully:** File "/usr/openv/netbackup/client/Linux/6.5/.sizes" not found. Couldn't rename file "/tmp/bp.6211/sizes" to "/tmp/bp.6211/.sizes": No such file or directory File "/usr/openv/NB-Java.tar.Z" not found. ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected ./sftp_to_client: line 793: [: : integer expression expected sftp completed successfully. The user on 192.168.176.31 must now execute the following command: *$ sh /tmp/bp.6211/client_config [-L].* **Note:** Although the command executed above instructs you to execute the client_config command, **DO NOT** execute that command, as it shall be executed by platcfg in the next step. **Note:** The optional argument, **"-L",** is used to avoid modification of the client's current bp.conf file

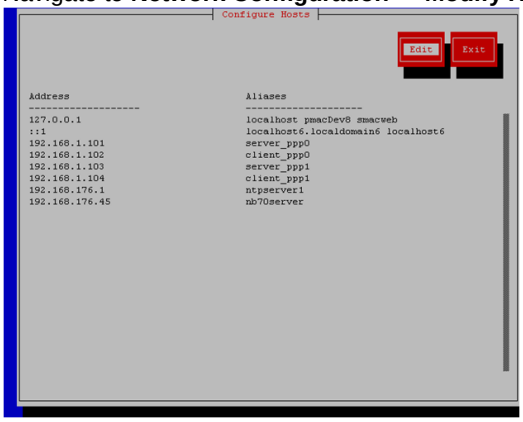
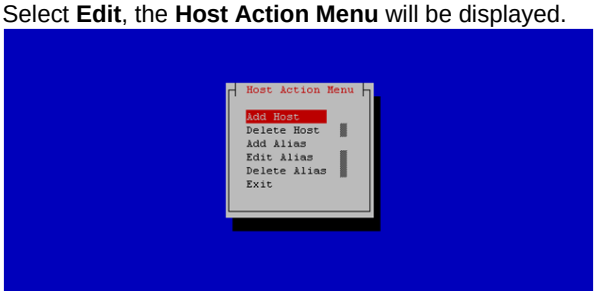
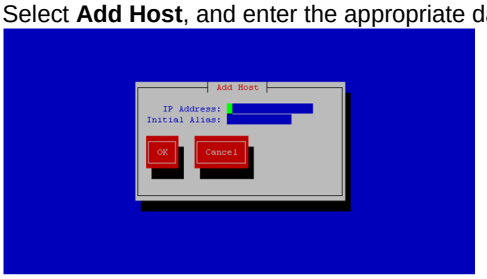
Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

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

Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

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

Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

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

Appendix J 1: Application NetBackup Client Installation (Using Platcfg)

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

NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

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

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

Appendix J 2: Application NetBackup Client Installation (NBAUTOINSTALL)

S T E P #	This procedure explains the Netbackup installation with NBAUTOINSTALL **Prerequisites:** • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. **Note:** If the customer does not have a way to push and install Netbackup Client, then use Netbackup Client Install/Upgrade with platcfg. **Note:** It is required that this procedure is executed before the customer does the Netbackup Client install. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Application server iLO:** Login	Login and launch the integrated remote console. SSH to the application Server (PMAC or NOAM) as ***admusr*** using the management network for the PMAC or XMI network for the NOAM.

Appendix J 2: Application NetBackup Client Installation (NBAUTOINSTALL)

2 ☐	**Application server iLO:** Enable nbAutoInstall	Execute the following command: **$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable**
3 ☐	**Application server iLO:** Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.	Execute the following commands **$ sudo mkdir -p /usr/openv/netbackup/bin/** **$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify** **$ sudo ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify** Note: An example of <path> is "/usr/TKLC/plat/sbin"
4 ☐	**Application server iLO:** Verify NetBackup configuration file	Open **/usr/openv/netbackup/bp.conf** and make sure it points to the NetBackup Server using the following command: **$ sudo vi /usr/openv/netbackup/bp.conf** SERVER = nb75server CLIENT_NAME = 10.240.10.185 CONNECT_OPTIONS = localhost 1 0 2 **Note:** Verify that the above server name matches the NetBackup Server, and verify that the CLIENT_NAME matches the hostname or IP of the local client machine, if they do not, update them as necessary. Edit **/etc/hosts** using the following command and add the NetBackup server: **$ sudo vi /etc/hosts** e.g.: 192.168.176.45 nb75server **Note:** The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly. At any time, the customer may now push and install a new version of Netbackup Client.

CREATE NETBACKUP CLIENT CONFIG FILE

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

Appendix J 3: Create NetBackup Client Config File

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

Appendix J 3: Create NetBackup Client Config File

2
☐
	Application server iLO: Create NetBackup Config script	Create the NetBackup Client config script file on the server using the contents that were previously determined. The config script file should be placed in the */usr/TKLC/plat/etc/netbackup/scripts* directory. The name of the NetBackup Client config script file should be determined from the contents of the NetBackup Client config file.
		
		As an example for the NetBackup 7.5 client the following is applicable:
		
		<u>NetBackup Client config:</u>
		/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf
		
		<u>NetBackup Client config script:</u>
		/usr/TKLC/plat/etc/netbackup/scripts/NB75
		
		Note: Change the client config and script permission by executing the following command:
		
		Illustrative purposes only:
		
		`$ sudo chmod 555 /usr/TKLC/plat/etc/netbackup/profiles/NB75.conf`
		
		`$ sudo chmod 55 /usr/TKLC/plat/etc/netbackup/scripts/NB75`

OPEN PORTS FOR NETBACKUP CLIENT SOFTWARE

This procedure will use iptables and ip6tables (if applicable) to open the applicable ports for the NetBackup client to communicate to the NetBackup Server.

Appendix J 4: Open ports for NetBackup Client Software

STEP #	This procedure will use iptables and ip6tables (if applicable) to open the applicable ports for the NetBackup client to communicate to the NetBackup Server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Active NOAM Server:** Login	Establish an SSH session to the active NOAM server. Login as ***admusr.***

2
☐
	Active NOAM Server: Open Ports for NetBackup Client Software	Change directories to */usr/TKLC/plat/etc/iptables*
		
		`$ cd /usr/TKLC/plat/etc/iptables`
		
		Using "vi", create a file named *60netbackup.ipt*
		
		`$ sudo vi 60netbackup.ipt`
		
		Insert the following contents into the file:
		
		`# 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`
		
		Now save and close the file using '**:wq**'
		
		Note: If system servers are to use IPv6 networks for NetBackup client-to-server communication, then repeat this procedure to create a file named 60netbackup.ip6t, with the same contents as shown above, in the directory /usr/TKLC/plat/etc/ip6tables.

3 ☐	**Standby NOAM:** Open Ports for NetBackup Client Software	Repeat **Steps 1-2** for the standby NOAM to open ports for NetBackup client software.

Appendix J 4: Open ports for NetBackup Client Software

4 ☐	**Active SOAM:** Open Ports for NetBackup Client Software	Repeat **Steps 1-2** for the active SOAM to open ports for NetBackup client software.
☐	**Standby SOAM:** Open Ports for NetBackup Client Software	Repeat **Steps 1-2** for the standby SOAM to open ports for NetBackup client software.

Appendix K: 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.
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

TVOE Blade

The TVOE Blade section should be commented out if you intend to install a Rack Mount Server. Be sure to fill out the sections properly. Enclosure ID, OA IP addresses and the Bay must be correct or the PMAC will not be able to 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 will not be able to discover the Rack Mount Server, server discovery must occur before the installation can begin.

TYPE

If your IDIH system is to be collocated with a PMAC on the same TVOE host make sure "Type=Management" is not commented out. It will setup a management network instead of an xmi network and it will remove the software stanza inside of the TVOE server stanza. If you are setting up a standalone IDIH then comment out "Type=Management" which will setup an xmi bridge.

TVOE CONFIGURATION

This section defines the hostname, network ip addresses for the TVOE bridges and it defines the network devices. You can define the devices you intend to use for bonded interfaces and the tagged bonded interfaces you intend to associate with a bridge.

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="oracle-7.1.0.0.0_71.14.0-x86_64"
MedIso="mediation-7.1.0.0.0_71.14.0-x86_64"
AppIso="apps-7.1.0.0.0_71.14.0-x86_64"

# Tvoe Blade OA IP and Bay uncomment if this server is blade #EncId="1401"
#Oa1="10.250.51.197"
#Oa2="10.250.51.198"
#Bay="15F"
#Hw="ProLiantBL460cGen8"
#Hw="ProLiantBL460cGen6"

# Tvoe RMS Out of Band Management IP and Hw # Comment these lines if server is blade OobIp="10.250.34.24"
Hw="ProLiantDL380pGen8"
#Hw="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"
```

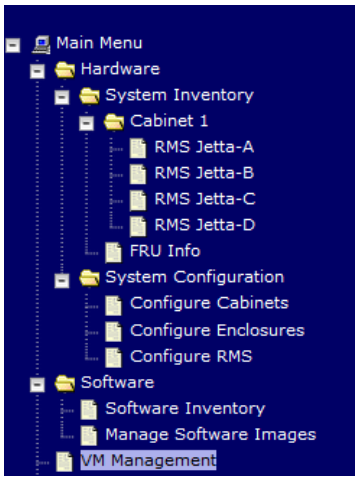
Appendix L: IDIH External Drive Removal

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

Appendix L 1: IDIH External Drive Removal

S T E P #	This procedure will destroy all of the data in the Oracle Database. Warning: Do ot perform this procedure on an IDIH system unless you intent to do a fresh TVOE installation. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `https://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

Appendix L 1: IDIH External Drive Removal

2 ☐	**PMAC GUI:** Delete VMs if Needed	Before a re-installation can be performed, the IDIH VMs must be removed first. Navigate to **Main Menu -> VM Management**  Select each of the IDIH VMs and select the **Delete** button. 
3 ☐	**IDIH TVOE HOST:** Login	Establish an SSH session to the TVOE host, login as ***admusr***

4
☐
	IDIH TVOE HOST: Verify External Drive Exists for **HP BL460 Blade**	Execute the following command to verify the external drive exists for **HP BL460 Blade:**
		
		`$ sudo hpssacli ctrl slot=3 ld all show`
		
		The following information should be displayed:
		
		`Smart Array P410i in Slot 3`
		`array A`
		`logicaldrive 1 (3.3 TB, RAID 1+0, OK)`

Appendix L 1: IDIH External Drive Removal

5
☐
	IDIH TVOE HOST: Verify External Drive Exists for **HP DL380 Gen8 RMS**	Execute the following command to verify the external drive exists for **HP DL380 Gen8 RMS:**
		
		`$ sudo hpssacli ctrl slot=2 ld all show`
		
		The following information should be displayed:
		
		`Smart Array P420 in Slot 2`
		
		`array A`
		
		`logicaldrive 1 (1.1 TB, RAID 1+0, OK)`

6
☐
	IDIH TVOE HOST: Verify External Drive Exists for **Netra X3**	Execute the following command to verify the external drive exists for **Netra X3:**
		
		`$ sudo storcli -ldinfo -l1 -a0 | head`
		
		The following information should be displayed:
		
		`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`

7
☐
	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:**
		
		`$ sudo hpssacli ctrl slot=0 ld all show`
		
		The following information should be displayed:
		
		`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)`

Appendix L 1: IDIH External Drive Removal

8
☐
	IDIH TVOE HOST: Remove the External Drive and Volume Group for **HP BL460 Blade**	Execute the following command to remote the external drive and volume group for **HP BL460 Blade:**
		
		`$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=3`
		
		The following information should be displayed:
		
		`Called with options: hpdisk --slot=3`
		`WARNING: This will destroy all application data on the server!`
		`Continue? [Y/N]`

9
☐
	IDIH TVOE HOST: Remove the External Drive and Volume Group for **HP DL380 Gen8 RMS**	Execute the following command to remote the external drive and volume group for **HP DL380 Gen8 RMS:**
		
		`$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2`
		
		The following information should be displayed:
		
		`Called with options: hpdisk --slot=2`
		`WARNING: This will destroy all application data on the server!`
		`Continue? [Y/N]`

10
☐
	IDIH TVOE HOST: Remove the External Drive and Volume Group for **Netra X3 with one external disk**	Execute the following command to remote the external drive and volume group for **Netra X3 with one external disk:**
		
		`$ 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`
		
		`$ 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`

Appendix L 1: IDIH External Drive Removal

11
☐
	IDIH TVOE HOST:
	Remove the External Drive and Volume Group for **Netra X3 with three external disks**
		Execute the following command to remote the external drive and volume group for **Netra X3 with three external disks:**
		`$ 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`
		
		`$ 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 -cfglddel –l3 -a0`
		`[root@hellcat ~]# sudo storcli -cfglddel –l2 -a0`
		`[root@hellcat ~]# sudo storcli -cfglddel -l1 -a0`

12
☐
	IDIH TVOE HOST:
	Remove the External Drive and Volume Group for **HP DL380 Gen9 RMS**
		Execute the following command to remote the external drive and volume group for **HP DL380 Gen9 RMS:**
		`$ 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`

Appendix M: DSR Fast Deployment Configuration

The following table contains the variables that the NOAM DSR fast deployment will prompt 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]	_____
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 PM&C 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 PM&C 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.	_____
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 PM&C 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	_____
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 N: 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 T.1 will explain how to add individual VMs and add various DSR/SDS servers. Appendix T.2 will explain how to delete individual VMs and move or remove various DSR/SDS servers.

Appendix N.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	Appendix N.1.1
Perform system health check	Appendix N.1.2
Identify Servers which will be affected by the Growth: • DR-NOAM • SOAM Spares • MP (SBR, SS7MP, IPFE)	
Add new servers Create and Configure the VMs on new servers (SOAM spare and DR-NOAMs Only)	Appendix N.1.3
Configure Servers in new VM locations	NOAM/DR-NOAM: Appendix N.1.4 SOAM: Appendix N.1.5 MP: Appendix N.1.6
Post Growth Health Check	Appendix N.1.7
Post Growth Backups	Appendix N.1.8

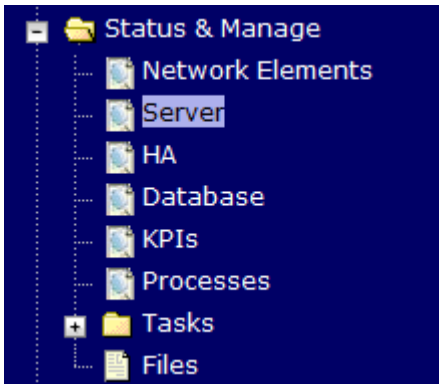
Appendix N.1.1 Perform Backups

S T E P #	This procedure will reference steps to backup all necessary items before a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Backup TVOE**	Backup all TVOE host configurations by executing **Procedure 39**
2 ☐	**Backup PMAC**	Backup the PMAC application by executing **Procedure 40**
3 ☐	**Backup NOAM/SOAM databases**	Backup the NOAM and SOAM Databases by executing **Procedure 41** and **Procedure 42**

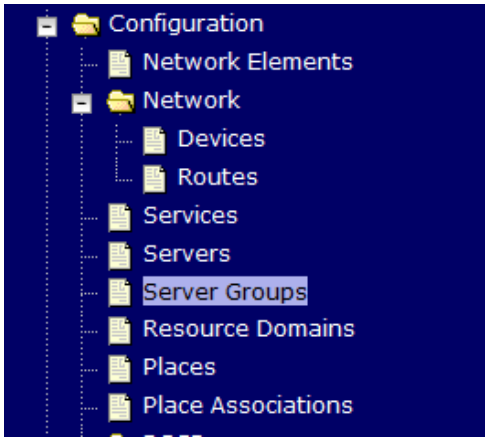
Appendix N.1.2 Perform Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Appendix N.1.2 Perform Health Check

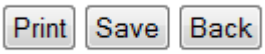
<table>
<tr>
<td>2
☐</td>
<td>NOAM VIP GUI:
Verify Server Status</td>
<td>Navigate to Main Menu -> Status & Manage -> Server
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>

Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms</td>
</tr>
<tr>
<td>3
☐</td>
<td>NOAM VIP GUI:
Verify Server Configuration</td>
<td>Navigate to Main Menu -> Configuration -> Server Groups
 

Verify the configuration data is correct for your network.</td>
</tr>
</table>

Appendix N.1.2 Perform Health Check

4 ☐	**NOAM VIP GUI:** Log Current Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Click on the **Report** button  **Save** or **Print** this report, keep copies for future reference. 
5 ☐	**SOAM VIP GUI:** Repeat For SOAM	Repeat **Steps 1-4** for the SOAM

Appendix N.1.3 Adding a new Server/VMs

S T E P #	This procedure will provide steps to add a new rack mount server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance..	
1 ☐	**Add/Configure Additional Servers**	Follow the sections below to install and configure additional servers: <u>DR-NOAMs:</u> **Section 4.2.1** Execute DSR Fast Deployment for DR-NOAMs <u>Spare SOAMs:</u> **Procedure 11** <u>MPs:</u> Insert blade in desired location
2 ☐	**Add/Configure New VMs**	1. Create new virtual Machines for the Spare SOAMs by following **Procedure 12** 2. Install TPD and DSR Software by following **Procedure 13**

Appendix N.1.4 Growth: DR-NOAM

STEP #	This procedure will reference steps to configure a DR-NOAM on the new virtual machine for VM Growth scenarios. **Prerequisites:** • NEW Virtual Machine Created • TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance..	
1 ☐	**NOAM VIP GUI:** Configure the DR-NOAM	Configure the DR-NOAM by executing the steps referenced in the following procedures: DSR DR-NOAM: **Section 4.2.2** Configure DR-NOAMs**(Section 4.2.3** Install NetBackup Client (Optional)
2 ☐	**DR-NOAM:** Activate Optional Features (DSR Only)	If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to **Section 3.2** Optional Features

3
☐
	NOAM VIP:
	Execute the key revocation Script on the Active NOAM (RADIUS Only)
		If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)
		
		Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new NOAM server created:
		
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_NOAM_hostname>`
		
		Note: Key transfer successful output should be given.

Appendix N.1.5 Growth: SOAM spare (PCA Only)

STEP #	This procedure will reference steps to configure an SOAM spare on the new virtual machine for VM growth scenarios. **Prerequisites:** • NEW Virtual Machine Created • TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Configure the SOAM spare	Configure the SOAM spare by executing the steps referenced in the following procedures: <u>DSR SOAM spare:</u> • Procedure 15 • Procedure 16 • Procedure 17 (Steps 1,4,6, and 9)
2 ☐	**NOAM GUI:** Activate Optional Features	If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to **Section 3.2** Optional Features.

3
☐
	NOAM VIP:
	Execute the key revocation Script on the Active NOAM (RADIUS)
		If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)
		
		Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new SOAM server created:
		
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_SOAM_hostname>`
		
		Note: Key transfer successful output should be given.

Appendix N.1.6 Growth: MP

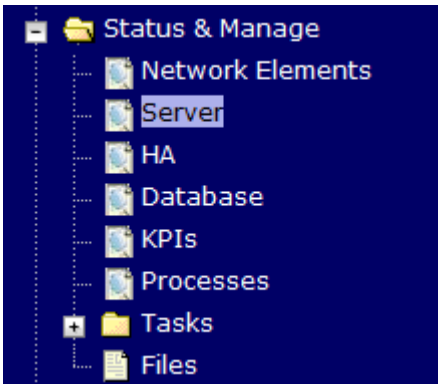
STEP #	This procedure will reference steps to configure an MP on the new virtual machine for growth scenarios. **Prerequisites:** • NEW Virtual Machine Created • TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Configure the MP	Configure the MP/DP by executing the steps referenced in the following procedures: DSR MP: Procedure 19 *(Steps 1-2, 7-14, 15-17(Optional))*

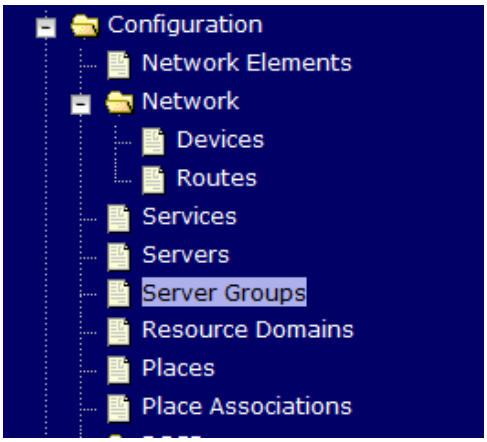
2
☐
	NOAM VIP:
	Execute the key revocation Script on the Active NOAM (RADIUS)
		If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)
		
		Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new MP server created:
		
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_MP_hostname>`
		
		Note: Key transfer successful output should be given.

Appendix N.1.7 Post Growth Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms after Growth. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

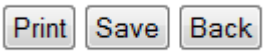
Appendix N.1.7 Post Growth Health Check

<table>
<tr><td>2
☐</td><td>NOAM VIP GUI:
Verify Server Status</td><td>Navigate to Main Menu -> Status & Manage -> Server
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table></td></tr>
<tr><td>3
☐</td><td>NOAM VIP GUI:
Verify Server Configuration</td><td>Navigate to Main Menu -> Configuration -> Server Groups
 

Verify the configuration data is correct for your network.</td></tr>
</table>

Appendix N.1.7 Post Growth Health Check

4 ☐	**NOAM VIP GUI:** Log Current Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Click on the **Report** button  **Save** or **Print** this report, keep copies for future reference.  Compare this alarm report with those gathered in procedure **Appendix N.1.2**
5 ☐	**SOAM VIP GUI:** Repeat	Repeat **Steps 1-3** for the SOAM

Appendix N.1.8 Post Growth Backups

STEP #	This procedure will reference steps to backup all necessary items after a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Backup TVOE**	Backup all TVOE host configurations by executing **Procedure 39**
2 ☐	**Backup PMAC**	Backup the PMAC application by executing **Procedure 40**
3 ☐	**Backup NOAM/SOAM databases**	Backup the NOAM and SOAM Databases by executing **Procedure 41** and **Procedure 42**

Appendix N.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	Appendix N.2.1
Perform system health check	Appendix N.2.2
Identify Servers which will be affected by the De-growth: • DSR MP (SBR, SS7MP, IPFE)	
Remove identified servers from Server Group	Appendix N.2.3
Shutdown and remove the identified server's VM.	Appendix N.2.4
Post De-Growth Health Check	Appendix N.2.5
Post De-Growth Backups	Appendix N.2.6

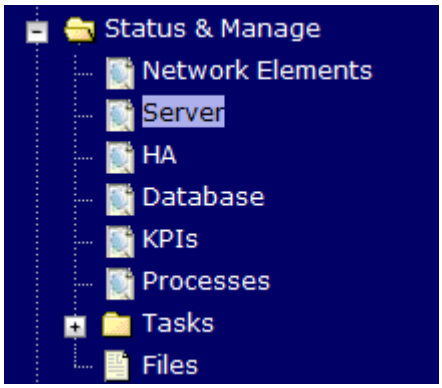
Appendix N.2.1 Perform Backups

STEP #	This procedure will reference steps to backup all necessary items before a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Backup TVOE**	Backup all TVOE host configurations by executing **Procedure 39**
2 ☐	**Backup PMAC**	Backup the PMAC application by executing **Procedure 40**
3 ☐	**Backup NOAM/SOAM databases**	Backup the NOAM and SOAM Databases by executing **Procedure 41** and **Procedure 42**

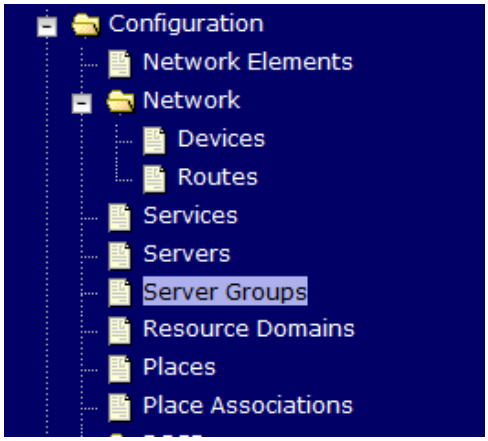
Appendix N.2.2 Perform Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Appendix N.2.2 Perform Health Check

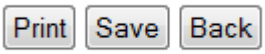
<table>
<tr>
<td>2
☐</td>
<td>NOAM VIP GUI:
Verify Server Status</td>
<td>Navigate to Main Menu -> Status & Manage -> Server
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>

Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms</td>
</tr>
<tr>
<td>3
☐</td>
<td>NOAM VIP GUI:
Verify Server Configuration</td>
<td>Navigate to Main Menu -> Configuration -> Server Groups
 

Verify the configuration data is correct for your network.</td>
</tr>
</table>

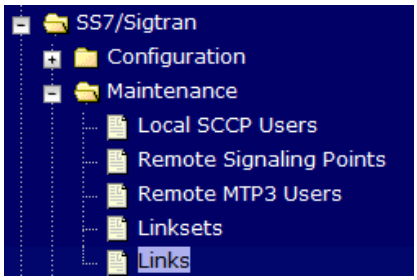
Appendix N.2.2 Perform Health Check

4 ☐	**NOAM VIP GUI:** Log Current Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Click on the **Report** button  **Save** or **Print** this report, keep copies for future reference. 
5 ☐	**SOAM VIP GUI:** Repeat For SOAM	Repeat **Steps 1-4** for the SOAM

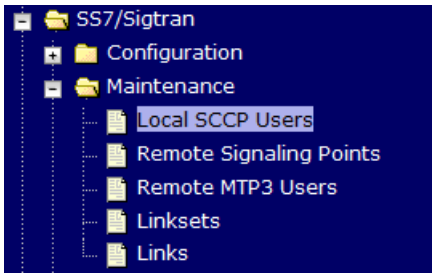
Appendix N.2.3 Removing Server from Server Group

STEP #	Once the server's that will be deleted have been identified, the server will first need to be removed from its server group. The following procedure will provide steps to remove a server from a server group. **Warning:** It is recommended that no more than one server from each server group be removed from a server group at a time. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**SOAM VIP GUI:** Login	**Execute this step if Removing SS7MP, otherwise skip to step 11** Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

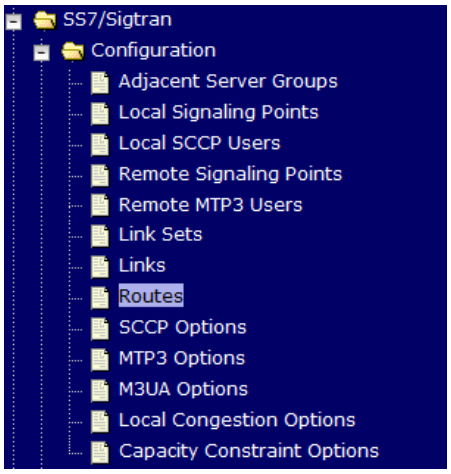
Appendix N.2.3 Removing Server from Server Group

2 ☐	**SOAM VIP GUI:** Disable SS7-MP Links	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Maintenance -> Links**  **Disable** the associated links of the identified SS7-MP: 

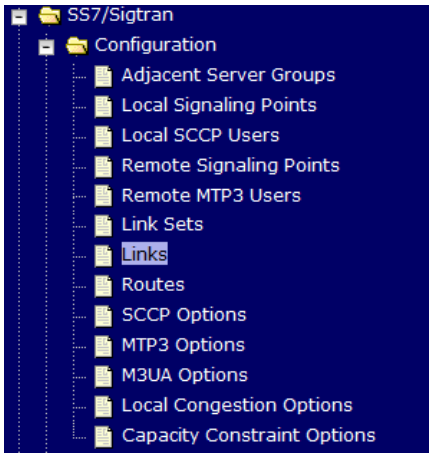
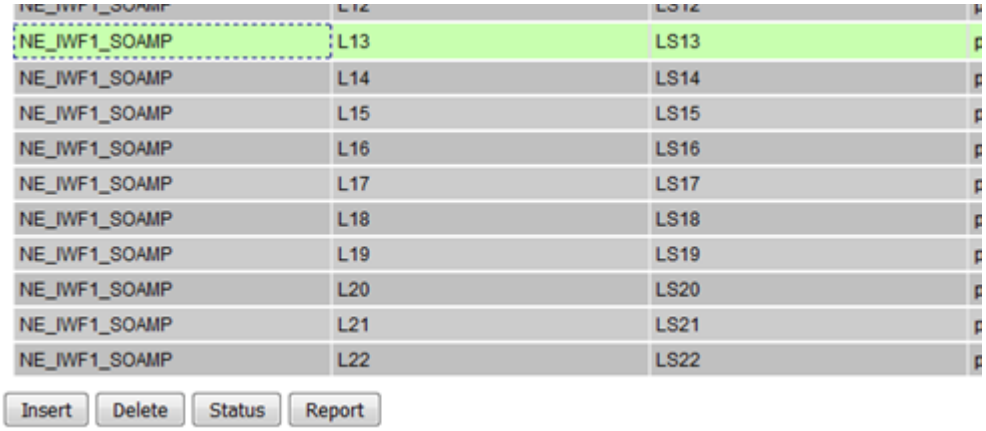
Appendix N.2.3 Removing Server from Server Group

3 ☐	**SOAM VIP GUI:** Disable SS7-MP SCCP Users	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Maintenance -> Local SCCP Users**  **Disable** the associated local SCCP users of the identified SS7-MP: 

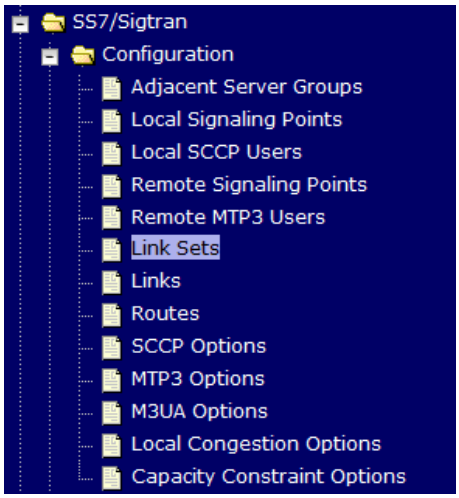
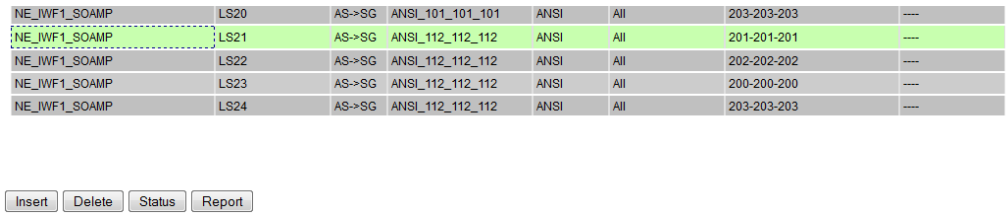
Appendix N.2.3 Removing Server from Server Group

4 ☐	**SOAM VIP GUI:** Delete SS7-MP Routes	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Routes**  **Delete** the associated routes of the identified SS7-MP: 

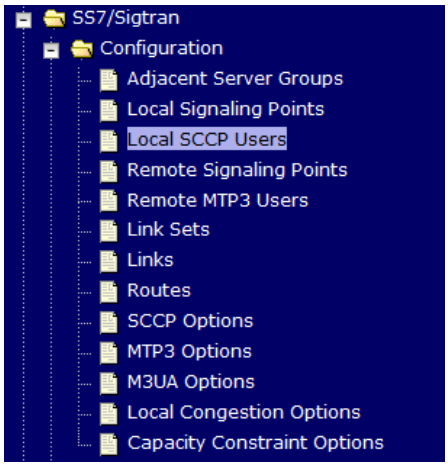
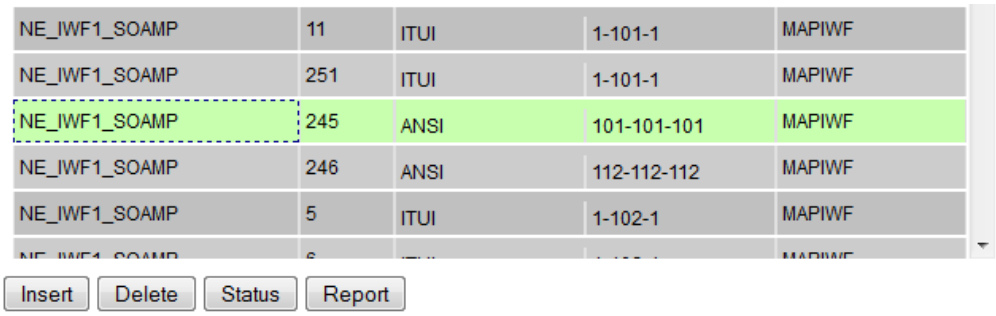
Appendix N.2.3 Removing Server from Server Group

5 ☐	**SOAM VIP GUI:** Delete SS7-MP Links	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Links**  **Delete** the associated links of the identified SS7-MP: 

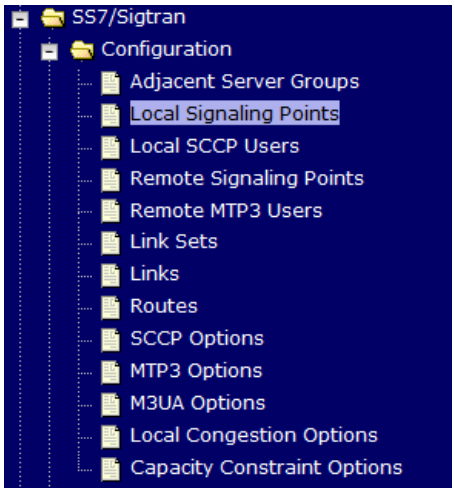
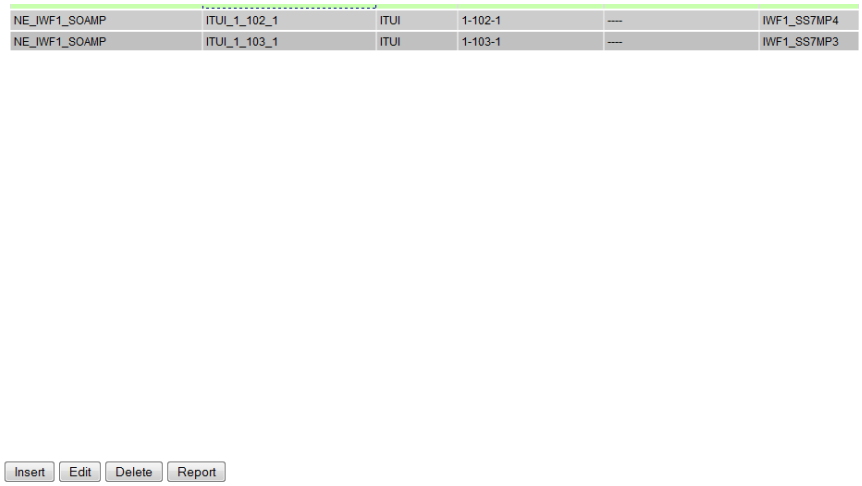
Appendix N.2.3 Removing Server from Server Group

6 ☐	**SOAM VIP GUI:** Delete SS7-MP Link Sets	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Link Sets**  **Delete** the associated link sets of the identified SS7-MP: 

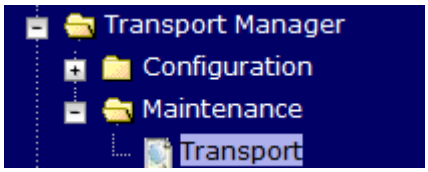
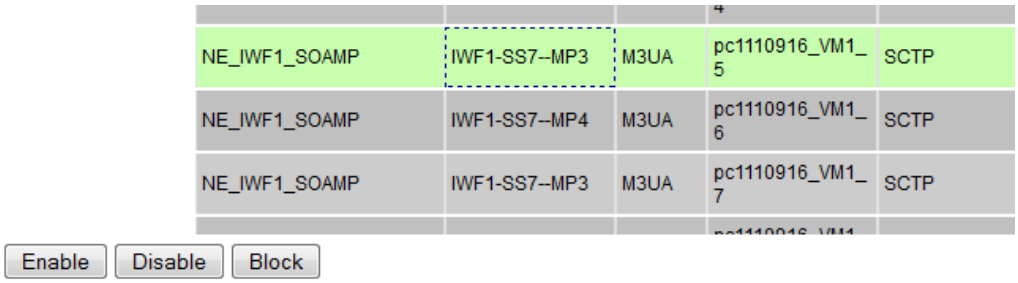
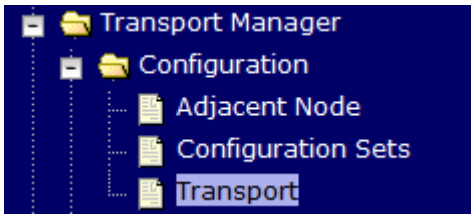
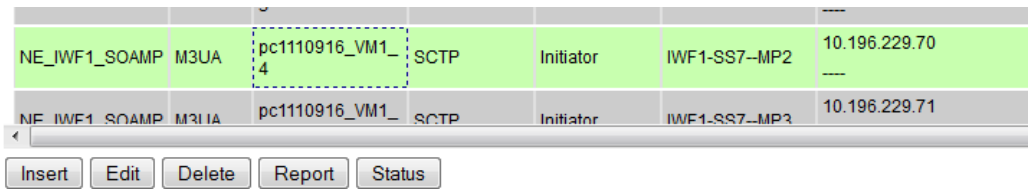
Appendix N.2.3 Removing Server from Server Group

7 ☐	**SOAM VIP GUI:** Delete SS7-MP Local SCCP Users	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Local SCCP Users**  **Delete** the associated Local SCCP Users from the identified SS7-MP: 

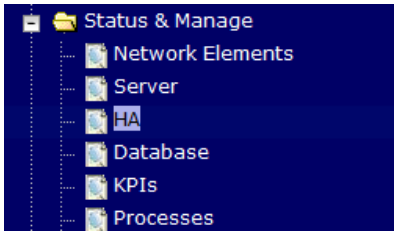
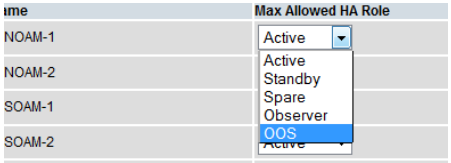
Appendix N.2.3 Removing Server from Server Group

8 ☐	**SOAM VIP GUI:** Delete SS7-MP Local Signaling Points	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Local Signaling Points**  **Delete** the associated Local signaling points from the identified SS7-MP: 

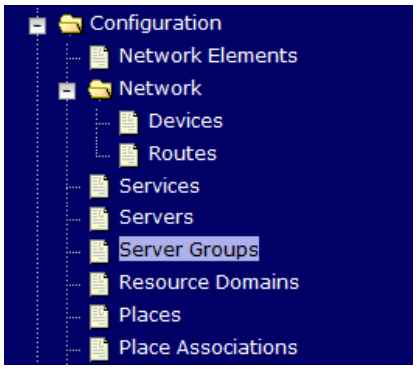
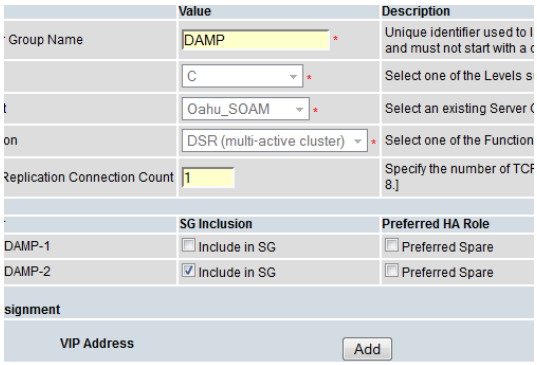
Appendix N.2.3 Removing Server from Server Group

9 ☐	**SOAM VIP GUI:** Disable SS7-MP transports	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> Transport Manager -> Maintenance -> Transport**  **Disable** the associated transports from the identified SS7-MP: 
10 ☐	**SOAM VIP GUI:** Delete SS7-MP transports	**Execute this step if Removing SS7MP, otherwise skip to step 11** Navigate to **Main Menu -> Transport Manager -> Configuration -> Transport**  **Delete** the associated transports from the identified SS7-MP: 

Appendix N.2.3 Removing Server from Server Group

11 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
12 ☐	**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**

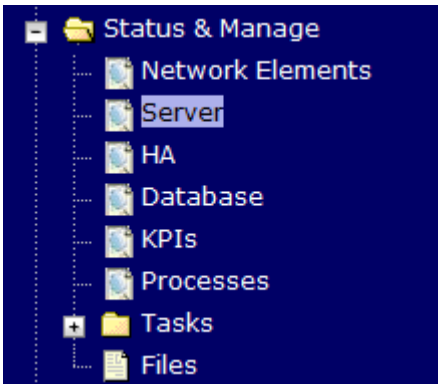
Appendix N.2.3 Removing Server from Server Group

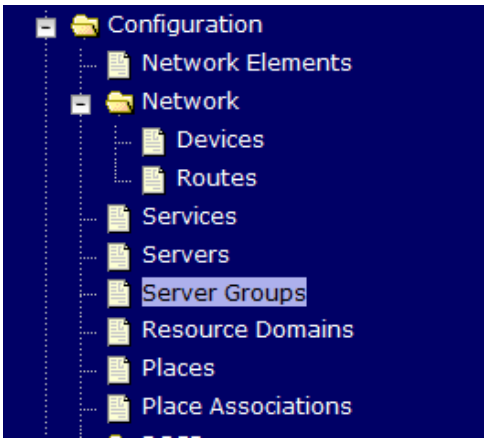
13 ☐	**NOAM VIP GUI:** Remove Server From Server Group	Navigate to **Main Menu -> Configuration -> Server Groups**  Select the server group for which the server from **step 2** that was placed OOS. Click **Edit** Insert Edit Delete Report Uncheck the server from **step 2** from the *SG Inclusion* column:  Click **Ok** Ok Apply Cancel

Appendix N.2.7 Post Growth Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms after Growth. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

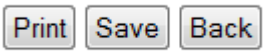
Appendix N.2.7 Post Growth Health Check

<table>
<tr>
<td>2
☐</td>
<td>NOAM VIP GUI:
Verify Server Status</td>
<td>Navigate to Main Menu -> Status & Manage -> Server
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>
</td>
</tr>
<tr>
<td>3
☐</td>
<td>NOAM VIP GUI:
Verify Server Configuration</td>
<td>Navigate to Main Menu -> Configuration -> Server Groups
 

Verify the configuration data is correct for your network.</td>
</tr>
</table>

Appendix N.2.7 Post Growth Health Check

4 ☐	**NOAM VIP GUI:** Log Current Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Click on the **Report** button  **Save** or **Print** this report, keep copies for future reference.  Compare this alarm report with those gathered in procedure **Appendix N.1.2**
5 ☐	**SOAM VIP GUI:** Repeat	Repeat **Steps 1-3** for the SOAM

Appendix N.1.8 Post Growth Backups

S T E P #	This procedure will reference steps to backup all necessary items after a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix O: My Oracle Support** (MOS), and ask for assistance.	
1 ☐	**Backup TVOE**	Backup all TVOE host configurations by executing **Procedure 39**
2 ☐	**Backup PMAC**	Backup the PMAC application by executing **Procedure 40**
3 ☐	**Backup NOAM/SOAM databases**	Backup the NOAM and SOAM Databases by executing **Procedure 41** and **Procedure 42**

Appendix O: My Oracle Support (MOS)

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

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

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1) For the first set of menu options, select 2, “New Service Request”. You will hear another set of menu options.
2) In this set of menu options, select 3, “Hardware, Networking and Solaris Operating System Support”. A third set of menu options begins.
3) In the third set of options, select 2, “Non-technical issue”. Then you will be connected to a live agent who can assist you with MOS registration and provide Support. Identifiers. Simply mention you are a Tekelec Customer new to MOS.