Oracle® Communications

Diameter Signaling Router

DSR C-Class Software Installation and Configuration Guide

Release

8.6.0.0.0

F56010-02

September 2022

Oracle ® Communication Diameter Signaling Router DSR C-Class Software Installation and Configuration Guide

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

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

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

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

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

DSR Hardware and Software Installation Part 1: Use document [6].

Table of Contents

List of Tables

1. Introduction

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

This document assumes that platform-related configuration has already been done. Before executing this document, please ensure procedures from [6] 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 Growth/De-Growth.

1.1 References

[1] DSR Meta Administration Feature Activation Procedure

[2] DSR Full Address Based Resolution (FABR) Feature Activation Procedure

[3] DSR Range Based Address Resolution (RBAR) Feature Activation Procedure

[4] SDS SW Installation and Configuration Guide

[5] DSR IPv6 Migration Guide

[6] DSR Hardware and Software Installation Part 1

[7] DSR PCA Activation Guide

[8] DSR DTLS Feature Activation Procedure

[9] Platform Configuration Procedure

[10] DSR Security Guide

[11] DCA Framework and Application Activation and Deactivation Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document

Table 1. Acronyms

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

Acronym	Definition
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PCA	Policy and Charging Application
PMAC	Platform Management & Configuration
RMS	Rack Mounted Server
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

1.3 Terminology

This section describes terminology as it is used within this document.

Table 2. Terminology

Term	Definition
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.
Management Server	HP ProLiant DL360/ DL380 deployed to run TVOE and host a virtualized PMAC application. Can also host a virtualized NOAM or IDIH. It is also used to configure the Aggregation switches (via the PMAC) and to serve other configuration purposes.
Place Association	Applicable for various applications, a **Place Association** is a configured object that allows places to be grouped together. A place can be a member of more than one place association. The Policy & Charging DRA application defines two place association types: policy binding region and policy & charging mated sites.
PMAC Application	PMAC is an application that provides platform-level management functionality for HP G6/G8/G9 system, such as the capability to manage and provision platform components of the system so it can host applications.

Term	Definition
SBR Server Group Redundancy	The Policy and Charging application uses SBR server groups to store the application data. The SBR server groups support both two and three site redundancy. The server group function name is **SBR**.
Server Group Primary Site	A server group primary site is a term used to represent the principle location within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single **Policy and Charging Mated Sites** place association. For the Diameter Custom Application (DCA), these sites (Places) are configured in **Applications Region** place association. The primary site may be in a different site (place) for each configured SOAM or SBR server group. A primary site is described as the location in which the active and standby servers to reside; however, there cannot be any preferred spare servers within this location. All SOAM and SBR server groups have a primary site.
Server Group Secondary Site	A server group secondary site is a term used to represent location in addition to the primary site within a SOAM or SBR SERVER GROUP. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single **Policy and Charging Mated Sites** place association. For the Diameter Custom Application (DCA), these sites (places) are configured in **Applications Region** place association. The secondary site may be in a different site (place) for each configured SOAM or SBR server group. A secondary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. If two or three site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups.
Server Group Tertiary Site	A server group tertiary site is a term used to represent location in addition to the primary and secondary sites within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy & Charging DRA application, these sites (places) are all configured within a single **Policy and Charging Mated Sites** place association. 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.
Session Binding Repository Server Group Redundancy	The DCA application may use SBR server groups to store application session data. The SBR server groups with support both two and three site redundancy. The server group function name is **Session and Binding Repository**.

Term	Definition
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.
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.
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 and 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 ensures there is always a functioning active server in a server group even if all the servers in two sites fail.
Two Site Redundancy	Two site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy and Charging Mated Sites Place Association containing two sites. Two site redundancy is a feature provided by server group configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in two geographically separate sites (locations). This feature ensures there is always a functioning active server in a server group even if all the servers in a single site fail.

1.4 General Procedure Step Format

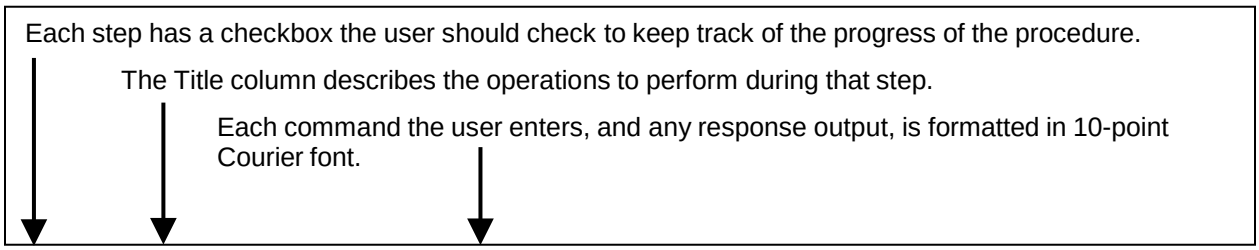
When executing the procedures in this document, there are a few key points to ensure you understand procedure convention. These points are:

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix N before attempting to continue.

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

- Each step has a checkbox that the user should check-off to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.

- The title box describes the operations to be performed during that step.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Each command that the user enters, as well as any response output, is formatted in `10-point Courier` font.



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

Figure 1. Example of a Procedure Steps Used in This Document

2. General Description

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

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

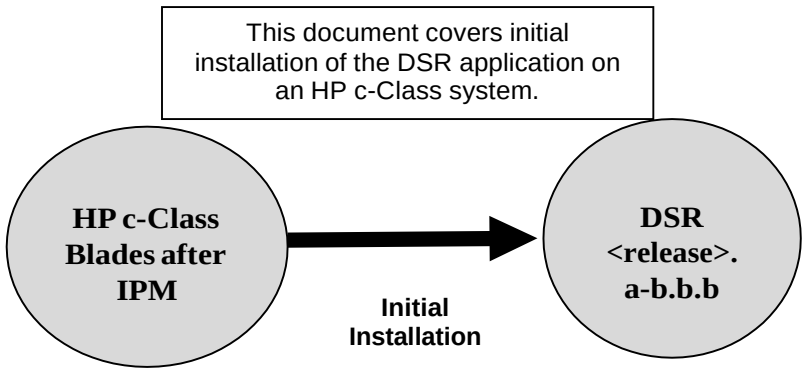


Figure 2. Example of Initial Application Installation Path

3. Installation Overview

This section provides a brief overview of the recommended method for installing DSR software on an HP C-Class system.

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

3.1 Required Materials

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

3.2 Installation Strategy

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

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

1. An overall installation requirement is decided upon. Among the data that should be collected:
   - The total number of sites
   - The number of servers at each site and their role(s)
   - Does DSR's networking interface terminate on a Layer 2 or Layer 3 boundary?
   - Number of enclosures at each site -- if any at all.
   - Will NOAMs use rack-mount servers or server blades?
   - (Per Site) Will MP's be in N+ 0 configurations?
   - What time zone should be used across the entire collection of DSR sites?
   - Will SNMP traps be viewed at the NOAM, or an external NMS be used? (Or both?)
2. A site survey (NAPD) is conducted with the customer to determine exact networking and site details.

   Note: XMI and IMI addresses are difficult to change once configured. It is very important that these addresses are well planned and not expected to change after a site is installed.
3. For each SOAM /MP/DR-NOAM only site (that is, sites NOT containing the main NOAM server), the installer executes the procedures in document [6] to set up PMAC, HP enclosures, and switches. Then, using the procedures in this document, all servers are IPMed with the proper TPD and DSR application ISO image. When this is complete, all non-NOAM sites are reachable through the network and ready for further installation when the primary NOAM site is brought up.
4. The installer moves to the main site that contains the primary NOAM. Again, [6] is executed for this site first and then use the procedures in this document. During this install, the user brings up the other sub-sites (if they exist) configured in step 3. For single sites where the NOAM/SOAM/MPs are all located together, then step 3 is skipped and the entire install is covered by this step.
5. Once the primary NOAM site has been installed according [6] and this document, and then full DSR installation is complete.

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

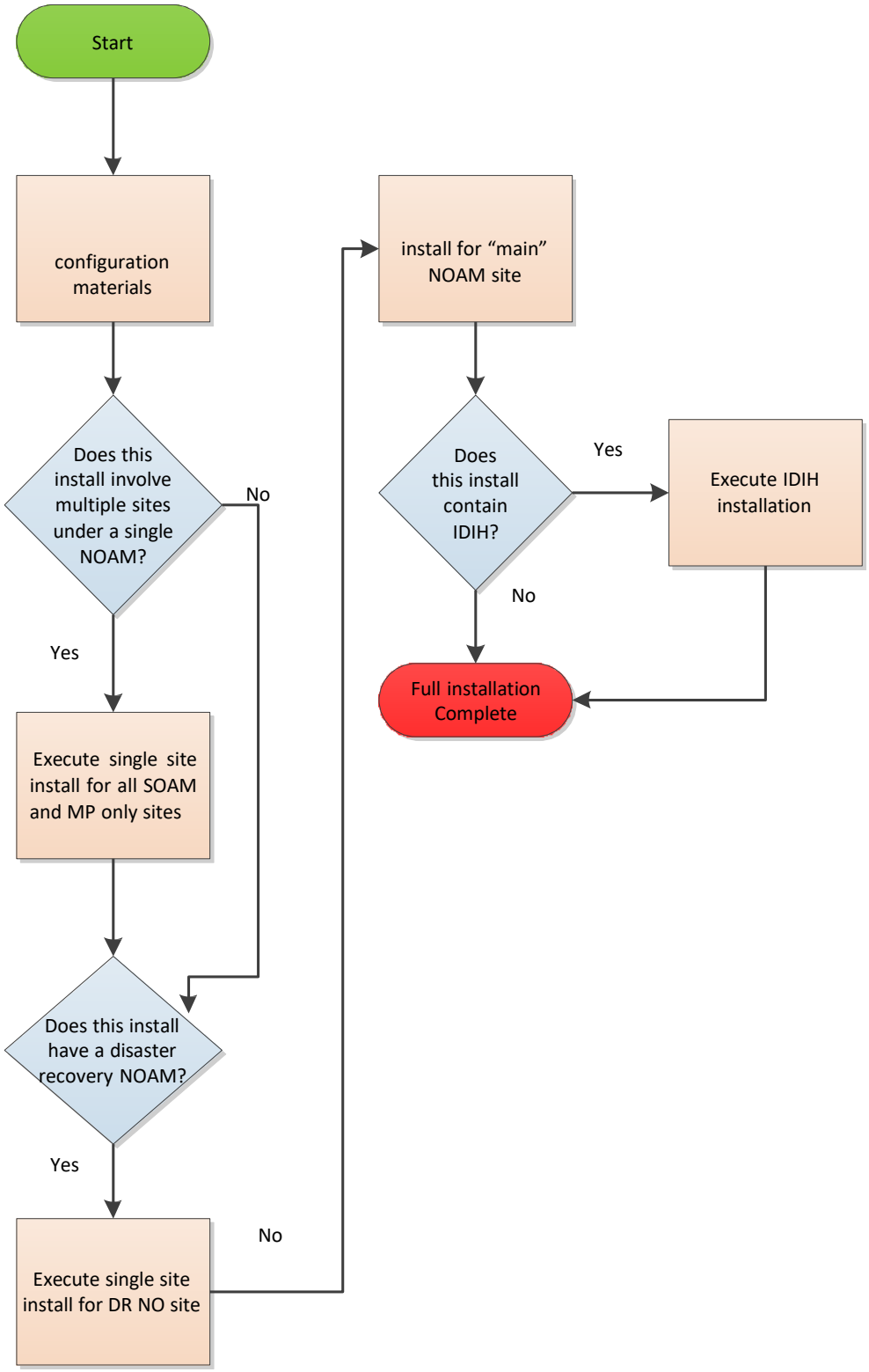


Figure 3. DSR Installation: High Level Sequence

3.3 SNMP Configuration

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

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

- DSR application servers (NOAM, SOAM, MPs of all types)
- DSR auxiliary components (OA, switches, TVOE hosts, PMAC)

DSR application servers can be configured to:

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

Application server SNMP configuration is done from the NOAM GUI, near the end of DSR installation. See the procedure list for details.

DSR auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAM VIP, the SOAMP VIP, or an external (customer) NMS. The recommended configuration is as follows:

The following components:

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

Should have their SNMP trap destinations set to:

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

3.4 Optional Features

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

Table 2. Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Guide
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure

Feature	Document
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
Host Intrusion Detection System (HIDS)	DSR Security Guide

4. Software Installation Procedure

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

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

SUDO

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

IPv6

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

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

If a dual-stack (IPv4 & IPv6) network is required, configure the topology first and then migrate to IPv6. Refer to [6] for instructions on how to accomplish this IPv6 migration.

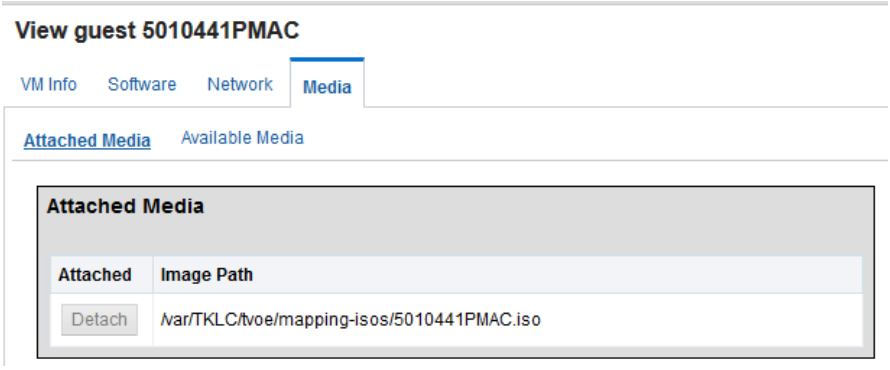
4.1 Install and Configure NOAM Servers

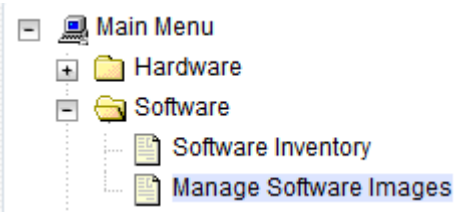
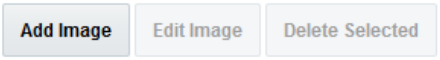
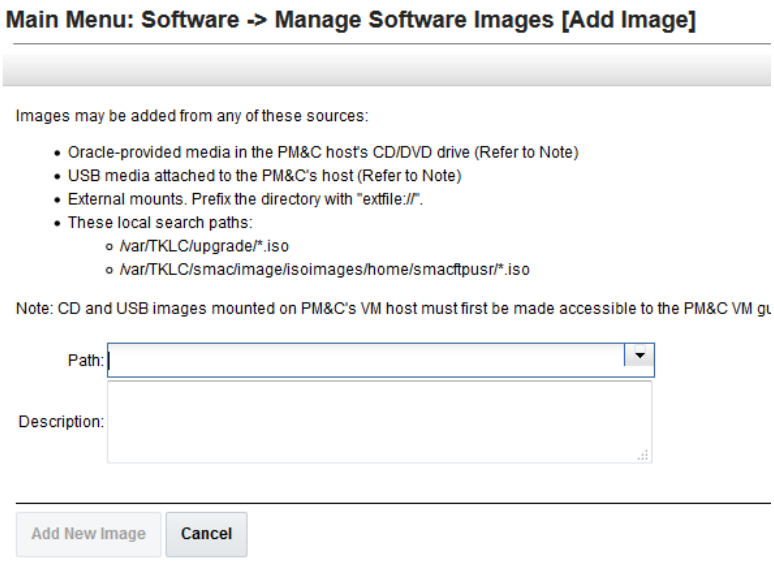
4.1.1 Load Application and TPD ISO onto the PMAC Server

Procedure 1. Load Application and TPD ISO onto PMAC Server

Step#	Procedure	Description
This procedure loads 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 My Oracle Support (MOS) and ask for assistance.		

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>1.
☐</td><td>TVOE Host: Load application ISO</td><td>Add the Application ISO image to the PMAC, 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 PMAC server into the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server).
Using sftp, connect to the PMAC server.
<code>$ sftp pmacftpusr@<pmac_management_network_ip></code>
<code>$ put <image>.iso</code>
After the image transfer is 100% complete, close the connection:
<code>$ quit</code></td></tr>
<tr><td>2.
☐</td><td>PMAC GUI: Login</td><td>1. Open web browser and enter:
<code>https://<PMAC_Mgmt_Network_IP></code>
2. Login as guiadmin user:
 
</td></tr>
</table>

Step#	Procedure	Description
3. ☐	**PMAC GUI**: Attach the software image to the PMAC guest	If the image is on a CD or USB device, continue with this step. If in step 1 the ISO image was transferred directly to the PMAC guest using sftp, skip the rest of this step and continue with step 4. 1. In the PMAC GUI, navigate to **VM Management**. 2. Select the PMAC guest. 3. On the resulting View VM Guest page, select the Media tab. 4. Under the Media tab, find the ISO image in the **Available Media** list, and click its **Attach** button. After a pause, the image displays in the **Attached Media** list. 

Step#	Procedure	Description
4. ☐	**PMAC GUI**: Add application image	1. Navigate to **Software > Manage Software Images**.  2. Click **Add Image**. 3. Select the image from the list.  If the image was supplied on a CD or a USB drive, it displays as a virtual device (**device://…**). These devices are assigned in numerical order as CD and USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, **device://dev/sr1**. If one or more CD or USB-based images were already present on the management server before you started this procedure, select a correspondingly higher device number. If in step 1 the image was transferred to PMAC using sftp, it displays in the list as a local file **/var/TKLC/....**  4. Select the appropriate path and click **Add New Image**. 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 GUI**: Load TPD ISO	If the TPD ISO has not been loaded onto the PMAC already, **repeat** steps 1 through 4 to load it using the TPD media or ISO.

4.1.2 Execute DSR Fast Deployment for NOAMs

Procedure 2. Configure NOAM Servers

Step#	Procedure	Description
This procedure extends the TVOE networking configuration on the first RMS server (if necessary), configure the networking on additional rack mount servers, create the NOAM VMs, and deploy the DSR and TPD images. ***Prerequisite***: TVOE and PMAC (virtualized) have been installed on the first RMS server as described in [6]. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**TVOE Host (Not PMAC)**: Configure control network bond for back-back configurations	Establish an SSH session to the second RMS server via the control IP address accessed from the site PMAC. Login as **admusr**.
		If the control network for the RMS servers consists of direct connections between the servers with no intervening switches (known as a back-to-back configuration), execute this step to set the primary interface of bond0 to <ethernet_interface_1>, otherwise **skip to the next step**.
		Note: Section TVOE Network Configuration, step 2, should have already been executed on the TVOE host that hosts the PMAC server.
		Note: The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=bond0 --primary=eth01`
		`Interface bond0 updated`

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

Step#	Procedure	Description

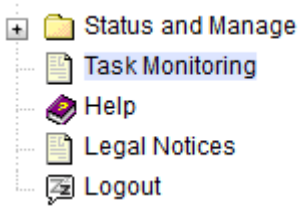
3. ☐	**PMAC Server**: Update the DSR fast deployment template (Part 1)	1. Perform the following command to navigate to the directory containing the DSR fast deployment template:
		`$ cd /usr/TKLC/smac/etc`
		DSR Fast Deployment Template Names:
		NOAM on Rack Mount Servers: DSR_NOAM_FD_RMS.xml
		NOAM on Blade Servers: DSR_NOAM_FD_Blade.xml
		2. 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- 7.7.0.0.0-88.68.0-OracleLinux6.10-x86_64</name>`
		`</image>`
		`<!--Target DSR release Image here -->`
		`<image id="dsr">`
		`<name>DSR-8.5.0.0.0_90.11.0-x86_64</name>`
		`</image>`
		`</software>`
		Note: These are the images uploaded from Procedure 1. Load Application and TPD ISO onto PMAC Server. Do **NOT** append **.iso** to the image name. To copy and paste the image name from the command line, issue the following command:
		`$ ls /var/TKLC/smac/image/repository`

Step#	Procedure	Description
4. ☐	**PMAC Server**: Update the DSR fast deployment template for bond 1 – optional (Part 2)	**Bond 1 Creation:** Skip this step if Bond1 will not be created. 1. Uncomment the following items from **BOTH** tvoe host id="NOAM1" and tvoe host id="NOAM2" by removing the encapsulated '<!—' '-->' brackets as highlighted below: 2. Update the Ethernet interfaces that are to be enslaved by bond1. <!-- <tpdinterface id="bond1"> <device>bond1</device> <type>Bonding</type> <bonddata> <bondinterfaces><bond1_eth_interface1>,<bond1_eth_interface2></bondinterfaces> <bondopts>mode=active-backup,miimon=100</bondopts> </bonddata> <onboot>yes</onboot> <bootproto>none</bootproto> </tpdinterface> -->
5. ☐	**PMAC Server**: Update the DSR fast deployment template management/ XMI combination (Part 3)	Only execute this step if your management network and xmi networks are combined; otherwise, skip this step. 1. Modify the template to reflect the following on **BOTH** tvoe host id="NOAM1" and tvoe host id="NOAM2": **Remove** the following stanzas: <mgmtbondinterface> <mgmtvlan> <mgmtsubnet> <mgmtdefaultgateway> <tpdinterface id="management"> (and all sub elements) <tpdbridge id="management"> (and all sub elements) **Replace** the following under <tpdroute id="management_default">: management with xmi for <device>management</device> $$mgmtdefaultgateway$$ with $$xmidefaultgateway$$ for <gateway>$$mgmtdefaultgateway$$</gateway> 2. Add the following under <tpdbridge id="xmi">: <address><TVOE_Host_Server_XMI_IP></address> <netmask> $$xmisubnet$$</netmask> **Note**: If the IP address is IPv6, then use <IPv6address> as the prefix. For example: <IPv6address>2405:200:330:A127:101::a5/112</IPv6address>

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>6.
☐</td><td>PMAC Server: Validate and run the fast deployment file</td><td>
1. Validate/Create the fast deployment file by executing the following command:
For NOAMs deployed on rack mount servers:
<pre>$ sudo fdconfig validate --file=DSR_NOAM_FD_RMS.xml</pre>
For NOAMs deployed on blade servers:
<pre>$ sudo fdconfig validate --
file=DSR_NOAM_FD_Blade.xml</pre>
Note: Refer to DSR Fast Deployment Configuration for information of the variables that must be input during execution of NOAM fast deployment.
2. 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:
<pre>---   NOTICE   ---
Config Data saved as a new file: "./DSR_NOAM_FD_Blade_20151217T102402.xml"
---   NOTICE   ---

Configuration file validation successful.
Validation complete
[admusr@GuestPMACeco upgrade]$</pre>
3. Execute the following commands to run the fast deployment file:
<pre>$ screen
$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
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.
</td></tr>
</table>

Step#	Procedure	Description

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

Step#	Procedure	Description

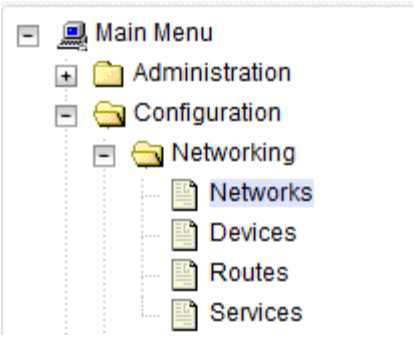
8. ☐	**PMAC Server**: Backup FDC file	Create the **fdc** directory so the NOAM fdc file is backed up by PMAC:
		Issue the following commands:
		1. Create the fdc backup directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc`
		2. Copy the fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/<fdc_file> /usr/TKLC/smac/etc/fdc/`

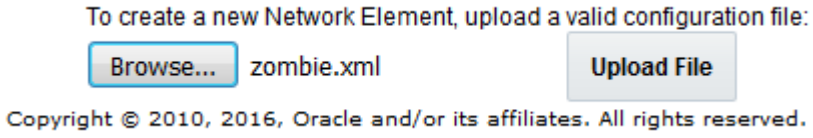
4.1.3 Configure NOAMs

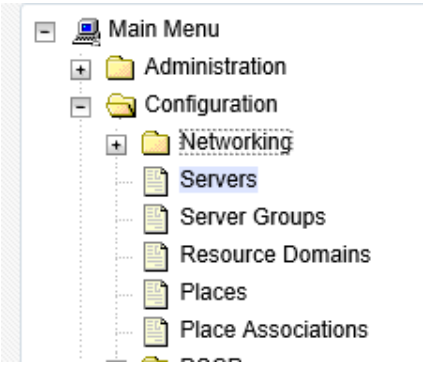
Procedure 3. Configure the First NOAM NE and Server

Step#	Procedure	Description
This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Save the NOAM network data to an XML file	1. Using a text editor, create a NOAM network element file that describes the networking of the target install environment of your first NOAM server. 2. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is **Appname_NEname_NetworkElement.XML**, so for example a DSR2 NOAM network element XML file would have a filename **DSR2_NOAM_NetworkElement.xml**. Alternatively, you can update the sample DSR network element file. It can be found on the management server at: `/usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml` A sample XML file can also be found in Sample Network Element and Hardware Profiles. ***Note***: These limitations apply when specifying a network element name: • A 1-32-character string. • Valid characters are alphanumeric and underscore. • Must contain at least one alpha and must not start with a digit.

Step#	Procedure	Description
2. ☐	**NOAM GUI**: Login	Using the XMI IP address configured in Procedure 2. Configure NOAM Servers ($NOAM1_xmi_IP_address), log into the NOAM GUI as the **guiadmin** user: 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>3.
☐</td><td>Create the NOAM network element using the XML file</td><td>1. Navigate to Configuration > Networking > Networks.
 

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

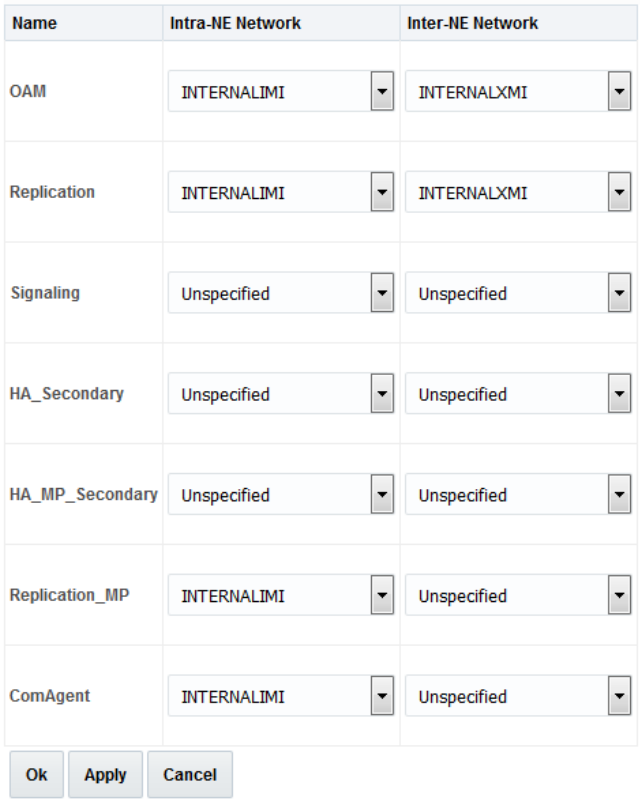
3. Click Upload File to upload the XML file and configure the NOAM network element.
4. Once the data has been uploaded, a tab displays with the name of your network element. Click this tab to display a screen with the individual networks that are now configured.
 
</td></tr>
<tr><td>4.
☐</td><td>Map services to networks</td><td>1. Navigate to Configuration > Services.
 

2. Click Edit and set the services as shown in the table.
<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>OAM</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>Replication</td><td><IMI Network></td><td><XMI Network></td></tr>
</table></td></tr>
</table>

Step#	Procedure	Description

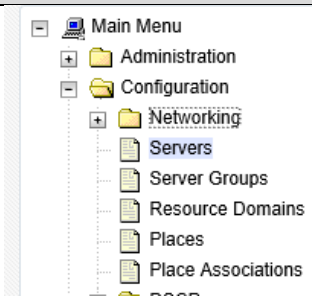
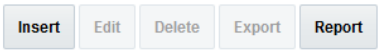
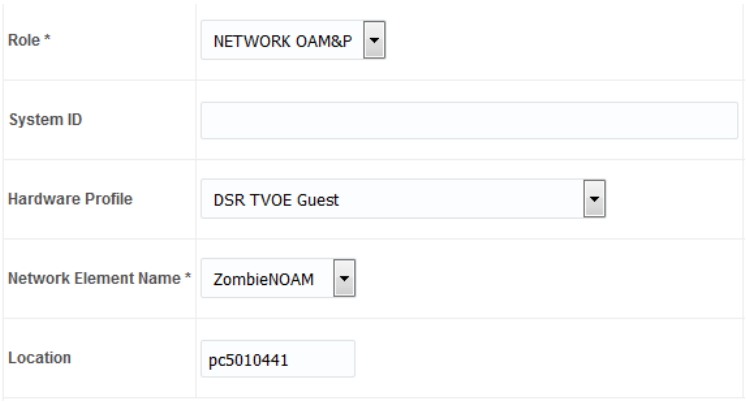
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	<IMI Network>	Unspecified
ComAgent	<IMI Network>	Unspecified

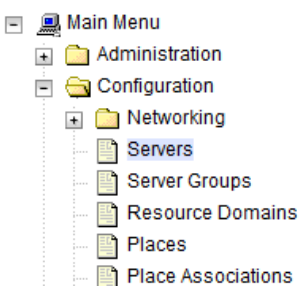
For example, if your IMI network is named **IMI** and your XMI network is named **XMI,** then your services config should look like the following:

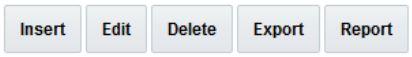


3. Click **OK** to apply the Service-to-Network selections.
4. Click **OK** when asked to restart all servers.

5. ☐	Insert the 1st NOAM server	1. Navigate to **Configuration > Servers**.

Step#	Procedure	Description
		 2. Click **Insert** to insert the new NOAM server into servers table (the first or server).  3. Enter the fields as follows: **Hostname**: <Hostname> **Role**: NETWORK OAM&P **System ID**: <Site System ID> **Hardware Profile**: DSR TVOE Guest **Network Element Name**: [Choose NE from Drop Down Box]  The network interface fields become available with selection choices based on the chosen hardware profile and network element. 4. Type the server IP addresses for the XMI network. Select **XMI** for the interface. Leave the **VLAN** checkbox unchecked. ***Note***: The XMI server IP must match **$NOAM1_xmi_IP_address** configured in Procedure 2. 5. Type the server IP addresses for the IMI network. Select **IMI** for the interface. Leave the **VLAN** checkbox unchecked. ***Note***: The IMI server IP must match **$NOAM1_imi_IP_address** configured in Procedure 2. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td></td><td></td><td>6. Add the following NTP servers:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><TVOE_XMI_IP_Address (NO1)/
TVOE_Mgmt_IP_Address (NO1)></td><td>Yes</td></tr>
</table>
7. Click OK when you have completed entering all the server data.</td></tr>
<tr><td>6. ☐</td><td>Export the initial configuration</td><td>1. Navigate to Configuration > Servers.
 

2. From the GUI screen, select the NOAM server and click Export to generate the initial configuration data for that server.
 
</td></tr>
<tr><td>7. ☐</td><td>NOAM: Copy configuration file to 1st NOAM server</td><td>1. Establish an SSH session to the 1st NOAM server by logging in as the admusr user.
2. Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the /var/tmp directory.
The configuration file has a filename like TKLCConfigData.<hostname>.sh. The following is an example:
<pre>$ sudo cp
/var/TKLC/db/filemgmt/TKLCConfigData.blade01.sh
/var/tmp/TKLCConfigData.sh</pre></td></tr>
<tr><td>8. ☐</td><td>NOAM: Wait for configuration to complete</td><td>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and then prompts the user to reboot the server.
Wait to be prompted to reboot the server, but DO NOT reboot the server, it is rebooted later on in this procedure.
Note: Ignore the warning about removing the USB key, since no USB key is present.</td></tr>
</table>

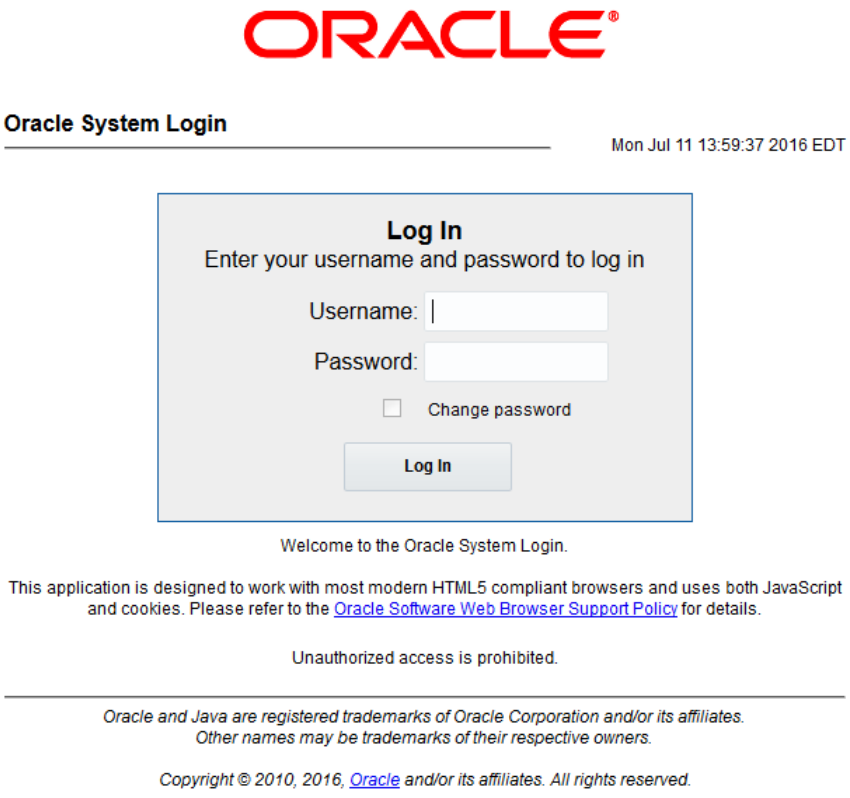
Step#	Procedure	Description

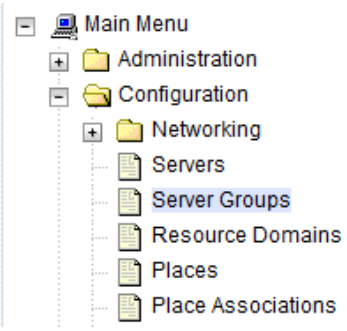
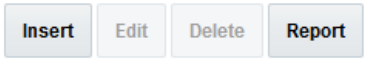
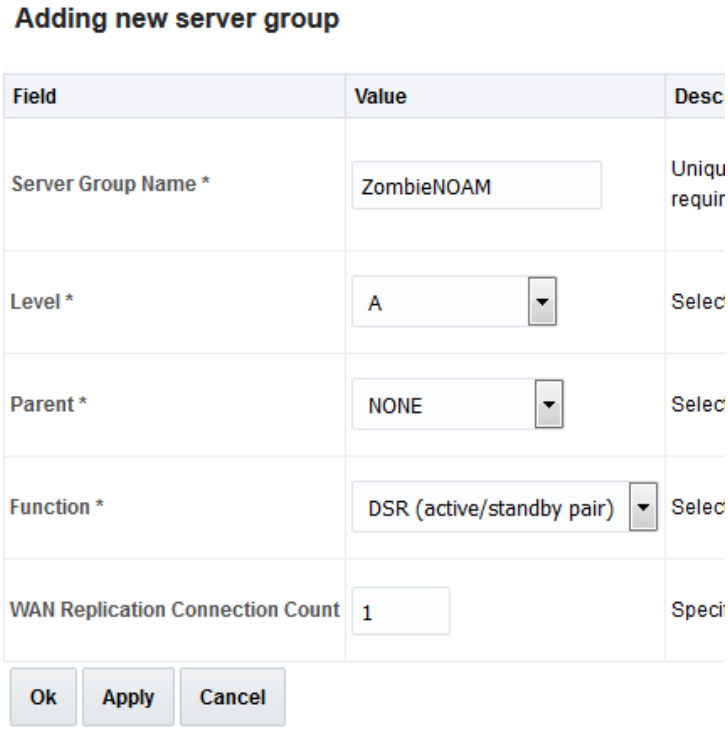
9. ☐	**NOAM**: Set the time zone and reboot the server	1. From the command line prompt, execute **set_ini_tz.pl**.
		This sets the system time zone. The following command example uses the America/New_York time zone.
		2. Replace as appropriate with the time zone you have selected for this installation.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

10. ☐	**1st NOAM**: Configure networking for dedicated netbackup interface (optional)	***Note***: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		Obtain a terminal window to the 1st NOAM server by 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=<NetBackup_Svr_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address>`

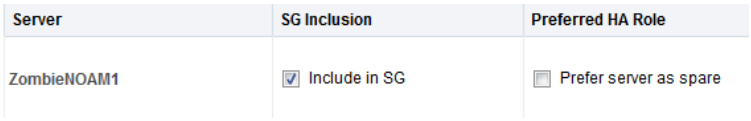
11. ☐	**1st NOAM Server**: Verify server health	Execute the following command on the 1st NOAM server and make sure that no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules in class system...OK`
		`Running modules in class proc...OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

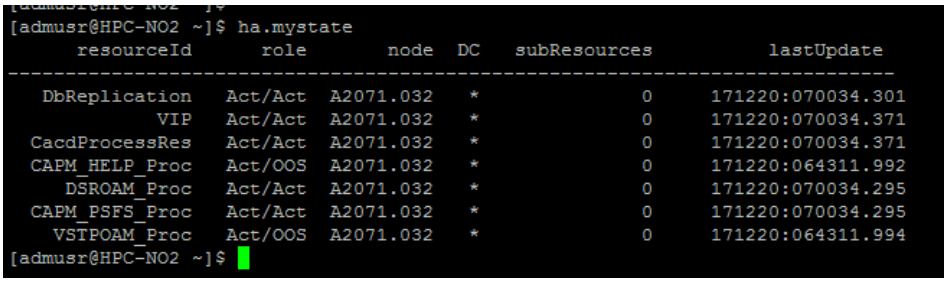
Procedure 4. Configure the NOAM Server Group

Step#	Procedure	Description
This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM GUI**: Login	1. Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of: `https://<NO1_XMI_IP_Address>` 2. Login as the **guiadmin** user. 

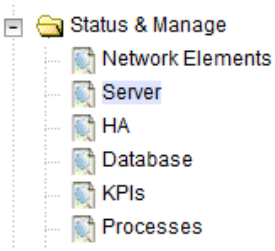
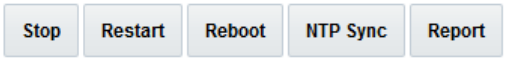
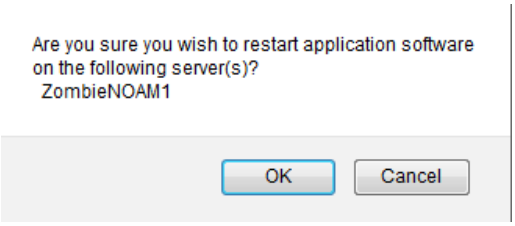
Step#	Procedure	Description
2. ☐	**NOAM GUI**: Enter NOAM server group data	1. Navigate to **Configuration > Server Groups**.  2. Click **Insert** and fill the following fields:  **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: DSR (Active/Standby Pair) **WAN Replication Connection Count**: Use Default Value  3. Click **OK** when all fields are filled in.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>3.
☐</td><td>NOAM GUI:
Edit the NOAM server group</td><td>
1. From the GUI, navigate to Configuration > Server Groups.
2. Select the new server group and click Edit.

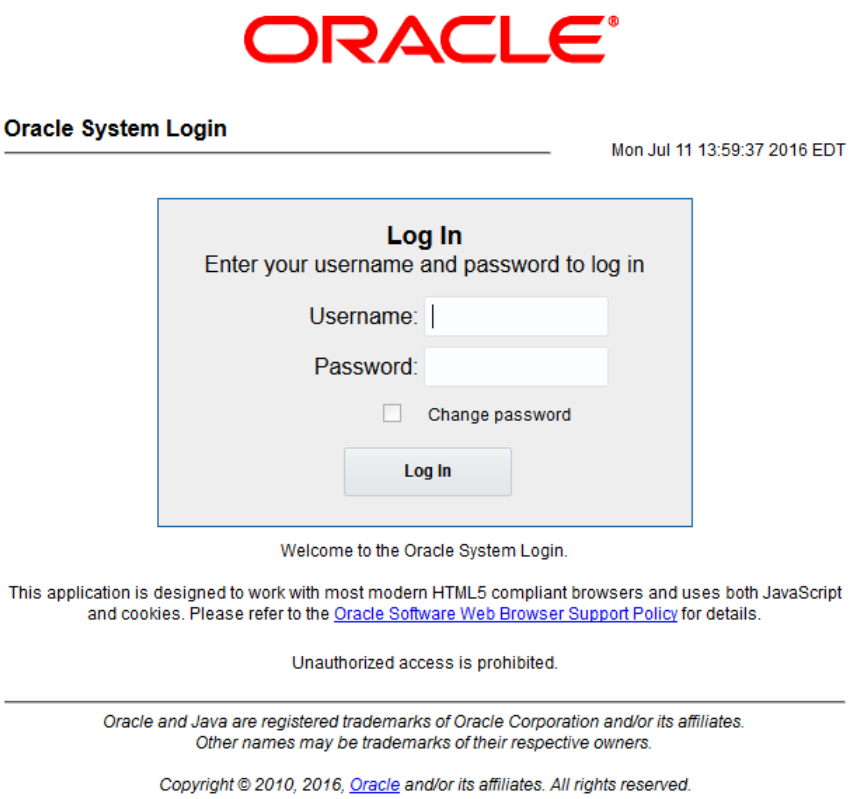
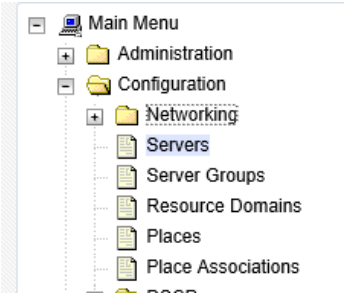

3. Select the network element that represents the NOAM.


4. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured.
5. Mark the Include in SG checkbox.
6. Leave other boxes blank.
7. Click OK.
</td></tr>
<tr><td>4.
☐</td><td>NOAM:
Verify NOAM blade server role</td><td>
1. From terminal window to the iLO of the first NOAM server, execute the following command:
<pre>$ha.mystate</pre>
2. Verify the DbReplication and VIP items under the resourceId column have a value of Active under the role column.
You might have to wait a few minutes for it to become in that state.
Example:


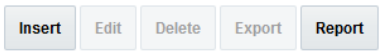
</td></tr>
</table>

Step#	Procedure	Description
5. ☐	**NOAM GUI**: Restart NOAM server	1. From the NOAM GUI, navigate to **Status & Manage** > **Server**.  2. Select the NOAM server. Click **Restart**.  3. Click **OK** on the confirmation screen.  4. Wait for restart to complete.

Procedure 5. Configure the Second NOAM Server

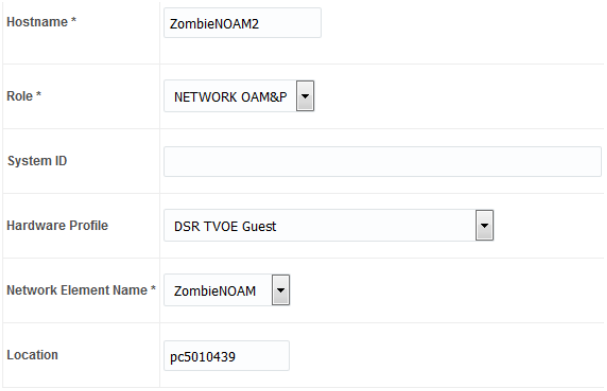
Step#	Procedure	Description
This procedure configures the second NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM GUI**: Login	1. If not already done, establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of: `https://<NO1_XMI_IP_Address>` 2. Login as the **guiadmin** user. 
2. ☐	**NOAM GUI**: Insert the 2nd NOAM server	1. Navigate to **Configuration > Servers**.  2. Click **Insert** to insert the 2nd NOAM server into servers table (the first or server).

Step#	Procedure	Description



3. Enter the fields as follows:

   Hostname: <Hostname>
   Role: NETWORK OAM&P
   System ID: <Site System ID>
   Hardware Profile: DSR TVOE Guest
   Network Element Name: [Choose NE from dropdown box]



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

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

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

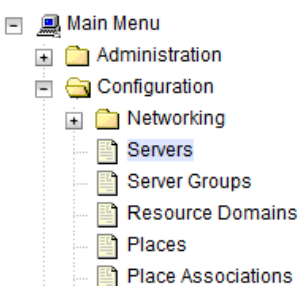
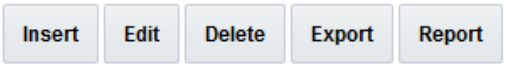
5. Type the server IP addresses for the IMI network. Select **IMI** for the interface. Leave the **VLAN** checkbox unchecked.

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

6. Add the following NTP servers:

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

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

Step#	Procedure	Description
3. ☐	**NOAM GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  2. From the GUI screen, select the NOAM server and click **Export** to generate the initial configuration data for that server. 
4. ☐	**1st NOAM Server**: Copy configuration file to 2nd NOAM server	1. Obtain a terminal session to the 1st NOAM as the **admusr** user. 2. 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	1. Establish an SSH session to the 2nd NOAM server (NOAM2_xmi_IP_address)
		2. Login as the **admusr** user.
		3. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
		4. Verify configuration 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!`
		5. Reboot the server.
		`$ sudo init 6`
		6. Wait for the server to reboot.

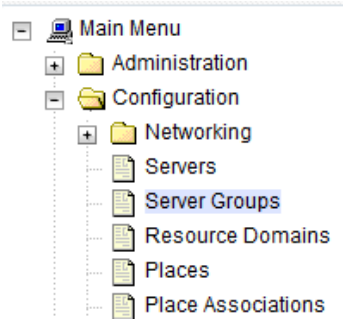
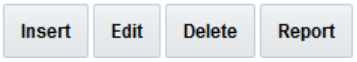
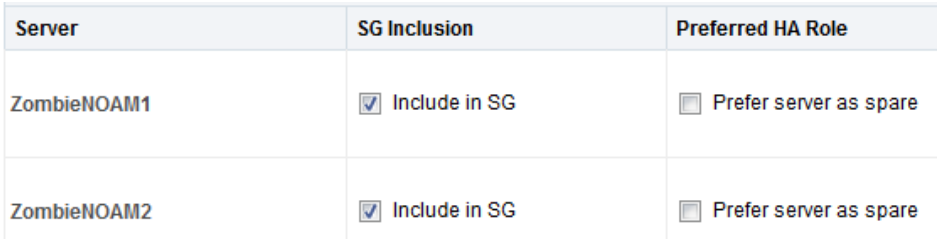
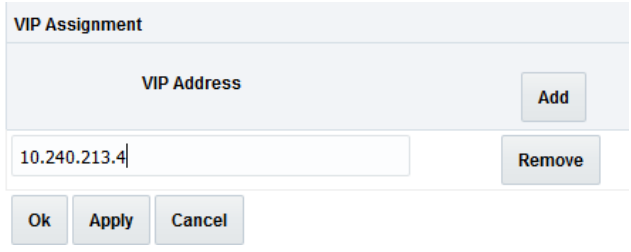
Step#	Procedure	Description

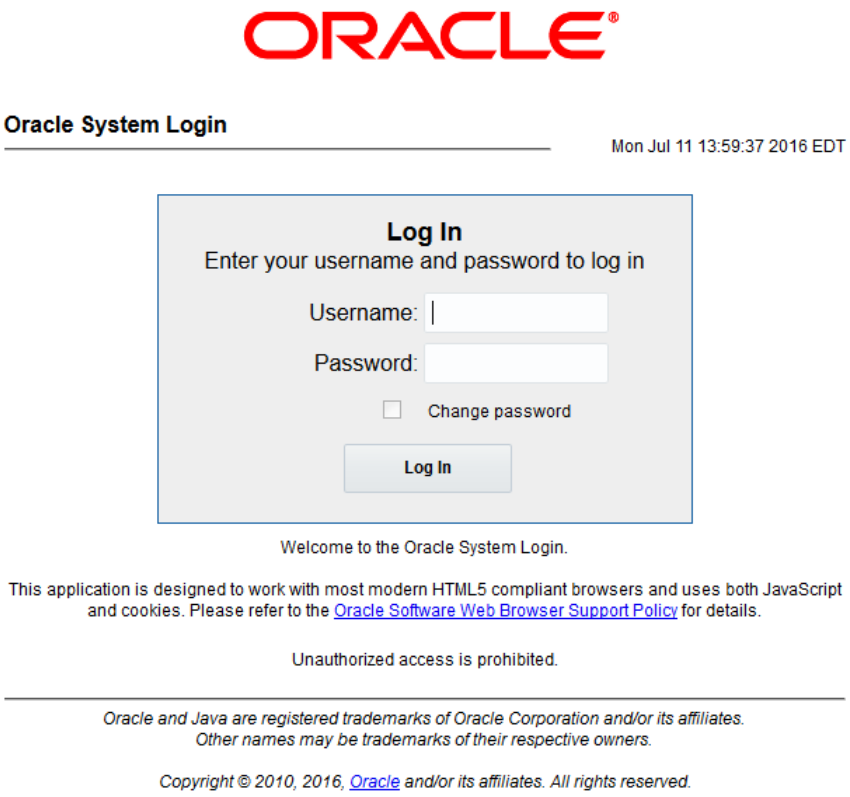
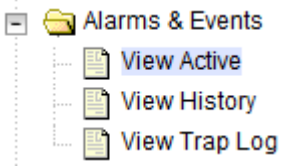
6. ☐	**2nd NOAM Server**: Configure networking for dedicated netbackup interface (optional)	***Note***: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		Obtain a terminal window to the 2nd NOAM server by logging in as the **admusr** user.
		`$ sudo /usr/TKLC/plat/bin/netAdm 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=<NetBackup_Svr_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>`

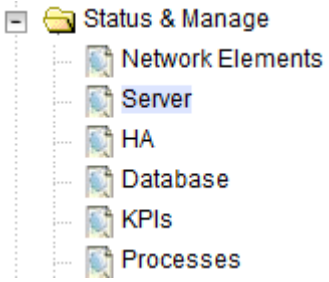
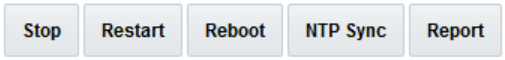
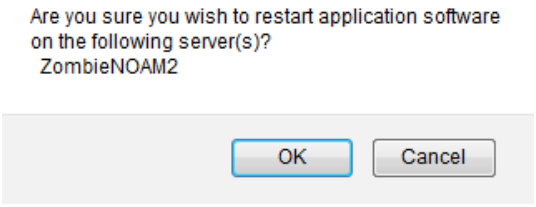
7. ☐	**2nd NOAM Server**: Verify server health	Execute the following command on the 2nd NOAM server and make sure that no errors are returned.
		`$ sudo syscheck`
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules 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

Step #	Procedure	Description
This procedure finishes 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM GUI**: Login	1. Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of: `https://<NO1_XMI_IP_Address>` 2. Login as the **guiadmin** user. 

Step #	Procedure	Description
2. ☐	**NOAM GUI**: Edit the NOAM server group data and add VIP address	1. Navigate to **Configuration > Server Groups**.  2. Select the NOAM server group and click **Edit**.  3. Add the 2nd NOAM server to the server group by marking the **Include in SG** checkbox for the 2nd NOAM server.  4. Click **Apply**. 5. Add a NOAM VIP by clicking **Add**. 6. Type the **VIP Address** and click **OK**. 

Step #	Procedure	Description
3. ☐	**NOAM VIP**: Establish GUI session	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
4. ☐	**NOAM VIP**: Wait for remote database alarm to clear	1. Navigate to **Alarms & Events > View Active**.  2. Wait for the alarm **Remote Database re-initialization in progress** to be cleared before proceeding.

Step #	Procedure	Description
5. ☐	**NOAM GUI**: Restart 2nd NOAM server	1. From the NOAM GUI, navigate to **Status & Manage** > **Server**.  2. Select the 2nd NOAM server. Click **Restart**.  3. Click **OK** to the confirmation screen.  4. Wait for restart to complete 3-5 minutes before proceeding.

4.1.4 Install NetBackup Client (Optional)

Procedure 7. Install NetBackup Client (Optional)

Step#	Procedure	Description
This procedure downloads and installs 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Install NetBackup client software	If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools (push configuration), then use NetBackup Client Install/Upgrade with NBAutoInstall. ***Note***: This is not common. If the answer to the previous question is not known, then use NetBackup Client Installation Using PLATCFG.
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

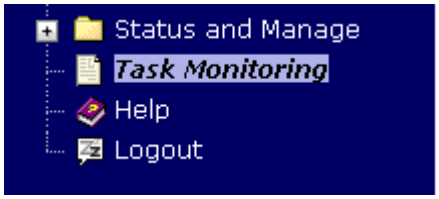
Procedure 8. NOAM Configuration for DR Site

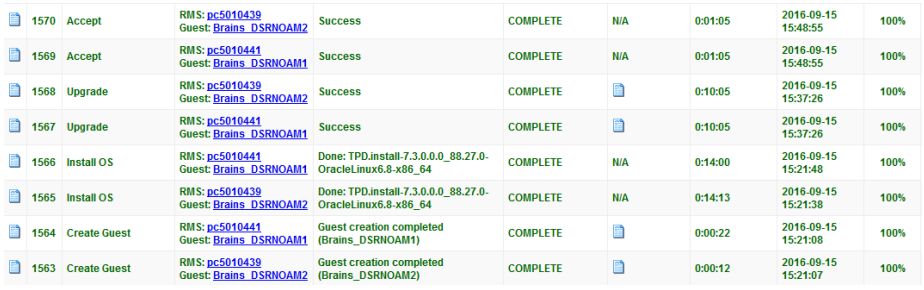
Step#	Procedure	Description
This procedure extends the TVOE networking configuration on the first DR-NOAM RMS server (if necessary), configures the networking on additional rack mount servers, creates the DR-NOAM VMs, and deploys the DSR and TPD images. ***Prerequisite***: TVOE and PMAC (virtualized) have been installed on the First DR-NOAM RMS server as described in [6]. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC Server**: Login	Establish an SSH session to the PMAC server and login as **admusr**.

2.
☐
	PMAC Server: Update the DSR fast deployment template (Part 1)	1. 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
		2. 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- 7.7.0.0.0-88.68.0-OracleLinux6.10-x86_64</name>`
		`</image>`
		`<!--Target DSR release Image here -->`
		`<image id="dsr">`
		`<name>DSR- 8.5.0.0.0_90.11.0-x86_64</name>`
		`</image>`
		`</software>`
		Note: These are the images uploaded from Procedure 1. Load Application and TPD ISO onto PMAC Server. Do **NOT** append **.iso** to the image name. To copy and paste the image name from the command line, issue the following command:
		`$ ls /var/TKLC/smac/image/repository`

Step#	Procedure	Description
3. ☐	**PMAC Server**: Update the DSR fast deployment template for bond 1 – optional (Part 2)	**Bond 1 Creation:** Skip this step if Bond1 will not be created. 1. Uncomment the following items from **BOTH** tvoe host id="NOAM1" and tvoe host id="NOAM2" by removing the encapsulated '<!—' '-->' brackets as highlighted below: 2. Update the Ethernet interfaces that are to be enslaved by bond1. <!-- <tpdinterface id="bond1"> <device>bond1</device> <type>Bonding</type> <bonddata> <bondinterfaces><bond1_eth_interface1>,<bond1_eth_interface2></bondinterfaces> <bondopts>mode=active-backup,miimon=100</bondopts> </bonddata> <onboot>yes</onboot> <bootproto>none</bootproto> </tpdinterface> -->
4. ☐	**PMAC Server**: Update the DSR fast deployment template management /XMI combination (Part 3)	Only execute this step if your management network and xmi networks are combined; otherwise, skip this step. 1. Modify the template to reflect the following on **BOTH** tvoe host id="NOAM1" and tvoe host id="NOAM2": **Remove** the following stanzas: <mgmtbondinterface> <mgmtvlan> <mgmtsubnet> <mgmtdefaultgateway> <tpdinterface id="management"> (and all sub elements) <tpdbridge id="management"> (and all sub elements) **Replace** the following under <tpdroute id="management_default">: management with xmi for <device>management</device> $$mgmtdefaultgateway$$ with $$xmidefaultgateway$$ for <gateway>$$mgmtdefaultgateway$$</gateway> 2. Add the following under <tpdbridge id="xmi">: <address><TVOE_Host_Server_XMI_IP></address> <netmask> $$xmisubnet$$</netmask> **Note**: If the IP address is IPv6, then use <IPv6address> as the prefix. For example: <IPv6address>2405:200:330:A127:101::a5/112</IPv6address>

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>5.
☐</td><td>PMAC Server: Validate and run the fast deployment file</td><td>
1. Validate/Create the fast deployment file by executing the following command:
For NOAMs deployed on rack mount servers:
<pre>$ sudo fdconfig validate --file=DSR_NOAM_FD_RMS.xml</pre>
For NOAMs deployed on blade servers:
<pre>$ sudo fdconfig validate --file=DSR_NOAM_FD_Blade.xml</pre>
Note: Refer to DSR Fast Deployment Configuration for information of the variables that must be input during execution of NOAM fast deployment.
2. 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:
<pre>---   NOTICE   ---
Config Data saved as a new file: "./DSR_NOAM_FD_Blade_20151217T102402.xml"
---   NOTICE   ---

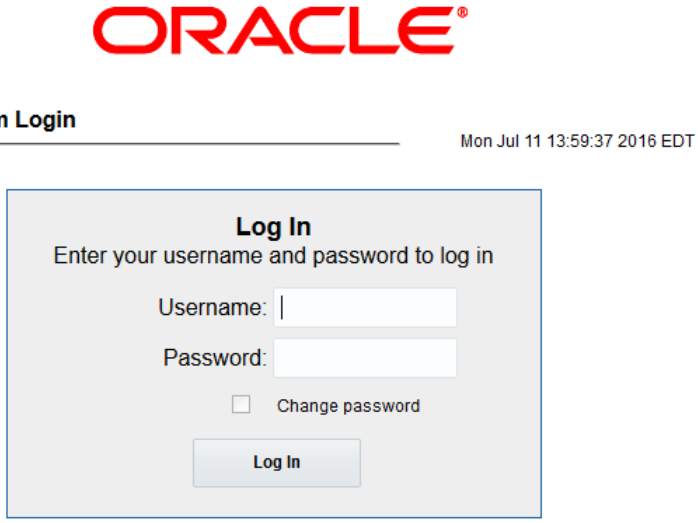
Configuration file validation successful.
Validation complete
[admusr@GuestPMACeco upgrade]$</pre>
3. Execute the following commands to run the fast deployment file:
<pre>$ screen
$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a screen -dr to resume the screen session in the event of a terminal timeout, etc.
</td></tr>
<tr><td>6.
☐</td><td>PMAC GUI: Monitor the configuration</td><td>
1. If not already done so, establish a GUI session on the PMAC server.
2. Navigate to Task Monitoring.


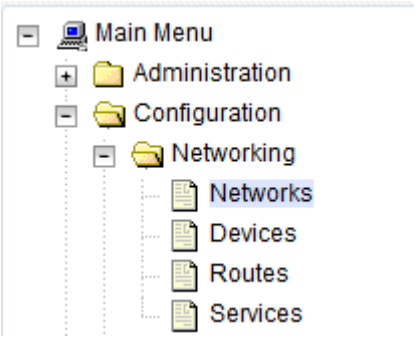
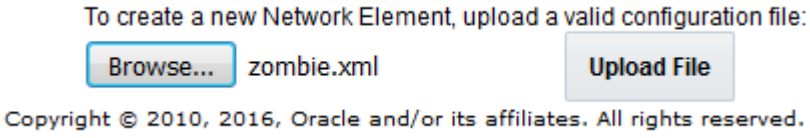
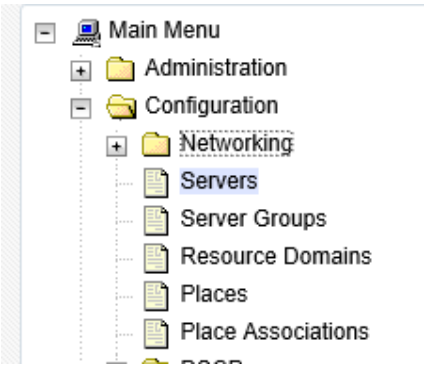
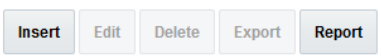
3. Monitor the DSR NOAM TVOE configuration to completion.


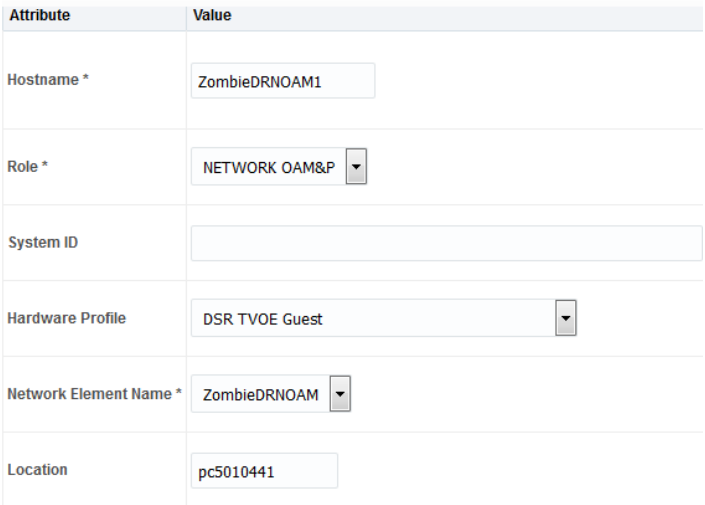
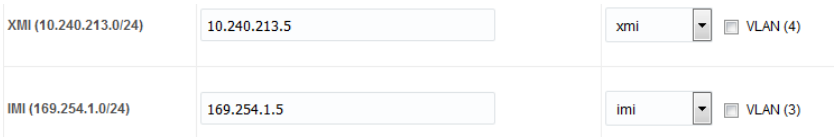
</td></tr>
</table>

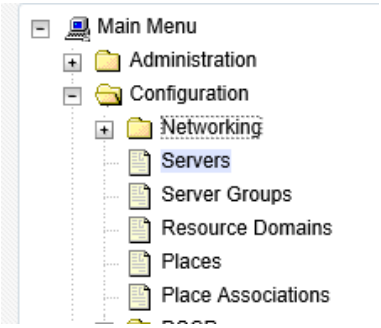
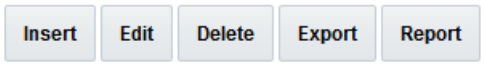
Step#	Procedure	Description

7. ☐	**PMAC Server**: Backup FDC file	Create the **fdc** directory so the DR-NOAM fdc file is backed up by PMAC:
		Issue the following commands:
		1. Create the fdc backup directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc`
		2. Copy the fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/<fdc_file> /usr/TKLC/smac/etc/fdc/`

8. ☐	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 DR-NOAM server. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is **Appname_NEname_NetworkElement.XML**, so for example a DSR2 NOAM network element XML file would have a filename **DSR2_NOAM_NetworkElement.xml**. Alternatively, you can update the sample DSR network element file. It can be found on the management server at: `/usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml` A sample XML file can also be found in 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.
9. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
10. ☐	**PRIMARY NOAM VIP GUI**: Insert the DR NOAM network element	1. Navigate to **Configuration > Networking > Networks**.  2. Click **Browse** and type the pathname to the DR-NOAM network XML file.  3. Click **Upload File** to upload the XML file and configure the DR-NOAM network element. 4. Once the data has been uploaded, a tab displays with the name of your network element. Click this tab to display a screen with the individual networks that are now configured. 
11. ☐	**Primary NOAM VIP GUI**: Insert the 1st DR-NOAM server	1. Navigate to **Configuration > Servers**.  2. Click **Insert** to insert the new DR-NOAM server into servers table.  3. Enter the fields as follows: **Hostname**: <Hostname> **Role**: NETWORK OAM&P

Step#	Procedure	Description
		System ID: <Site System ID> **Hardware Profile**: DSR TVOE Guest **Network Element Name**: [Choose NE from dropdown box] **Adding a new server**  The network interface fields become available with selection choices based on the chosen hardware profile and network element. 4. Type the server IP addresses for the XMI network. Select **XMI** for the interface. **Leave the VLAN checkbox unchecked**. ***Note***: The XMI server IP must match '$DR-NOAM_xmi_IP_address' configured in step 2. 5. Type the server IP addresses for the IMI network. Select **IMI** for the interface. Leave the **VLAN** checkbox unchecked. ***Note***: The IMI server IP must match '$DR-NOAM_xmi_IP_address' configured in step 2.  6. Add the following NTP servers: **NTP Server** / **Preferred?** <TVOE_XMI_IP_Address (DR-NO1)/ TVOE_Mgmt_IP_Address (DR-NO1)> / Yes 7. Click **OK** when you have completed entering all the server data.

Step#	Procedure	Description
12. ☐	**PRIMARY NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  2. From the GUI screen, select the DR-NOAM server and click **Export** to generate the initial configuration data for that server. 
13. ☐	**1st NOAM Server**: Copy configuration file to DR-NOAM NOAM server	1. Obtain a terminal session to the primary NOAM as the **admusr** user. 2. Execute the following command to configure the DR-NOAM server. `$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DR-NOAM_Hostname>.sh admusr@<DR-NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh`

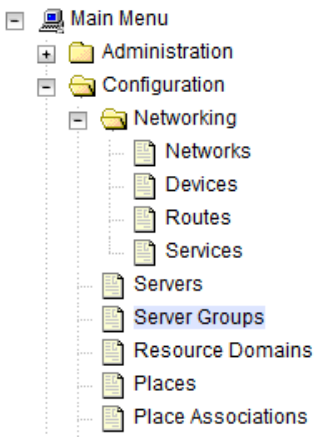
14. ☐	**1st DR-NOAM Server**: Verify configuration was called and reboot the server	1. Establish an SSH session to the DR-NOAM server (DR-NOAM_XMI_IP_address)
		2. Login as the **admusr** user.
		3. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
		4. Verify configuration 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!`
		5. Reboot the server:
		`$ sudo init 6`
		6. Wait for the server to reboot.

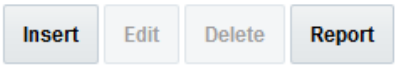
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>15.
☐</td><td>1st DR-NOAM: Configure networking for dedicated NetBackup interface (optional)</td><td>Note: Only execute this step if your DR-NOAM is using a dedicated Ethernet interface for NetBackup.
Obtain a terminal window to the 1st DR-NOAM server by logging in as the admusr user.
<code>$ 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=<NetBackup_Svr_Network_ID>
--netmask=<NO1_NetBackup_NetMask>
--gateway=<NO1_NetBackup_Gateway_IP_Address></code></td></tr>
<tr><td>16.
☐</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.
<code>$ 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</code></td></tr>
<tr><td>17.
☐</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>

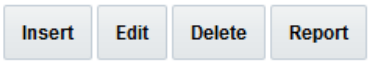
4.2.2 Pair DR-NOAMs

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

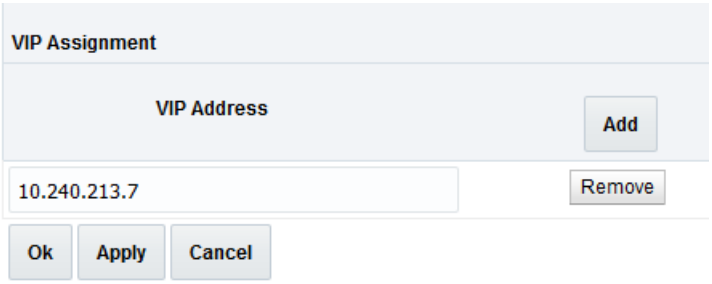
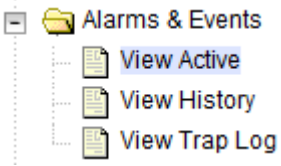
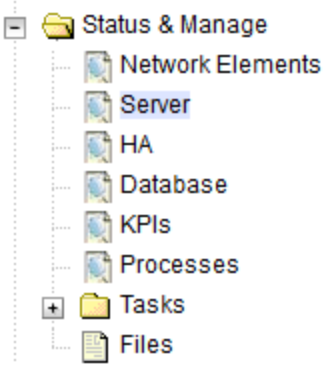
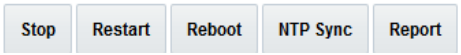
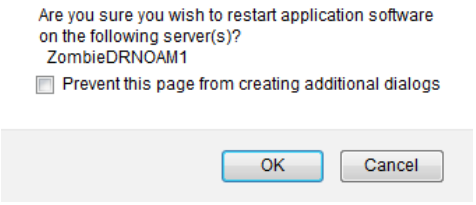
Step#	Procedure	Description
This procedure pairs the DR-NOAM site. ***Prerequisite***: Installation for DR-NOAM site complete. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the primary NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
☐</td><td>Primary NOAM VIP GUI:
Enter DR-NOAM server group data</td><td>1. Navigate to Configuration > Server Groups.
 

2. Click 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
3. Click OK when all fields are filled in.</td></tr>
<tr><td>3.
☐</td><td>Primary NOAM VIP GUI:
Update server group</td><td>1. Select the Server Group that was created in the previous step and click Edit.
 

2. Mark the Include in SG checkboxes for both DR-NOAM servers.
3. Click Apply.
 
</td></tr>
</table>

Step#	Procedure	Description
4. ☐	Primary NOAM VIP GUI: Add DR NOAM VIP	1. Click **Add** for the VIP Address and enter an **IP Address** for the VIP.  2. Click **Apply**. Verify the banner information message states data committed.
5. ☐	**Primary NOAM VIP GUI**: Wait for remote database alarm to clear	1. Navigate to **Alarms & Events > View Active**.  2. Wait for the alarm **Remote Database re-initialization in progress** to be cleared before proceeding.
6. ☐	**Primary NOAM VIP GUI**: Restart 1st DR NOAM server	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  2. Select the 1st DR NOAM server. Click **Restart**.  3. Click **OK** on the confirmation screen.  4. Wait for the restart to complete 3-5 minutes before proceeding.

Step#	Procedure	Description
7. ☐	**Primary NOAM VIP GUI**: Restart the application on the 2nd DR NOAM server	**Repeat** steps 6. , but this time, select the 2nd DR NOAM server.

8. ☐	**Primary NOAM**: Modify DSR OAM process	1. Establish an SSH session to the primary NOAM, login as **admusr**.
		2. 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)

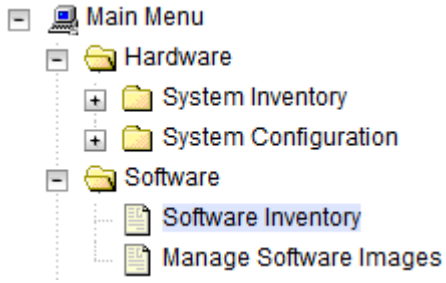
Procedure 10. Install NetBackup Client (Optional)

Step#	Procedure	Description
This procedure downloads and installs 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Install NetBackup client software	If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools (push configuration), then use NetBackup Client Install/Upgrade with NBAutoInstall. ***Note***: This is not common. If the answer to the previous question is not known, then use Appendix H.1 NetBackup Client Installation Using PLATCFG.
2. ☐	Install NetBackup client software	Choose the same method used in step 1 to install NetBackup on the 2nd NOAM.

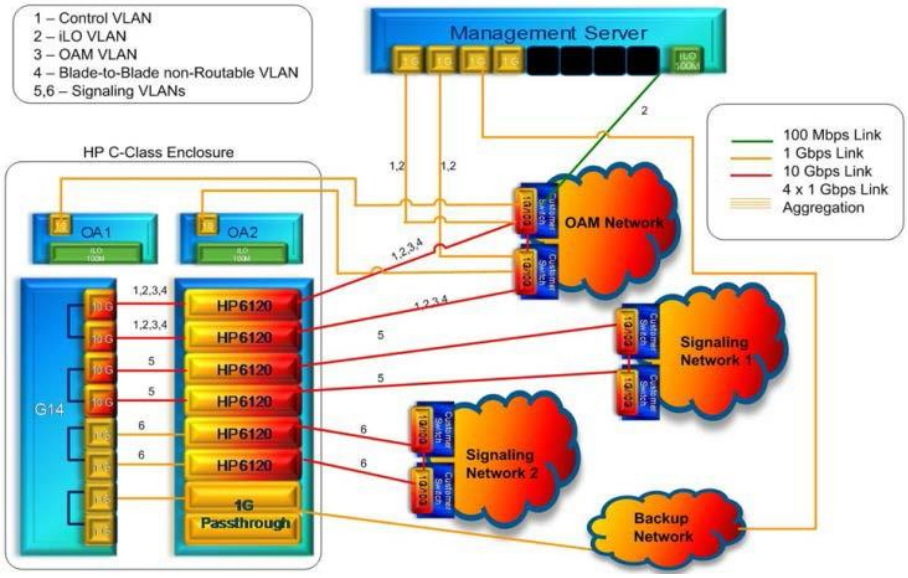
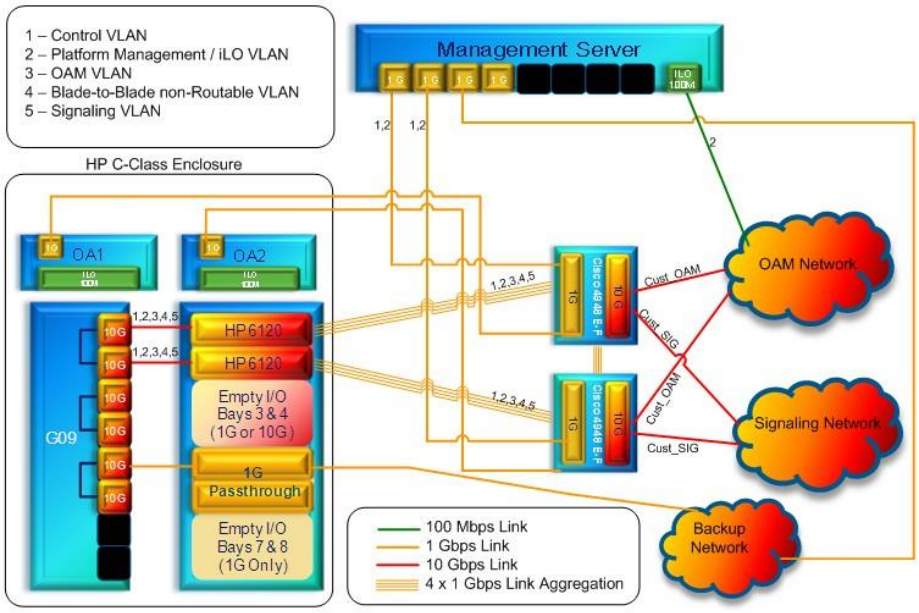
4.3 Install and Configure SOAM Servers

4.3.1 Configure SOAM TVOE Server Blades

Procedure 11. Configure SOAM TVOE Server Blades

Step#	Procedure	Description
This procedure configures TVOE on the server blades that host DSR SOAM VMs. It details the configuration for a single server blade and should be repeated for every TVOE blade that was IPMed for this install. ***Note***: TVOE should only be installed on Blade servers run as DSR SOAMs. They should NOT be installed on Blade servers intended to run as DSR MPs. ***Prerequisite***: TVOE OS has been installed on the target server blades as per instructions in [6]. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC Server**: Exchange SSH keys between PMAC and TVOE server	Use the PMAC GUI to determine the control network IP address of the TVOE server. 1. From the PMAC GUI, navigate to **Software > Software Inventory**.  2. Note the IP address TVOE server.  3. From a terminal window connection on the PMAC, login as the **admusr** user. 4. Exchange SSH keys between the PMAC and the TVOE server using the keyexchange utility and the control network IP address for the TVOE blade server. 5. When asked for the password, type the password for the TVOE server. `$ keyexchange admusr@<TVOE_Control_Blade_IP_address>`

2. ☐	**TVOE Server**: Login and copy configuration scripts from PMAC	1. Login as **admusr** on the TVOE server using the control IP address noted above.
		2. Execute the following commands:
		You can copy the scripts to any path even on /home/admusr. In this case, instead of /usr/TKLC, the new path should be used, for example, /home/admusr.
		`$ sudo scp admusr@<PMAC_Control_IP_address>:/usr/TKLC/smac/etc/TVOE* /usr/TKLC/`
		`$ sudo chmod 777 /usr/TKLC/TVOE*`

Step#	Procedure	escription
3. ☐	**TVOE Server**: Mezzanine card/ segregated OAM/XMI network configuration	Perform this step if your TVOE server blade DOES have mezzanine cards AND you are running OAM/XMI traffic on a separate physical network (example below). If you do not have mezzanine cards, skip this step.  Execute the following command: `$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID> mezz`
4. ☐	**TVOE Server**: No mezzanine card/ No segregated OAM/XMI network configuration	Perform this step if your TVOE server blade **DOES NOT** have mezzanine cards AND/OR you are NOT running OAM/XMI traffic over a separate physical network (example below).  Execute the following command: `$ sudo /usr/TKLC/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID>`

Step#	Procedure	escription

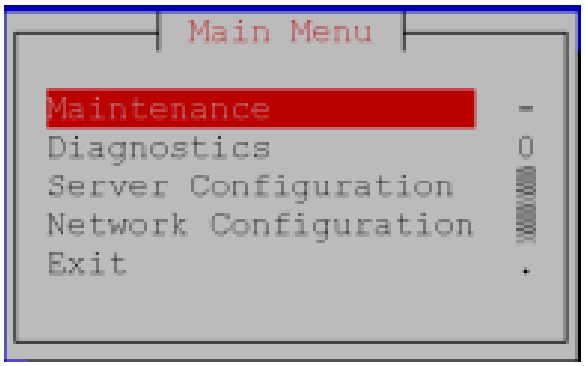
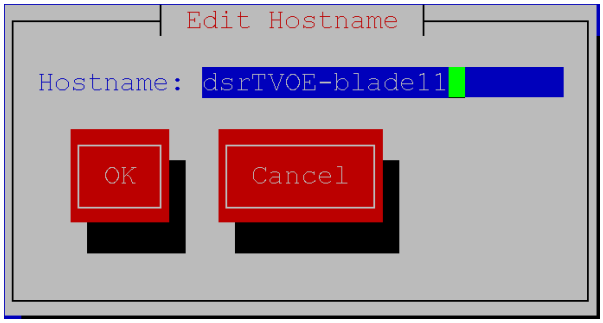
5. ☐	**TVOE Server**: Verify TVOE configuration	XMI_VLAN_ID is the VLAN ID for the XMI network in this installation, and IMI_VLAN_ID is the VLAN ID for the IMI network in this installation. For deployments with aggregation switches, the IMI and XMI VLAN IDs are the values of the **INTERNAL-IMI** and **INTERNAL-XMI** VLAN IDs, respectively. For layer-2 only deployments, the IMI and XMI VLAN IDs are obtained from the customer.
		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!`
		Note: If for any reason, you run the wrong version of the TVOEcfg.sh command, you can execute the following command to reset the network configuration so you can **repeat** either step 3 or 4.
		`sudo ./usr/TKLC/TVOEclean.sh`

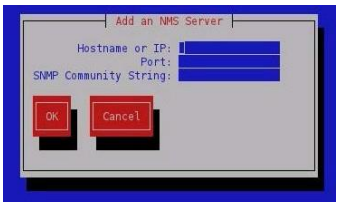
6. ☐	**TVOE Server**: Configure XMI IP and default route	1. Configure IP address on the XMI network:
		`$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=xmi --address=<TVOE_XMI_IP_ADDRESS> --netmask=<TVOE_XMI_Netmask/Prefix>`
		`/sys/class/net/bond1/bonding/primary has 0 lines, nothing to do.`
		`Bridge xmi was added.`
		2. Restart network services:
		`$ sudo service network restart`
		`[wait for the prompt to return]`
		3. 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.`

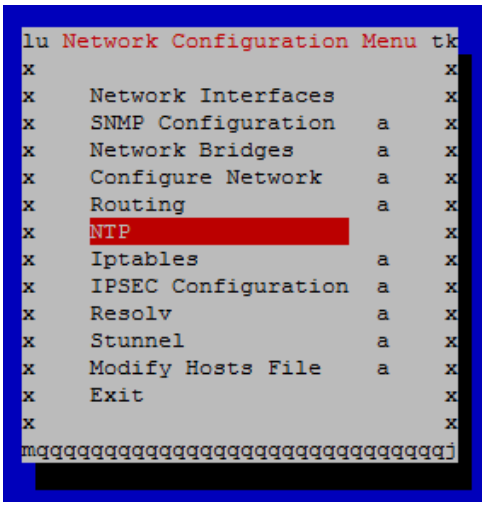
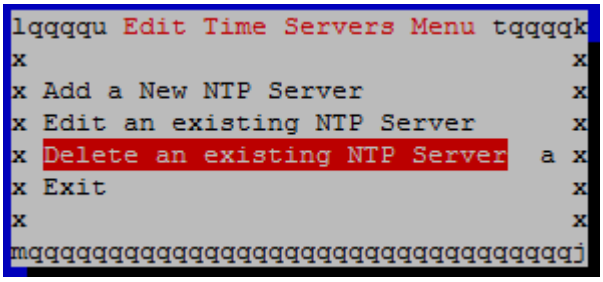
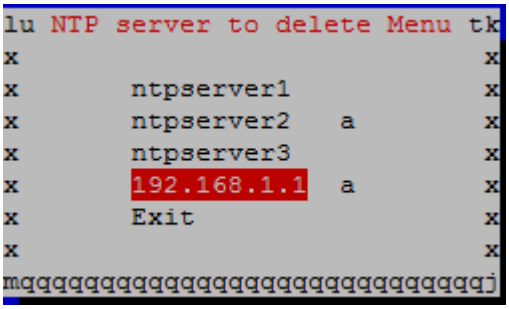
Step#	Procedure	escription

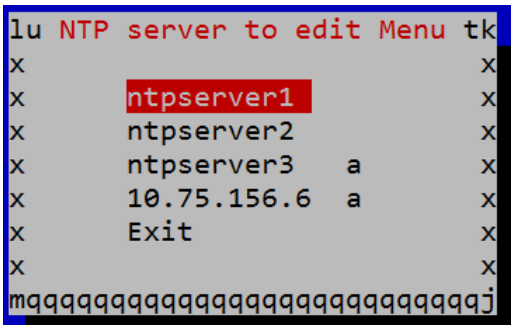
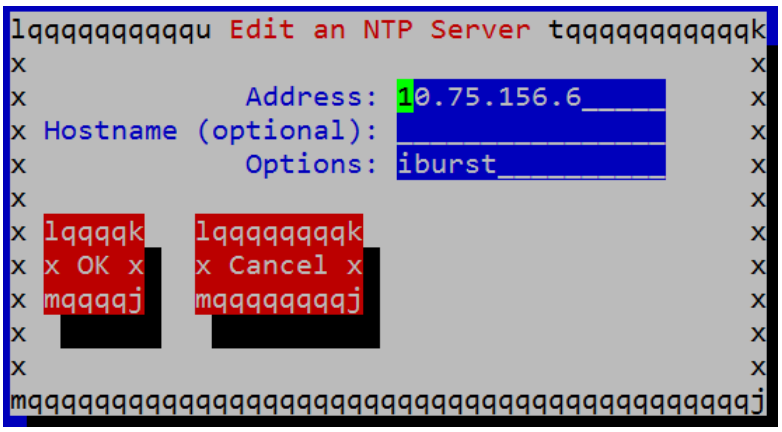
7. ☐	**TVOE Server**: Configure NetBackup dedicated interface and bridge (optional)	In these examples, <interface> is replaced with the actual ethernet interface that is used as the dedicated NetBackup port. For instance, **eth01** or **eth22**.
		Un-bonded ethernet interface:
		`$ sudo /usr/TKLC/plat/bin/netAdm 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`

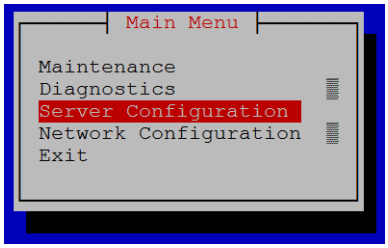
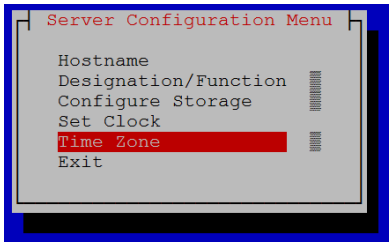
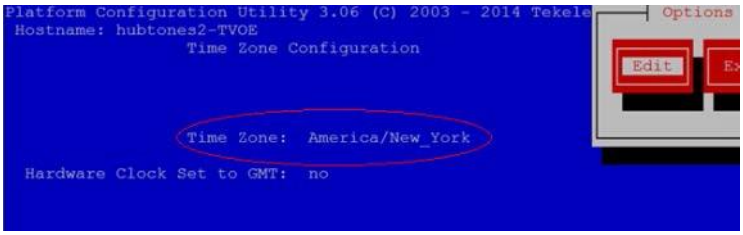
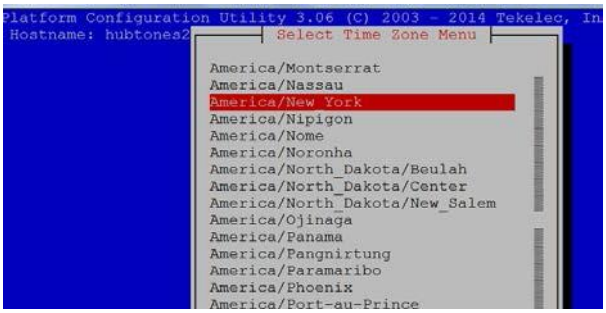
8. ☐	**TVOE Server**: Configure networking for dedicated NetBackup interface (optional)	***Note***: Only execute this step if using a dedicated ethernet interface for NetBackup.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=NetBackup --type=Ethernet --onboot=yes --address=<NO1 NetBackup IP Adress> --netmask=<NO1_NetBackup_NetMask>`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NetBackup_Svr_Network_ID> --netmask=<NO1_NetBackup_NetMask> --gateway=<NO1_NetBackup_Gateway_IP_Address>`

Step#	Procedure	escription
9. ☐	**TVOE Server**: Set hostname	`$ sudo su - platcfg`  4. Navigate to **Server Configuration > Hostname > Edit** and enter a new hostname for your server:  5. Click **OK** and click **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 does not display on your command prompt unless you log out and log back in again.

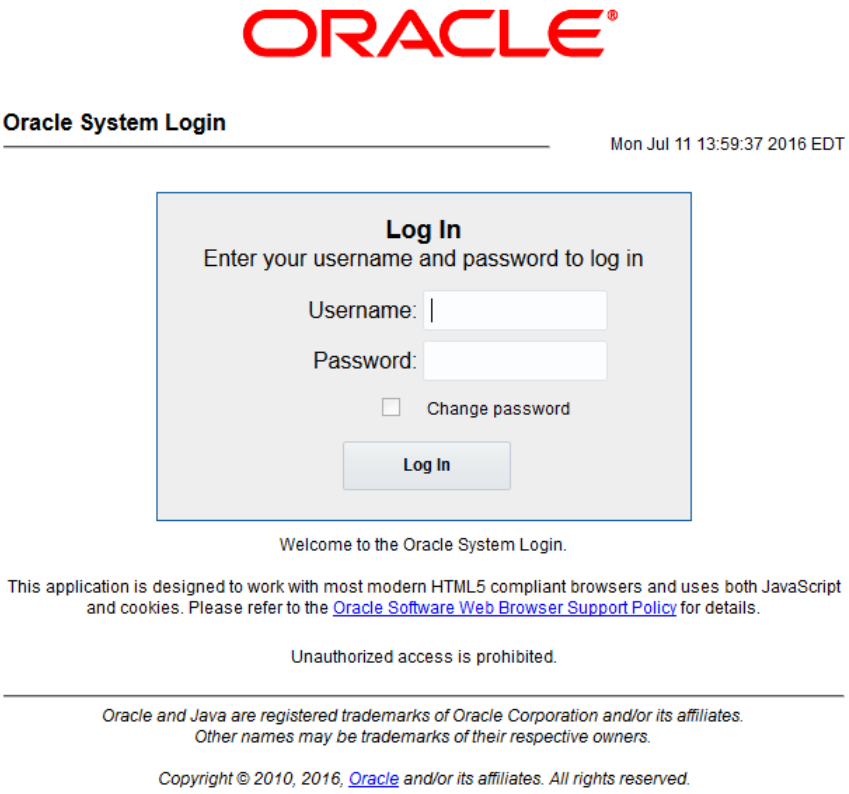
Step#	Procedure	escription
10. ☐	**TVOE Server**: Configure SNMP	1. From the platcfg main menu, navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.  2. Click **Edit**. 3. Click **Add a New NMS Server**.  4. Enter the following NMS servers, clicking **OK** after each one and then selecting the **Add NMS** option again: 5. Enter the **Hostname/IP** of the customer NMS server. 6. For port, enter **162**. 7. For Community String, enter the community string provided in the customer specific NAPD document. 8. Enter the **IP** of the SOAM VIP 9. Click **Exit**. 10. Select **Yes** when asked to restart the Alarm Routing Service. 11. Once done, click **Exit** to quit to the platcfg main menu.

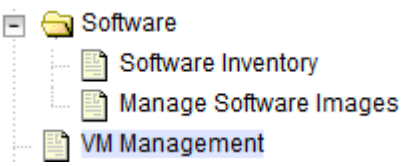
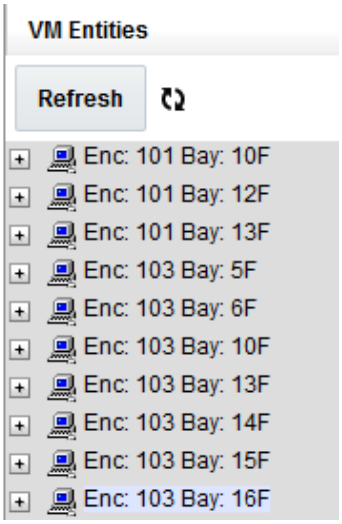
Step#	Procedure	escription
11. ☐	**RMS iLO/iLOM**: Delete PMAC VM as NTP source on RMS	1. Navigate to **Network Configuration > NTP**.  2. Select **Delete an existing NTP Server**.  3. Select the PMAC VM Control **IP** and click **Enter**.  The NTP Menu screen displays.

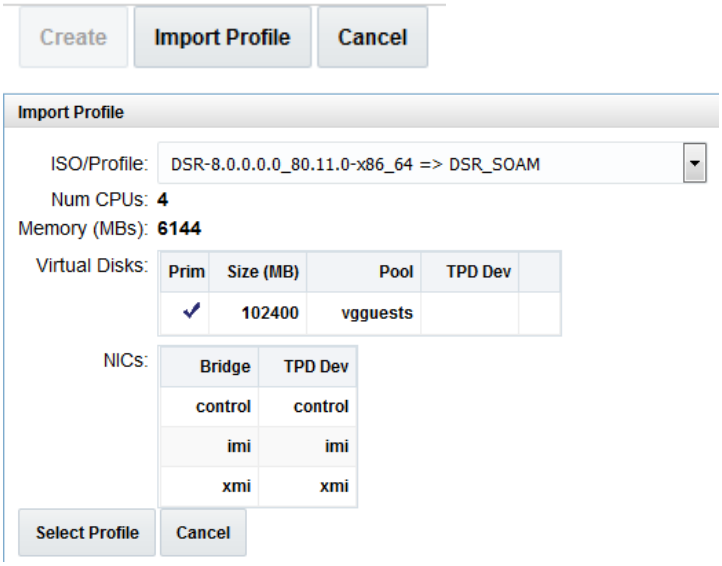
Step#	Procedure	escription
12. ☐	**TVOE Server**: Configure NTP. Edit an existing NTP server	Edit an existing NTP server.  1. Select appropriate NTP server and edit the details.  2. Enter appropriate data and click **OK**. 3. Click **Exit** to return to the platcfg menu.

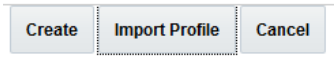
Step#	Procedure	escription
13. ☐	**TVOE Server**: Configure time zone	1. If not already in the utility, then use this command: `$ sudo su - platcfg` 2. Navigate to Server Configuration > Time Zone.    If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction. 3. Click **Edit**.  4. Select the desired time zone from the list and click **Enter**. 5. Continue clicking **Exit** until you are out of the platcfg program.
14. ☐	TVOE Server: Reboot	Reboot the server by executing the following command: `$ sudo init 6`
15. ☐	**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.
16. ☐	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

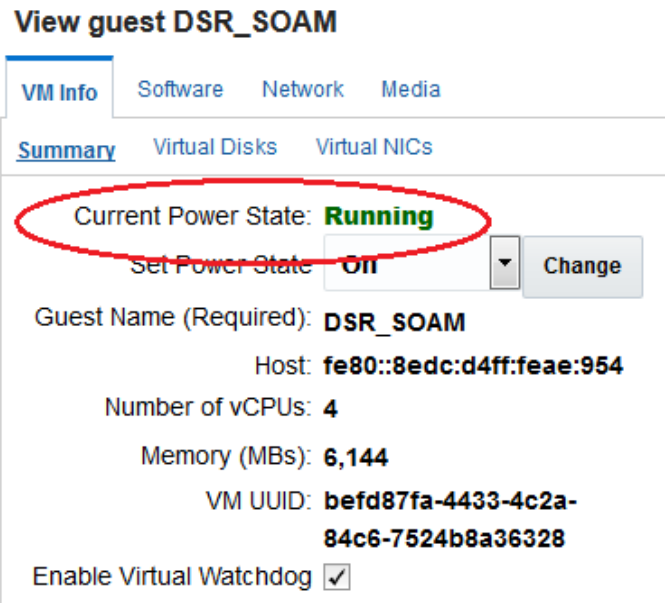
Step#	Procedure	Description
This procedure creates a DSR SOAM virtual machine (referred to as a guest) on a TVOE server blade. It must be repeated for every SOAM server you want to install. ***Prerequisite***: TVOE has been installed and configured on the target blade server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_Mgmt_Network_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
2. ☐	**PMAC GUI**: Navigate to VM management of the target server blade	1. Navigate to **VM Management**.  2. Select the TVOE server blade server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window.  3. Click **Create Guest**.

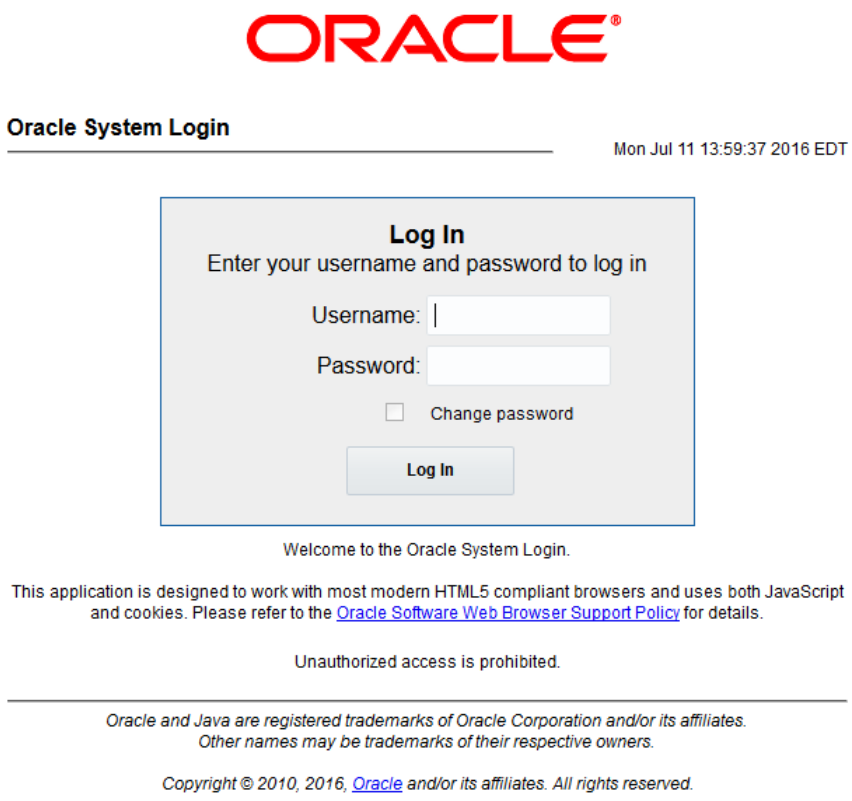
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>3.
☐</td><td>PMAC GUI:
Configure VM guest parameters</td><td>
1. Click Import Profile.


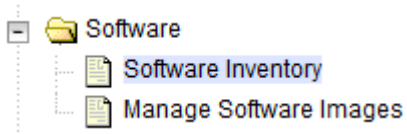
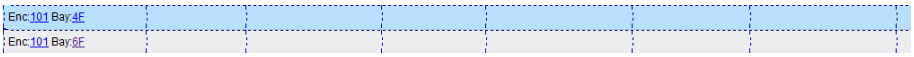
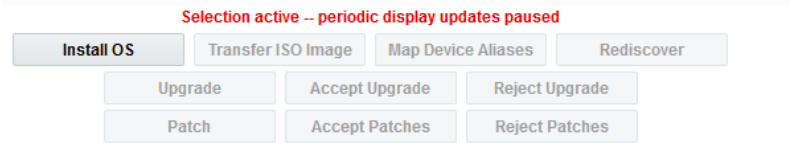
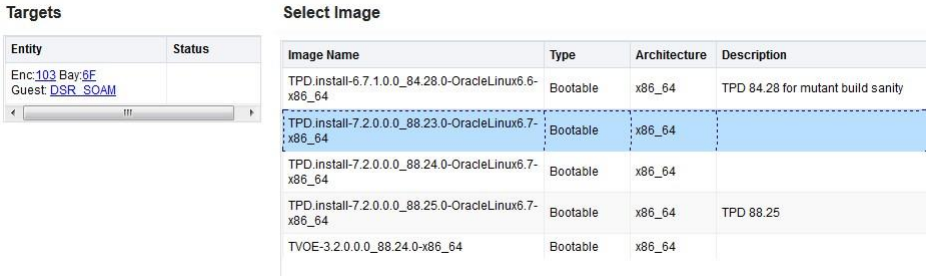
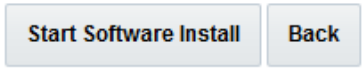
2. From the ISO/Profile list, select the entry that matches depending on the hardware your SOAM VM TVOE server is running on and your preference for NetBackup interfaces:
Note: Select the LARGE SOAM profile specific to the release if the number of connections is greater than 5k.
<table>
<tr><th>SOAM VM TVOE Hardware Type(s)</th><th>Dedicated Netbackup Interface?</th><th>Choose Profile (<Application ISO NAME>)➔</th></tr>
<tr><td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td><td>No</td><td>DSR_SOAM</td></tr>
<tr><td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td><td>Yes</td><td>DSR_SOAM_NBD</td></tr>
</table>
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM
3. Click Select Profile.
4. You can edit the name, if you wish. For instance, DSR_SOAM_A or DSR_SOAM_B. (This does not become the ultimate hostname. It is just an internal tag for the VM host manager.)
5. Click Create.


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

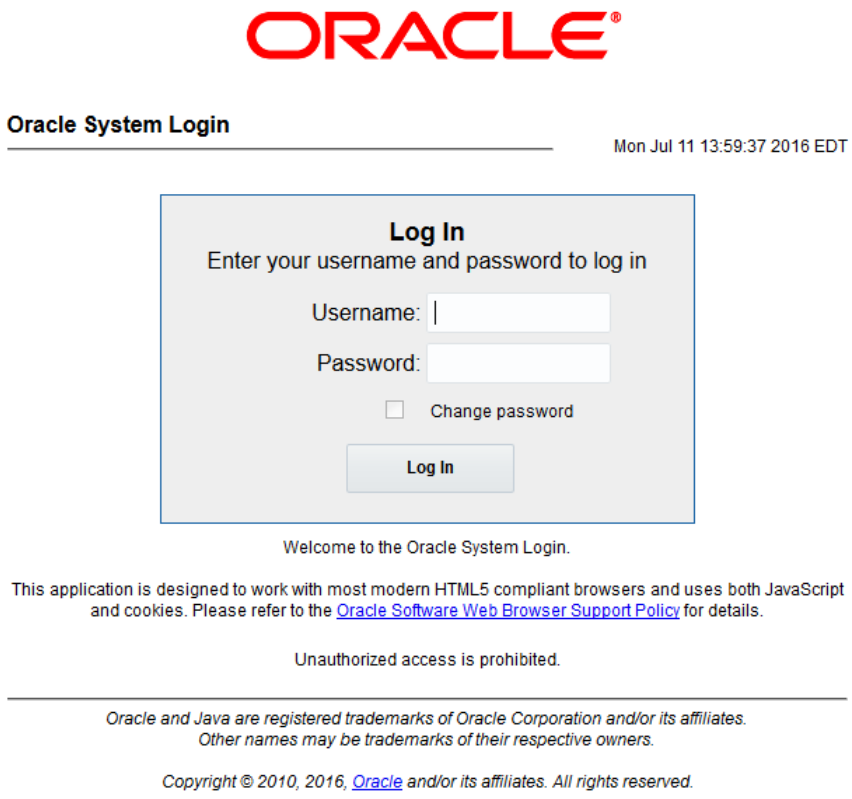
Step#	Procedure	Description
4. ☐	**PMAC GUI**: Wait for guest creation to complete	1. Navigate to **Task Monitoring** to monitor the progress of the guest creation task. A separate task displays for each guest creation you have launched. 2. Wait or refresh the screen until you see that the guest creation task has completed successfully. 
5. ☐	**PMAC GUI**: Verify guest machine is running	1. Navigate to **VM Management**. 2. Select the TVOE server blade on which the guest machine was just created. 3. 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 SOAM VMs (for instance, the standby SOAM) that must be created.

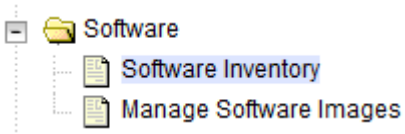
Procedure 13. IPM Blades and VMs

Step#	Procedure	Description
This procedure installs TPD on blade servers and blade server guest VMS. ***Prerequisites***: • Enclosures containing the blade servers targeted for IPM that have been configured. • TVOE has been installed and configured on blade servers that will host DSR NOAM VMs. • DSR NOAM and SOAM guest VMs have been created successfully. ***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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_Mgmt_Network_IP_Address>` 2. Login as the **guiadmin** user. 

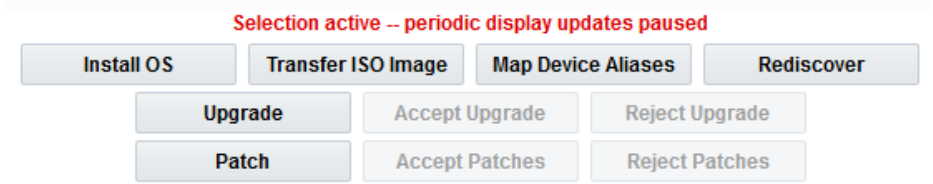
Step#	Procedure	Description
2. ☐	**PMAC GUI**: Select servers for OS install	1. Navigate to **Software > Software Inventory**.  2. Select the servers (VMs, IPFEs, MPs, etc.) you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows are highlighted in green. ***Note***: VMs have the text **Guest**: **<VM_GUEST_NAME>** underneath the physical blade or RMS that hosts them.  3. Click Install OS. 
3. ☐	**PMAC GUI**: Initiate OS install	1. The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  2. Click **Start Software Install**.  3. When a confirmation screen displays, click **OK** to proceed.
4. ☐	**PMAC GUI**: Monitor OS install	Navigate to **Task Monitoring** to monitor the progress of the OS Installation background task. A separate task displays for each blade affected.  When the installation is complete, the task changes to green and the progress bar indicates 100%.

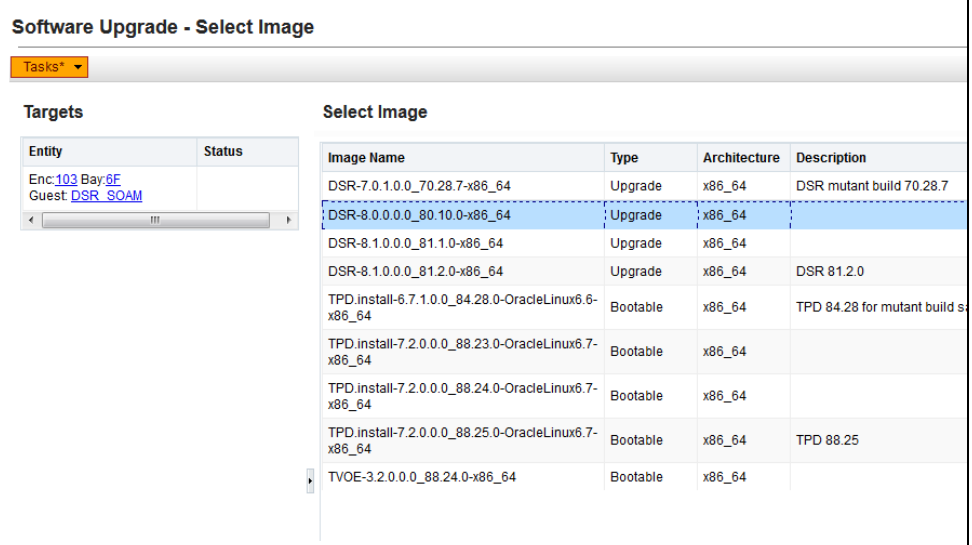
Procedure 14. Install the Application Software

Step#	Procedure	Description
This procedure installs 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_Mgmt_Network_IP_Address>` 2. Login as the **guiadmin** user. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
☐</td><td>PMAC GUI: Select servers for application install</td><td>
1. Navigate to Software > Software Inventory.


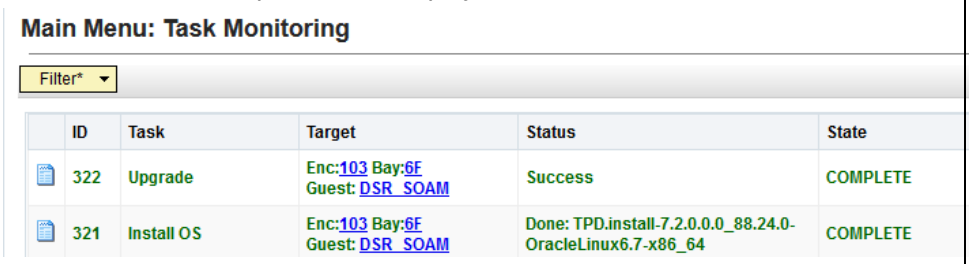
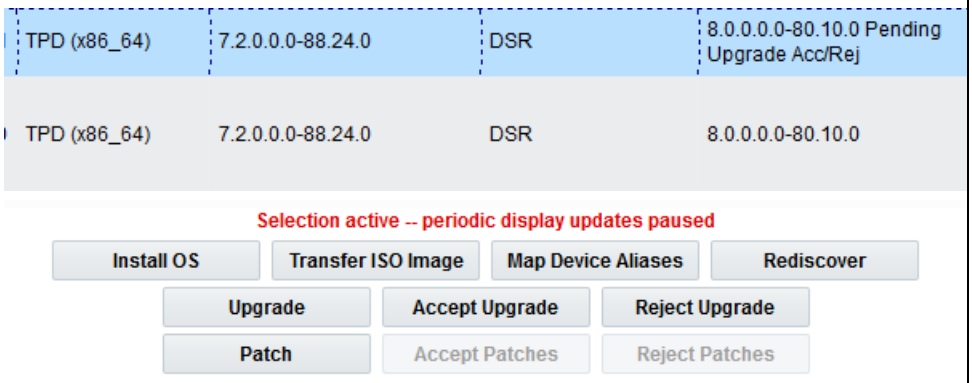
2. Select the servers on which the application is to be installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows are highlighted in green.
Note: VMs have the text Guest: <VM_GUEST_NAME> underneath the physical blade that hosts them.


3. Click Upgrade.


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


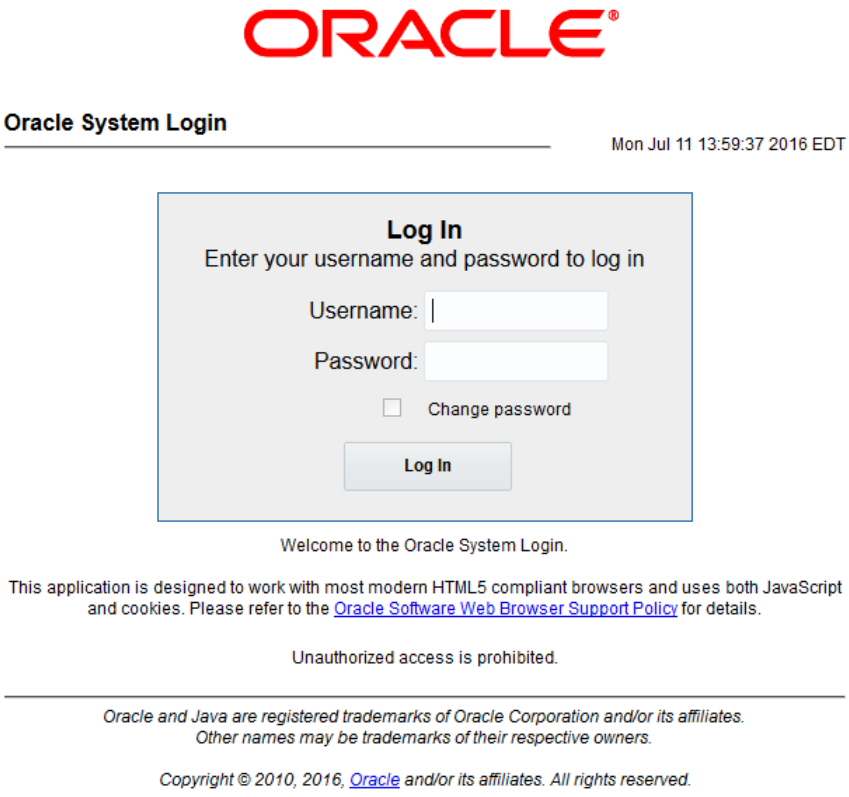
2. Click Start Software Upgrade.

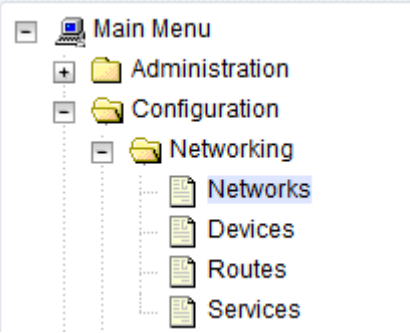
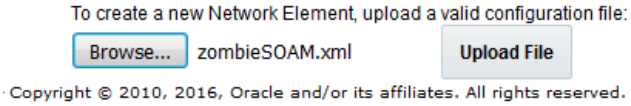
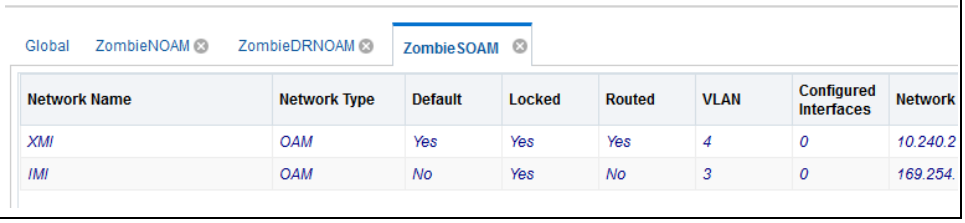

3. When a confirmation screen displays, click OK to proceed with the install.
</td></tr>
</table>

Step#	Procedure	Description
4. ☐	**PMAC GUI**: Monitor the installation status	Navigate to **Task Monitoring** to monitor the progress of the Application Installation task. A separate task displays for each blade affected.  When the installation is complete, the task changes to green and the progress bar indicates 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 **Accept Upgrade**.  ***Note***: Once the upgrade has been accepted, the App version changes from **Pending Acc/Rej** to the version number of the application.

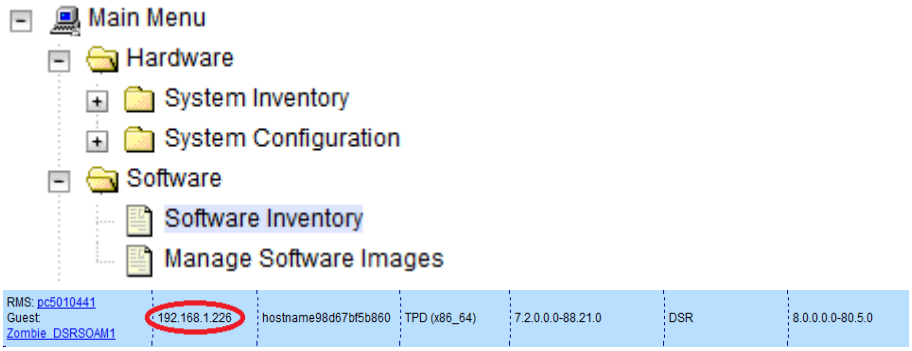
4.3.2 Configure SOAMs

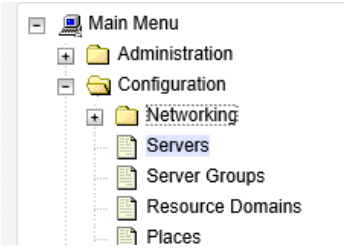
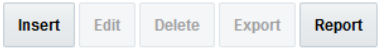
Procedure 15. Configure SOAM NE

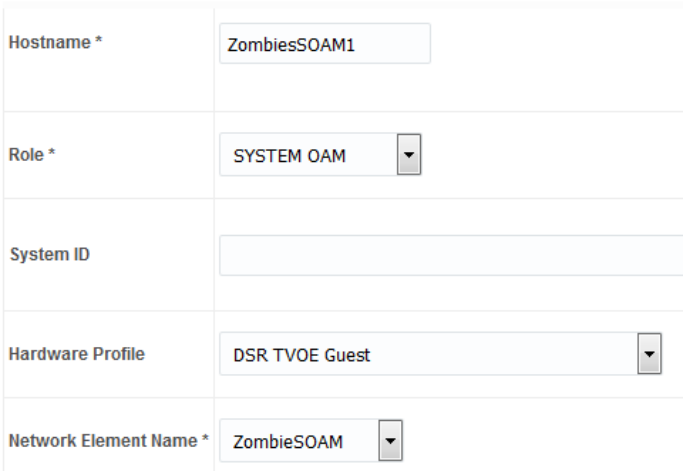
Step#	Procedure	Description
This procedure configures the SOAM network element. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

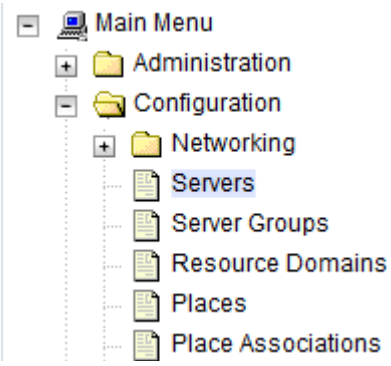
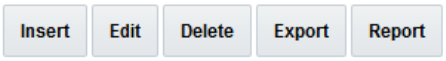
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Create the SOAM network element using an XML file	1. Navigate to **Networking > Networks**.  Refer to Sample Network Element and Hardware Profiles for a sample network element xml file. 2. Click **Browse** and type the pathname to the SOAM network XML file.  3. Click **Upload File** to upload the XML file and configure the SOAM network element. Once the data has been uploaded, a tab displays with the name of your network element. Click this folder to display the list of individual networks now configured. 

Procedure 16. Configure the SOAM Servers

Step#	Procedure	Description
This procedure configures 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 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. 1. From the PMAC GUI, navigate to **Software > Software Inventory**.  2. Note the IP address for the SOAM server. 3. From a terminal window connection on the PMAC, login as the **admusr** user. 4. Exchange SSH keys between the PMAC and the SOAM server using the keyexchange utility and the control network IP address for the SOAM server. 5. When asked for the password, type the password for the **admusr**. `$ 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. 1. 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. 2. When asked for the password, enter the **admusr** password for the PMAC server. `$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address>`

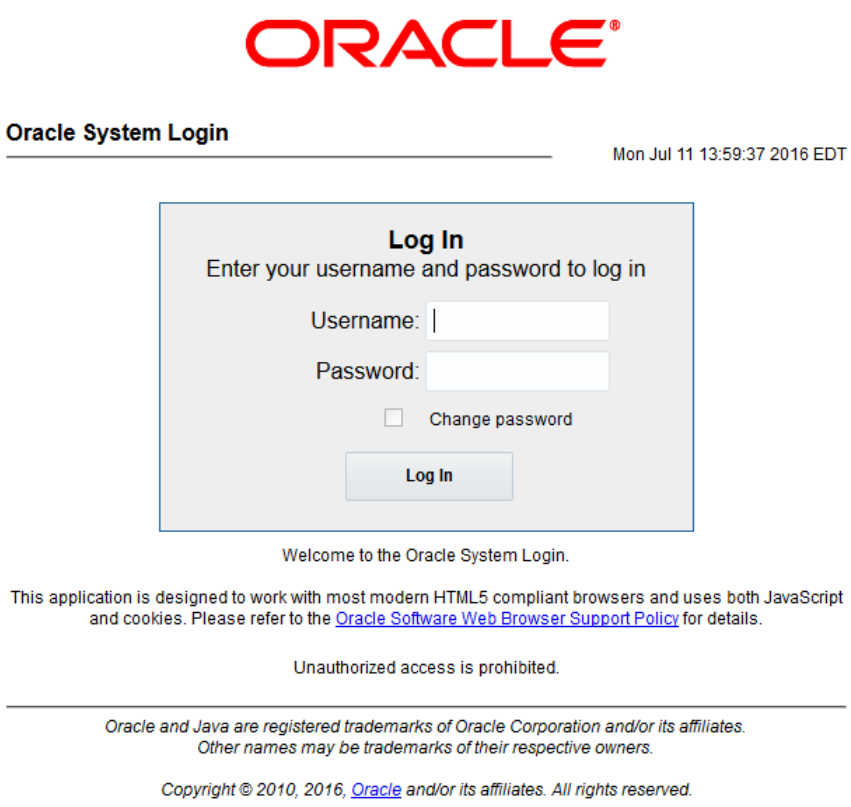
Step#	Procedure	Description
3. ☐	NOAM VIP GUI: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
4. ☐	**NOAM VIP GUI**: Insert the 1st SOAM server	1. Navigate to **Configuration > Servers**.  2. Click **Insert** to insert the 1st SOAM server into servers table (the first or server).  3. Enter the fields as follows: **Hostname**: <Hostname> **Role**: SYSTEM OAM **System ID**: <Site System ID>

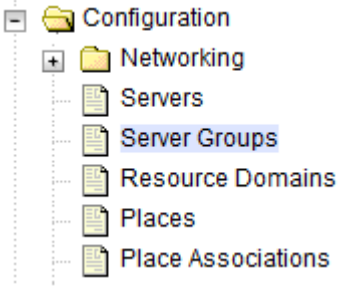
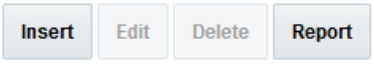
Step#	Procedure	Description
		Hardware Profile: DSR TVOE Guest **Network Element Name**: [Choose NE from dropdown box] **Adding a new server**  The network interface fields become available with selection choices based on the chosen hardware profile and network element. 4. Type the server IP addresses for the XMI network. Select XMI for the interface. Leave the VLAN checkbox unchecked. 5. Type the server IP addresses for the IMI network. Select IMI for the interface. Leave the VLAN checkbox unchecked.  6. Add the following NTP servers: **NTP Server** | **Preferred?** <TVOE_XMI_IP_Address (SO1)> | Yes 7. Click **OK** when you have completed entering all the server data.

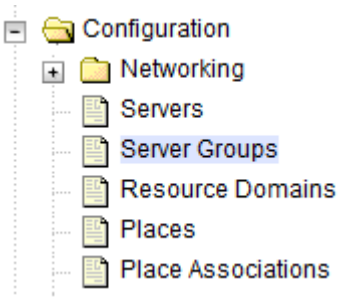
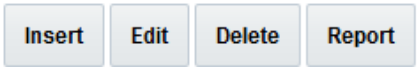
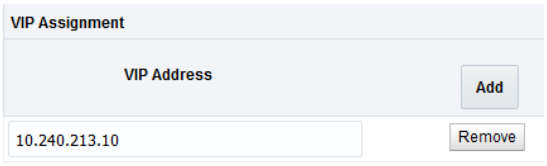
Step#	Procedure	Description
5. ☐	**NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  2. From the GUI screen, select the SOAM server and click **Export** to generate the initial configuration data for that server. 
6. ☐	**NOAM VIP**: Copy configuration file to 1st SOAM server	1. Obtain a terminal session to the NOAM VIP as the **admusr** user. 2. Use the **awpushcfg** utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the 1st SOAM server, using the Control network IP address for the 1st SOAM server. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user is asked for the following: • IP address of the local PMAC server: Use the management network address from the PMAC. • Username: Use **admusr** • Control network IP address for the target server: In this case, enter the control IP for the 1st SOAM server. • Hostname of the target server: Enter the server name configured in step 4.

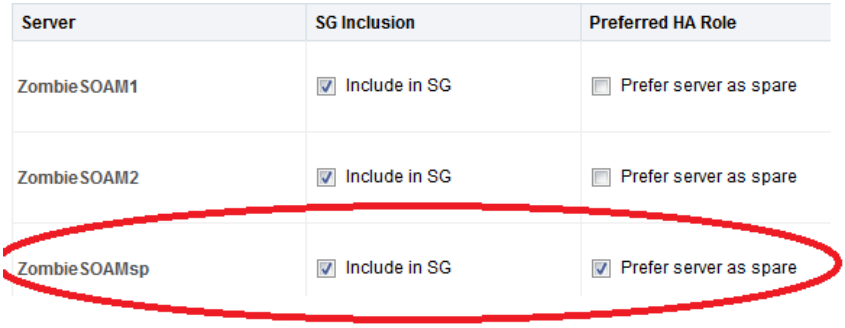
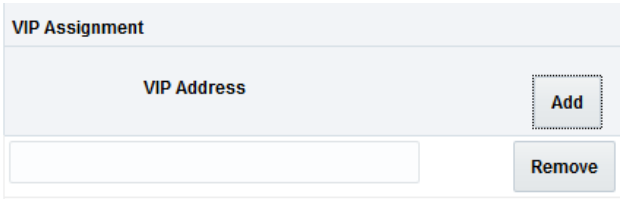
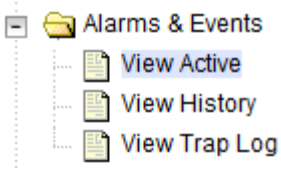
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>7.
☐</td><td>1st SOAM Server: Verify awpushcfg was called and reboot the server</td><td>1. Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the NOAM VIP terminal console.
<code>$ ssh admusr@<SO1_Control_IP></code>
2. Login as the admusr user.
3. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server.
4. Verify awpushcfg was called by checking the following file.
<code>$ sudo cat /var/TKLC/appw/logs/Process/install.log</code>
Verify the following message is displayed:
<code>[SUCCESS] script completed successfully!</code>
5. Reboot the server.
<code>$ sudo init 6</code>
6. Wait for the server to reboot.</td></tr>
<tr><td>8.
☐</td><td>1st SOAM Server: Verify server health</td><td>Execute the following command on the 1st SOAM server and make sure that no errors are returned:
<code>$ 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</code></td></tr>
<tr><td>9.
☐</td><td>Insert and Configure the 2nd SOAM server</td><td>Repeat this procedure to insert and configure the 2nd SOAM server:
<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><TVOE_XMI_IP_Address (SO2)></td><td>Yes</td></tr></table>Instead of data for the 1st SOAM server, insert the network data for the 2nd SOAM server, transfer the TKLCConfigData file to the 2nd SOAM server, and reboot the 2nd SOAM server when prompted at a terminal window.</td></tr>
<tr><td>10.
☐</td><td>Install NetBackup client software on SOAMs (optional)</td><td>If you are using NetBackup at this site, then execute Procedure 10. Install NetBackup Client (Optional) again to install the NetBackup Client on all SOAM servers.</td></tr>
</table>

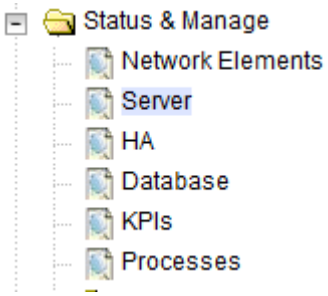
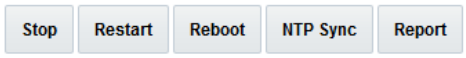
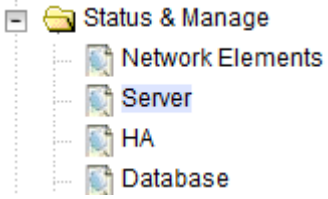
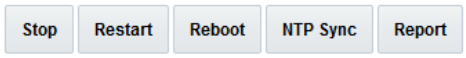
Procedure 17. Configure the SOAM Server Group

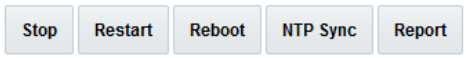
Step#	Procedure	Description
This procedure configures the SOAM server group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Enter SOAM server group data	Allow approximately **5 minutes** for the 2nd SOAM server to reboot. 1. Navigate to the GUI **Configuration > Server Groups**.  2. Select **Insert**.  3. 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 4. Click **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 before the active/standby SOAMs.

Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Edit the SOAM server group and add a VIP address	1. From the GUI, navigate to **Configuration > Server Groups**.  2. Select the new SOAM server group and click **Edit**.  3. Add both SOAM servers to the server group primary site by marking the **Include in SG** checkbox. 4. Do not check any of the **Preferred Spare** checkboxes.  5. Click **Apply**. 6. Add a SOAM VIP by clicking **Add**. Type the **VIP Address** and click **OK**. 

Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: Edit the SOAM server group and add preferred spares for site redundancy (optional)	If the Two Site Redundancy feature is wanted for the SOAM server group, add a SOAM server that is located in its server group secondary site by marking the **Include in SG** checkbox. Also, mark the **Preferred Spare** checkbox.  If the Three Site Redundancy feature is wanted for the SOAM server group, add an additional SOAM server that is located in its server group tertiary site by marking the **Include in SG** checkbox. Also, mark the **Preferred Spare** checkbox. ***Note***: The preferred spare servers must be server group secondary and tertiary sites. There should be servers from three separate sites (locations). For more information about server group secondary site, tertiary site, or site redundancy, see the 1.3 Terminology section.
5. ☐	**NOAM VIP GUI**: Edit the SOAM server group and add additional SOAM VIPs (optional)	1. To add additional SOAM VIPs, click **Add**. 2. Type the **VIP Address**. 3. Click **OK**. ***Note***: Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs. 
6. ☐	**NOAM VIP GUI**: Wait for remote database alarm to clear	Navigate to **Alarms & Events > View Active**.  Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.

Step#	Procedure	Description
7. ☐	**NOAM VIP GUI**: Restart 1st SOAM server	1. From the NOAMP GUI, select **Status & Manage > Server**.  2. Select the **1st** SOAM server. 3. Click **Restart**. 4. Click **OK** on the confirmation screen. 5. Wait for restart to complete. 
8. ☐	**NOAM VIP GUI**: Restart 2nd SOAM server	1. From the NOAMP GUI, select **Status & Manage > Server**.  2. Select the **2nd** SOAM server. 3. Click **Restart**. 4. Click **OK** on the confirmation screen. 5. Wait for restart to complete. 

Step#	Procedure	Description
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. 1. If additional preferred spare servers are configured for Secondary and/or Tertiary Sites, navigate to **Status & Manage > Server**.  2. Select all **Preferred Spare** SOAM servers. 3. Click **Restart**. 4. Click **OK** on the confirmation screen. 

Procedure 18. Activate PCA (PCA Only)

Step#	Procedure	Description
This procedure activates 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	(PCA Only) Activate PCA Feature	If you are installing PCA, execute applicable procedures (added SOAM site activation or complete system activation) from [7] to activate PCA. ***Note***: If not all SOAM sites are ready at this point, then you should repeat activation for each **new** SOAM site that comes online. ***Note***: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

Procedure 19. Activate DCA (DCA Only)

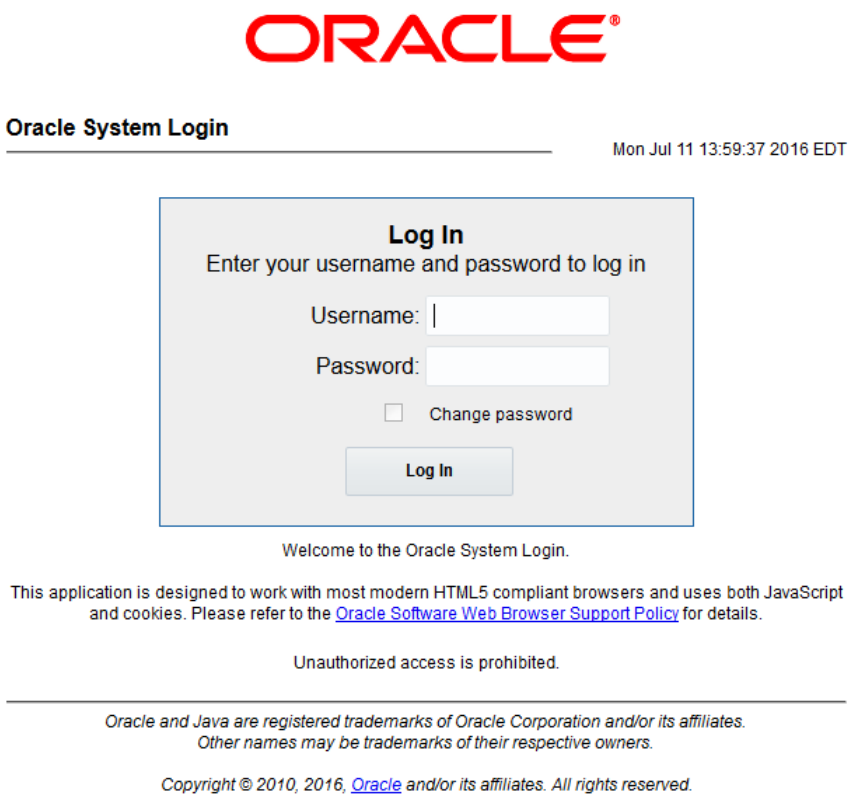
Step#	Procedure	Description
This procedure activates DCA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	(DCA Only) Activate PCA Feature	If you are installing DCA, execute procedures [11] to activate DCA Framework and Feature. ***Note***: If not all SOAM sites are ready at this point, then you should repeat activation for each **new** SOAM site that comes online. ***Note***: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

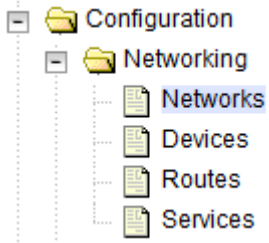
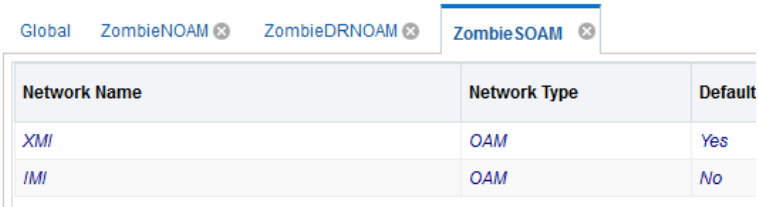
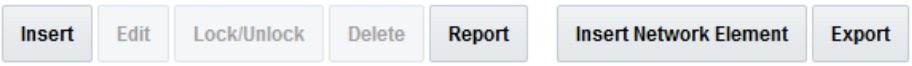
4.4 Configure MP Servers

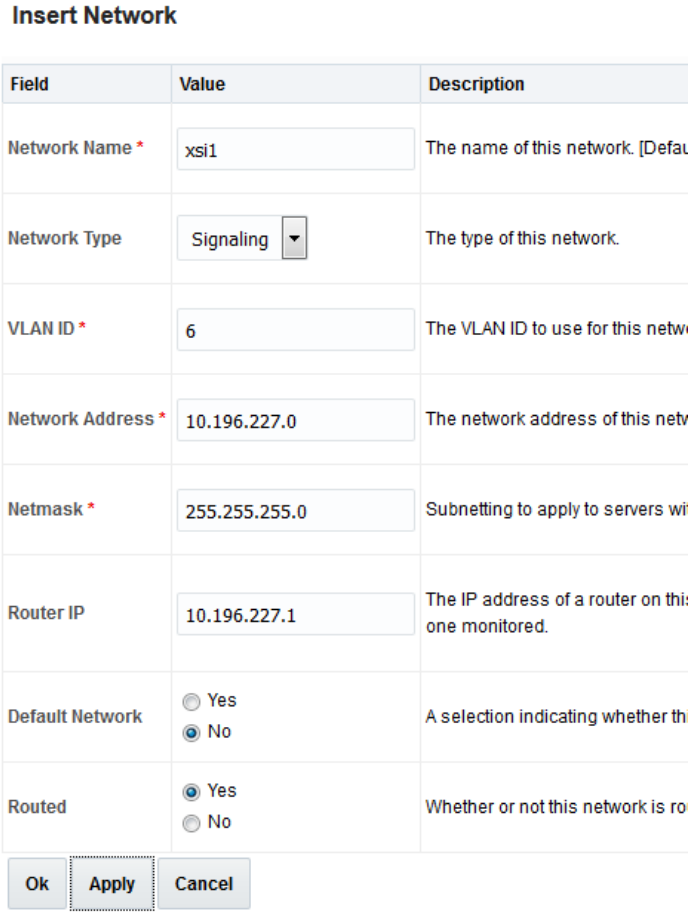
4.4.1 Configure MP Blade Servers

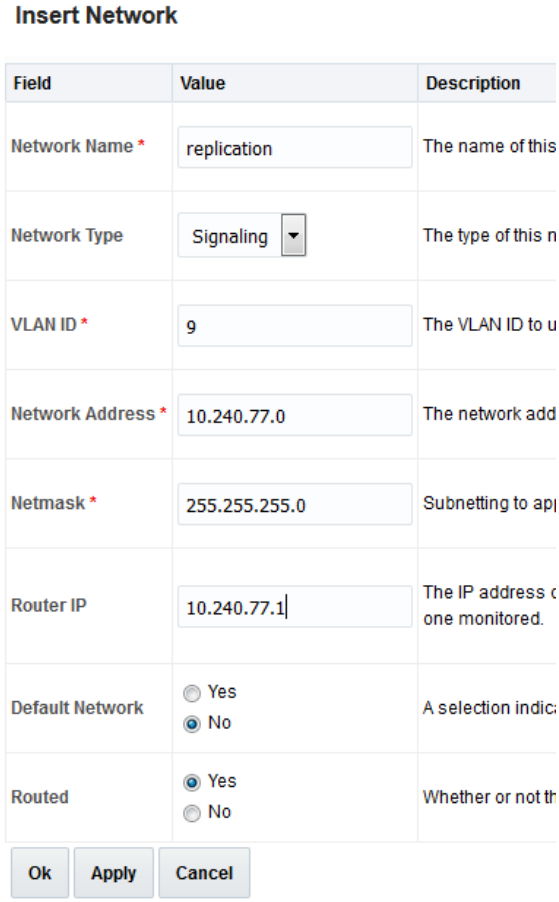
Procedure 20. Configure MP Blade Servers

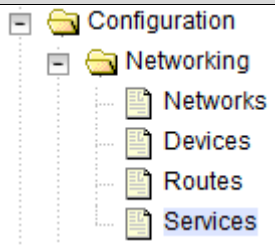
Step#	Procedure	Description
This procedure configures MP blade servers (IPFE, SBR, DA-MP). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Login	If not already done, establish a GUI session on the NOAM server by using the 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.

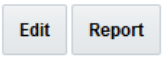


Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Navigate to signaling network configuration screen	1. Navigate to **Configuration > Networking > Networks**.  2. Select the associated SOAM tab for the MP server.  3. Click **Insert** in the lower left corner. 

Step#	Procedure	Description
3. ☐	**NOAMP VIP**: Add signaling networks	1. 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. 1. Select **Signaling** for Network Type. 2. Select **No** for Default Network. 3. Select **Yes** for Routable. 4. Click **OK**, if you are finished adding signaling networks. –OR– Click **Apply** to save this signaling network and **repeat** this step to enter additional signaling networks.

Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: [PCA/DCA Only]: Define SBR DB replication network	***Note***: Execute this step only if you are defining a separate, dedicated network for SBR replication. 1. 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. 2. Click **Signaling** for Network Type. 3. Click **No** for Default Network. 4. Click **Yes** for Routable. 5. Click **OK**. If you are finished adding signaling networks. –OR– Click **Apply** to save this signaling network and **repeat** this step to enter additional signaling networks.
5. ☐	**NOAM VIP GUI**: [PCA/DCA Only]: Perform	***Note***: Execute this step only if you are defining a separate, dedicated network for SBR Replication. 1. Navigate to **Configuration > Services**.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td></td><td>additional service to networks mapping</td><td>


2. Click Edit.


3. Set the services according to one of these scenarios:

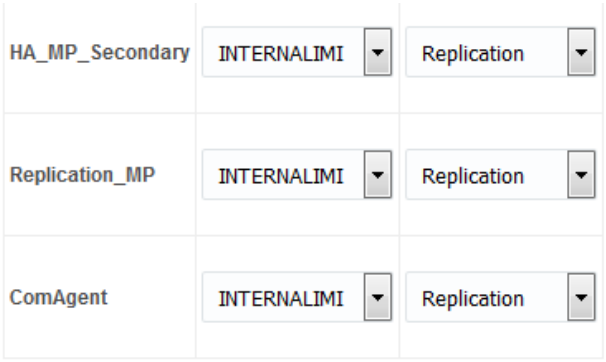
If the dual path HA configuration is required:
Set up the inter-NE network to the XMI network
Set up the intra-NE network to the IMI network for HA_MP secondary.
This configuration uses the XMI network as a secondary path to preserve the HA status of SBRs grouped between multiple sites. If the primary HA path SBR DB Replication Network becomes lost or impaired, the XMI network preserves the HA state and prevents the servers from entering into a scenario known as HA Split-Brain. Preventing HA Split-Brain keeps the existing database in sync, but the DSR mate site is isolated from the active SBR and results in traffic loss until SBR DB replication network is restored.
<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>HA_MP_Secondary</td><td><IMI Network></td><td><XMI Network></td></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>
</table>


If the dual path HA configuration is NOT required:
Set up the inter-NE network to SBR DB replication (configured in step 5).
Set up the intra-NE network to the IMI network for HA_MP secondary.
This condition allows an HA Split-Brain condition between the SBRs if the SBR DB replication network becomes lost or impaired. During an HA Split-Brain condition, an active SBR server exists at each site, but the database is not in sync between the SBRs.

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

Step#	Procedure	Description

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

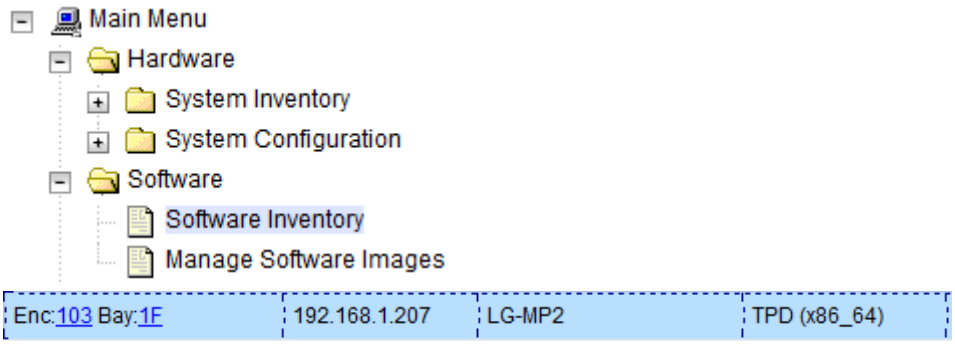


4. Click **OK** to apply the Service-to-Network selections.

6. ☐ **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.

1. From the MP site's PMAC GUI, navigate to **Software** > **Software Inventory**.

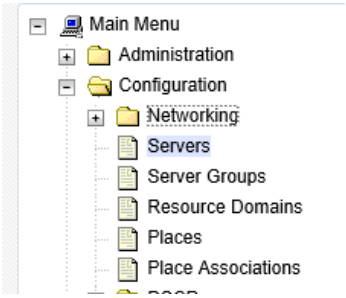
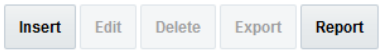
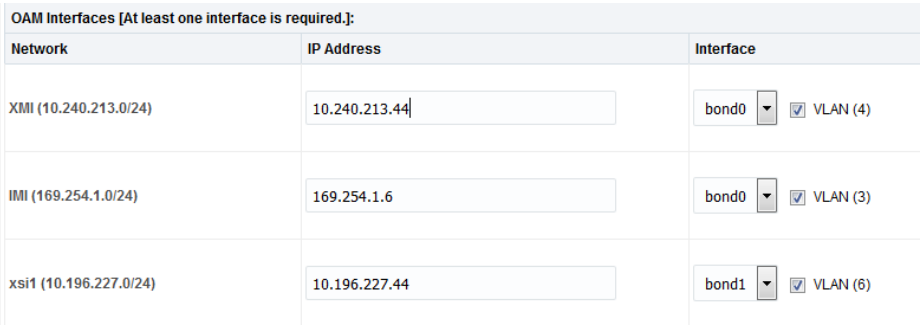


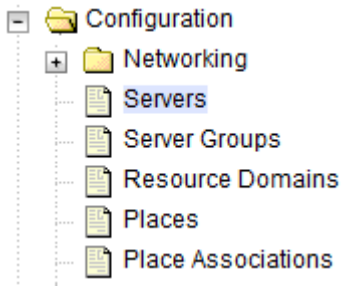
2. Note the IP address for an MP server.
3. From a terminal window connection on the MP site's PMAC, login as the **admusr** user.
4. Exchange SSH keys for admusr between the PMAC and the MP blade server using the keyexchange utility and the control network IP address for the MP blade server.

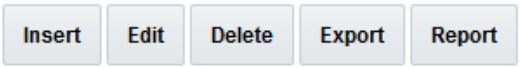
```
$ keyexchange admusr@<MP_Control_Blade_IP Address>
```

5. When asked for the password, type the password for the **admusr** of the MP server.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>7.
☐</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, 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 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 since it is used in server creation in the following step.
</td></tr>
</table>

Step#	Procedure	Description
8. ☐	**NOAM VIP GUI**: Insert the MP server (Part 2)	1. Navigate to **Configuration > Servers**.  2. Click **Insert** to insert the new MP server into servers table.  3. Enter the following values: **Hostname**: <Hostname> **Role**: MP **Network Element Name**: [Choose Network Element] **Hardware Profile**: Select the profile that matches your MP physical hardware and enclosure networking environment from step 7. **Location**: <Enter an optional location description>  The interface configuration form displays. ***Note***: If networks have been configured previously, but are not required on the server, simply remove the populated network IP from the IP address field and this device is not created on the server. 4. Type the IP addresses for all networks. Select the correct bond or interface. Ensure the correct bond and VLAN tagging (if required) is selected. 5. (**Optional**) If dedicated network for SBR replication has been defined, enter the SBR replication IP address. Select the proper bond or interface, and select the **VLAN** checkbox if VLAN tagging is required.

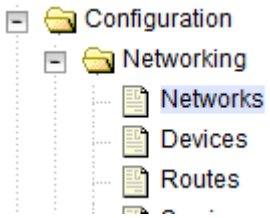
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>9.
☐</td><td>NOAM VIP GUI: Insert the MP server (Part 3)</td><td>1. Add the following NTP servers:
<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><TVOE_XMI_IP_Address (SO1)></td><td>Yes</td></tr><tr><td><TVOE_XMI_IP_Address (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.
2. Click OK when all fields are entered to finish MP server insertion.</td></tr>
<tr><td>10.
☐</td><td>NOAM VIP GUI: Export the configuration</td><td>1. Navigate to Configuration > Servers.
 

2. From the GUI screen, select the MP server and click Export to generate the initial configuration data for that server.
 
</td></tr>
<tr><td>11.
☐</td><td>NOAM VIP: Copy configuration file to MP server</td><td>1. Obtain a terminal session to the NOAM VIP as the admusr user.
2. Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the MP server, using the Control network IP address for the MP server.
The configuration file has a filename like TKLCConfigData.<hostname>.sh.
<code>$ sudo awpushcfg</code>
The awpushcfg utility is interactive, so the user is asked for the following:
• IP address of the local PMAC server: Use the management network address from the PMAC.
• Username: Use admusr
• Control network IP address for the target server: In this case, enter the control IP for the MP server).
• Hostname of the target server: Enter the server name configured in step 9.</td></tr>
</table>

Step#	Procedure	Description

12. ☐	**MP Server**: Verify awpushcfg was called and reboot the configured server	1. 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>`
		2. Login as the **admusr** user.
		3. 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!`
		4. Reboot the server:
		`$ sudo init 6`
		5. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt is displayed.

13. ☐	**MP Server**: Verify server health	1. After the reboot, login as admusr.
		2. 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`

Step#	Procedure	Description
14. ☐	**MP Server**: Delete auto-configured default route on MP and replace it with a network route via the XMI network-Part 1 (optional)	***Note***: THIS STEP IS **OPTIONAL** AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A **DEFAULT ROUTE** ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. Not executing this step means a default route is not configurable on this MP and you have to create separate network routes for each signaling network destination. 1. 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. 2. Determine <XMI_Gateway_IP> from your SO site network element info. 3. 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 **Configuration > Network Elements** screen. 

Step#	Procedure	Description

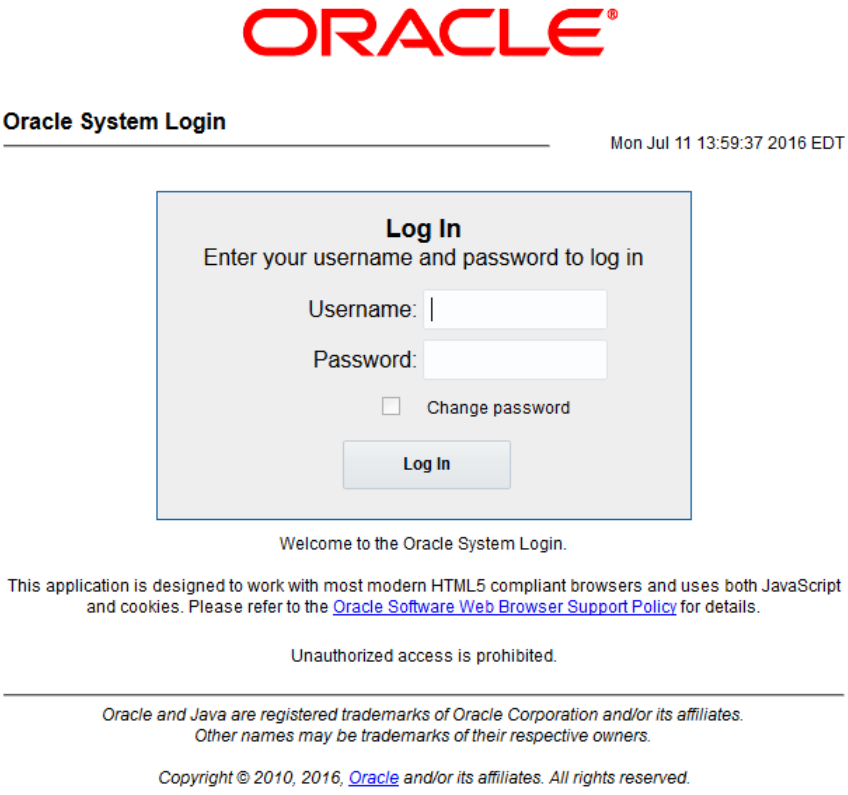
15. ☐	**MP Server**: Delete auto-configured default route on MP and replace it with a network route via the XMI network-Part 2 (optional)	1. Establish a connection to the MP server and login as **admusr**.
		2. Create network routes to the NO's XMI(OAM) network:
		Note: If your NOAM XMI network is exactly the same as your MP XMI network, then you should skip this command and only configure the DR NO route.
		`$ sudo /usr/TKLC/plat/bin/netAdm add -route=net --address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>`
		3. Create network routes to the DR NO's XMI (OAM) network:
		`$ sudo /usr/TKLC/plat/bin/netAdm add -route=net --address=<DR-NO_Site_Network_ID> --netmask=<<DR-NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>`
		4. Create network routes to the management server TVOE XMI (OAM) network for NTP:
		`$ sudo /usr/TKLC/plat/bin/netAdm add -route=net --address=<TVOE_Mgmt_Network_Address> --netmask=<TVOE_Mgmt_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>`
		5. (**Optional**) If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:
		`$ sudo /usr/TKLC/plat/bin/netAdm add -route=host --address=<Customer NMS IP> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>`
		6. Repeat for any existing customer NMS stations.
		7. Delete the existing default route:
		1. Login to primary NOAM VIP GUI.
		2. Navigate to **Configuration > Networking > Networks**.
		3. Select the respective SOAM tab.
		4. Select the XMI network and click **Unlock**. Click **OK** to confirm.
		5. Navigate to **Configuration > Networking > Routes**.
		6. Select the XMI route and click **Delete**.
		7. Click **OK** to confirm.
		8. Repeat steps 1 through 7 for all required MPs to delete the XMI routes.
		9. Navigate to **Configuration > Networking > Networks**.
		10. Select the respective SOAM tab.
		11. Select the XMI network and click **Lock**.
		12. Click **OK** to confirm.

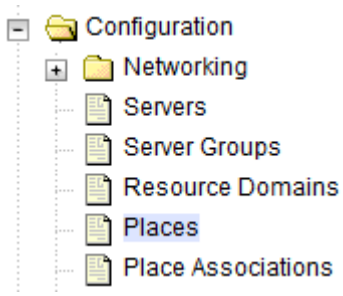
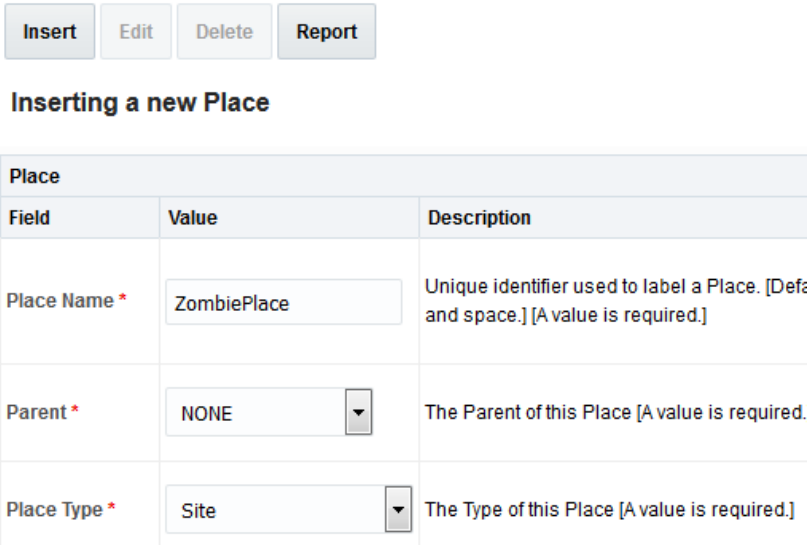
Step#	Procedure	Description

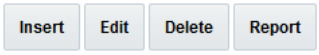
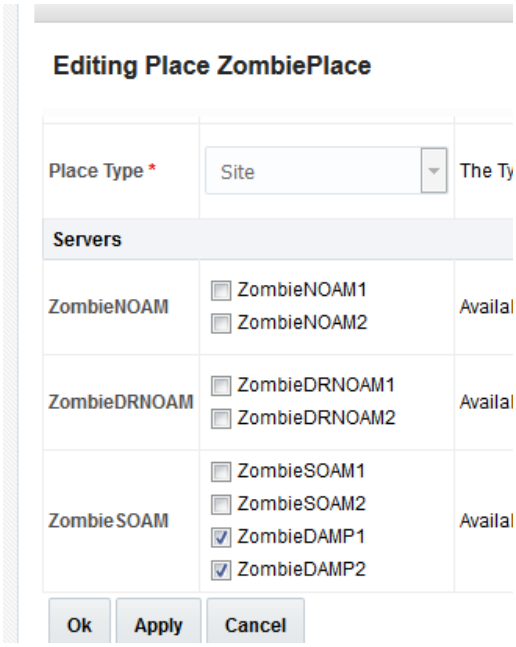
16. ☐	**MP Server**: Verify connectivity	1. Establish a connection to the MP server and login as **admusr**.
		2. Ping active NO XMI IP address to verify connectivity:
		`$ ping <ACTIVE_NO_XMI_IP_Address>`
		`PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.`
		`64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms`
		3. (Optional) Ping Customer NMS Station(s):
		`$ ping <Customer_NMS_IP>`
		`PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.`
		`64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms`
		4. If you do not get a response, then verify your network configuration. If you continue to get failures, then stop the installation and contact Oracle customer support.

17. ☐	Repeat for remaining MP at all sites	**Repeat** this entire procedure for all remaining MP blades (DA-MP, and IPFE).

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

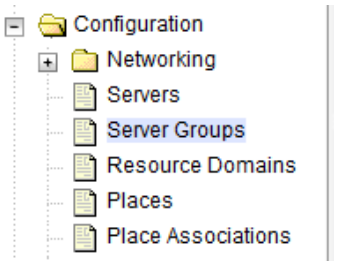
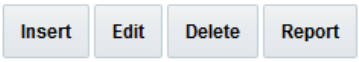
Step#	Procedure	Description
This procedure adds places in the Policy and Charging DRA network. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

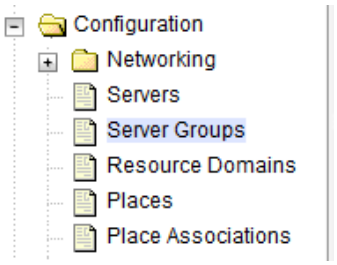
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Configure Places	1. Navigate to **Configuration > Places**.  2. Click **Insert**.  3. Enter the fields as follows: **Place Name**: <Site Name> **Parent**: NONE **Place Type**: Site 4. **Repeat** this step for each of the PCA Places (Sites) in the network. See the Terminology section for more information on Sites and Places.

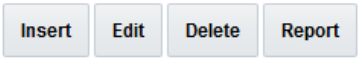
Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Assign MP servers to places	1. Select the place configured in step 2 and click **Edit**.  2. For each place you have defined, select the set of MP servers that are assigned to those places.  3. Check all the checkboxes for **PCA DA-MP** and **SBR** servers assigned to this place. 4. **Repeat** this step for all other DA-MP or SBR servers you want to assign to places. ***Note***: All PCA DA-MPs, and SBR MPs must be added to the Site Place that corresponds to the physical location of the server. See the Terminology section for more information on sites.

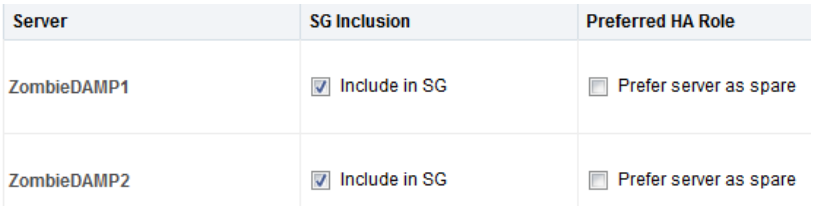
Procedure 22. Configure the MP Server Group(s) and Profile(s)

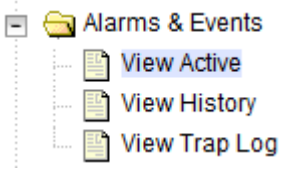
Step#	Procedure	Description
This procedure configures MP server groups. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

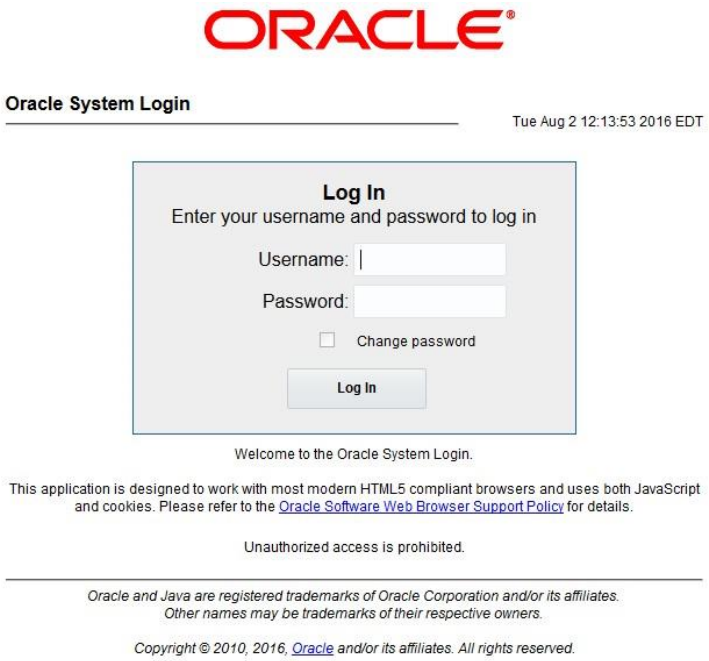
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Enter MP server group data	From the data collected from step 2, create the server group with the following: 1. Navigate to **Configuration > Server Groups**.  2. Select **Insert**.  3. Enter the following fields: **Server Group Name**: <Server Group 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) **WAN Replication Connection Count**: Use Default Value 4. Click **OK** when all fields are filled in.

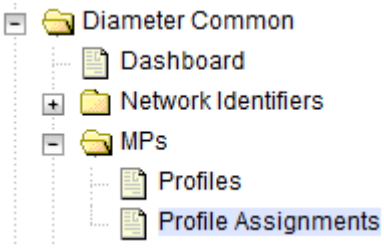
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>3.
☐</td><td>NOAM VIP GUI: Edit the MP server groups to include MP blades</td><td>1. From the GUI, navigate to Configuration > Server Groups.
 

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

3. Mark the Include in SG checkbox for every MP server you want to include in this server group. Leave other checkboxes blank.
 

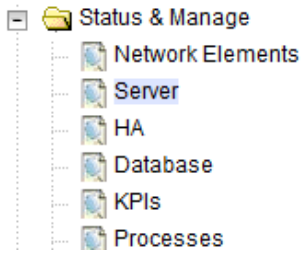
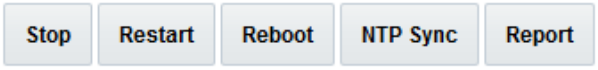
Note: The MPs should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.
4. Click OK.</td></tr>
<tr><td>4.
☐</td><td>NOAM VIP GUI: Wait for remote database alarm to clear</td><td>1. Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.
2. Navigate to Alarms & Events > View Active.
 
</td></tr>
</table>

Step#	Procedure	Description
5. ☐	SOAM VIP GUI: Login	1. 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: `https://<Primary_SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

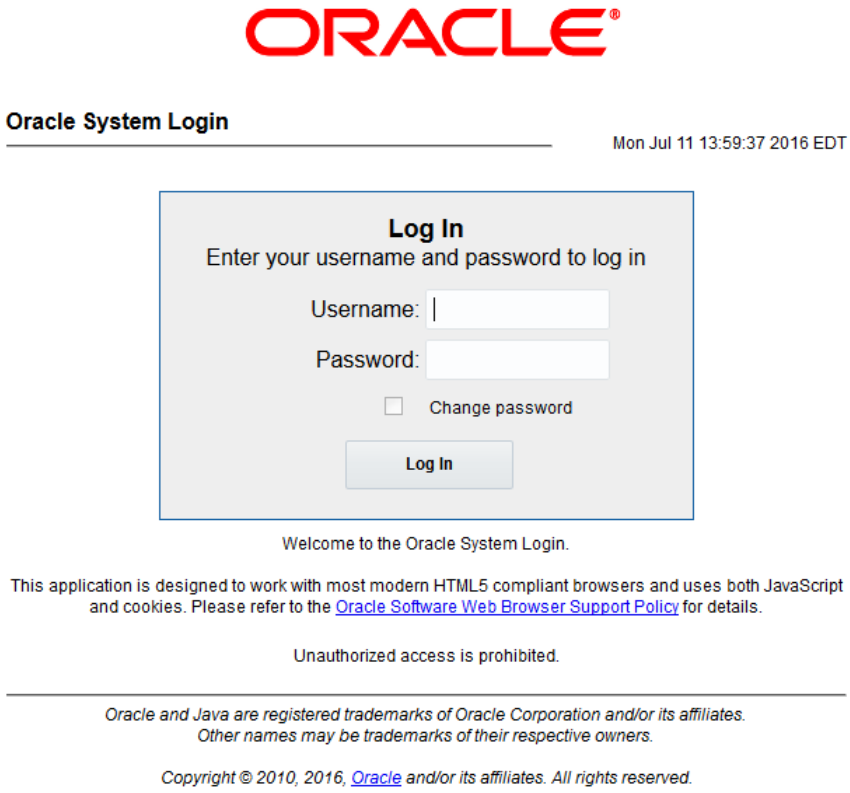
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>6.
☐</td><td>SOAM VIP GUI: Assign Profiles to DA-MPs from SOAM GUI</td><td>
1. Navigate to Diameter Common > MPs > Profile Assignments.


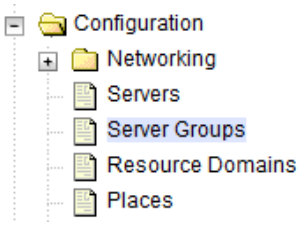
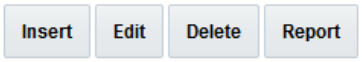
Refer to the DA-MP section profile table below for profiles.
<table>
<tr><th>DA-MP</th><th>MP Profile</th></tr>
<tr><td>ZombieDAMP1</td><td>G8/G9:Relay</td></tr>
<tr><td>ZombieDAMP2</td><td>G8/G9:Relay</td></tr>
</table>
2. For each MP, select the proper profile assignment based on the MP's hardware type and the function it serves:
<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>
3. When finished, click Assign.
</td></tr>
</table>

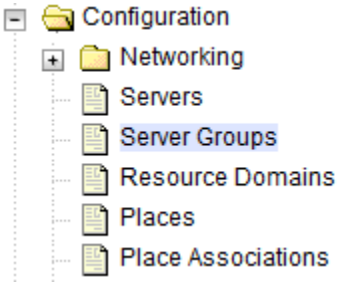
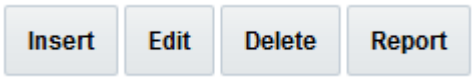
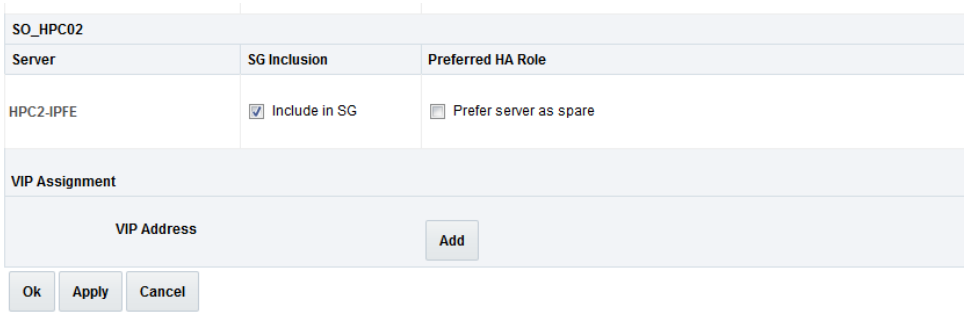
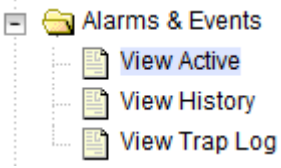
Step#	Procedure	Description
7. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

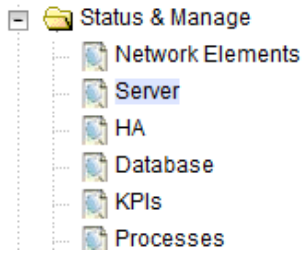
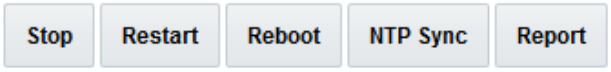
Step#	Procedure	Description
8. ☐	**NOAM VIP GUI**: Restart MP blade servers	1. Navigate to **Status & Manage > Server**.  2. For each MP server: • Select the MP server. • Click **Restart**. • Click **OK** on the confirmation screen. Wait for the message that tells you that the restart was successful.  ***Note***: Policy and Charging DRA installations/DCA installations: You may continue to see alarms related to ComAgent until you complete the PCA/DCA installation.

Procedure 23. Configure IPFE Server Groups

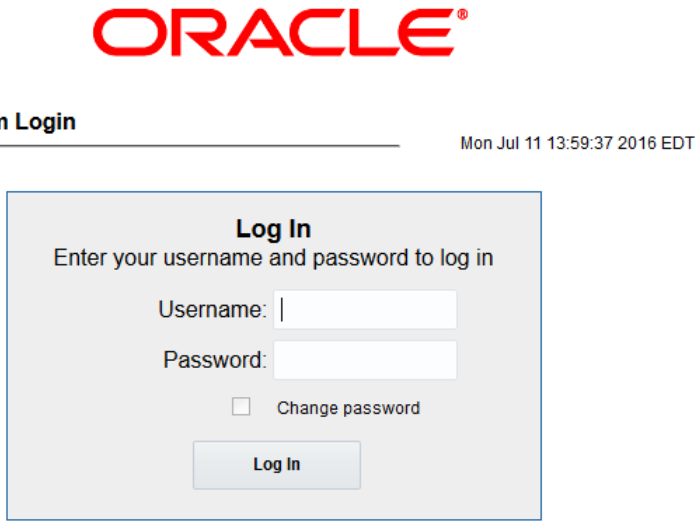
Step#	Procedure	Description
This procedure configures the VIPs for the signaling networks on the MPs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

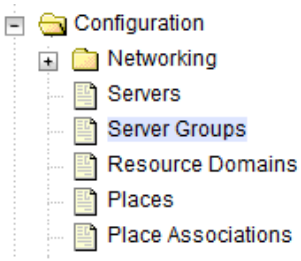
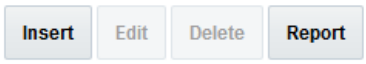
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Enter MP server group data	Create the server group for each individual IPFE as follows: 1. Navigate to **Configuration > Server Groups**.  2. Click **Insert**.  3. Fill out the following fields: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: [SOAMP Server Group That is Parent To this MP] **Function**: IP Front End **WAN Replication Connection Count**: Use Default Value 4. Select **OK**.

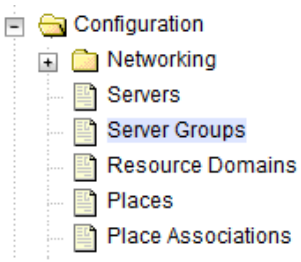
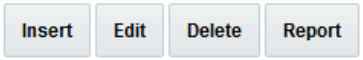
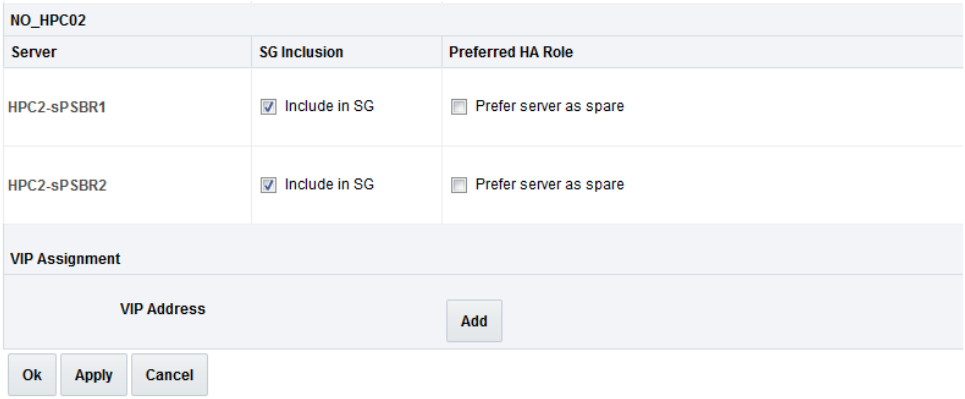
Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Edit the MP server group and add VIPs (only for 1+1)	1. Navigate to **Configuration > Server Groups**.  2. Select the server group you just created and click **Edit**.  3. Mark the **Include in SG** checkbox for the MP server to include in this server group. Leave other checkboxes unmarked. ***Note***: Each IPFE MP server should be have an individual Server Group of type IPFE.  4. Click **OK**.
4. ☐	**NOAM VIP GUI**: Wait for Remote Database Alarm to Clear	1. Navigate to **Alarms & Events > View Active**.  2. Wait for the alarm **Remote Database re-initialization in progress** to clear before proceeding.

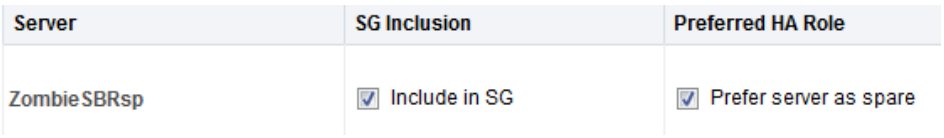
Step#	Procedure	Description
5. ☐	**NOAM VIP GUI**: Restart MP blade servers	1. Navigate to **Status & Manage** > **Server**.  2. For each MP server: • Select the MP server. • Click **Restart**. • Click **OK** to the confirmation screen. Wait for the message that tells you the restart was successful. 

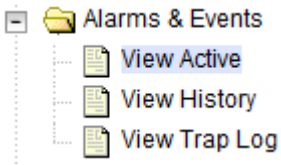
Procedure 24. Configure the Session SBR Server Group(s)

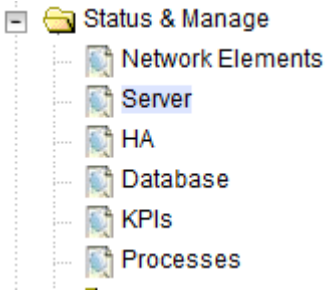
Step#	Procedure	Description
This procedure configures MP server groups as session SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

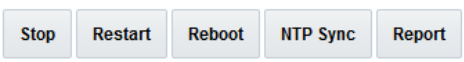
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Create a server group for each site	1. Navigate to **Configuration > Server Group**.  2. Click **Insert** and fill the following fields.  **Server Group Name**: <Server Group Name> **Level**: C **Parent**: <SOAMP Server Group that is Parent to this MP> **Function**: SBR **WAN Replication Connection Count**: 8 3. Click **OK**.

Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Edit the MP server groups to include MP blades	1. Navigate to **Configuration > Server Groups**.  2. Select a server group you just created and click **Edit**.  3. Mark the **Include in SG** checkbox for the MP server you want to include in this server group. 4. Leave other checkboxes blank. ***Note***: The MPs should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.  5. Click **OK**.

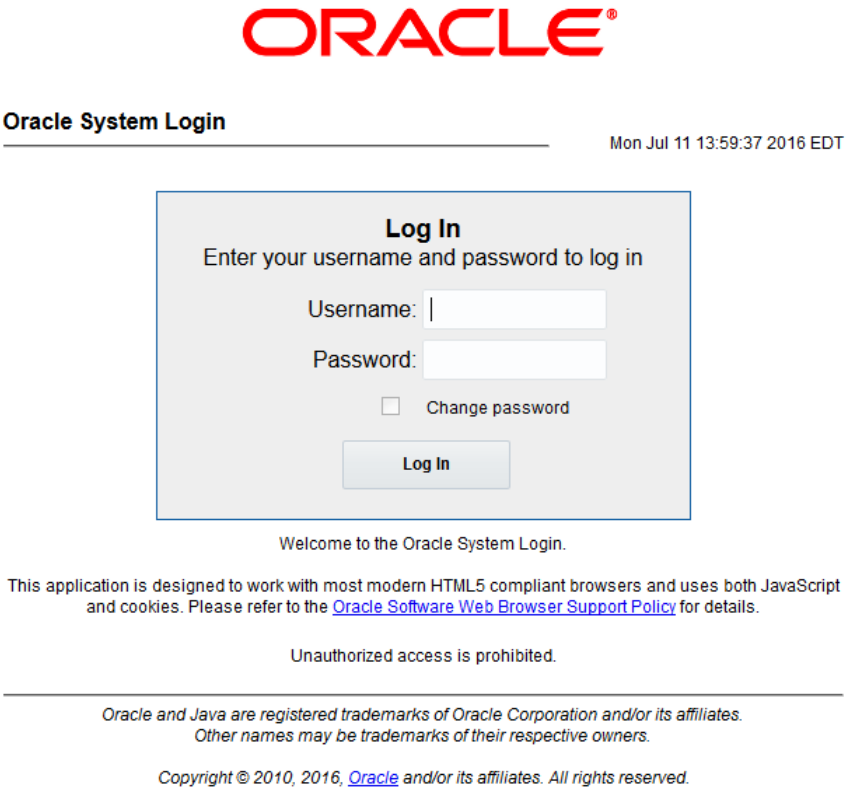
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>4.
☐</td><td>NOAM VIP GUI: (PCA/DCA ONLY) Edit the MP Server Group and add Preferred Spares for Site Redundancy (Optional)</td><td>If the Two Site Redundancy feature for the policy and charging SBR server group/session binding repository SBR server group is wanted, add a MP server that is located in a separate site (location) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox.
 

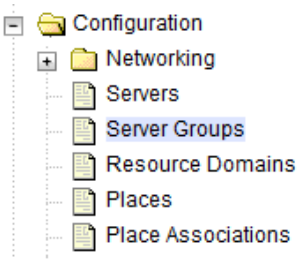
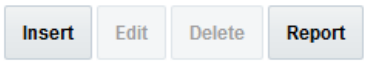
If the Three Site Redundancy feature for the SBR MP server group is wanted, add two SBR MP servers that are located in separate sites (locations) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox for both servers.
Note: The Preferred Spare servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations).
For more information about Site Redundancy for Policy and Charging SBR/Session Binding Repository Server Groups, see the 1.3 Terminology section.
Click OK to save.</td></tr>
<tr><td>5.
☐</td><td>NOAM VIP GUI: Wait for remote database alarm to clear</td><td>Navigate to Alarms & Events > View Active.
 

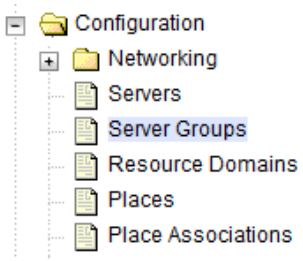
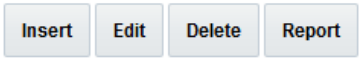
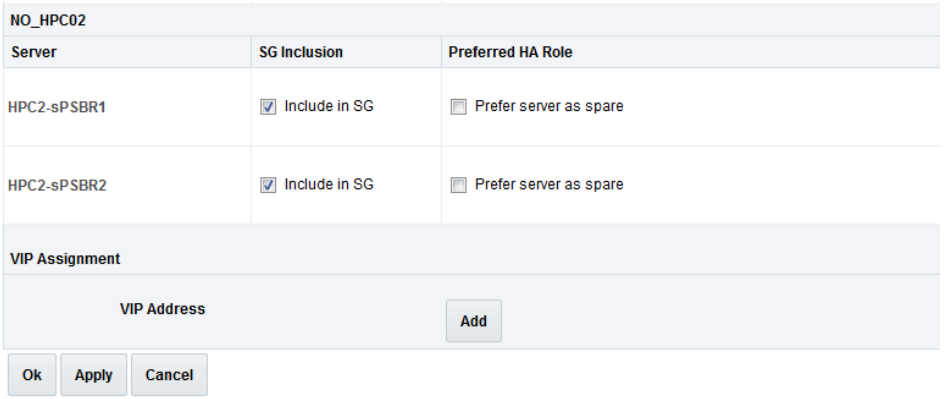
Wait for the Remote Database re-initialization in progress alarm to clear before proceeding.</td></tr>
<tr><td>6.
☐</td><td>NOAM VIP GUI: Restart MP blade servers</td><td>1. Navigate to Status & Manage > Server.
 

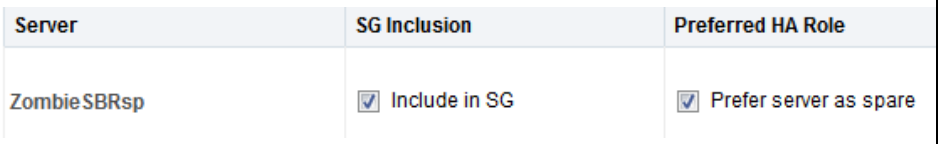
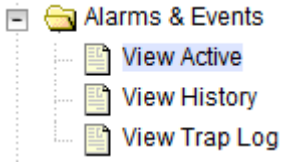
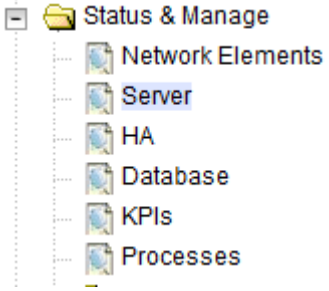
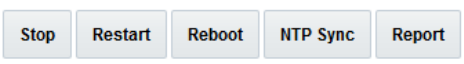
2. Select the MP server.
3. Click Restart.
4. Click OK on the confirmation screen.
5. Wait for restart to complete.
 
</td></tr>
</table>

Procedure 25. Configure the Binding SBR Server Group(s)

Step#	Procedure	Description
This procedure configures MP server groups as binding SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

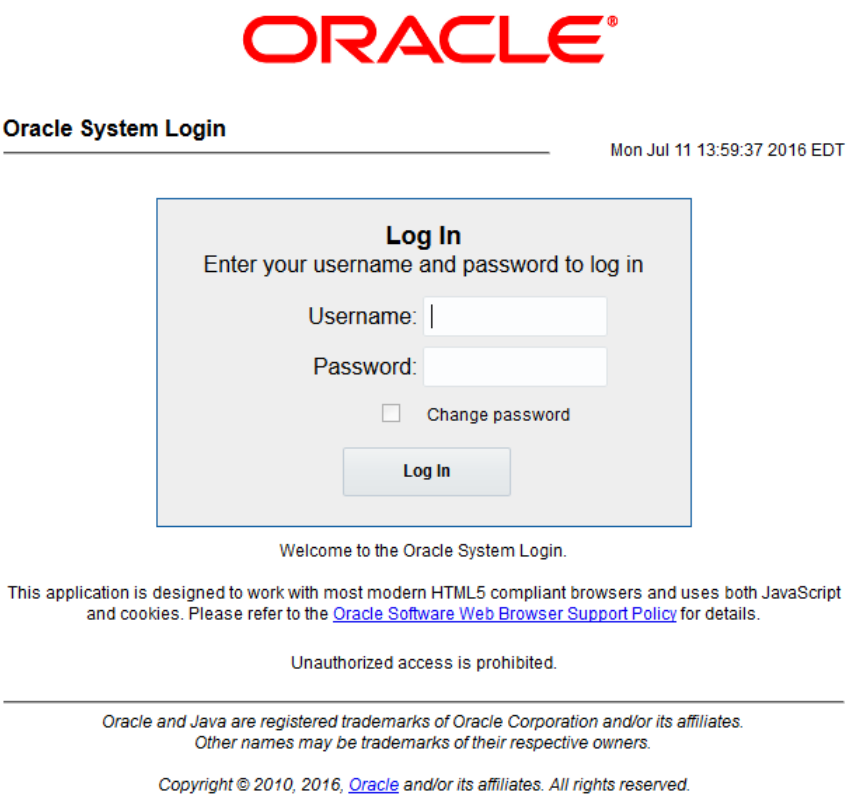
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Create a server group for each site	1. Navigate to **Configuration > Server Group**.  2. Click **Insert** and fill the following fields.  **Server Group Name**: <Server Group Name> **Level**: C **Parent**: <SOAMP Server Group that is Parent to this MP> **Function**: SBR **WAN Replication Connection Count**: 8 3. Click **OK**.

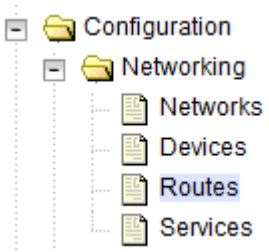
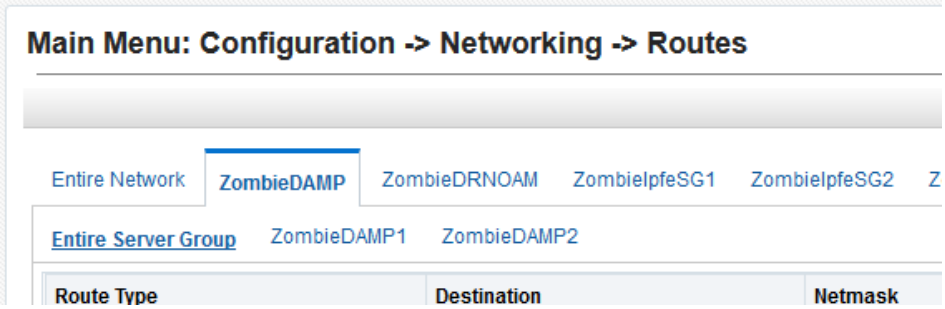
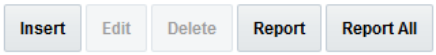
Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Edit the MP server groups to include MP blades	1. Navigate to **Configuration > Server Groups**.  2. Select a server group you just created and click **Edit**.  3. Mark the **Include in SG** checkbox for the MP server you want to include in this server group. 4. Leave other checkboxes blank. ***Note***: The MPs should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.  5. Click **OK**.

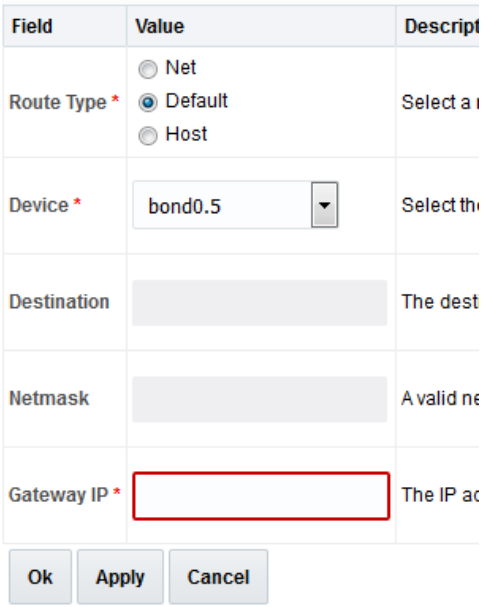
Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: (PCA/DCA ONLY) Edit the MP Server Group and add Preferred Spares for Site Redundancy (Optional)	If the Two Site Redundancy feature for the policy and charging SBR server group/session binding repository SBR server group is wanted, add a MP server that is located in a separate site (location) to the server group by marking the **Include in SG** checkbox. Also, mark the **Preferred Spare** checkbox.  If the Three Site Redundancy feature for the SBR MP server group is wanted, add two SBR MP servers that are located in separate sites (locations) to the server group by marking the **Include in SG** checkbox. Also, mark the **Preferred Spare** checkbox for both servers. ***Note***: The **Preferred Spare** servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations). For more information about Site Redundancy for Policy and Charging SBR/Session Binding Repository Server Groups, see the 1.3 Terminology section. Click **OK** to save.
5. ☐	**NOAM VIP GUI**: Wait for remote database alarm to clear	Navigate to **Alarms & Events > View Active**.  Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.
6. ☐	**NOAM VIP GUI**: Restart MP blade servers	1. Navigate to **Status & Manage > Server**.  2. Select the MP server. 3. Click **Restart**. 4. Click **OK** on the confirmation screen. 5. Wait for restart to complete. 

4.4.2 Configure Signaling Devices

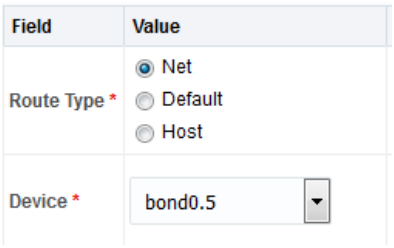
Procedure 26. Configure the Signaling Network Routes

Step#	Procedure	Description
This procedure configures signaling network routes on MP-type servers (DA-MP, IPFE, 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>`
		2. Login as the **guiadmin** user. 

Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Add route	1. Navigate to **Configuration > Networking > Routes**.  2. Select the MP server group tab and verify the **Entire Server Group** link is selected, if not, select the link.  3. Click **Insert** to add additional routes. 

Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Add a default route for MPs going through signaling network gateway (Optional)	Only execute this step if you performed Procedure 20. , step 15. , 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 to use one of the signaling network gateways. **Insert Route on DAMP_SG**  1. Enter the fields as follows: **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. 2. Click **OK**.

Step#	Procedure	Description

4. ☐	**NOAM VIP GUI**: Add network routes for diameter peers	This step adds the IP and/or IPv6 routes to diameter peer destination networks. This ensures diameter traffic uses the gateway(s) on the signaling networks.
		 
		
		1. Enter the fields as follows:
		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 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.
		2. Click **Apply** and repeat to enter more routes, if necessary.
		3. Click **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 destination networks configured in this step are reachable. This can be done by running the following **netconfig** commands from the site's local PMAC. For example:
		Add routes (IPv4 and IPv6):
		`$ sudo netConfig --device=switch1A addRoute network=10.10.10.0/24 nexthop=10.50.76.81`
		`$ sudo netConfig --device=switch1A addRoute network6=2001::/64 nexthop=fd0f::1`
		Delete routes (IPv4 and IPv6):
		`$ sudo netConfig --device=switch1A deleteRoute network=10.10.10.0/24 nexthop=10.50.76.81`
		`$ sudo netConfig -device=switch1A deleteRoute network6=2001::/64 nexthop=fd0f::1`

Step#	Procedure	Description

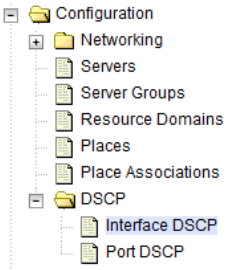
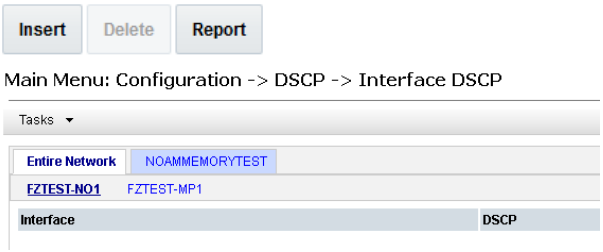
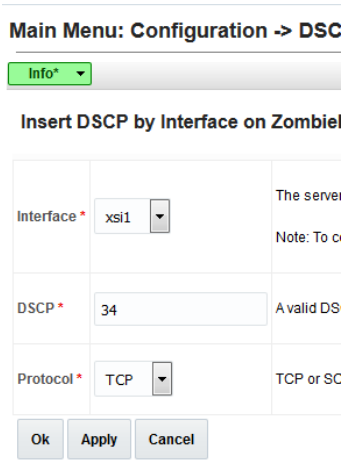
5. ☐	**Local PMAC**: Perform a netConfig backup	After the routes are added to the aggregation switches using netconfig, take a **netconfig backup** so the new routes are retained in the backup.
		1. Execute the following command:
		`$ netConfig backupConfiguration --device=<Switch Hostname service=<ssh_Service> filename=<Backup Filename>`
		2. Copy the files to the backup directory:
		`$ sudo /bin/mv -i ~<switch_backup_user>/<switch_name>-backup* /usr/TKLC/smac/etc/switch/backup`

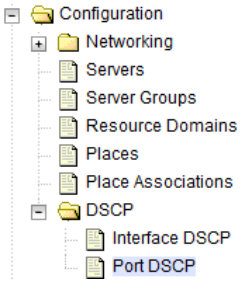
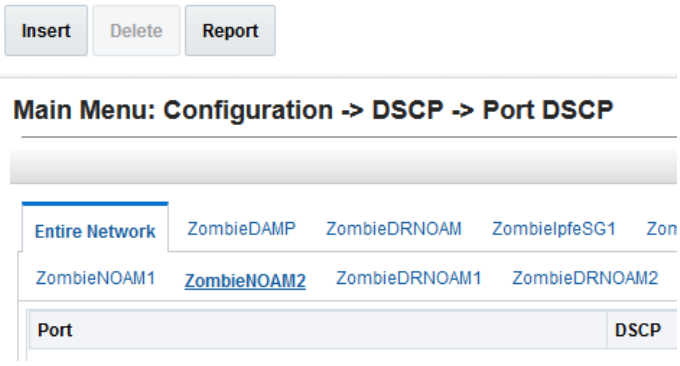
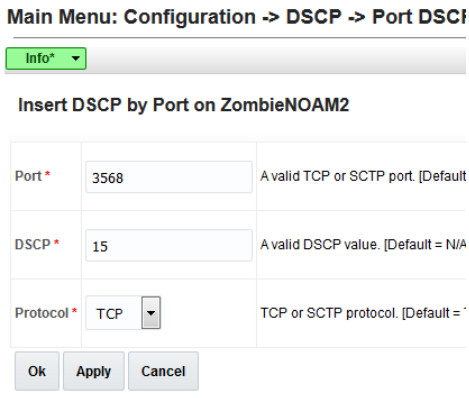
6. ☐	**NOAM VIP GUI**: Repeat for all other MP server groups	The routes entered in this procedure are now configured on all MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat this procedure, but this time select an MP from the next MP server group.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

4.4.3 Configure DSCP (Optional)

Procedure 27. Configure DSCP Values for Outgoing Traffic

Step#	Procedure	Description
This procedure configures the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network uses packet DSCP markings for quality-of-service purposes. ***Note***: If your enclosure switches already have DSCP configuration for the signaling VLANs, then the switch configuration override the settings in this procedure. It is strongly recommended, however, that you configure DSCP here at the application level where you have the most knowledge about outgoing traffic patterns and qualities. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Option 1: Configure interface DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site vary. 1. Navigate to **Configuration > DSCP > Interface DSCP**.  2. Select the server you want to configure from the list of servers on the 2nd line. You can view all servers with **Entire Network** selected; or limit yourself to a particular server group by clicking on that server group name's tab. 3. Click **Insert**.  4. Select the network interface from the dropdown box. Enter the **DSCP value** you wish to have applied to packets leaving this interface and select the transport protocol.  5. Click **OK** if there are no more interfaces on this server to configure, or click **Apply** to finish this interface and continue with more interfaces by selecting them from the drop down and entering their **DSCP values**.

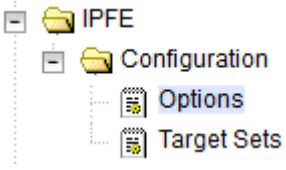
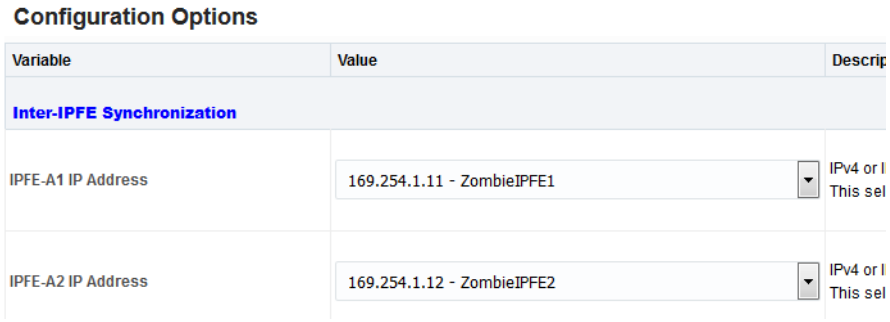
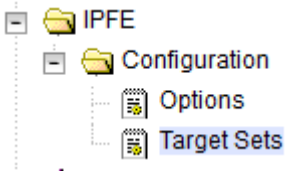
Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Option 2: Configure port DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site vary. 1. Navigate to **Configuration > DSCP > Port DSCP**.  2. Select the server you want to configure from the list of servers on the 2nd line. You can view all servers with **Entire Network** selected; or limit yourself to a particular server group by clicking on that server group name's tab. 3. Click **Insert**.  4. Enter the source port, DSCP value, and select the transport protocol.  5. Click **OK** if there are no more port DSCPs on this server to configure, or **Apply** to finish this port entry and continue entering more port **DSCP mappings**.

Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: Repeat for additional servers	**Repeat** steps 2-3 for all remaining servers.

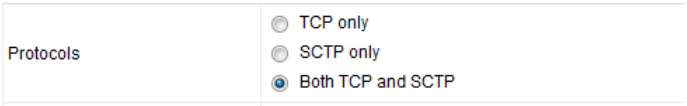
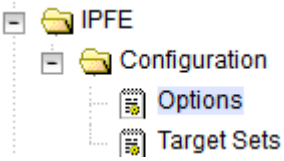
4.4.4 Configure IP Front End Servers (Optional)

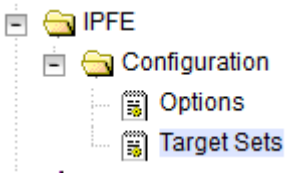
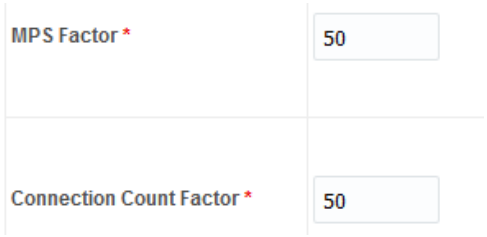
Procedure 28. IP Front End (IPFE) Configuration

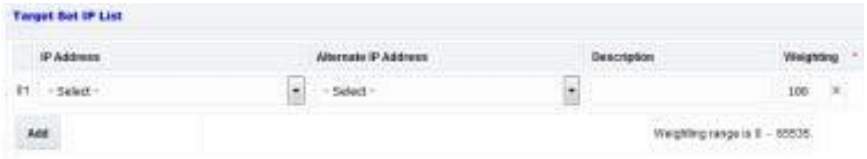
Step#	Procedure	Description
This procedure configures IP Front End (IPFE), and optimize performance. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**SOAM VIP GUI**: Login	1. Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

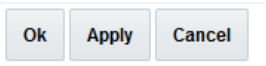
Step#	Procedure	Description
2. ☐	**SOAM VIP GUI**: Configuration of replication IPFE association data	3. Navigate to **IPFE > Configuration > Options**.  4. Enter the IP address of the 1st IPFE in the **IPFE-A1 IP Address** field and the IP address of the 2nd IPFE in the **IPFE-A2 IP Address** field. 5. If applicable, enter the address of the third and fourth IPFE servers in **IPFE-B1 IP Address** and **IPFE-B2 IP Address fields**.  ***Notes***: • It is recommended that the address reside on the IMI (Internal Management Interface) network. • IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2. • Accept default configuration for remaining entries.
3. ☐	**SOAM VIP GUI**: Configuration of IPFE target sets, Part 1 (insert target set)	1. Navigate to **IPFE > Configuration > Target Sets**.  2. Click either **Insert IPv4** or **Insert IPv6** depending on the IP version of the target set you plan to use. 

Step#	Procedure	Description

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

Step#	Procedure	Description
5. ☐	**SOAM VIP GUI**: Configuration of IPFE target sets, Part 3 (target set configuration)	5. Navigate to **IPFE > Configuration > Target Sets**.  6. **(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.  To configure Reserved Ingress MPS, navigate to **Diameter > Configuration > Configuration Sets > Capacity Configuration Sets**. If you choose not to use Reserved Ingress MPS, set **MPS Factor** to 0 and **Connection Count Factor**, described below, to 100. **Connection Count Factor**: This is the other component of the **least load** algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern. **Allowed Deviation**: Percentage within which two application server's load calculation results are considered to be equal. If very short, intense connection bursts are expected to occur, increase the value to smooth out the distribution. 
6. ☐	**SOAM VIP GUI**: Configuration of IPFE Target sets-Part 4 (Target Set Configuration)	**Primary Public IP Address**: IP address for the target set. 

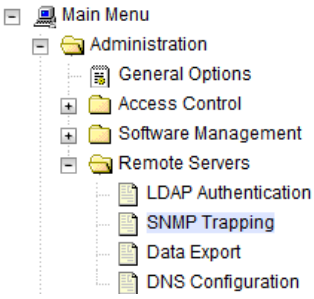
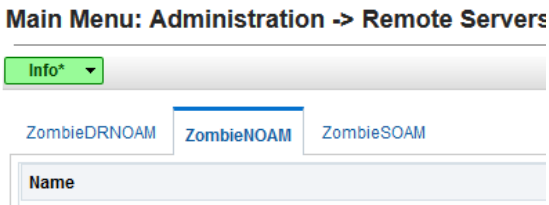
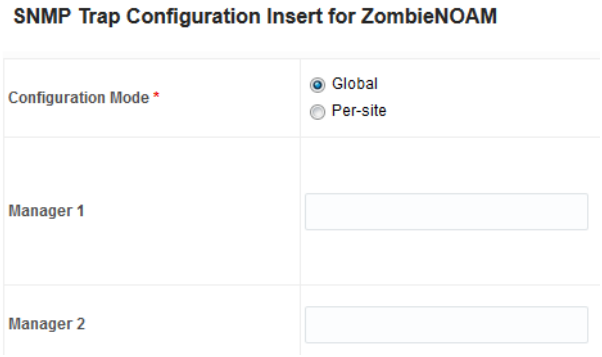
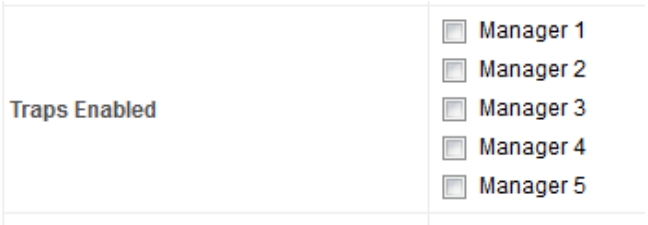
Step#	Procedure	Description
		Note: This address must reside on the XSI (External Signaling Interface) network because it is used by the application clients to reach the application servers. This address MUST NOT be a real interface address (that is, must not be associated with a network interface card). **Active IPFE**: IPFE to handle the traffic for the target set address. **Secondary Public IP Address**: If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.  ***Notes***: • A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections will not be multi-homed. • If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure that SCTP failover functions as designed. **Target Set IP List**: Select an IP address; a secondary IP address, if supporting SCTP multi-homing; a description; and a weight for the application server.  ***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. 7. Click **Add** to add more application servers (up to 16).

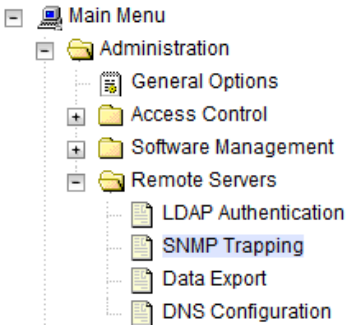
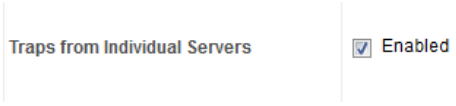
Step#	Procedure	Description
		8. Click **Apply**. 
7. ☐	**SOAM VIP GUI**: Repeat for additional configuration of IPFE target sets	**Repeat** steps 3-6 for each target set (up to 16). At least one target set must be configured.

4.5 SNMP Configuration

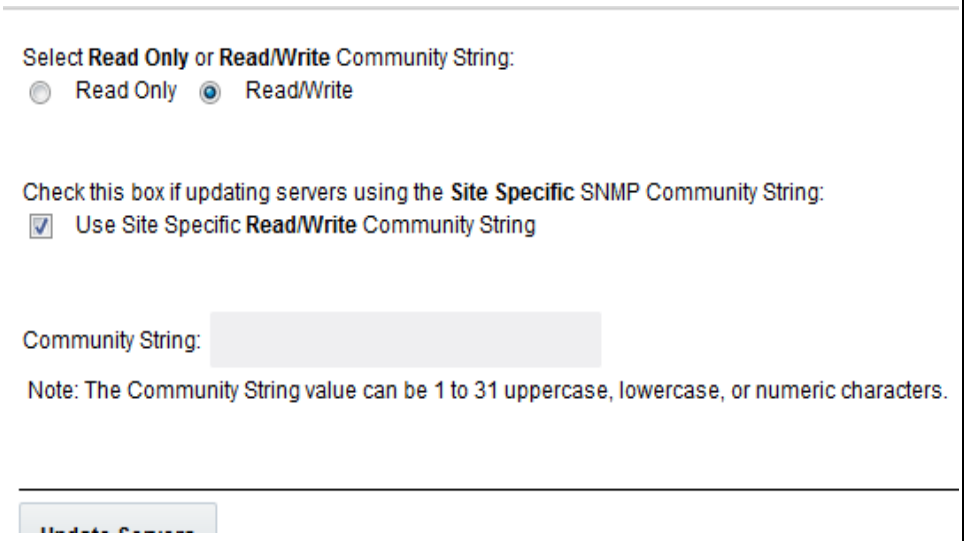
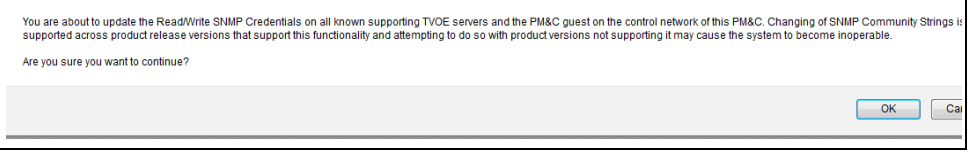
Procedure 29. Configure SNMP Trap Receiver(s)

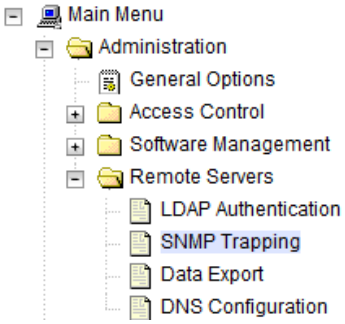
Step#	Procedure	Description
This procedure configures forwarding of SNMP Traps from each individual server. ***Note***: If SNMP configuration is not required, skip to step 6. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

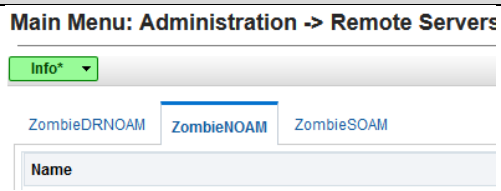
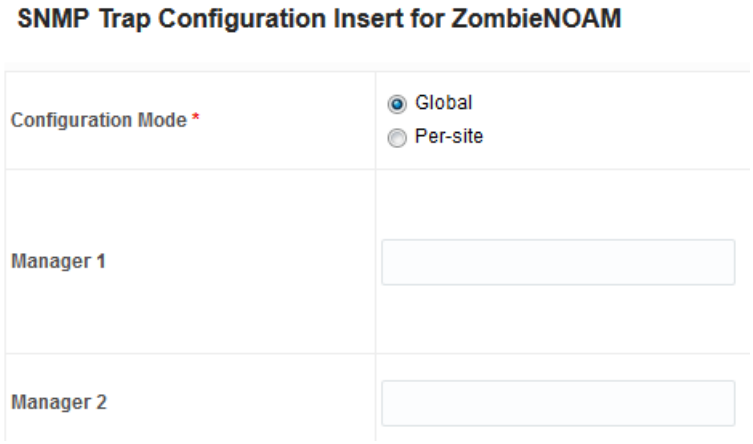
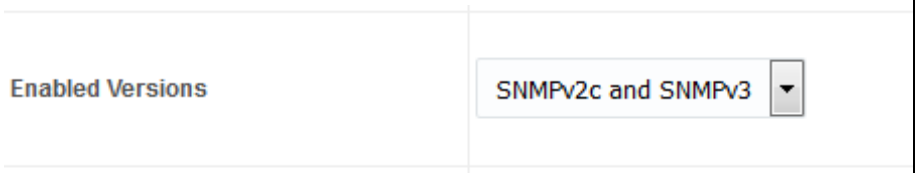
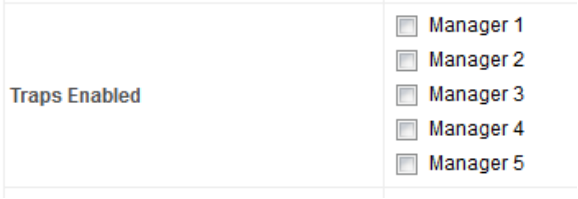
Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Select the Server Group tab for SNMP trap configuration:  3. Type the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP's **XMI** network. 4. Continue to type additional secondary, tertiary, etc., manager IPs in the corresponding slots if desired.  5. Check **Traps Enabled** checkboxes for the manager servers being configured:  6. Enter the **SNMP Community Name**.

Step#	Procedure	Description
		 7. Leave all other fields at their default values. 8. Click **OK**.
3. ☐	**NOAMP VIP**: Enable traps from individual servers (optional)	***Note***: By default, SNMP traps from DPs are aggregated and displayed at the active NOAMP. If instead, you want every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires all servers, including DPs, have an XMI interface on which the customer SNMP target server (NMS) is reachable. 1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Make sure the checkbox next to **Enabled** is checked, if not, check it.  3. Click **Apply** and verify the data is committed.

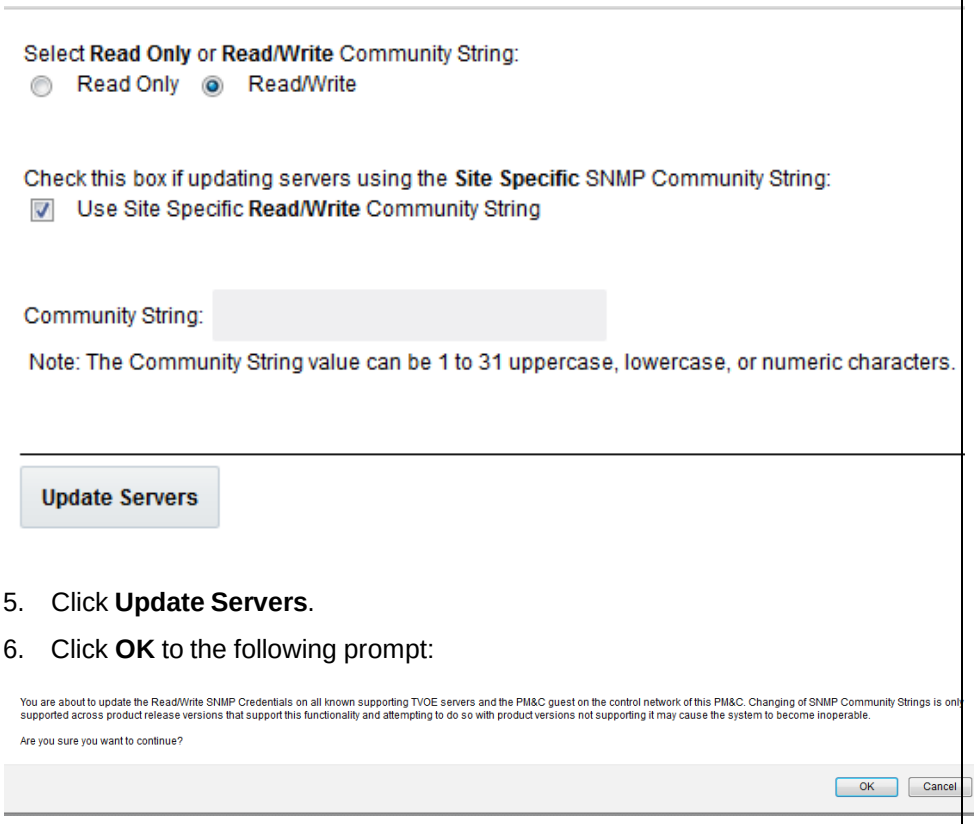
Step#	Procedure	Description
4. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_network_Network_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
5. ☐	**PMAC GUI**: Update the TVOE host SNMP community string	1. Navigate to **Administration > Credentials > SNMP Community String Update**. 2. Mark the **Use Site Specific Read/Write Community String** checkbox.  3. Click **Update Servers**. 4. Click **OK** to the following prompt: 

Step#	Procedure	Description
6. ☐	(Workaround) **NOAM VIP GUI**: Login	***Note***: Perform this workaround step only in the following cases: • If SNMP is not configured (i.e., if above steps 1-5 are skipped). •If SNMP is already configured and **SNMPv3** is selected as enabled version. ***Note***: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3. 1. If not already done, establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
7. ☐	**NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Select the Server Group tab for SNMP trap configuration:

Step#	Procedure	Description
		 3. Type the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP's **XMI** network. (If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here) 4. Continue to type additional secondary, tertiary, etc., manager IPs in the corresponding slots if desired.  5. Set the **Enabled Versions** as **SNMPv2c and SNMPv3**.  6. Check Traps Enabled boxes for the Manager servers being configured:  7. Enter the SNMP Community Name:  8. Leave all other fields at their default values. 9. Click **OK**.

Step#	Procedure	Description
8. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_network_Network_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
9. ☐	**PMAC GUI**: Update the TVOE host SNMP community string	3. Navigate to **Administration > Credentials > SNMP Community String Update**. 4. Mark the **Use Site Specific Read/Write Community String** checkbox.  5. Click **Update Servers**. 6. Click **OK** to the following prompt:
10. ☐	SNMPv3 (optional)	Refer to Restore SNMP Configuration to SNMPv3 (Optional) to restore SNMPv3 after installation, if required

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 IDIH External Drive Removal before proceeding.

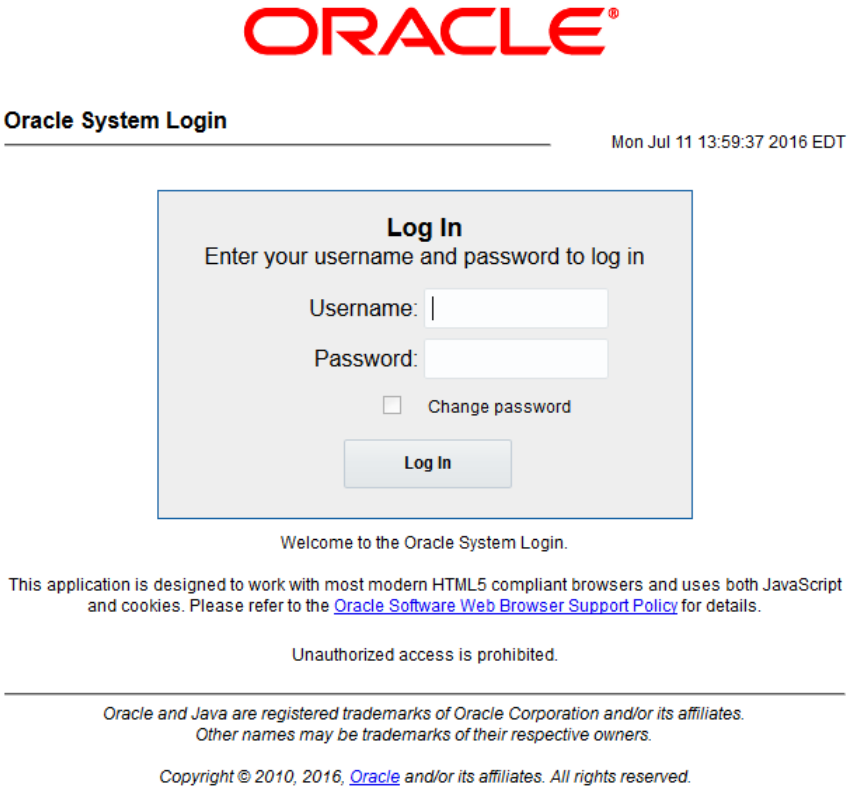
4.6.1 IDIH Installation

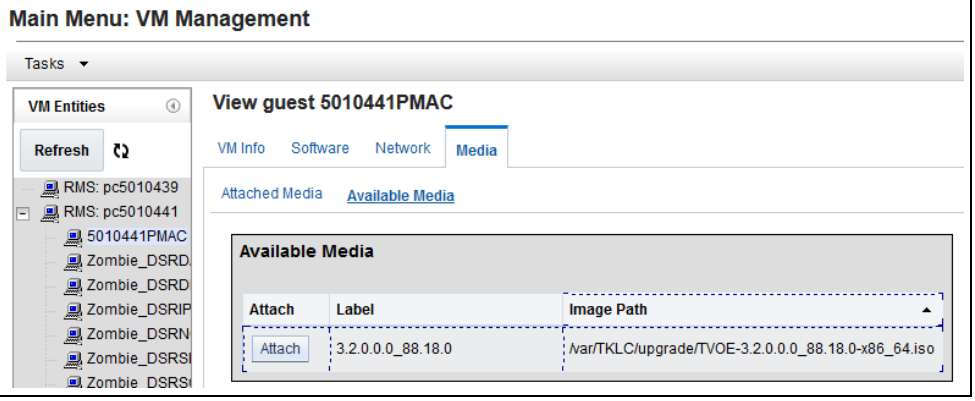
The installation procedure uses the **fast deployment** utility (fdconfig) bundled with the PMAC server to install and configure IDIH.

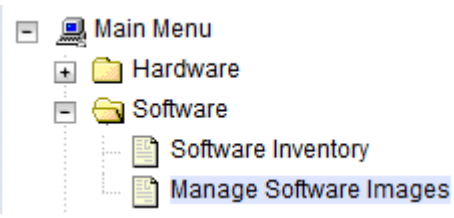
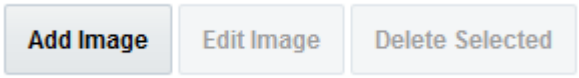
Procedure 30. IDIH Configuration

Step#	Procedure	Description
This procedure installs and configures IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**TVOE Host**: Load application ISO	Add the Application ISO images (**mediation, application, and oracleGuest**) to the PMAC, this can be done in one of three ways:
		1. Insert the Application CD required by the application into the removable media drive.
		2. Attach the USB device containing the ISO image to a USB port.
		3. Copy the application iso file to the PMAC server into the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as pmacftpusr user:
		cd into the directory where your ISO image is located on the **TVOE Host** (**not on the PMAC server**)
		4. Using sftp, connect to the PMAC server
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		5. 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 the "Configure PMAC Application Guest isoimages Virtual Disk" section in [1] Platform Configuration Procedure to increase it.

Step#	Procedure	Description
2. ☐	**PMAC GUI**: Login	1. Open web browser, navigate to the PMAC GUI, and enter a URL of: `https://<pmac_network_Network_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
3. ☐	**PMAC GUI**: Attach the software image to the PMAC guest	If the image is on a CD or USB device, continue with this step. If in step 1 the ISO image was transferred directly to the PMAC guest via sftp, skip the rest of this step and continue with step 4. 1. In the PMAC GUI, navigate to **VM Management**. Select the **PMAC guest** from the VM Entities list. On the resulting View VM Guest page, select the Media tab. 2. Under the Media tab, find the ISO image in the **Available Media** list, and click its **Attach** button. After a pause, the image displays in the **Attached Media** list. 

Step#	Procedure	Description
4. ☐	**PMAC GUI**: Add application image	1. Navigate to **Software > Manage Software Images**.  2. Click **Add Image**. Select the image from the list.  If the image was supplied on a CD or a USB drive, it displays as a virtual device (**device://…**). These devices are assigned in numerical order as CD and USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, **device://dev/sr1**. If one or more CD or USB-based images were already present on the management server before you started this procedure, choose a correspondingly higher device number. If in step 1 the image was transferred to PMAC via sftp, it displays in the list as a local file **/var/TKLC/....** 3. Select the appropriate path and click **Add New Image**. 4. You may check the progress using the **Task Monitoring** link. Observe the green bar indicating success. 5. 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 and login as **admusr**.

6. ☐	**PMAC**: Reset the create guest default timeout and other timeout parameters	1. Execute the following commands:
		`$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=3000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"';`
		`$ sudo pmacadm setParam --paramName=defaultTpdProvdTimeout --paramValue=120`
		`$ sudo pmacadm setParam --paramName=guestDiskDeployTimeout --paramValue=50`
		2. To verify whether the above values are set correctly, run the below commands.
		`$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'select name, value from params where name like "%TIMEOUT%"';`
		`$ sudo pmacadm getParam --paramName=defaultTpdProvdTimeout`
		`$ sudo pmacadm getParam --paramName=guestDiskDeployTimeout`

Step#	Procedure	Description
7. ☐	**PMAC**: Copy the fdc.cfg file to the guest-dropin directory	1. Copy the fdc.cfg file to the pmac guest-dropin directory. 2. Execute the following command: `$ sudo cp /usr/TKLC/smac/html/TPD/mediation-*/fdc.cfg /var/TKLC/smac/guest-dropin`
8. ☐	**PMAC**: Configure the fdc.cfg file	1. Configure the fdc.cfg file. See IDIH Fast Deployment Configuration for a breakdown of the parameters. 2. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.

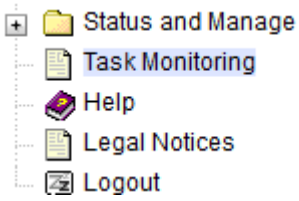
9. ☐	**PMAC**: Run the FDC creation script idihFdc.sh	1. Rename the fdc.cfg file to your preference; also note that two files are generated by the fdc shell script. One is for the Installation procedure and the other file is used for the upgrade procedure. The upgrade FDC is named upgrade.
		Example: 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
		2. Run the FDC creation script **fdc.sh**.
		3. Execute the following commands:
		`$cd /var/TKLC/smac/guest-dropin/`
		`$sudo /usr/TKLC/smac/html/TPD/mediation-8.5.0.0.0_90.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.

Step#	Procedure	Description

10. ☐	**TVOE Host**: Verify/Remove external devices	1. Establish an SSH session to the TVOE host that hosts the IDIH and login as **admusr**.
		2. 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 IDIH External Drive Removal. Reboot the tvoe and verify the extra device(s) are still removed (> ls /dev/sd*)

11. ☐	**TVOE Host**: Verify logical bond, int and imi bridge	1. Establish an SSH session to the TVOE Host which will host the IDIH, login as **admusr**.
		2. On the TVOE host, Execute the following command to verify the logical bond [0.x], int and imi bridge exist or not.
		`$ brctl show`
		3. If Logical bond does not exist, run following commands to create the logical bond, int and imi bridge.
		`$ sudo netAdm add --device=bond0.<imi_vlan> --onboot=yes`
		`$sudo netAdm add --type=Bridge --name=imi --bridgeInterfaces=bond0. <imi_vlan> --onboot=yes`
		`$ sudo netAdm add --type=Bridge --name=int  --onboot=yes`
		4. After adding the logical bond, int and imi bridge, execute following command and verify the logical bond,int and imi bridge added successfully.
		`$ brctl show`
		Note: Logical bond [0.x] x could be any valid integer number.

12. ☐	**PMAC**: 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.

Step#	Procedure	Description
13. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done so, establish a GUI session on the PMAC server. 2. Navigate to **Task Monitoring**.  3. Monitor the IDIH configuration to completion.

4.6.2 Post IDIH Installation Configuration

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

Procedure 31. Configure DSR Reference Data Synchronization for IDIH

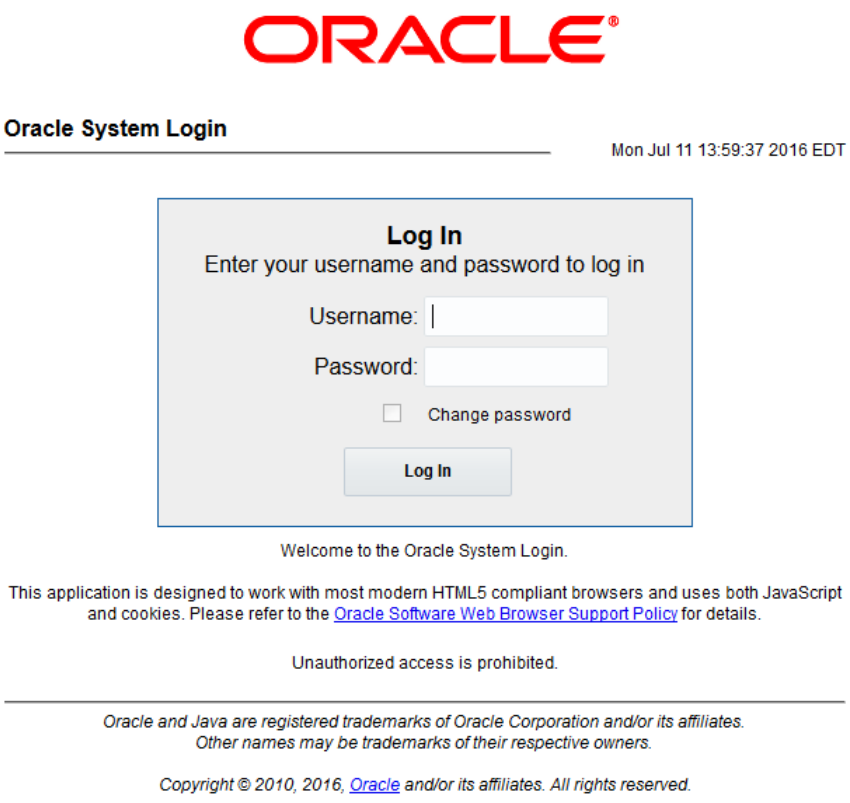
Step#	Procedure	Description
This procedure configures DSR reference data synchronization for IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1.	**IDIH Application Server**: Login	1. Establish an SSH session to the IDIH application server. Login as user **admusr**. 2. Issue the following commands to login as **tekelec** user. `$ sudo su - tekelec`

2.	**IDIH Application Server**: Execute configuration script.	1. 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:`

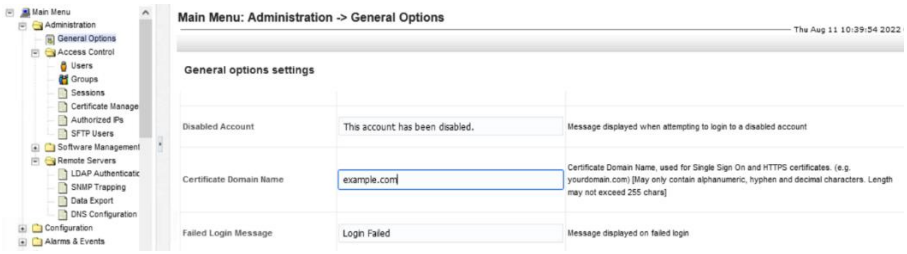
Step#	Procedure	Description
		Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options SQL> SQL> 2 3 4 5 1 row merged. SQL> Commit complete. SQL> Disconnected from Oracle 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:

Step#	Procedure	Description
		[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 **2.** For prompt **Please enter DSR SOAM server IP address**, enter the VIP of the DSR SOAM and click **Enter.** ***Note***: If the address entered is unreachable the script exits with an **Unable to connect to <ip-address>!** error.
3.	**IDIH App Server**: Monitor completion	1. Monitor the log file located at: `/var/TKLC/xIH/log/apps/weblogic/apps/application.log` 2. Examine the log file for entries containing text **Trace Reference Data Adapter**.

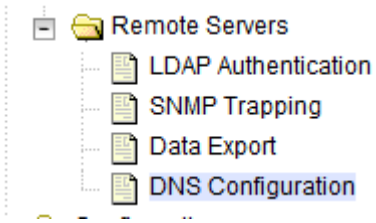
Procedure 32. IDIH Configuration: Configuring the SSO Domain (Optional)

Step#	Procedure	Description
This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

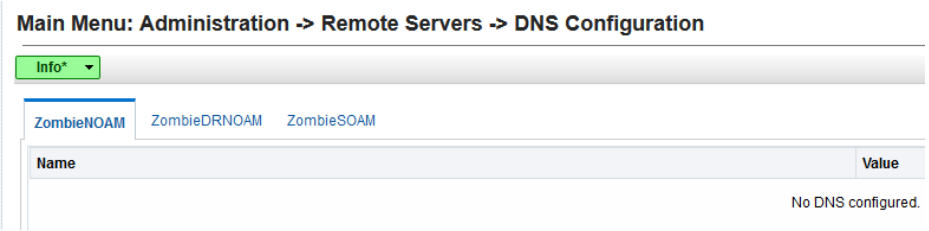
Step#	Procedure	Description
2.	**NOAM VIP GUI**: Configure DNS	1. Navigate to **Main Menu > Administration** a. Verify / Edit the parameter Certificate Domain Name



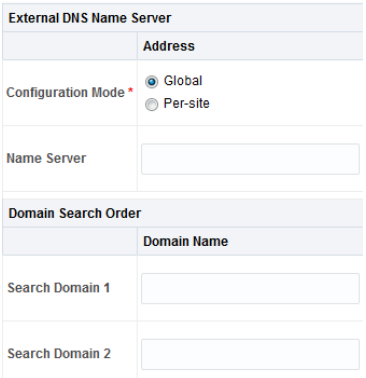
2. Navigate to **Administration > Remote Servers > DNS Configuration**.



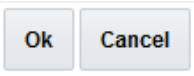
3. Select the NOAM tab:



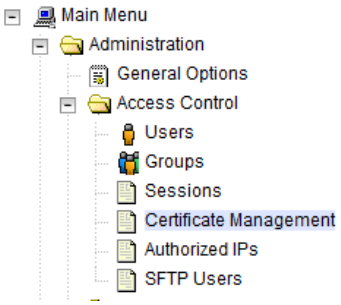
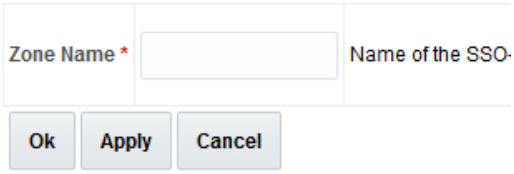
4. Configure values for the following fields:
   - Domain Name
   - Name Server
   - Search Domain 1

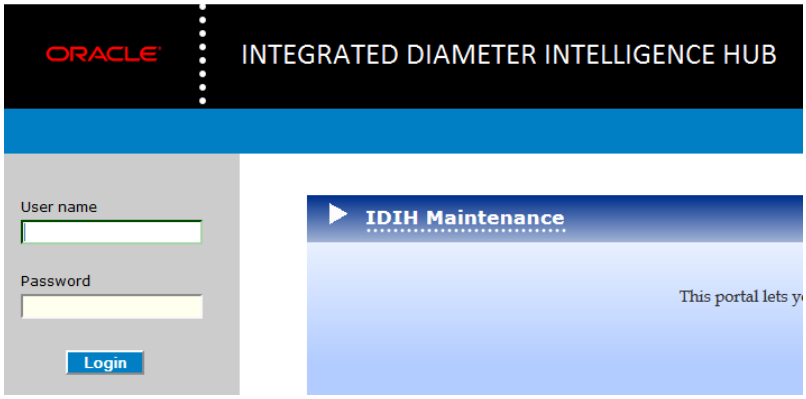
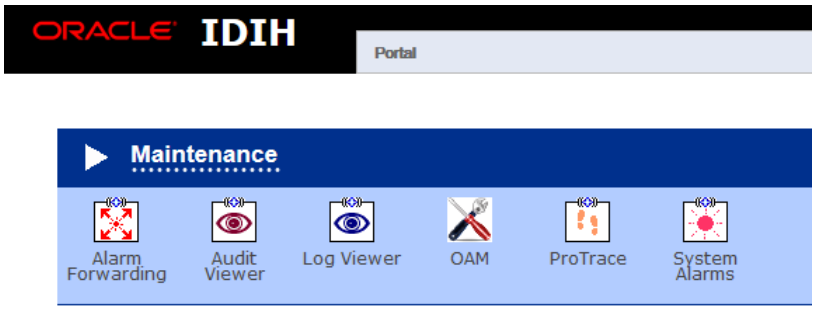
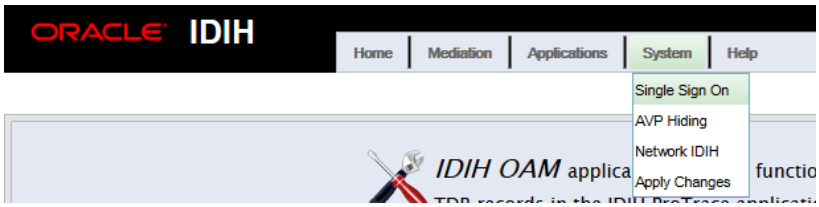
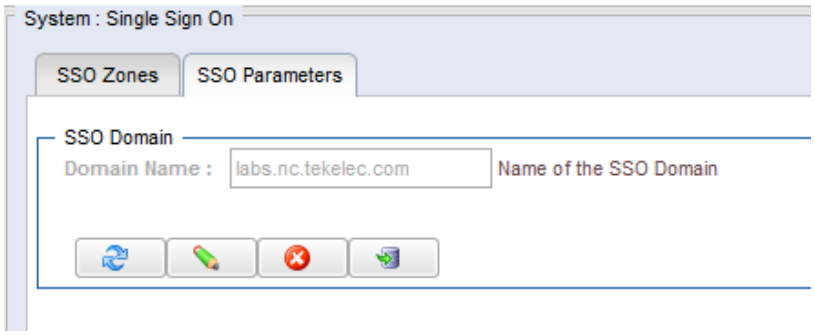


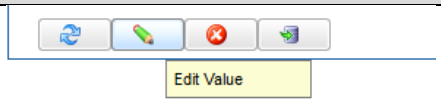
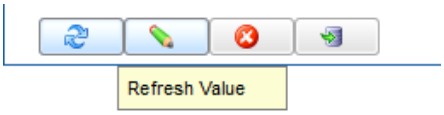
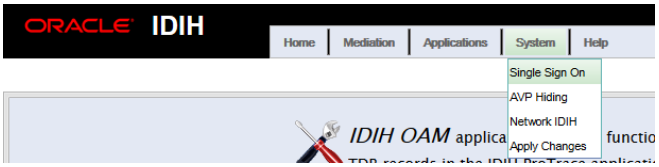
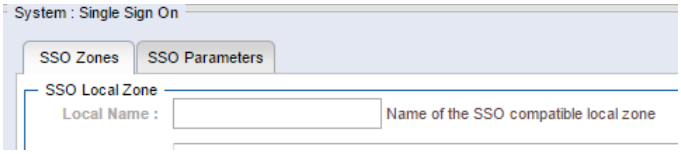
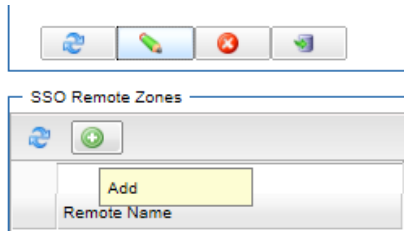
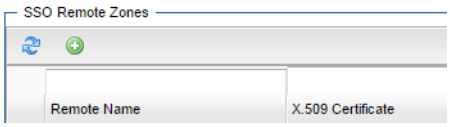
5. If values have already been configured, click **Cancel**; otherwise, configure the above values and click **OK**.



6. The Certificate Management window is updated with the SSO Certificate.

Step#	Procedure	Description
3.	**NOAM VIP GUI**: Establish SSO local zone	1. Navigate to **Access Control > Certification Management**.  2. Click **Establish SSO Zone**.  Enter a value for **Zone Name**:  3. Click **OK**. Information for the new Certificate type of SSO Local displays. 4. Click **Report**.  The Certificate Report displays. 5. Select and copy the encoded certificate text to the clipboard for future access. Example of Certificate 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-----

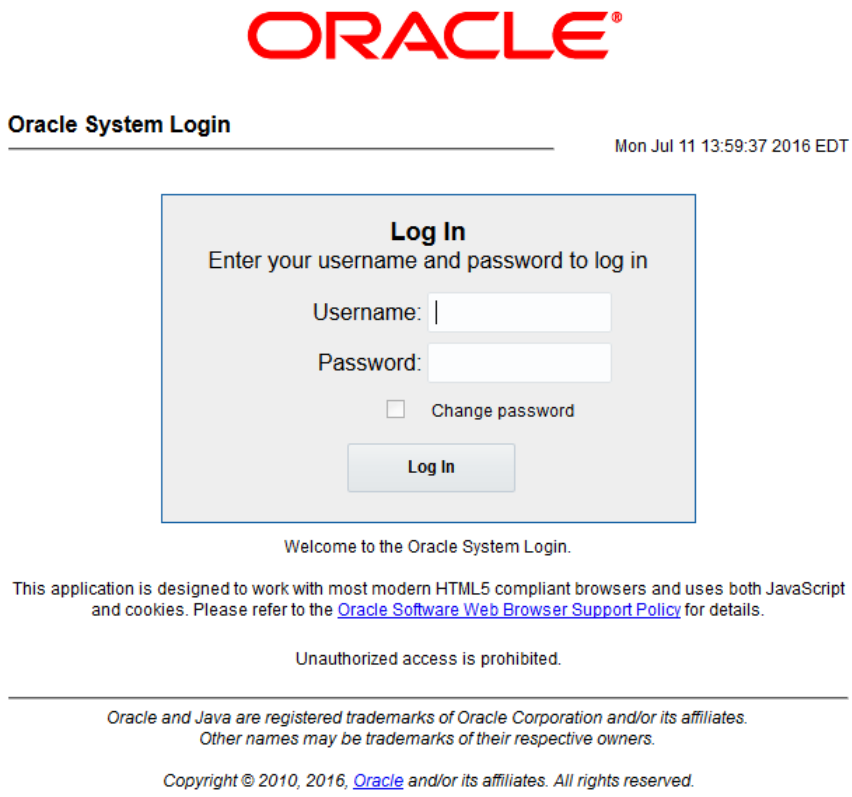
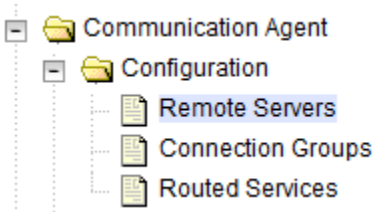
Step#	Procedure	Description
4. ☐	**IDIH Application Server GUI**: Login	1. Establish a GUI session on the IDIH application server: 2. Login as the **idihadmin** user: 
5. ☐	**IDIH Application Server GUI**: Launch the OAM portal	Navigate to the OAM portal Icon to Launch the OAM web application: 
6. ☐	**IDIH Application Server GUI**: Configure the SSO domain	1. Navigate to **System > Single Sign On**.  2. Select the SSO Parameters tab.  3. Click the **Edit Value** icon.

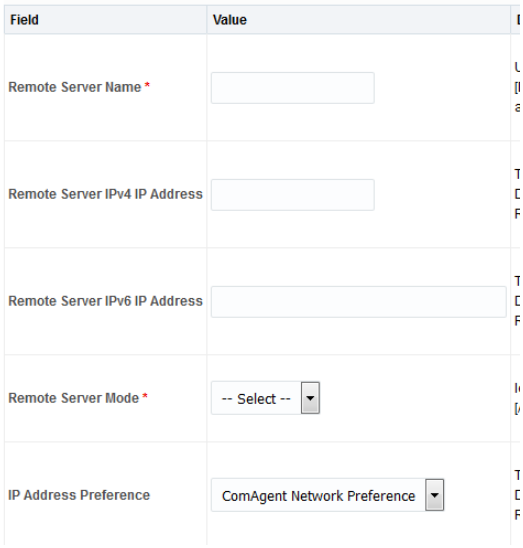
Step#	Procedure	Description
		 4. Enter a value for the Domain Name. ***Note***: This should be the same domain name assigned in the DSR NOAM DNS configuration (step 2). 5. Click the **Save** icon.  6. Click the **Refresh** icon to display data saved for the remote zone. 
7. ☐	**IDIH Application Server GUI**: Configure the SSO remote zone	1. Navigate to **System > Single Sign On**.  2. Select the **SSO Zones** tab.  3. Click the **Add** icon.  4. Enter a value for field **Remote Name**.  5. For field **X.509 Certificate**, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.

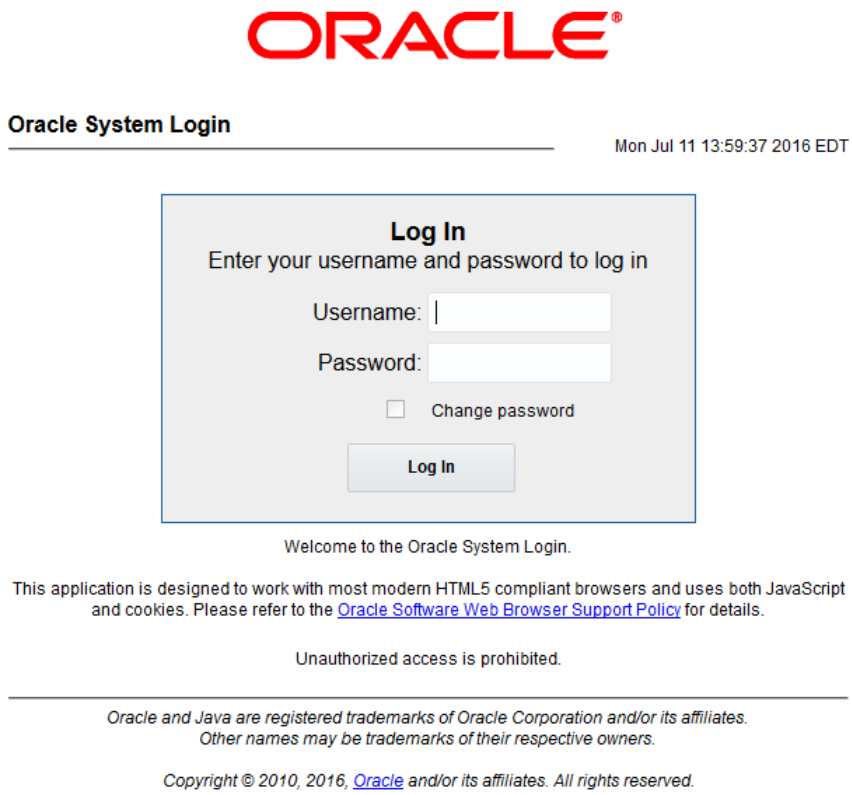
Step#	Procedure	Description
		X.509 Certificate -----BEGIN CERTIFICATE----- MIIENTCCAx2gAwIBAgIBA MA0GA1UECgwGT3JhY2xlMREwDwYDVQQLDAhBcHBX CQEWEnN1cHBvcnRAb3JhY2xlLmNvbTAeFw0xNTA3MT FDASBgNVBAcMC01vcnJpc3ZpbGxlMQ8wDQYDVQQKD dHlwZT1BV1NTTzEhMB8GCSqGSIb3DQEJARYSc3Vwc ywYDdhXchb5bhORLUGCsSpo4RzHHlvKAu7DNi2GSs9p DrVBDyqDqmBhP1stxGAaBFhnbSuUma2Qgy4mKppfeyX LLx5+c5EwkS8OhB9AVqwjX+oETf58WYKgAgIX82c8rAW FoAUnwCZ+1CZucSz4AivgXb122X/SLYwDAYDVR0TBAI tJi7N8HC9AEe0Sn8akEdE9pJHP7NwGjY1v5581Z2dnJ2a dxoXMVS5tEOO5Ea5PKk6Zyl3QCet1sEa5CRjilbOU94hjc CERTIFICATE----- 6. Click the **Save** icon.  7. Click the **Refresh** icon to display the data saved for remote zone. 

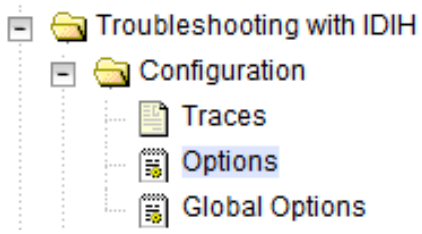
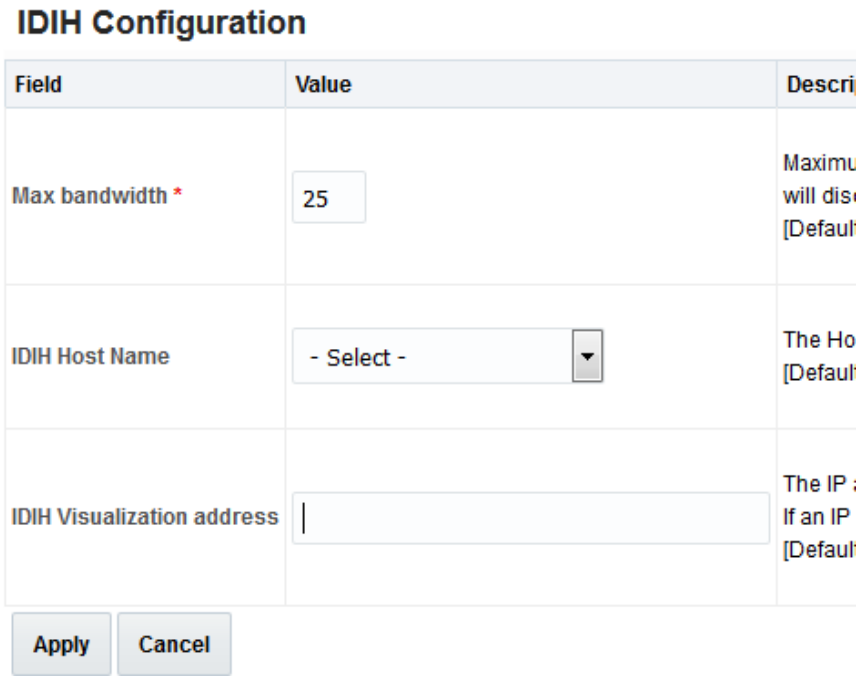
Procedure 33. IDIH Configuration: Configure IDIH in the DSR

Step#	Procedure	Description
This procedure completes 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.

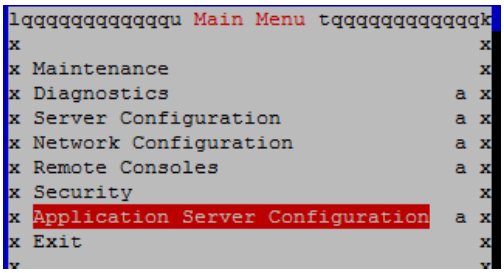
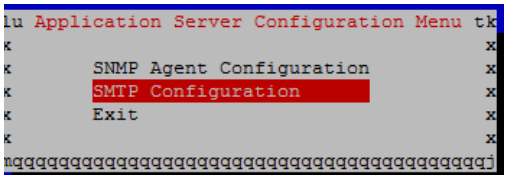
Step#	Procedure	Description
		
2.	**NOAM VIP GUI**: Configure ComAgent connection	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  2. Click **Insert**.  3. Add the IDIH mediation server. 4. For the remote server IP address field, type the IMI IP address of the IDIH Mediation Server. 5. For the IP address preference field, type the IP protocol preference (if IPv6 and IPv4 are configured).

Step#	Procedure	Description
		Inserting Remote Servers  6. Set the Remote Server Mode to **Server**. 7. Select the DA-MP server group from the **Available Local Server Groups** column. 8. Click the **>>** button to move the DA-MP server group to the **Assigned Local Server Groups** column.  9. Click **OK**.

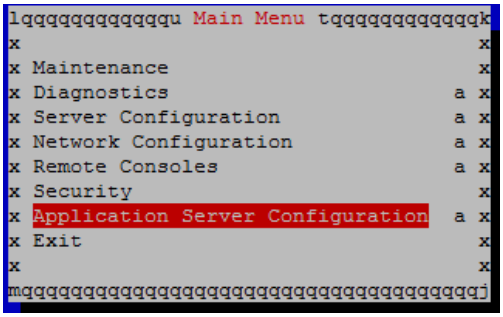
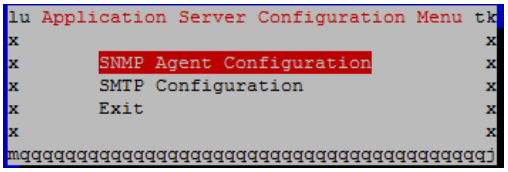
Step#	Procedure	Description
3. ☐	**SOAM VIP GUI**: Login	1. Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
4. ☐	**SOAM VIP GUI**: Configure IDIH hostname	1. Navigate to **Diameter > Troubleshooting with IDIH > Configuration > Options**.  2. Select the mediation server configured in step to in the **IDIH Host Name** field from the list. 3. Type the fully qualified domain name (or IP address) of the application server in the I**DIH Visualization Address** field:  4. Click **Apply**.

Procedure 34. IDIH Configuration: Configure Mail Server (Optional)

Step#	Procedure	Description
This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Application Server**: Login	Establish an SSH session to the IDIH Application Server and login as **admusr**.
2. ☐	**IDIH Application Server**: Configure the authenticated mail server	5. Enter the platcfg menu, execute the following command: `$ sudo su - platcfg` 6. Select Application Server Configuration.  7. Select **SMTP Configuration**.  8. Click **Edit**. 9. Enter the following parameters: • Mail Server IP Address • User • Password • Email Address (From) • Mail smtp timeout • Mail smtp connectiontimeout • SNMP over SSL used? 10. Click **OK**. 11. Click **Exit** to exit the platcfg menu.

Procedure 35. IDIH Configuration: Configure SNMP Management Server (Optional)

Step#	Procedure	Description
This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Application Server**: Login	Establish an SSH session to the IDIH application server and login as **admusr**.
2. ☐	**IDIH Application Server**: Configure SNMP Management Server	1. Enter the platcfg menu, execute the following command: `$ sudo su - platcfg` 2. Select **Application Server Configuration**.  3. Select **SNMP Agent Configuration**.  4. Click **Edit**. 5. Type the IP address of the SNMP management server. ***Note***: The SNMP agent configuration is updated and the SNMP management server is automatically restarted. 6. Click **OK**. 7. Click **Exit** to exit the platcfg menu.

Procedure 36. IDIH Configuration: Change Network Interface (Optional)

Step#	Procedure	Description
This procedure changes 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Mediation Server**: Login	1. Establish an SSH session to the IDIH mediation server. Login as user **admusr**. 2. 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 37. IDIH Configuration: Backup the Upgrade and Disaster Recovery FDC File

(Optional)

Step#	Procedure	Description
This procedure generates 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 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 click **Enter**. If the Customer System is a Windows system please refer to reference [1] Using WinSCP to copy the backup image to the customer system.

Step#	Procedure	Description

5. ☐	**PMAC Server**: Backup FDC file	Transfer the fdc file to the fdc directory so that the file can be backed up with PMAC backups.
		Issue the following command to ensure the directory where the backups are stored exists:
		`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/fdc`
		If you receive an error such as the following:
		`-bash: ls: /usr/TKLC/smac/etc/fdc: No such file or directory`
		Create the directory by issuing the following command:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc`
		Issue the following command to copy the fdc files to the fdc backup directory:
		`$ sudo cp /var/TKLC/smac/etc/<idih_upgrade.xml> /usr/TKLC/smac/etc/fdc/`

Procedure 38. IDIH Configuration: Change Alarm Ignore List (Optional)

Step#	Procedure	Description
This procedure changes the alarm severity and/or identifiers to ignore on the mediation server. ***Note***: Initially the default is to ignore alarms with severity 4 (informational) ***Note***: A script is provided to manage the settings so that the operator does not need to know the details required to apply the settings. There are two settings 'ignore.event' and 'ignore.severity' Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Mediation Server**: Login	1. Establish an SSH session to the IDIH mediation server. Login as user **admusr**. 2. Issue the following commands to login as **tekelec** user. `$ sudo su - tekelec`

Step#	Procedure	Description

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

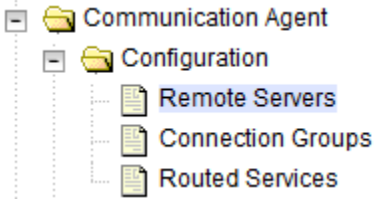
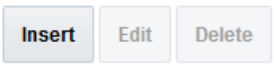
4.7.1 Activate Optional Features

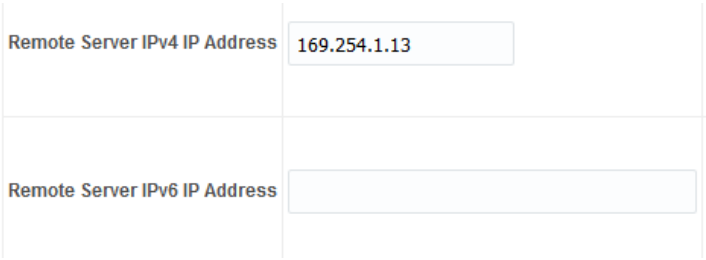
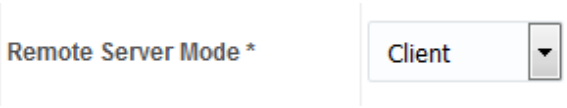
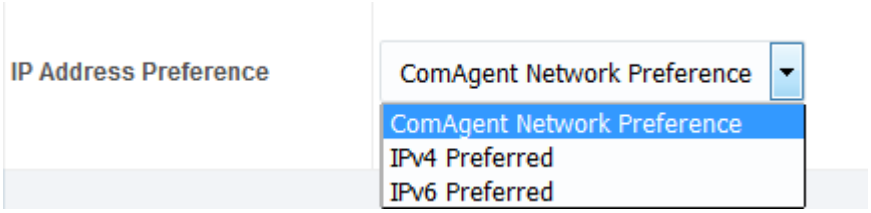
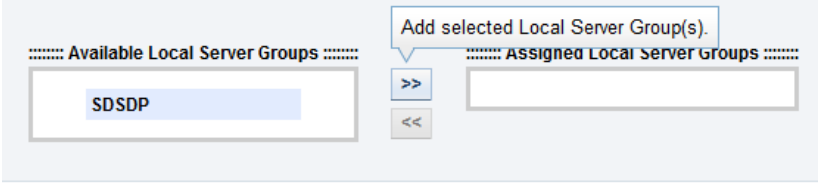
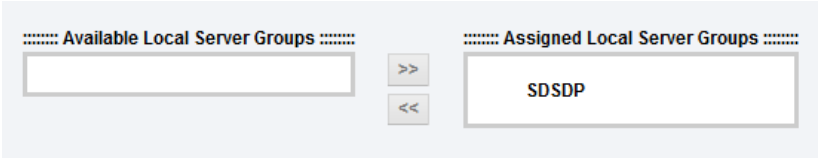
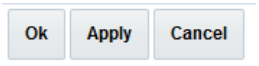
Procedure 39. Activate Optional Features

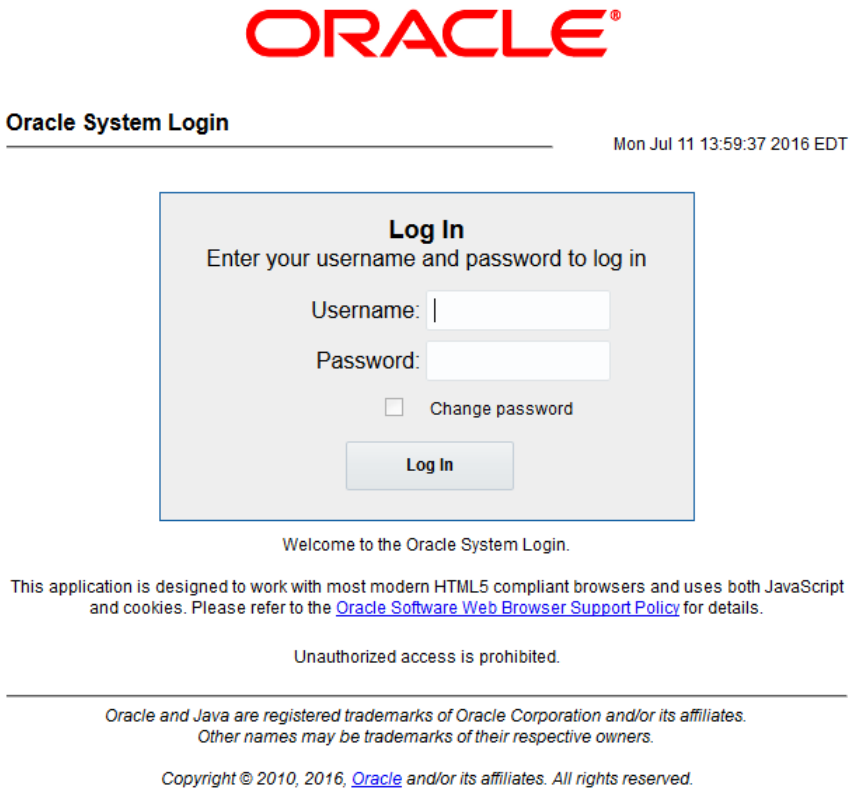
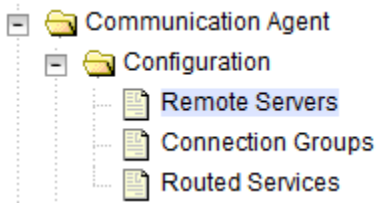
Step#	Procedure	Description
This procedure installs DSR optional components once regular installation is complete. ***Prerequisite***: All previous DSR installation steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Refer to Activation Guides for optional features	Refer to 3.4 Optional Features for a list of feature activation documents whose procedures are to be executed at this moment.

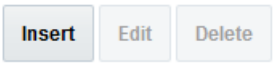
4.7.2 Configure ComAgent Connections (DSR + SDS)

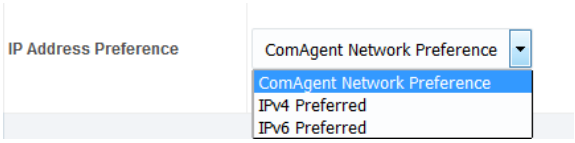
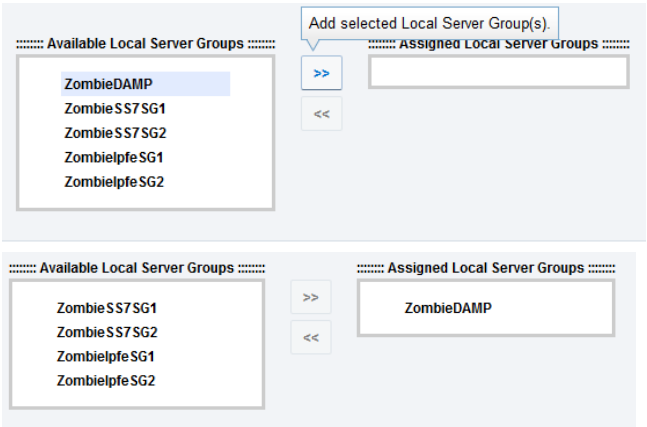
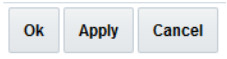
Procedure 40. Configure ComAgent Connections (DSR + SDS)

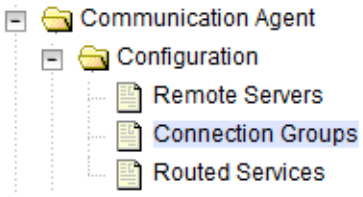
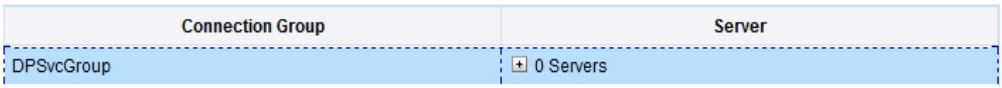
Step#	Procedure	Description
This procedure configures ComAgent connections on DSR/SDS for use in the FABR application. ***Prerequisite*:** FABR application is activated. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the SDS NOAM by using the XMI VIP address. Open the web browser and enter a URL of: `https://<Primary_SDS_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
2. ☐	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  2. Click **Insert**. 

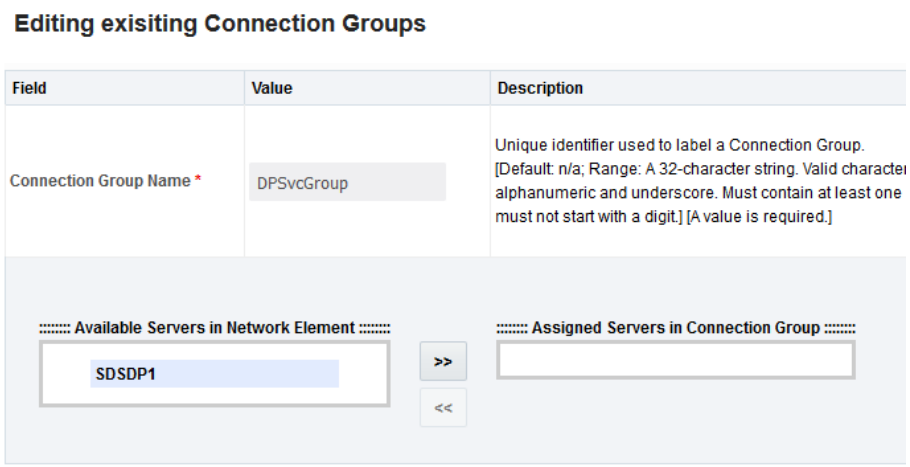
Step#	Procedure	Description
3. ☐	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Type the **Remote Server Name** for the DSR MP server:  2. Type the **Remote Server IMI IP Address**.  ***Note***: This should be the IMI IP address of the DAMP server. 3. Select **Client** for the **Remote Server Mode** from the list.  4. Select **IP Address Preference** (ComAgent Network Preference, IPv4 Preferred, or IPv6 Preferred) from the list.  Select the **Local Server Group** for the SDS DP server group and click **>>**.   5. Click **Apply**. 
4. ☐	**SDS NOAM VIP GUI**: Repeat	**Repeat** steps 2-3 for each remote MP in the same SOAM NE.

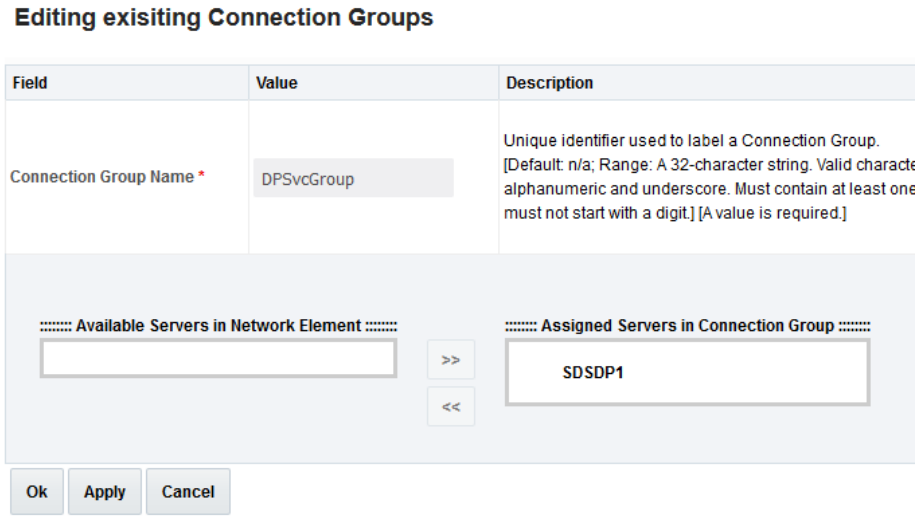
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>5.
</td><td>DSR NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
<code>https://<Primary_DSR_NOAM_VIP_IP_Address></code>
2. Login as the guiadmin user.
 
</td></tr>
<tr><td>6.
</td><td>DSR NOAM VIP GUI: Configure remote server IP address</td><td>1. Navigate to Communication Agent > Configuration > Remote Servers.
 

2. Click Insert.
 
</td></tr>
</table>

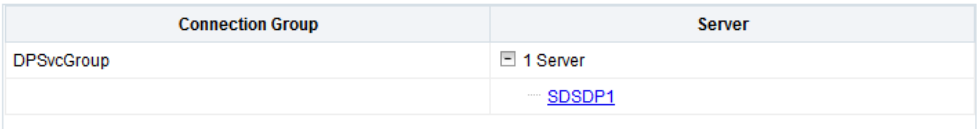
Step#	Procedure	Description
7. ☐	**DSR NOAM VIP GUI**: Configure remote server IP address	1. Type the **Remote Server Name** for the SDS DP server:  2. Type the Remote Server IMI IP Address.  ***Note***: This should be the IMI IP address of the DP server. 3. Select **Server** for the **Remote Server Mode** from the list.  4. Select **IP Address Preference** (ComAgent Network Preference, IPv4 Preferred, or IPv6 Preferred) from the list.  5. Select the **Local Server Group** for the DSR MP server group, click **>>**.  6. Click **Apply**. 
8. ☐	**DSR NOAM VIP GUI**: Repeat	**Repeat** steps 6-7 for each remote DP in the same SOAM NE.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>9.</td><td>DSR NOAM VIP GUI: Configure Connection Groups</td><td>Navigate to Communication Agent > Configuration > Connection Groups.
 
</td></tr>
<tr><td>10.</td><td>DSR NOAM VIP GUI: Edit connection groups</td><td>1. Select the DPSvcGroup Connection Group.
 

2. Click Edit.
3. Select the desired DP servers from the Available Servers in Network Element.
 

4. Click >>.
 

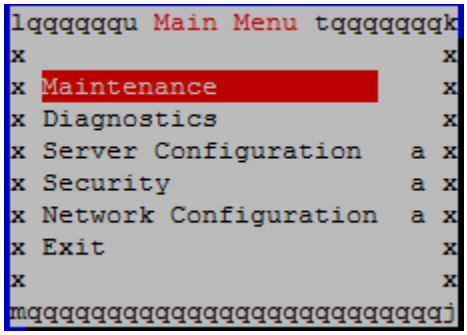
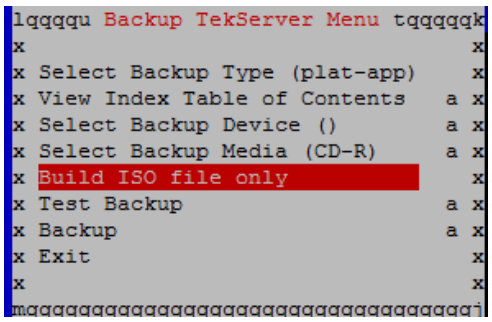
5. Click OK.</td></tr>
</table>

Step#	Procedure	Description
11. ☐	**DSR NOAM VIP GUI**: Verify correct number of servers in group	Verify correct number of servers are in the connection group. 

4.7.3 Back Up TVOE Configuration

Procedure 41. Back Up TVOE Configuration

Step#	Procedure	Description
This procedure backs 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 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 and login as **admusr**.

Step#	Procedure	Description
3. ☐	**TVOE Server**: Build ISO backup file	1. Execute the following command from the TVOE server: `$ sudo su - platcfg`  2. Navigate to **Maintenance > Backup and Restore > Backup Platform (CD/DVD).** The Backup TekServer Menu screen displays. ***Note***: If no cdrom device is found by TPD, the No disk device available. This is normal on systems without a cdrom device message displays. Press Enter. 3. 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 display for an instant. 4. After the ISO is created, platcfg returns 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** 5. Exit out of platcfg by selecting **Exit**.

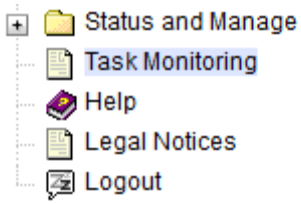
Step#	Procedure	Description
4. ☐	**Backup Server**: Transfer TVOE files to backup server	1. Log into the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/` 2. When pasked, type the tvoexfer user password and press **Enter**. 3. If the customer system is a Windows system, refer [6] 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.

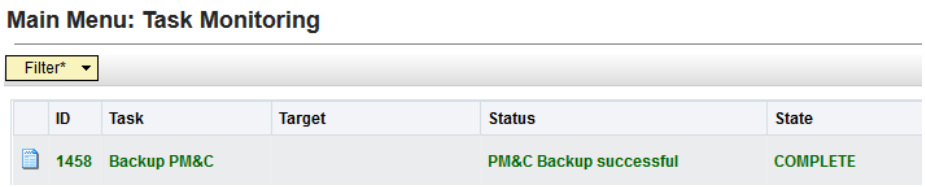
4.7.4 Back Up PMAC Application

Procedure 42. Back Up PMAC Application

Step#	Procedure	Description
This procedure backs 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 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 and 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 `sudo pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>4.
</td><td>PMAC GUI:
Login</td><td>1. Open web browser, navigate to the PMAC GUI, and enter a URL of:
<code>https://<pmac_network_Network_IP_Address></code>
2. Login as the guiadmin user.
 
</td></tr>
<tr><td>5.
</td><td>PMAC Server GUI:
Monitor/Verify backup task completion</td><td>1. Navigate to Task Monitoring.
 

2. Monitor the Backup PMAC task.
 

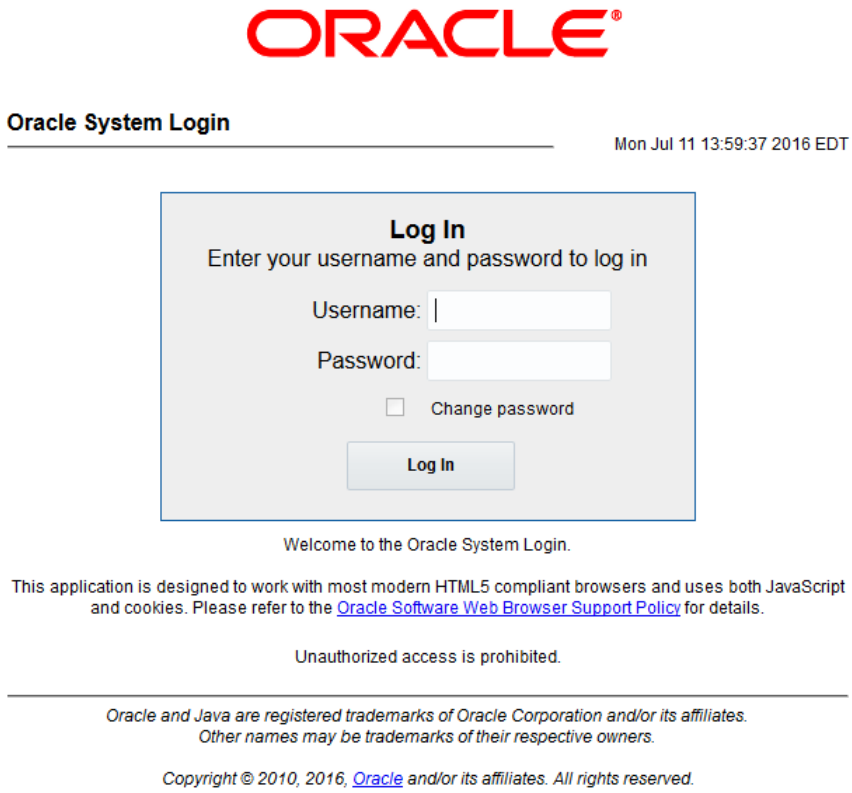
Note: Alternatively, you can monitor the Backup task by executing the following command:
<code>$ sudo pmaccli getBgTasks</code></td></tr>
</table>

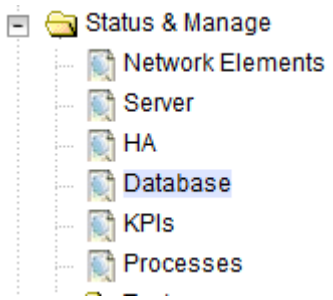
Step#	Procedure	Description
6. ☐	**Backup Server**: Transfer PMAC file to backup server	1. Log into the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/` 2. When asked, type the admusr user password and click **Enter.** 3. If the customer system is a Windows system, refer to reference [6] using WinSCP to copy the backup image to the customer system.

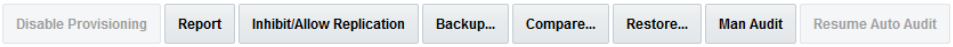
4.7.5 Backup NOAM Database

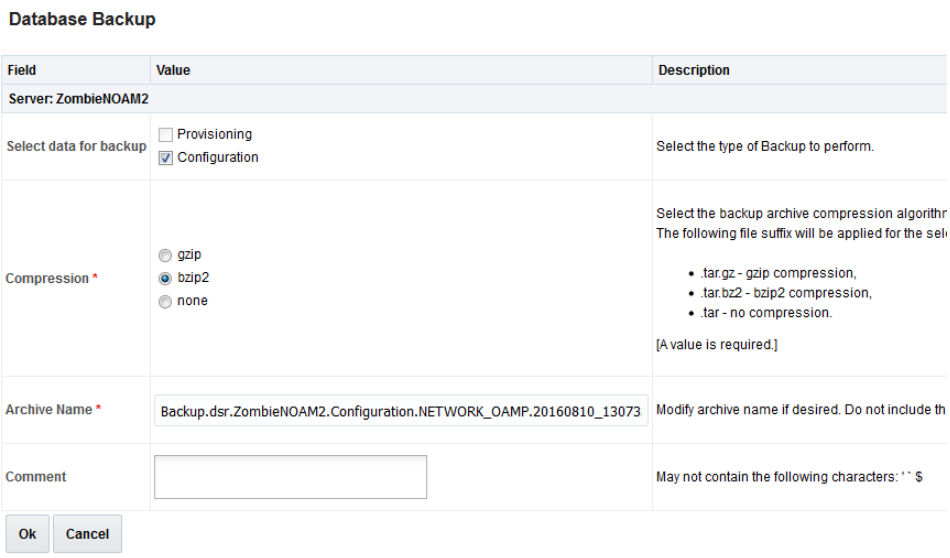
Procedure 43. NOAM Database Backup

Step#	Procedure	Description
This procedure backs 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 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

Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Login	4. 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>` 5. Login as the **guiadmin** user. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>3.
</td><td>NOAM VIP GUI:
Perform database backup</td><td>1. Navigate to Status & Manage > Database.
 

2. Select the Active NOAM.
3. Click Backup.
 

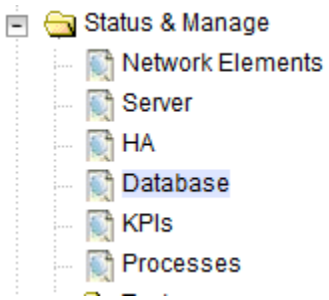
4. Select the desired file compression method.
 

5. Set the archive file name, if needed.
6. Click OK.</td></tr>
<tr><td>4.
</td><td>Backup Server:
Transfer file to backup server</td><td>1. Log into the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.
<pre>$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/</pre>
2. When asked, type the admusr user password and press Enter.
3. If the customer system is a Windows system, refer to reference [6] using WinSCP to copy the backup image to the customer system.</td></tr>
</table>

4.7.6 Backup SOAM Database

Procedure 44. SOAM Database Backup

Step#	Procedure	Description
This procedure backs 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 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	1. Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

Step#	Procedure	Description
3. ☐	**SOAM VIP GUI**: Perform database backup	1. Navigate to **Status & Manage > Database**.  2. Select the Active SOAM. 3. Click **Backup**.  4. Select the desired file compression method. **Database Backup** Field / Value / Descrip Server: ZombieSOAM1 Select data for backup: ☐ Provisioning ☑ Configuration Compression *: ○ gzip ◉ bzip2 ○ none Archive Name *: Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.N Comment Ok Cancel 5. Set the archive file name, if needed. 6. Click **OK**.

Step#	Procedure	Description
4. ☐	**Backup Server**: Transfer SOAM file to backup server	1. Log into the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. `$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/` 2. When asked, enter the admusr user password and press **Enter**. 3. If the Customer System is a Windows system, refer to [6] using WinSCP to copy the backup image to the customer system.
5. ☐	Repeat for additional TVOE servers	**Repeat** steps 2-4 for additional DSR SOAM sites.

4.7.7 Enable/Disable DTLS (SCTP Diameter Connections Only)

Procedure 45. Enable/Disable DTLS (SCTP Diameter Connections Only)

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

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

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

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

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

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

Figure 4. Example Network Element XML File

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

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

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

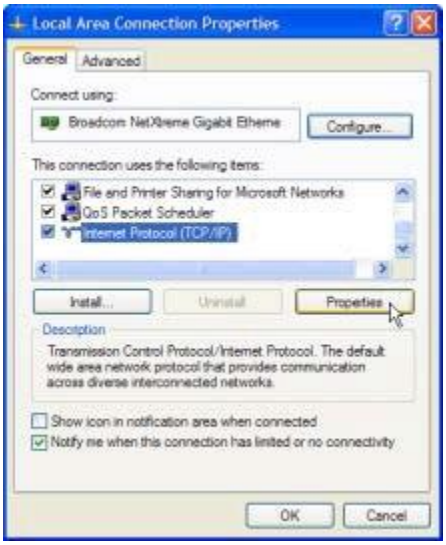
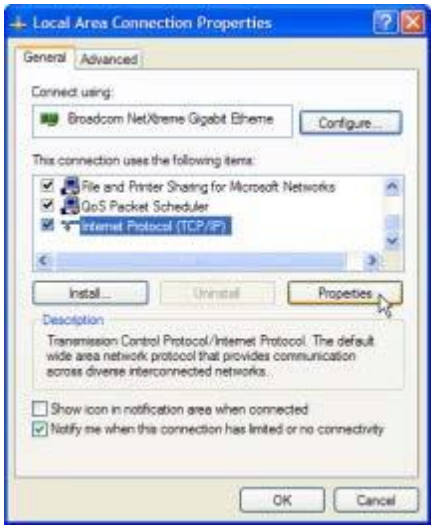
Figure 5. Example Server Hardware Profile XML-HP c-Class Blade

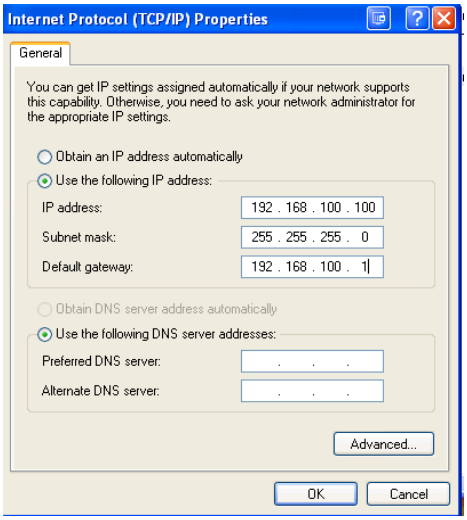
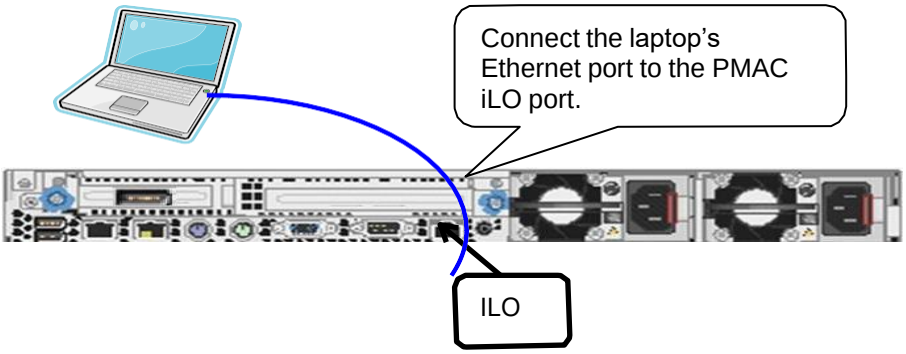
```
<profile>
<serverType>TVOE Guest</serverType>
<available>
<device>Management</device>
<device>Control</device>
<device>xmi</device>
<device>imi</device>
<device>xsi</device>
</available>
<devices>
<device>
<name>management</name>
<type>ETHERNET</type>
</device>
<device>
<name>control</name>
<type>ETHERNET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

Figure 6. Example Server Hardware Profile XML- Virtual Guest on TVOE

Appendix B. Configure for TVOE iLO Access

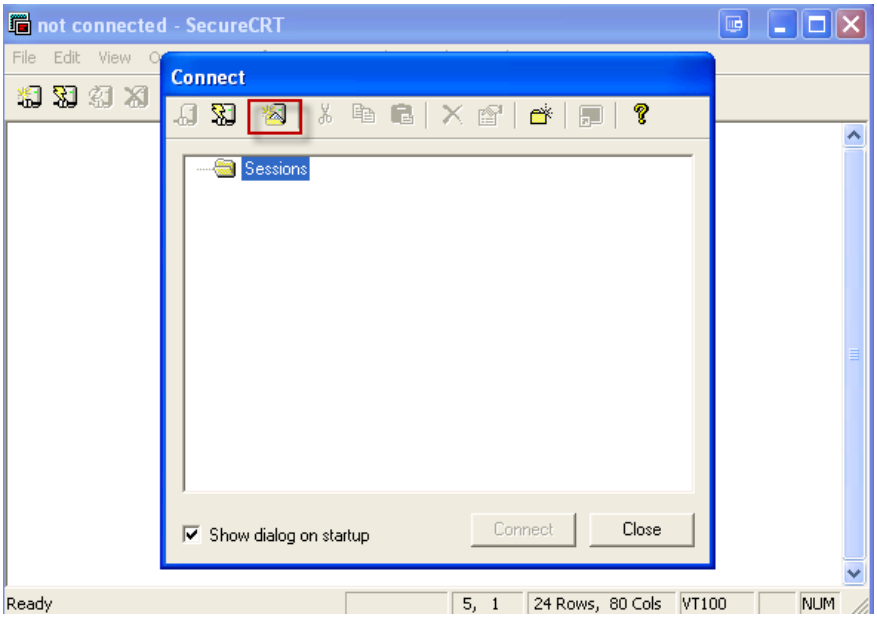
Procedure 46. Connect to the TVOE iLO

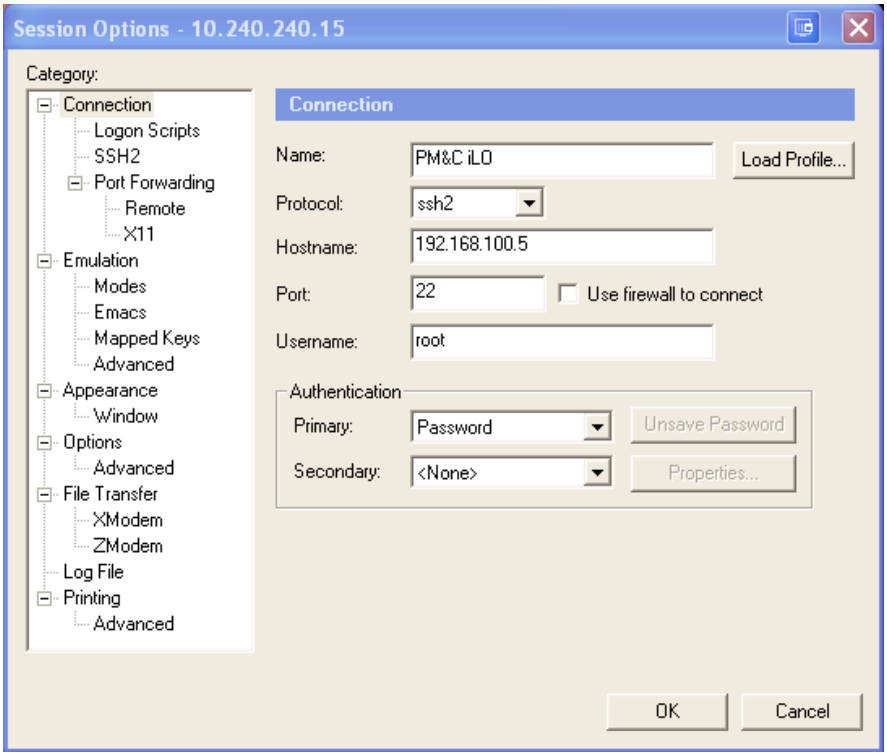
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th><th></th></tr>
<tr><td colspan="4">This procedure connects a laptop to the TVOE iLO via a directly cabled ethernet connection.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Access the laptop network interface cards TCP/IP Properties screen.
Note: For this step, follow the instructions specific to the laptop's OS (Windows XP or Windows 7)</td><td>Windows XP
1. Go to Control Panel.
2. Double-click on Network Connections.
3. Right-click the wired Ethernet Interface icon and select Properties.
4. Click Internet Protocol (TCP/IP).
5. Click Properties.
 
</td><td>Windows 7
1. Go to Control Panel.
2. Double-click on Network and Sharing Center.
3. Click Change Adapter Settings (left menu).
4. Right-click the Local Area Connection icon and click Properties.
5. Click Internet Protocol Version 4 (TCP/IPv4).
 
</td></tr>
</table>

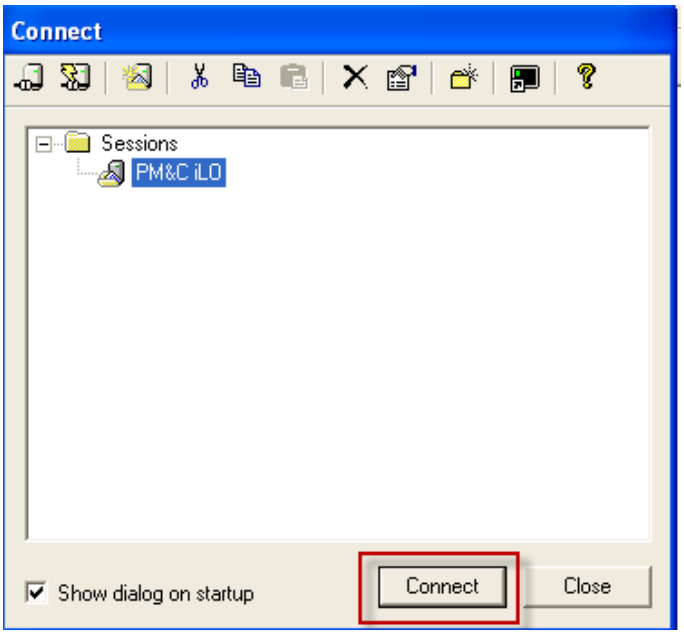
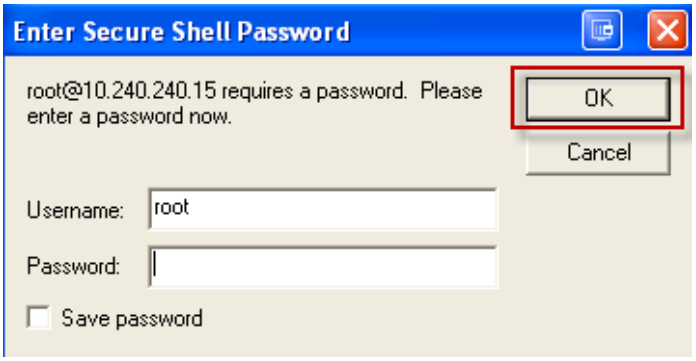
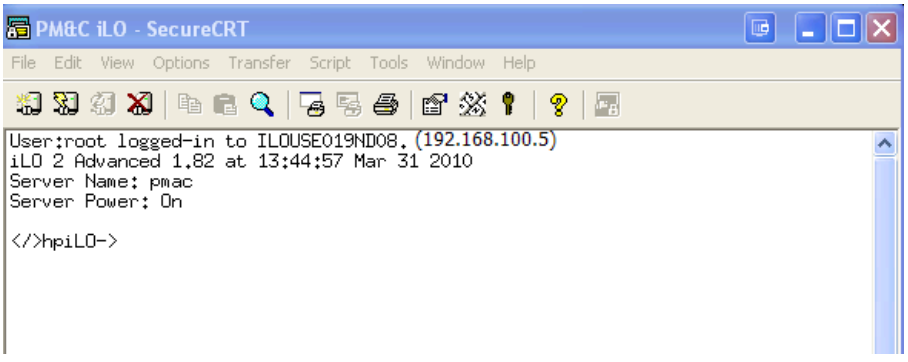
Step#	Procedure	Description
2. ☐	Configure IP address	1. Click Use the following IP address. 2. Set the **IP address** to 192.168.100.100. 3. Set the **Subnet mask** to 255.255.255.0. 4. Set the **Default gateway** to 192.168.100.1. 5. Select **OK**. 6. Click **Close** from the network interface card's main Properties screen.  
3. ☐	Connect ports	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

Procedure 47. Access the TVOE iLO

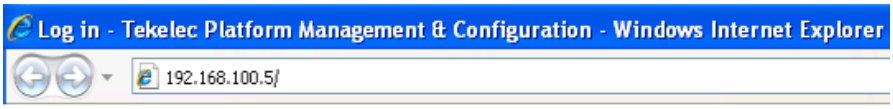
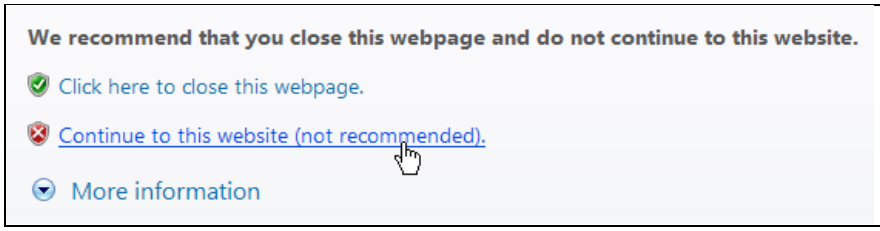
Step#	Procedure	Description
This procedure contains the steps to access the TVOE iLO. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Launch terminal emulator	1. Open a terminal emulator, for example, Putty, Secure CRT. 2. Navigate to **File > Connect**. 3. Click the **New Session** icon. ***Note***: This example demonstrates Secure CRT. 

Step#	Procedure	Description
2. ☐	Configure TVO ILO	**Name**: Type TVOE iLO **Hostname**: 192.168.100.5 (Manufacturing default) or customer IP set during installation **Username**: Type **admusr** Click **OK**. ***Note***: See Configure for TVOE iLO Access to configure your system network to access the TVOE iLO. 

Step#	Procedure	Description
3. ☐	Connect to TVO iLOE	1. Navigate **File > Connect** to open the Connect window. 2. Highlight the session you created and click **Connect.** 
4. ☐	Log into TVO iLOE	Login to the TVOE iLO using the appropriate password.  The TVOE iLO displays. 

Appendix D. TVOE iLO4 GUI Access

Procedure 48. TVOE iLO4 GUI Access

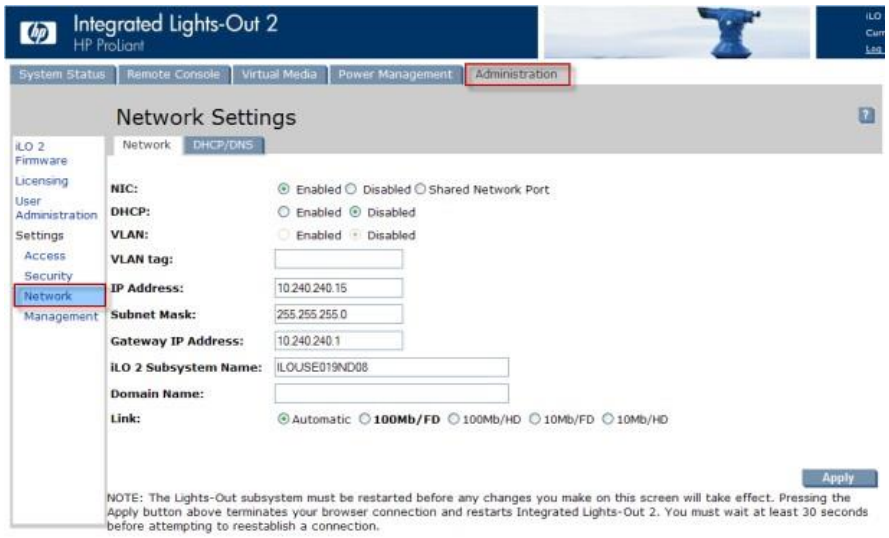
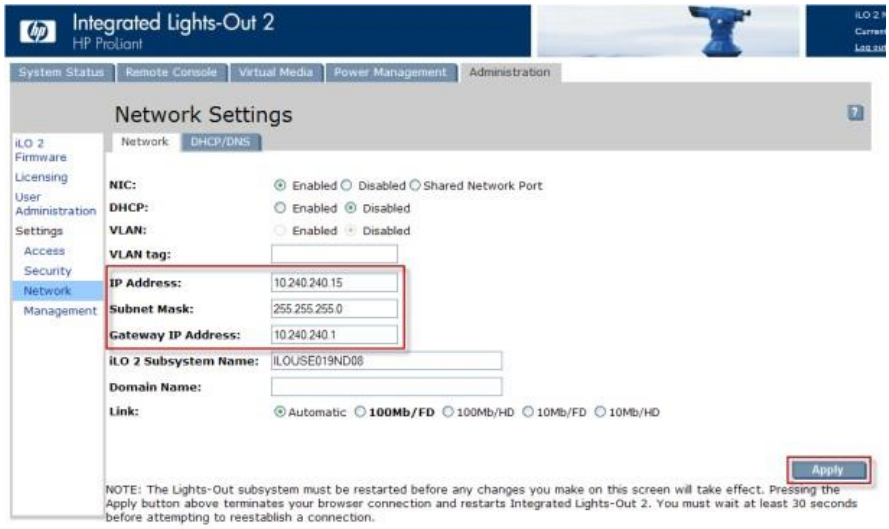
Step#	Procedure	escription
This procedure accesses the TVOE iLO4 GUI. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. □	Launch Internet Explorer	avigate to 192.168.100.5 (manufacturing default) or customer IP set during i stallation.  nternet Explorer may display a warning message regarding the security ertificate. elect the option to **Continue to the website (not recommended)**. 
2. □	Log into the iLO4	into the iLO4.  he iLO4 Home page displays. 

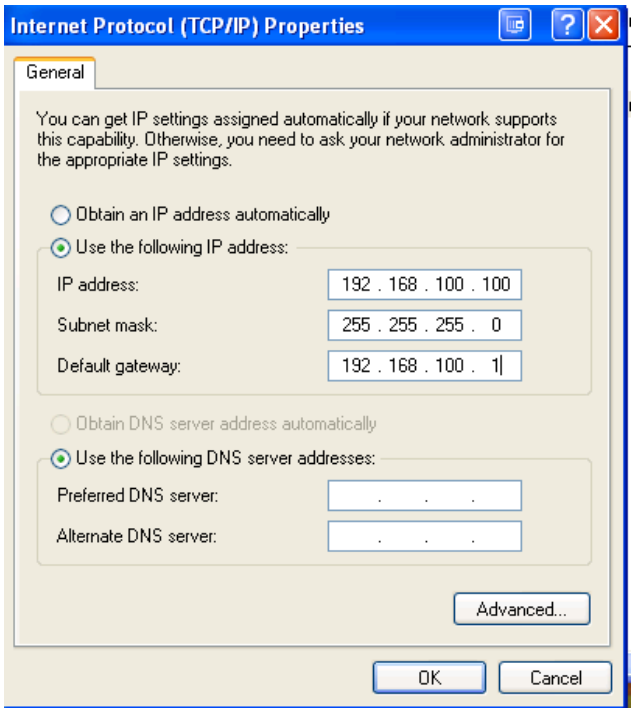
Step#	Procedure	Description
3. ☐	Launch the PMAC iLO4 CLI	Click **Launch** to start the PMAC iLO4 CLI. 

Appendix E. Change the TVOE iLO Address

Procedure 49. Change the TVOE iLO Address

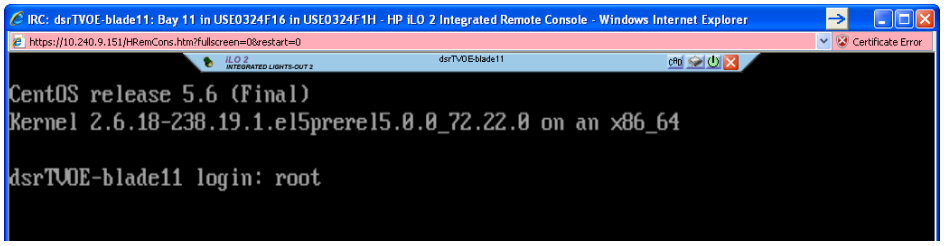
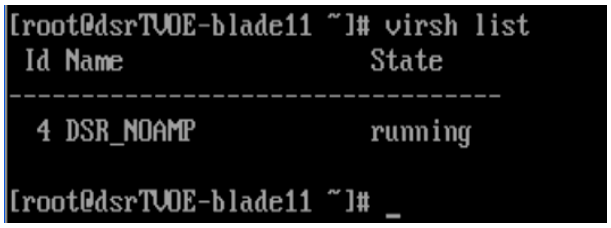
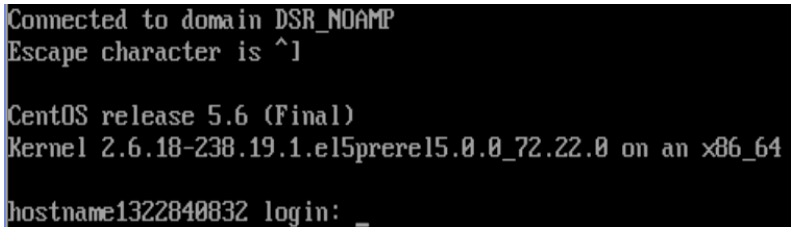
Step#	Procedure	Description
This procedure sets the IP address of the TVOE iLO to the customer's network so it can be accessed by Oracle support. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Connect to the TVOE iLO GUI	Using the instructions in TVOE iLO4 GUI Access, connect to TVOE iLO GUI. 

Step#	Procedure	Description
2. ☐	**ILO GUI**: Navigate to the network menu	1. Click the Administration tab. 2. Under Settings in the left column, click **Network**. 
3. ☐	**ILO GUI**: Configure TVOE iLOE ***Note***: You lose access after you click **Apply**.	1. Change the **IP Address, Subnet Mask**, and **Gateway IP Address** to the values supplied in the IP site survey for the TVOE iLO. 2. Click **Apply**. 

Step#	Procedure	Description
4. ☐	**Local Machine**: Reset PC's network connection	Reset the PC's network connection replacing the **Subnet Mask** and **Gateway** with those just used for the TVOE iLO. Use an appropriate **IP address** for this subnet. 
5. ☐	**Local Machine**: Connect to the TVOE iLO GUI	Connect to the TVOE iLO GUI using the instructions in TVOE iLO4 GUI Access. ***Note***: Use the IP address entered in step 3. 

Appendix F. PMAC/NOAM/SOAM Console iLO Access

Procedure 50. PMAC/NOAM/SOAM Console iLO Access

Step#	Procedure	escription
This procedure logs 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Log into TVOE	Login as **admusr** on the TVOE server hosting the NOAM using either ILO or SSH to the TVOE server's XMI or Mgmt. address. 
2. ☐	Locate VM	1. On the TVOE host, execute the following command: `$sudo virsh list` This produces a list of currently running virtual machines.  2. Find the VM name for your DSR NOAM and note its ID number in the first column. ***Note***: If the VM state is not listed as **running** or you do not find a VM you configured for your NOAM at all, then halt this procedure and contact Oracle Customer Support.
3. ☐	Connect to console of the VM using the VM number obtained in step 2.	1. On the TVOE host, execute: `$sudo virsh console <DSRNOAM-VMID>` 2. Where **DSRNOAM-VMID** is the VM ID you obtained in step 2.  You are now connected to the DSR NOAMs console. 3. If you wish to return to the TVOE host, you can exit the session by pressing **CTRL +]**.

Appendix G. List of Frequently Used Time Zones

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

Table 3. List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico City	Central Time — most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01
Asia/Hong Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time — west British Columbia	UTC-08
America/Edmonton	Mountain Time — Alberta, east British Columbia & west Saskatchewan	UTC-07
America/Toronto	Eastern Time — Ontario — most locations	UTC-05
America/Montreal	Eastern Time — Quebec — most locations	UTC-05
America/Sao Paulo	South & Southeast Brazil	UTC-03

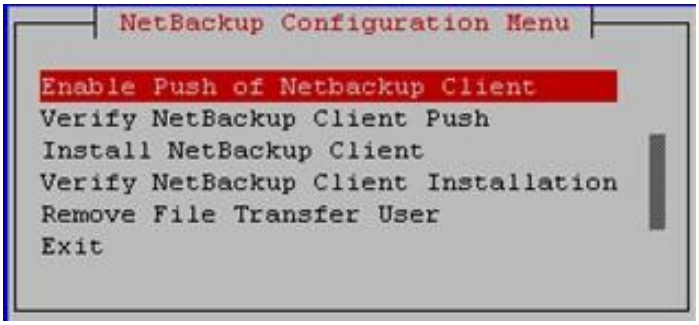
Time Zone Value	Description	Universal Time Code (UTC) Offset
Europe/Brussels		UTC+01
Australia/Perth	Western Australia — most locations	UTC+08
Australia/Sydney	New South Wales — most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto Rico		UTC-04
Europe/Moscow	Moscow+00 — west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

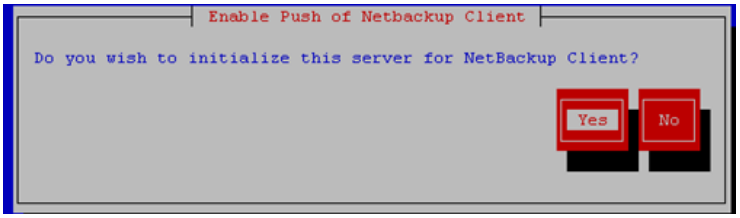
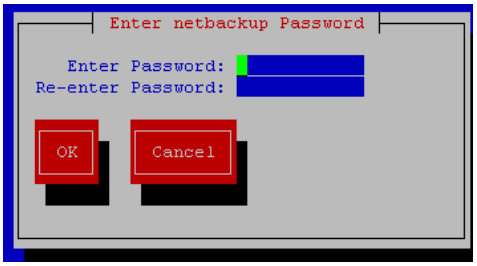
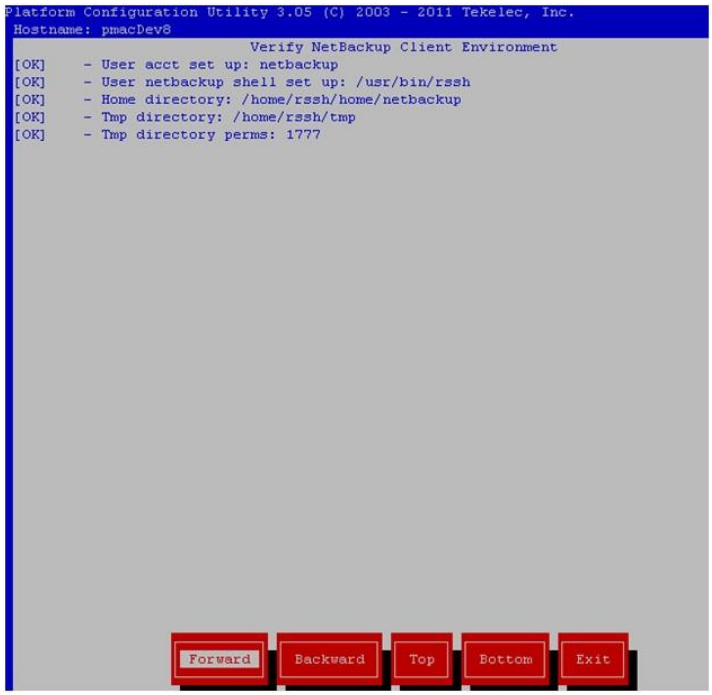
Appendix H. Application NetBackup Client Installation Procedures

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

Appendix H.1 NetBackup Client Installation Using PLATCFG

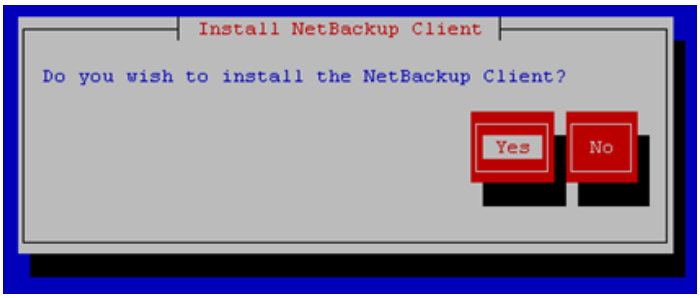
Procedure 51. Application NetBackup Client Installation (Using Platcfg)

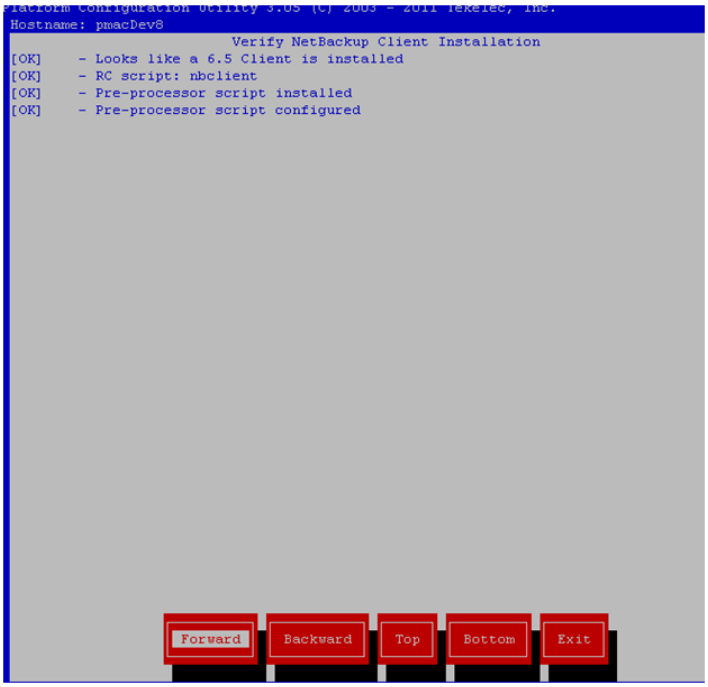
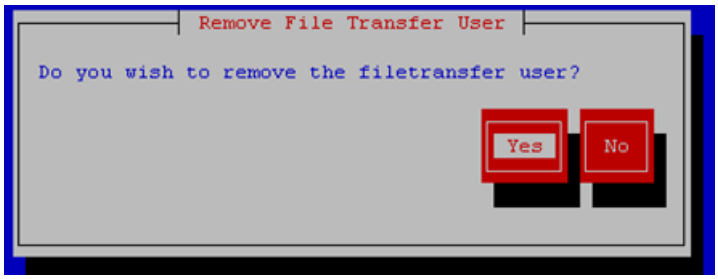
Step#	Procedure	Description
This procedure explains the NetBackup installation using platcfg. ***Prerequisites***: • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. • Execute Appendix A.3 of [1] ***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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Application Server iLO: Login	1. Login and launch the integrated remote console. 2. ssh to the application server (PMAC or NOAM) as **admusr** using the management network for the PMAC or XMI network for the NOAM.
2. ☐	Application Server iLO: Navigate to NetBackup configuration	1. Configure NetBackup Client on application server. `$ sudo su - platcfg` 2. Navigate to NetBackup > Configuration. 

Step#	Procedure	Description
3. ☐	**Application Server iLO**: Enable push of NetBackup client	Navigate to **NetBackup Configuration > Enable Push of NetBackup Client**. 
4. ☐	**Application Server iLO**: Enter NetBackup password	1. Enter the NetBackup password.  2. Click **OK**. ***Note***: If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.
5. ☐	**Application Server iLO**: Verify NetBackup client software push is enabled	1. Navigate to **NetBackup Configuration > Verify NetBackup Client Push**.  2. Verify list entries indicate **OK** for NetBackup client software environment. 3. Click **Exit** to return to NetBackup Configuration menu.

Step#	Procedure	Description

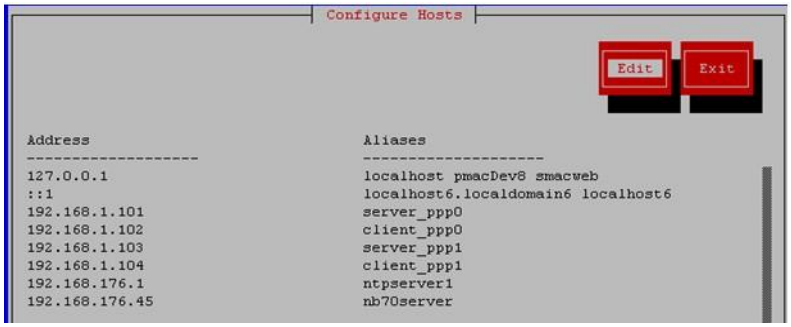
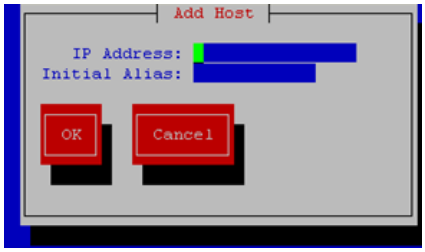
6. ☐	**NetBackup Server**: Push appropriate NetBackup client software to application server	***Note***: The NetBackup server is not an application asset. Access to the NetBackup server and location path of the NetBackup Client software is under the control of the customer. Below are the steps that are 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.
		1. Log into the NetBackup server using password provided by customer.
		2. 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`
		3. 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:`
		4. 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`

Step#	Procedure	Description
		./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. 5. 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.
7. ☐	**Application Server iLO**: Install NetBackup client software on application server	1. Execute the command: $ sudo chmod 555 /var/TKLC/home/rssh/tmp/client_config **NETBACKUP_BIN** is the temporary directory where the NetBackup client install programs were copied in step 5. The directory should look similar to **/tmp/bp.XXXX/**. 2. Navigate to **NetBackup Configuration > Install NetBackup Client**.  3. Verify list entries indicate **OK** for NetBackup client software installation. 4. Click **Exit** to return to NetBackup Configuration menu.

Step#	Procedure	Description
8. ☐	**Application Server iLO**: Verify NetBackup client software installation on the application server	1. Navigate to **NetBackup Configuration > Verify NetBackup Client Installation**.  2. Verify list entries indicate **OK** for NetBackup Client software installation. 3. Click **Exit** to return to NetBackup Configuration menu.
9. ☐	**Application Server iLO**: Disable NetBackup client software transfer to the application server	1. Navigate to **NetBackup Configuration > Remove File Transfer User**.  2. Click **Yes** to remove the NetBackup file transfer user from the application server.
10. ☐	**Application Server iLO**: Exit platform configuration utility (platcfg)	**Exit** platform configuration utility (platcfg).

11. ☐	**Application Server iLO**: Verify server bp.conf file	Verify the server has been added to the **/usr/openv/NetBackup/bp.conf** file.
		Issue the following command:
		`$ sudo cat /usr/openv/NetBackup/bp.conf`
		`CLIENT_NAME = 10.240.34.10`
		`SERVER = NB71server`

Step#	Procedure	Description

12. ☐	**Application Server iLO**: Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias	***Note***: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup **/usr/openv/NetBackup/bp.conf** file, identified by the **Server** configuration parameter.
		1. The NetBackup server hostname and IP address must be added to the application server's host's file. List NetBackup servers hostname:
		`$ sudo cat /usr/openv/NetBackup/bp.conf`
		`SERVER = nb70server`
		`CLIENT_NAME = pmacDev8`
		2. Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.
		`$ sudo su - platcfg`
		3. Navigate to Network Configuration > Modify Hosts File.
		4. Click **Edit**.
		 
		5. Click **Add Host** and enter the appropriate data.
		 
		6. Click **OK**.
		 
		7. Confirm the host alias added and exit Platform Configuration Utility.

Step#	Procedure	Description

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

Appendix H.2 NetBackup Client Install/Upgrade with NBAutoInstall

Note: Execute the following procedure to switch/migrate to having NetBackup installed via NBAutoInstall (push configuration) instead of manual installation using platcfg.

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

Procedure 52. Application NetBackup Client Installation (NBAutoInstall)

Step#	Procedure	Description
This procedure installs NetBackup 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Application Server iLO**: Login	1. Login and launch the integrated remote console. 2. ssh to the application server (PMAC or NOAM) as admusr using the management network for the PMAC or XMI network for the NOAM.
2. ☐	**Application Server iLO**: Enable nbAutoInstall	Execute the following command: `$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable`

Step#	Procedure	Description

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	1. 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 the server name matches the NetBackup Server, and the CLIENT_NAME matches the hostname or IP of the local client machine. If they do not, update them as necessary.
		2. 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 periodically checks to see if a new version of NetBackup Client has been installed and performs necessary TPD configuration accordingly.
		3. At any time, the customer may push and install a new version of NetBackup client.

Appendix H.3 Create NetBackup Clint Configuration File

Procedure 53. Create NetBackup Client Configuration File

Step#	Procedure	Description
This procedure copies a NetBackup Client configuration file into the appropriate location on the TPD based application server. This configuration file allows a customer to install previously unsupported versions of the NetBackup client by providing necessary information to TPD. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Application Server iLO**: Create NetBackup configuration file	Create the NetBackup Client config file on the server using the contents that were previously determined. The config file should be placed in the **/usr/TKLC/plat/etc/NetBackup/profiles** directory and should follow the following naming conventions:
		`NB$ver.conf`
		Where **$ver** is the client version number with the periods removed. For the 7.5 client, the value of **$ver** would be 75 and the full path to the file would be:
		`/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf`
		Note: The config files must start with **NB** and must have a suffix of **.conf**.
		The server is now capable of installing the corresponding NetBackup Client.

2. ☐	**Application Server iLO**: Create NetBackup configuration script	Create the NetBackup Client config script file on the server using the contents that were previously determined. The config script file should be placed in the **/usr/TKLC/plat/etc/NetBackup/scripts** directory. The name of the NetBackup Client config script file should be determined from the contents of the NetBackup Client config file.
		As an example for the NetBackup 7.5 client, the following is applicable:
		NetBackup Client config:
		`/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf`
		NetBackup Client config script:
		`/usr/TKLC/plat/etc/NetBackup/scripts/NB75`

Appendix H.4 Open Ports for NetBackup Client Software

Procedure 54. Open Ports for NetBackup Client Software

Step#	Procedure	Description
This procedure uses 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Active NOAM Server: Login	Establish an SSH session to the active NOAM server and login as **admusr.**

2.
☐
	Active NOAM Server: Open ports for NetBackup client software	1. Change directories to **/usr/TKLC/plat/etc/iptables**.
		`$ cd /usr/TKLC/plat/etc/iptables`
		2. Using vi, create a file named **60netbackup.ipt**.
		`$ sudo vi 60netbackup.ipt`
		3. 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`
		4. 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 **/usr/TKLC/plat/etc/ip6tables** directory.

3. ☐	**Standby NOAM**: Open ports for NetBackup client software	**Repeat** steps 1-2 for the standby NOAM to 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.

5. □	**Standby SOAM**: Open ports for NetBackup client software	**Repeat** steps 1-2 for the standby SOAM to open ports for NetBackup client software.

Appendix I. IDIH Fast Deployment Configuration

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

Section	Description
Software Images	A list of the TVOE, TPD, and iDIH application versions.
TVOE Blade	Contains the enclosure ID, OA addresses, location, name and hardware type of an HP blade.
TVOE RMS	Includes hardware type and ILO address of the rack mount server.
Type	Management or Standalone
TVOE Configuration	Contains all IP addresses, hostname and network devices for the TVOE host.
Guest Configurations (3)	The guest sections contain network and hostname configuration for the Oracle, Mediation and Application guests.

Software Images

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

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

Note: For installation, oracleGuest-8.5.0.0.0_90.x.x-x86_64.iso is to be used.

TVOE Blade

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

TVOE RMS

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

TYPE

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

TVOE Configuration

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

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

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

Guest Configuration

These sections contain the hostname, IPv4 addresses, IPv4 netmask, IPv4 gateway, and IPv6 addresses. If you do not intend to configure IPv6 addresses then leave those IP addresses commented out. The IPv6 netmask is included in the IPv6 address.

Below is FDC configuration template included on the mediation ISO:

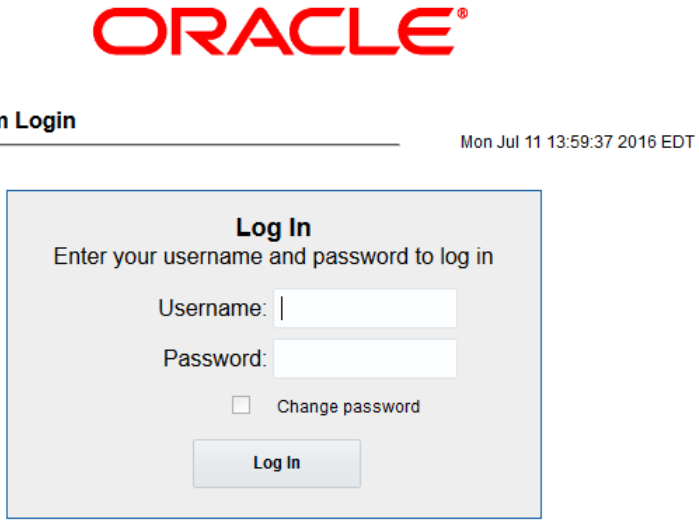
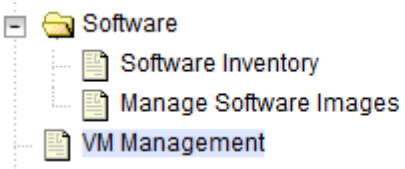
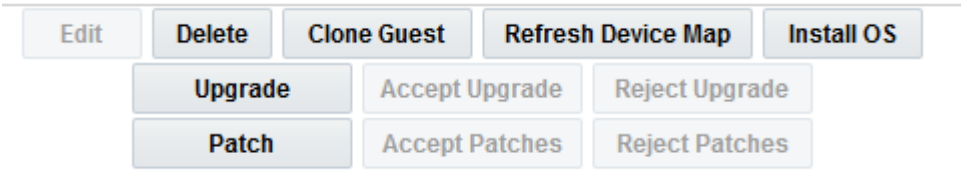
```
# Software Images
TvoeIso="TVOE-3.0.1.0.0_86.20.0-x86_64"
TpdIso="TPD.install-7.5.0.0.0_88.41.0-OracleLinux6.9-x86_64”
OraIso="oracleGuest-8.2.0.0.0_82.23.0-x86_64"
MedIso="mediation-8.2.0.0.0_82.23.0-x86_64"
AppIso="apps-8.2.1.0.0_82.23.0-x86_64"
# Tvoe Blade OA IP and Bay uncomment if this server is blade #EncId="1401"
#Oa1="10.250.51.197"
#Oa2="10.250.51.198"
#Bay="15F"
#Hw="ProLiantBL460cGen8"
#Hw="ProLiantBL460cGen6"
# Tvoe RMS Out of Band Management IP and Hw # Comment these lines if server
is blade OobIp="10.250.34.24"
Hw="ProLiantDL380pGen8"
#Hw="SUNNETRAX4270M3"
# Comment this line out if server is standalone Type="Management"
# Tvoe Config
#
TvoeName="thunderbolt"
TvoeIp="10.250.51.8"
Mask="255.255.255.0"
Gateway="10.250.51.1"
TvoeNtp="10.250.32.10"
TvoeIp6="2607:f0d0:1002:51::4/64"
TvoeIp6Gw="fe80::0"
```

```
# xmibond
XmiDev="bond0"
XmiEth="eth01,eth02"
# imibond
ImiDev="bond1"
ImiEth="eth03,eth04"
# xmi/management
MgmtInt="bond0.3"
MgmtIntType="Vlan"
MgmtIntVlanid="3"
# imi
ImiInt="bond1.5"
ImiIntType="Vlan"
ImiIntVlanid="5"
# Oracle Guest Config
OraName="thunderbolt-ora"
OraIp="10.250.51.6"
OraMask=$Mask
OraGw=$Gateway
OraIp6="2607:f0d0:1002:51::5/64"
OraIp6Gw="$TvoeIp6Gw"
# Mediation Guest Config
MedName="thunderbolt-med"
MedIp="10.250.51.10"
MedMask=$Mask
MedGw=$Gateway
ImiIp="192.168.32.11"
ImiMask="255.255.255.224"
MedIp6="2607:f0d0:1002:51::6/64"
MedIp6Gw="$TvoeIp6Gw"
ImiIp6="2608:f0d0:1002:51::6/64"
# Application Guest Config
AppName="thunderbolt-app"
AppIp="10.250.51.11"
AppMask=$Mask
AppGw=$Gateway
AppIp6="2607:f0d0:1002:51::7/64"
AppIp6Gw="$TvoeIp6Gw"
```

Appendix J. IDIH External Drive Removal

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

Procedure 55. IDIH External Drive Removal

Step#	Procedure	Description
This procedure destroys all of the data in the Oracle database. Warning: Do not perform this procedure on an IDIH system unless you intent to do a fresh TVOE installation. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `https://<PMAC_Mgmt_Network_IP>` 2. Login as **guiadmin** user: 
2. ☐	**PMAC GUI**: Delete VMs, if needed	Before a re-installation can be performed, the IDIH VMs must be removed first. 1. Navigate to **VM Management**.  2. Select each of the IDIH VMs and click **Delete**. 

Step#	Procedure	Description
3. ☐	IDIH TVOE Host: Login	Establish an ssh session to the TVOE host and login as admusr.

4. ☐	**IDIH TVOE Host**: Verify external drive exists 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 displays:
		`Smart Array P410i in Slot 3`
		`  array A`
		`  logicaldrive 1 (3.3 TB, RAID 1+0, OK)`

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 displays:
		`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 displays:
		`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`
		`MirrorData: 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 displays:
		`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)`

Step#	Procedure	Description

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 displays:
		`Called with options: hpdisk --slot=3`
		`WARNING: This destroys 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 displays:
		`Called with options: hpdisk --slot=2`
		`WARNING: This destroys 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`

Step#	Procedure	Description

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 K. DSR Fast Deployment Configuration

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

Fast Deployment Variable	Description	Value
Cabinet ID of this Enclosure? (NOAM Blade Deployment Only)	This value should match the value entered from Section “Enclosure and Blades Setup” from reference [6].	_____
Enclosure ID? (NOAM Blade Deployment Only)	This value should match the value entered from Section “Enclosure and Blades Setup” from reference [1].	_____
Bay number of the First NOAM TVOE Host (NOAM Blade Deployment Only)	This value will be the blade number of the first NOAM server. ***Note***: ‘F’ MUST append the bay number (example: 8F)	_____
Bay number of the Second NOAM TVOE Host (NOAM Blade Deployment Only)	This value will be the blade number of the second NOAM server. ***Note***: ‘F’ MUST append the bay number (example: 16F).	_____
iLO/iLOM IP address of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM IP address of the First rack mount server. ***Note***: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure “Add Rack Mount Server to the PMAC System Inventory” from reference [1].	_____
iLO/iLOM IP address of the Second Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM IP address of the First rack mount server.	_____
iLO/iLOM username of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM username of the first rack mount server. ***Note***: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure “Add Rack Mount Server to the PMAC System Inventory” from reference [1].	_____
iLO/iLOM username of the Second Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM username of the second rack mount server.	_____

Fast Deployment Variable	Description	Value
iLO/iLOM password of the First Rack Mount Server (NOAM Rack Mount Server Deployments Only)	This value will be the iLO/iLOM password of the first rack mount server. ***Note***: If the NOAM is located on the same TVOE host as the PMAC, this value will be the one entered in procedure "Add Rack Mount Server to the PMAC System Inventory" from reference [1].	_____
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 **VM Management** on the PMAC).	_____
PMAC VM Name of the Second NOAM	This value will be the VM name (visible from **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 [1].	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	_____

Fast Deployment Variable	Description	Value
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 [1].	_____
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 [1].	_____
xmi Network IP Subnet Mask	This value will be the xmi IP network subnet mask.	_____
Management Network IP subnet mask	This value will be the management IP network subnet mask.	_____
xmi Network IP default gateway	This value will be the default gateway of the xmi network.	_____
Management Network IP default gateway	This value will be the default gateway of the management network.	_____

Appendix L. Growth/De-Growth

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

Appendix L.1 Growth

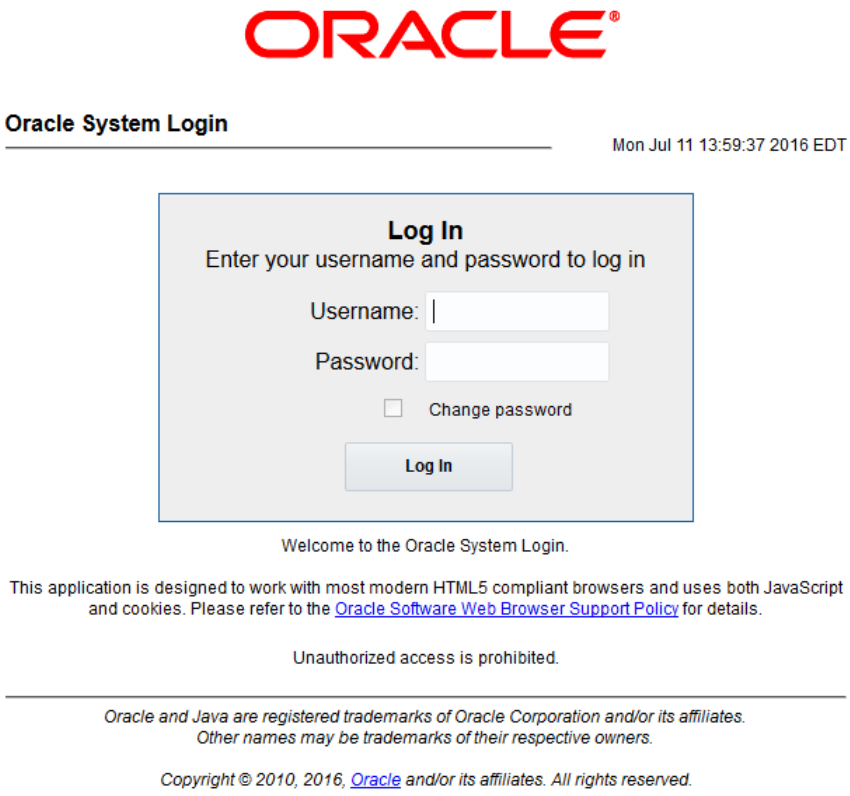
For growth scenarios where it is necessary to add DSR servers, the following sequence of steps should be followed:

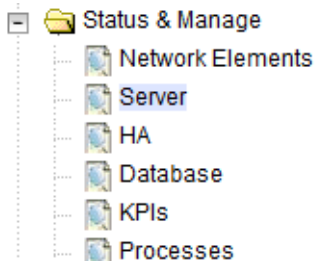
Step	Procedure(s)
Perform backups	Procedure 56. Perform Backups
Perform system health check	Procedure 57. Perform Health Check
Identify servers which are affected by the growth: • DR-NOAM • SOAM Spares • MP (SBR, IPFE)	
Add new servers Create and Configure the VMs on new servers (SOAM spare and DR-NOAMs only)	Procedure 58. Add a New Server/VMs
Configure servers in new VM locations	NOAM/DR-NOAM: Procedure 59. Growth: DR-NOAM SOAM: Procedure 60. Growth: SOAM spare (PCA Only) MP: Procedure 61. Growth: MP or Procedure 62.
Post growth health check	Procedure 62. Post Growth Health Check
Post growth backups	Procedure 63. Post Growth Backups

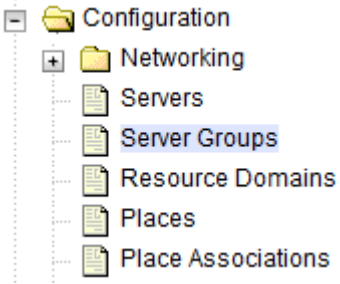
Procedure 56. Perform Backups

Step#	Procedure	Description
This procedure backs up all necessary items before a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Back up all TVOE host configurations by executing Procedure 41. Back Up TVOE Configuration.
2. ☐	Backup PMAC	Backup the PMAC application by executing Procedure 42. Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM databases by executing Procedure 43. NOAM Database Backup and Procedure 44. SOAM Database Backup.

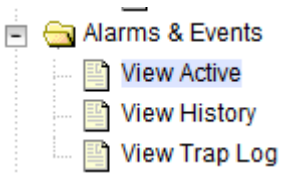
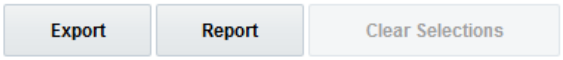
Procedure 57. Perform Health Check

Step#	Procedure	Description
This procedure verifies 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
</td><td>NOAM VIP GUI: Verify server status</td><td>1. Navigate to Status & Manage > Server.
 

2. Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>
Do not proceed with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.</td></tr>
<tr><td>3.
</td><td>NOAM VIP GUI: Verify server configuration</td><td>1. Navigate to Configuration > Server Groups.
 

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

Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  2. Click **Report**.  3. **Save** or **Print** this report, keep copies for future reference. 
5. ☐	**SOAM VIP GUI**: Repeat for SOAM	**Repeat** steps 1-4 for the SOAM.

Procedure 58. Add a New Server/VMs

Step#	Procedure	Description
This procedure adds a new rack mount server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Add/Configure additional servers	Follow the sections below to install and configure additional servers: **DR-NOAMs**: Section 4.2.1 Execute DSR Fast Deployment for DR-NOAMs **Spare SOAMs**: Procedure 11. Configure SOAM TVOE Server Blades **MPs**: Insert blade in desired location.
2. ☐	Add/Configure new VMs	1. Create new virtual Machines for the Spare SOAMs by following Procedure 12. Create SOAM Guest VMs. 2. Install TPD and DSR Software by following Procedure 13. IPM Blades and VMs.

Procedure 59. Growth: DR-NOAM

Step#	Procedure	Description
This procedure configures a DR-NOAM on the new virtual machine for VM growth scenarios. Prerequisites: • NEW Virtual Machine Created • TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Configure the DR-NOAM	Configure the DR-NOAM by executing the steps referenced in the following procedures: **DSR DR-NOAM**: Section 4.2.2 Pair 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 need to be run again. Refer to Section 3.4 Optional Features.

Procedure 60. Growth: SOAM spare (PCA Only)

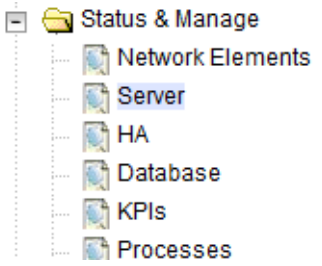
Step#	Procedure	Description
This procedure configures an SOAM spare on the new virtual machine for VM growth scenarios. Prerequisites: • NEW Virtual Machine Created • TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Configure the SOAM spare	Configure the SOAM spare by executing the following procedures: • Procedure 15. Configure SOAM NE • Procedure 16. Configure the SOAM Servers • Procedure 17. Configure the SOAM Server Group (steps 1, 4, 6, and 9)
2. ☐	**NOAM GUI**: Activate optional features	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to Section 3.3 Optional Features.

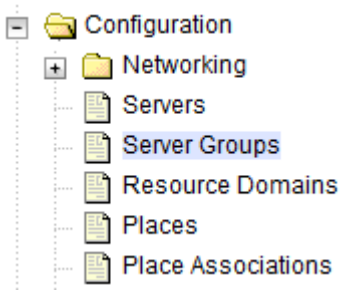
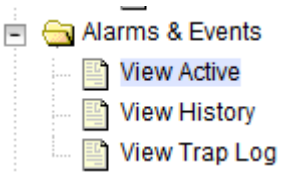
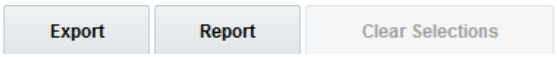
Procedure 61. Growth: MP

Step#	Procedure	Description
This procedure configures an MP on the new virtual machine for growth scenarios. ***Prerequisite***: TPD/DSR software installed Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Configure the MP	Configure the MP/DP by executing the steps referenced in the following procedures: **DSR MP**: Procedure 20. Configure MP Blade Servers (steps 1-2, 7-14, 15-17 (Optional))

Procedure 62. Post Growth Health Check

Step#	Procedure	Description
This procedure verifies system status and logs all alarms after growth. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

Step#	Procedure	Description
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
2. ☐	**NOAM VIP GUI**: Verify server status	1. Navigate to **Status & Manage > Server**.  2. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). Appl State | Alm | DB | Reporting Status | Proc Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm

Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Verify server configuration	1. Navigate to **Configuration > Server Groups**.  2. Verify the configuration data is correct for your network.
4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  2. Click **Report**.  3. **Save** or **Print** this report and keep copies for future reference.  4. Compare this alarm report with those gathered in Procedure 57. Perform Health Check.
5. ☐	SOAM VIP GUI: Repeat	**Repeat** steps 1-3 for the SOAM.

Procedure 63. Post Growth Backups

Step#	Procedure	Description
This procedure backs up all necessary items after a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Backup all TVOE host configurations by executing Procedure 41. Back Up TVOE Configuration.
2. ☐	Backup PMAC	Backup the PMAC application by executing Procedure 42. Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM databases by executing Procedure 43. NOAM Database Backup and Procedure 44. SOAM Database Backup.

Appendix L.2 De-Growth

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

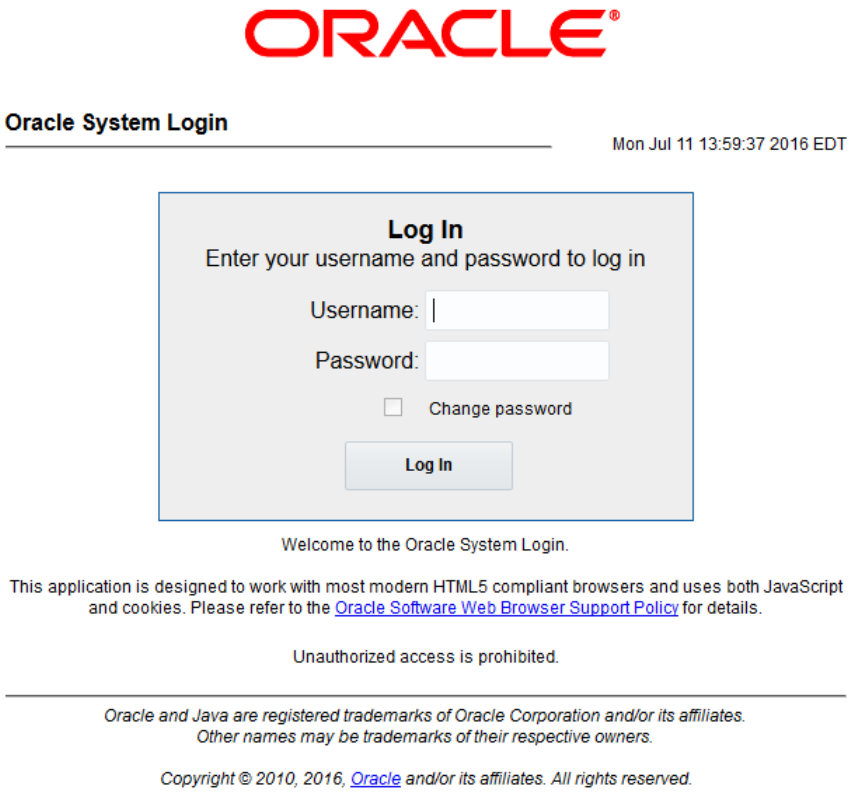
Step	Procedure(s)
Perform backups	Procedure 64. Perform Backups
Perform system health check	Procedure 65. Perform Health Check
Identify servers affected by the de-growth: DSR MP (SBR, IPFE)	
Remove identified servers from server group	Procedure 66. Remove Server from Server Group
Shutdown and remove the identified server's VM	
Post de-growth health check	Procedure 67. Post Growth Health Check
Post de-growth backups	Procedure 68. Post Growth Backups

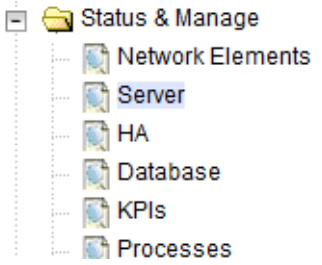
Procedure 64. Perform Backups

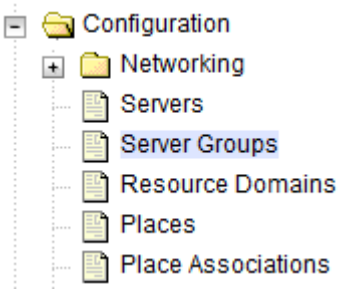
Step#	Procedure	Description
This procedure backs up all necessary items before a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Backup all TVOE host configurations by executing Procedure 41. Back Up TVOE Configuration.
2. ☐	Backup PMAC	Backup the PMAC application by executing Procedure 42. Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM databases by executing Procedure 43. NOAM Database Backup and Procedure 44. SOAM Database Backup.

Procedure 65. Perform Health Check

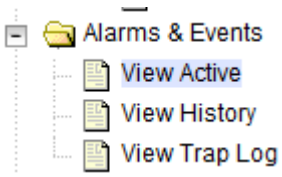
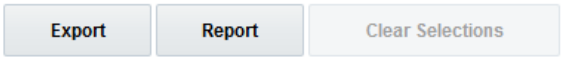
Step#	Procedure	Description
This procedure verifies system status and logs all alarms. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

Step#	Procedure	Description
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

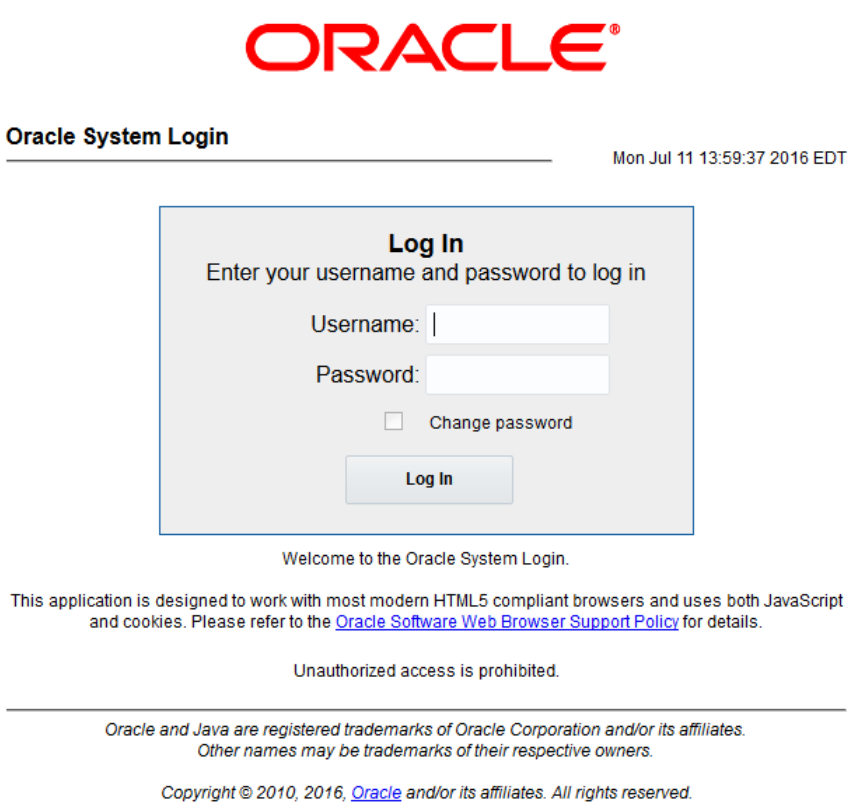
<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
</td><td>NOAM VIP GUI: Verify server status</td><td>1. Navigate to Status & Manage > Server.
 

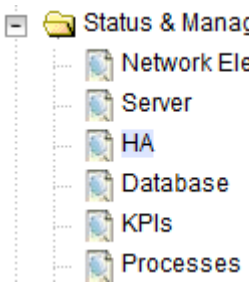
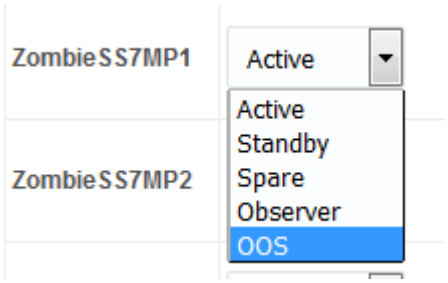
2. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>
Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms</td></tr>
<tr><td>3.
</td><td>NOAM VIP GUI: Verify server configuration</td><td>1. Navigate to Configuration > Server Groups.
 

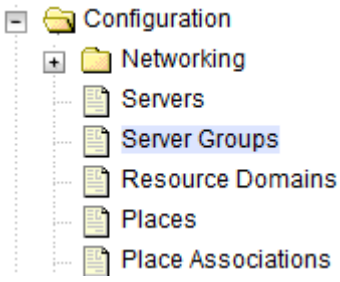
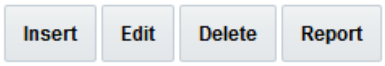
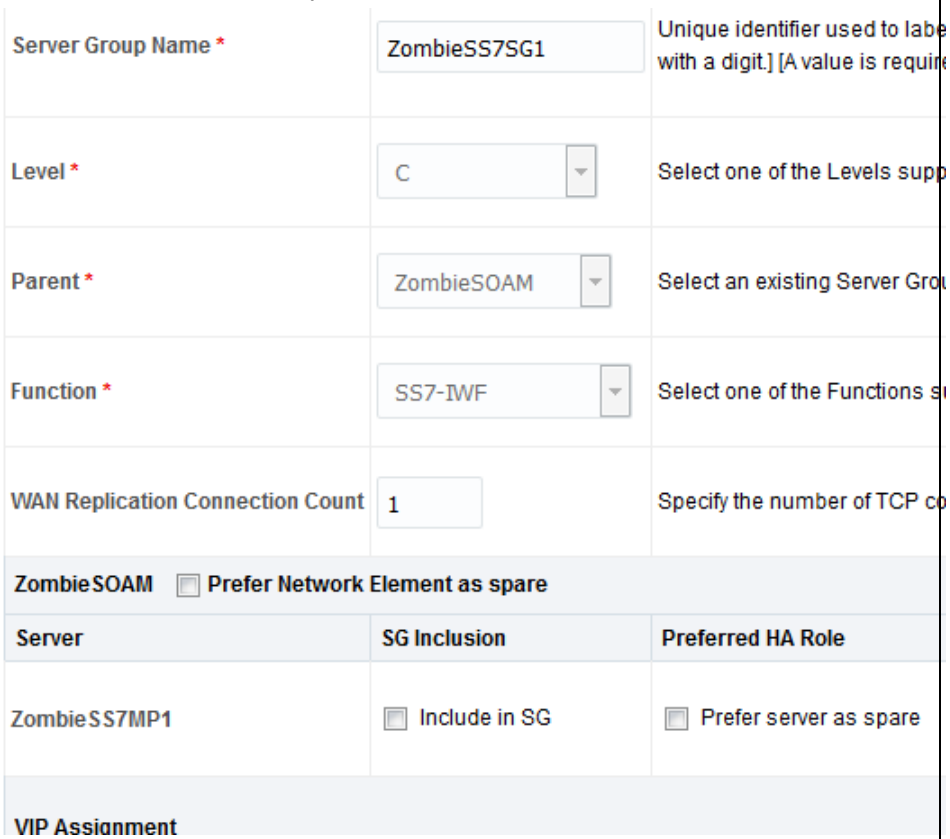
2. Verify the configuration data is correct for your network.</td></tr>
</table>

Step#	Procedure	Description
4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  2. Click **Report**.  3. Save or Print this report and keep copies for future reference. 
5. ☐	**SOAM VIP GUI**: Repeat for SOAM	**Repeat** steps 1-4 for the SOAM.

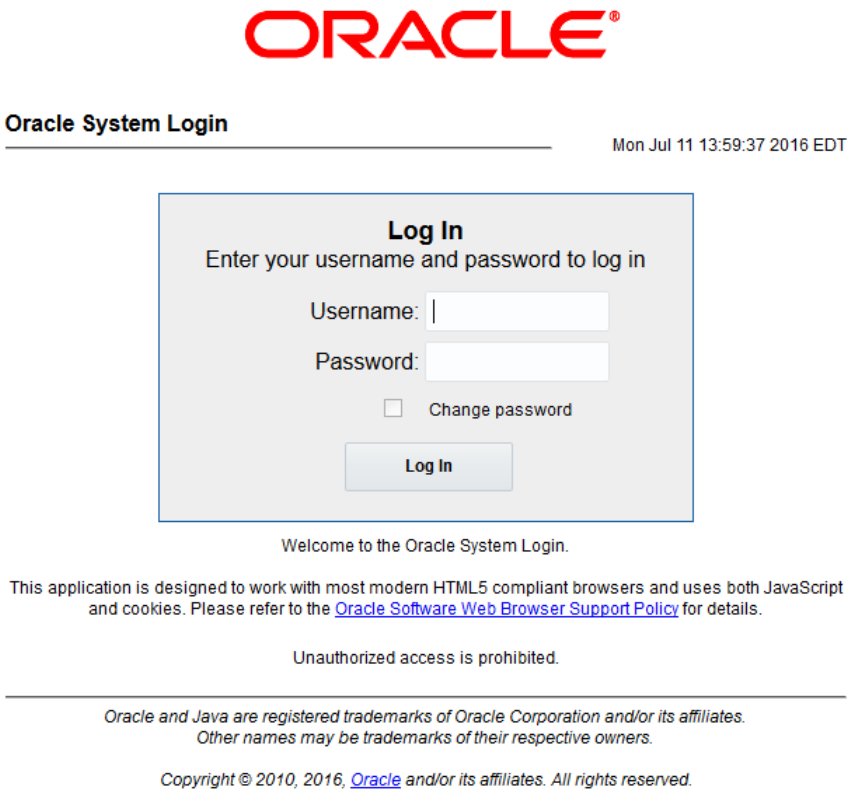
Procedure 66. Remove Server from Server Group

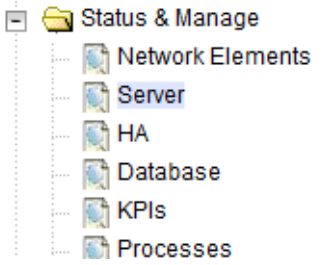
Step#	Procedure	Description
Once the server's that will be deleted have been identified, the server first needs to be removed from its server group. The following procedure removes a server from a server group. **Warning**: It is recommended that no more than one server from each server group be removed from a server group at a time. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

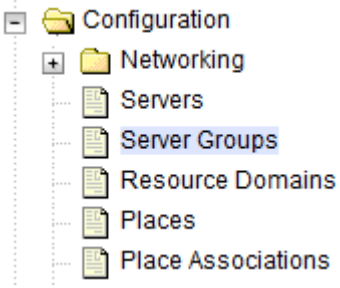
Step#	Procedure	Description
2.	**NOAM VIP GUI**: Set server to OOS	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Set the server's Max Allowed HA Role to **OOS**.  4. Click **OK**.

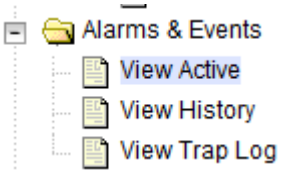
Step#	Procedure	Description
3. ☐	**NOAM VIP GUI**: Remove server from server group	1. Navigate to **Configuration > Server Groups**.  2. Select the server group for which the server from step 2 that was placed OOS. 3. Click **Edit**.  Uncheck the server from step 2 from the SG Inclusion column:  4. Click **OK**. 

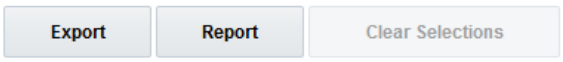
Procedure 67. Post Growth Health Check

Step#	Procedure	Description
This procedure verifies system status and logs all alarms after growth. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
</td><td>NOAM VIP GUI: Verify server status</td><td>1. Navigate to Status & Manage > Server.
 

2. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table></td></tr>
<tr><td>3.
</td><td>NOAM VIP GUI: Verify server configuration</td><td>1. Navigate to Configuration > Server Groups.
 

2. Verify the configuration data is correct for your network.</td></tr>
<tr><td>4.
</td><td>NOAM VIP GUI: Log current alarms</td><td>1. Navigate to Alarms & Events > View Active.
 

2. Click Report.
 

3. Save or Print this report, keep copies for future reference.
 

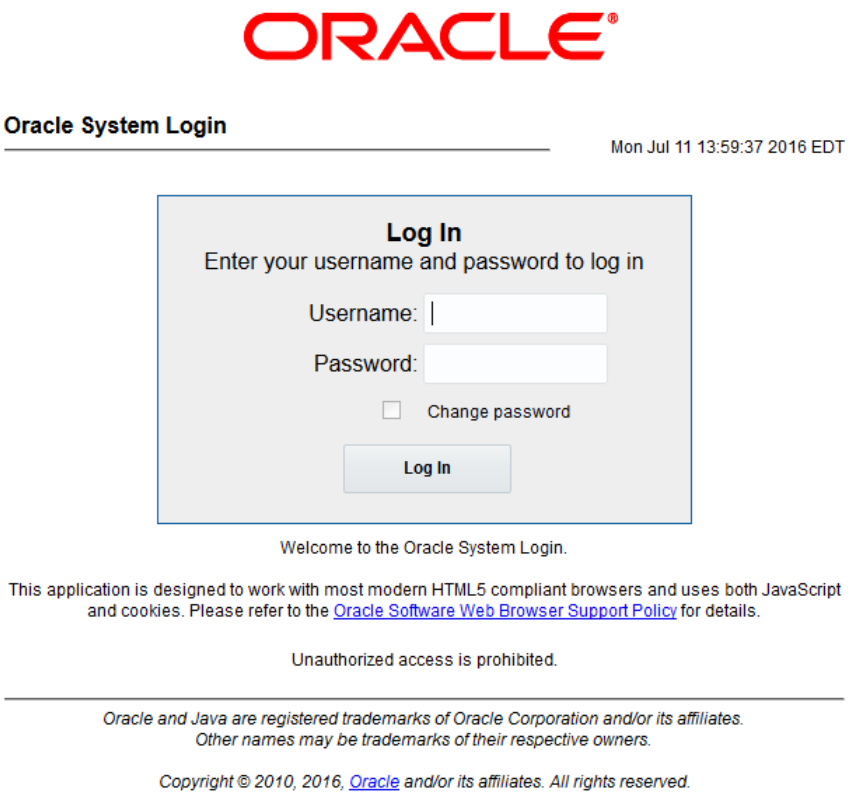
4. Compare this alarm report with those gathered in Procedure 57. Perform Health Check.</td></tr>
<tr><td>5.
</td><td>SOAM VIP GUI: Repeat</td><td>Repeat steps 1-3 for the SOAM.</td></tr>
</table>

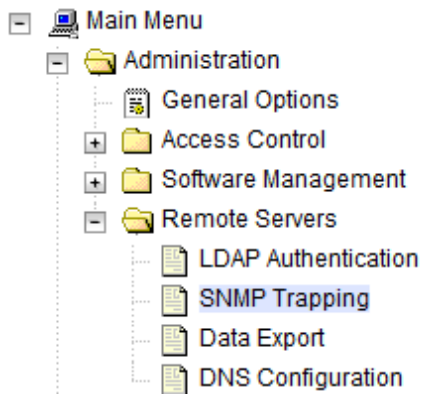
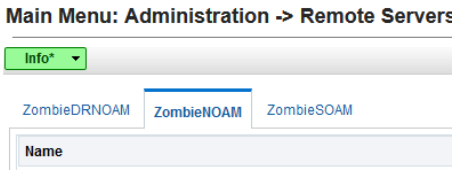
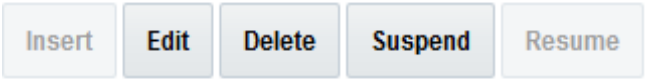
Procedure 68. Post Growth Backups

Step#	Procedure	Description
This procedure backs up all necessary items after a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Backup all TVOE host configurations by executing Procedure 41. Back Up TVOE Configuration.
2. ☐	Backup PMAC	Backup the PMAC application by executing Procedure 42. Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Procedure 43. NOAM Database Backup and Procedure 44. SOAM Database Backup.

Appendix M.Restore SNMP Configuration to SNMPv3 (Optional)

Procedure 69. Restore SNMP Configuration to SNMP v3

Step#	Procedure	Description
This procedure restores SNMP configuration to SNMPv3 for forwarding of SNMP traps from each individual server. ***Note***: If SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a workaround step (section 4.5, steps 6-9) and the SNMPv3 is required to be configured.. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	(Workaround) **Primary NOAM VIP GUI**: Login	***Note***: This workaround should be performed only if SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a workaround (section 4.5, steps 6-9) and the SNMPv3 is required to be configured. 1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  	

Step#	Procedure	Description
2. ☐	**NOAM VIP GUI**: Configure system-wide SNMP Trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Select the Server Group tab for SNMP trap configuration. The server group that is configured for SNMPv2c & SNMPv3 as a workaround:  3. Click **Edit**.  4. Update the Enabled Versions as **SNMPv3**:  5. Click **OK**.

Appendix N. My Oracle Support (MOS)

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

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

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

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications** documentation link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or Platforms.
4. Click on your **Product** and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.