Oracle® Communications

Diameter Signaling Router

DSR 7.2/7.3 Cloud Installation

E64814 Revision 01

April 2017

Oracle Communications Diameter Signaling Router Cloud Installation Procedure, Release 7.2/7.3

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

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

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

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

See more information on MOS in the Appendix section.

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

1.1 Purpose and Scope

This document describes the application-related installation procedures for Diameter Signaling Router Cloud systems.

This document assumes platform-related configuration has already been done.

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.

1.2 References

1.2.1 External

[1] Communication Agent Configuration Guide, E58922

[2] PCA Configuration, E58667

[3] DSR Meta Administration Feature Activation Procedure, E58661

[4] DSR Full Address Based Resolution (FABR) Feature Activation Procedure, E58664

[5] DSR Range Based Address Resolution (RBAR) Feature Activation, E58664

[6] SDS SW Installation and Configuration Guide, CGBU_010592 /E64816-02

[7] MAP-Diameter IWF Feature Activation Procedure. E58666

[8] Operations, Administration, and Maintenance (OAM) User’s Guide, E53463

[9] Communication Agent User’s Guide, E53464

[10] Policy DRA User’s Guide, E53472

[11] Diameter User’s Guide, E53467

[12] Mediation User’s Guide, E53468

[13] Range Based Address Resolution (RBAR) User’s Guide, E53469

[14] Full Address Based Resolution (FABR) User’s Guide, E53470

[15] IP Front End (IPFE) User’s Guide, E53473-01

[16] DSR Alarms, KPIs, and Measurements Reference, E53474

[17] Diameter Common User’s Guide, E53480

[18] Diameter Administrator’s Guide, E53475

[19] Map-Diameter IWF User’s Guide, E53476

[20] Gateway Location Application (GLA) User’s Guide, E58659

[21] DSR PCA Configuration E63560-1, CGBU_010561

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DA-MP	Diameter Agent Message Processor
DSR	Diameter Signaling Router
ESXi	Elastic Sky X Integrated
FABR	Full Address Based Resolution
iDIH	Integrated Diameter Intelligence Hub
IPFE	IP Front End
IPM	Initial Product Manufacture – the process of installing TPD
IWF	Inter Working Function
KVM	Kernel-based Virtual Machine
MP	Message Processor
NAPD	Network Architecture Planning Diagram
NE	Network Element
NOAM	Network Operation Administration and Maintenance
OS	Operating System (e.g. TPD)
OVA	Open Virtualization Archive
PDRA	Policy Diameter Routing Agent
PCA	Policy and Charging Application
RBAR	Range Based Address Resolution
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SOAM	Software Operation Administration and Maintenance
TPD	Tekelec Platform Distribution
TSA	Target Set Address
VIP	Virtual IP
VM	Virtual Machine

1.4 Terminology

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

Table 2. Terminology

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
Place Association	Applicable for various applications, a “Place Association” is a configured object that allows places to be grouped together. A place can be a member of more than one place association. The Policy & Charging DRA application defines two place association types: policy binding region and policy & charging mated sites.
Two Site Redundancy	Two site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy & Charging Mated Sites Place Association containing two sites. Two site redundancy is a feature provided by server group configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in two geographically separate Sites(locations). This feature ensures there is always a functioning active server in a server group even if all the servers in a single site fail.
Server Group Primary Site	A server group primary site is a term used to represent the principle location within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy & Charging DRA application, these sites (places) are all configured within a single “Policy and Charging Mated Sites” place association. The primary site may be in a different site (place) for each configured SOAM or SBR server group. A primary site is described as the location in which the active and standby servers to reside, however there cannot be any preferred spare servers within this location. All SOAM and SBR server groups have a primary site.
Server Group Secondary Site	A server group secondary site is a term used to represent location in addition to the primary site within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several Sites(Places). For the Policy & Charging DRA application, these sites (places) are all configured within a single “Policy and Charging Mated Sites” place association. The secondary site may be in a different site (place) for each configured SOAM or SBR server group. A secondary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. If two site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups.

2. General Description

This document defines the steps to execute the initial installation of the Diameter Signaling Router (DSR) 7.2/7.3 application on a supported Cloud platform.

3. Installation Overview

This section provides a brief overview of the recommended method for installing the source release software that is installed and running on a Cloud to the Target Release software. The basic install process and approximate time required is outlined in Table 2.

3.1 Required Materials

1. One target release DSR OVA Media
2. Three (3) iDIH Mediation OVA (Optional iDIH)
   a. iDIH Application OVA
   b. iDIH Oracle OVA
   c. iDIH Mediation OVA

3.2 Installation Overview

This section describes the overal strategy to be employed for a single or multi-site DSR 7.2/7.3 and iDIH 7.2/7.3 installation. It also lists the procedures required for installation with estimated times. Section 3.2.1 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. Section 3.2.3 lists the steps required to install a DSR 7.2/7.3 system. These latter sections expand on the information from the matrix and provide a general timeline for the installation. Additionally, basic firewall port information is included in Firewall Ports.It should also be noted that some procedures are cloud platform dependent and that not all procedures are performed on all cloud platforms.

3.2.1 Installation Strategy

A successful installation of DSR requires careful planning and assessment of all configuration materials and installation variables.

Figure 1: DSR Single Site Installation Procedure Map 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 virtual machines at each site and their role(s)
   - What timezone should be used across the entire collection of DSR sites?
   - Will SNMP traps be viewed at the NOAM or will an external NMS be used? (Or both?)
2. A site survey (NAPD) is conducted with the customer to determine exact networking and site details.

   Note: XMI and IMI addresses are difficult to change once configured. It is **very important these addresses are well planned and not expected to change after a site is installed.**

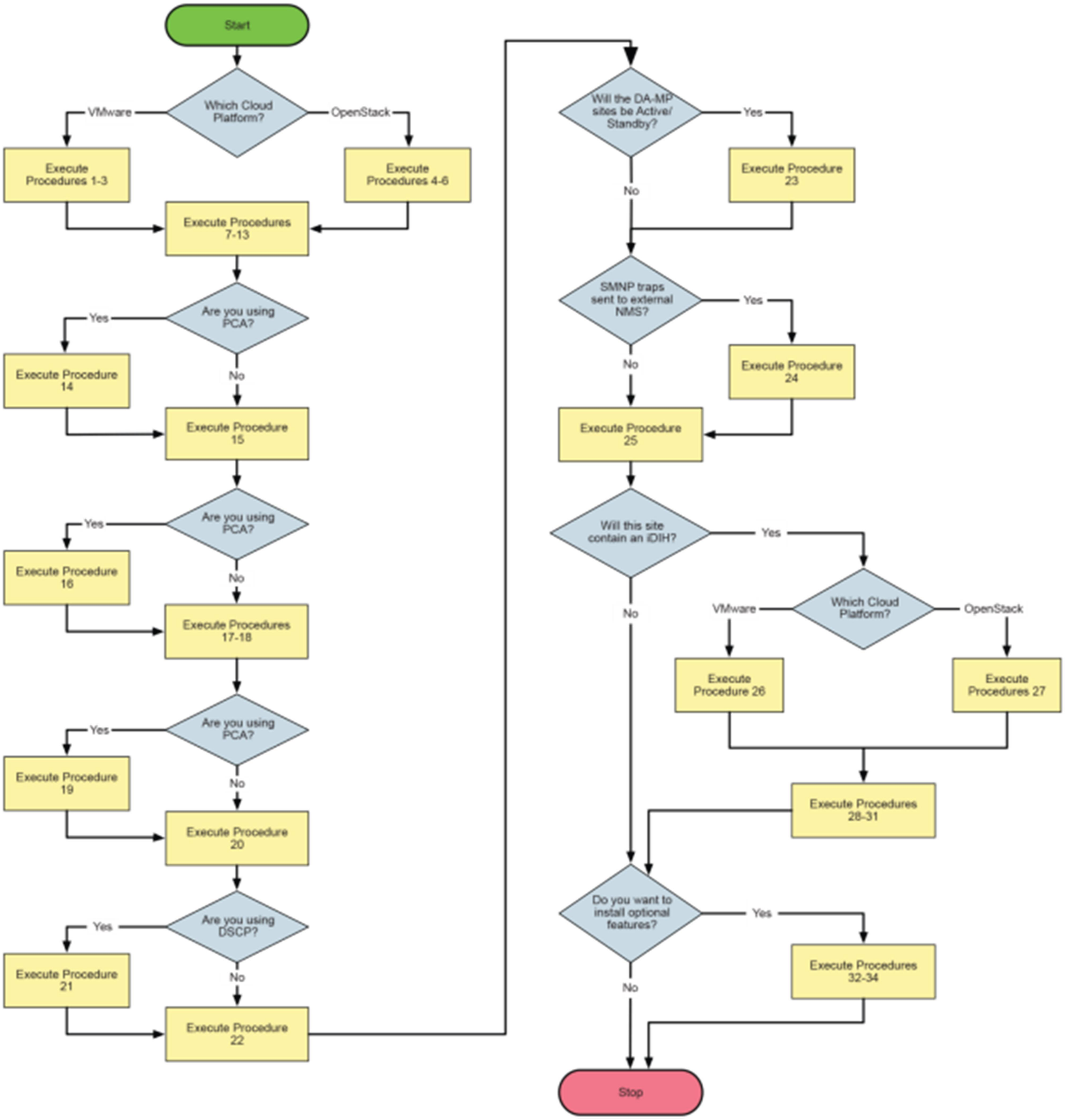


Figure 1: DSR Single Site Installation Procedure Map

3.2.2 SNMP Configuration

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

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

- DSR Application Servers (NOAM, SOAM, MPs of all types)

DSR 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 auxillary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAM VIP, the SOAM VIP, or an external (customer) NMS.

Should have their SNMP trap destinations set to:

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

3.2.3 Installation Procedures

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

Table 3. Installation Overview

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 1 or 4	Import DSR OVA	5	5
Procedure 2 or 5	Configure DSR NOAM guest role based on resource profile	10	15
Procedure 3 or 6	Configure DSR Remaining guests role based on resource profile	40	55
Procedure 7	Configure the First NOAM NE and Server	25	80
Procedure 8	Configure the NOAM Server Group	15	95
Procedure 9	Configure the Second NOAM Server	15	110
Procedure 10	Complete Configuring the NOAM Server Group	10	120
Procedure 11	Configure the SOAM NE	15	135
Procedure 12	Configure the SOAM Servers	10	145
Procedure 13	Configure the SOAM Server Group	10	155
Procedure 14 (Optional)	Activate PCA (PCA Only)	10	165
Procedure 15	Configure the MP Virtual Machines	5	170
Procedure 16 (Optional)	Configure Places and Assign MP Servers to Places (PCA Only)	10	180
Procedure 17	Configure the MP Server Group(s) and Profiles	10	190
Procedure 18	Configure the Signaling Networks	5	195
Procedure 19 (Optional)	Addional Servers to Network Mapping (PCA Only)	10	205
Procedure 20	Configure the Signaling Devices	10	215

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 21 (Optional)	Configure DSCP Values for Outgoing Traffic	10	225
Procedure 22	Configure the Signaling Network Routes	15	240
Procedure 23 (Optional)	Add VIP for Signaling Networks	5	245
Procedure 24 (Optional)	Configure SNMP for Trap Receiver(s)	5	250
Procedure 25	IP Front End (IPFE) Configuration	15	265
Procedure 26 or 27 (Optional)	Create iDIH Oracle, Mediation and Application VM's	45	310
Procedure 28 (Optional)	Configure iDIH VM Networks	15	325
Procedure 29 (Optional)	Run Post Installation Scripts on iDIH VM's	60	385
Procedure 30 (Optional)	Integrate iDIH into DSR	30	415
Procedure 31 (Optional)	iDIH Application Final Configuration	10	425
Procedure 32 (Optional)	Activate Optional Features	15	440
Procedure 33 (Optional)	Configure ComAgent Connections	15	455
Procedure 34 (Optional)	Complete PCA configuration	30	485
Procedure 35	Backups and Disaster Prevention	30	515

3.3 Optional Features

When DSR installation is complete, further configuration and/or installation steps are needed for optional features that may be present in this deployment. Please refer to Table 4 for the post-DSR installation configuration documentation needed for their components.

Table 4: Post-DSR Installation Configuration Step

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure, E58661-01
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E58664-01
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation, Procedure, E58664-01
MAP-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation, E58666-01
Policy and Charging Application (PCA)	PCA Configuration, E63560-1

4. Software Installation Procedure

As mentioned earlier, the host configuration and virtual networks should be done before executing the procedures in this document. It is assumed that at this point, the user has access to:

- consoles of all guests and hosts at all sites
- ssh access to the guests at all sites
- GUI access to hosts at all sites
- A configuration station with a web browser , ssh client, and scp client.
- VM Manager Privilages to add OVA's to catalog (VMware only)
- KVM/OpenStack admin and tenant privileges.

SUDO

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

VIP/TSA (OpenStack Only)

OpenStack release Kilo or later is required to configure VIP and Target Set addresses. Kilo release 2015.1.2 or later is preferred.

4.1 Create DSR Guests (VMware)

Procedure 1. (VMware). Import DSR OVA

S T E P #	This procedure adds the DSR OVA to the VMware catalog or repository. Check off (√) each step as it is completed. Steps with shaded boxes require user input. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1 □	Add DSR OVA image	1. Launch the VMware client of your choice. 2. Add the DSR OVA image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.

Procedure 2. (VMware only). Configure NOAM Guests Role Based On Resource Profile

S T E P #	This procedure configures networking on virtual machines. 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 □	Create the NO1 VM, from the OVA image	1. Browse the library or repository that you placed the OVA image. 2. Deploy the OVA Image using vSphere Client or the vSphere Web Client. 3. Name the NO1 VM and select the datastore.
2 □	Configure resources for the NO1 VM	Configure the NO1 per the Appendix D Resource Profile for the DSR NOAM using the vSphere Client or the vSphere Web Client.
3 □	Power on NO1	Use the vSphere client or vSphere web client to Power on the NO1 VM.

Procedure 2. (VMware only). Configure NOAM Guests Role Based On Resource Profile

4
□
	Configure NO1	1. Access the NO1 VM console via the vSphere client or vSphere web client.
		2. Login as **admusr**.
		3. Set the <ethX> device:
		Note: Where ethX is the interface associated with the XMI network
		`$ sudo netAdm add --device=<ethX> --address=<IP Address in External management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
		4. Add the default route for ethX:
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External management network> --device=<ethX>`

5 □	Configure NO2 (Optional for small lab deployment)	Repeat steps 1 through 4 for the NO2 VM.

Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile

STEP #	This procedure adds network addresses for all virtual machines. 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 □	Create the SO1 VM from the OVA image	1. Browse the library or repository that you placed the **OVA** image. 2. Deploy the OVA image using vSphere Client or the vSphere Web Client. 3. Name the **SO1 VM** and select the datastore.
2 □	Configure resources for the SO1 VM	Configure the **SO1 VM** per the Appendix D Resource Profile for the **DSR SO** using the vSphere Client or the vSphere Web Client. Interfaces must be added per the network interface table at the bottom of the Appendix D Resource Profile.
3 □	Power on SO1 VM	1. Power on the DSR SO1 VM with the vSphere client or vSphere web client. 2. Monitor the vApps screen's Virtual Machines tab until the DSR VM reports **Powered On** in the Status column.

4
□
	Configure XMI interface	1. Access the VM console via the vSphere client or vSphere web client.
		2. Login as **admusr**.
		3. Set the ethX device:
		Note: Where ethX is the interface associated with the XMI network
		`$ sudo netAdm add --device=<ethX> --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
		4. Add the default route for ethX:
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External management network> --device=<ethX>`

Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile

5 □	Verify Network connectivity	1. Access the **SO1 VM console** via the vSphere client or vSphere web client. 2. Login as **admusr**. 3. Ping the NO1. `$ ping -c3 <IP Address in External Management Network>`

6
□
	Procedure overview	Repeat steps 1 through 5 for the following VMs. Use unique labels for the VM names:
		MP(s)
		MP(s) SS7 (optional components)
		IPFE(s)
		NOAM(s)
		SOAM(s)
		SBR s, SBR b (optional components)

4.2 Create DSR Guests (KVM/OpenStack)

Procedure 4. Import DSR OVA (KVM/OpenStack Only)

STEP #	This procedure adds the DSR image to the glance image catalog. Check off (√) each step as it is completed. Steps with shaded boxes require user input. If this procedure fails, contact My Oracle Support (MOS)and ask for assistance.	
1 □	Preparation	1. Create instance flavors. If not yet done, use the Appendix D Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the “Admin” section, or with the “nova flavor-create” command line tool. Make the flavor names as informative as possible. As flavors describe resource sizing, a common convention is to use a name like “0406060” where the first two figures (04) represent the number of virtual CPUs, the next two figures (06) might represent the RAM allocation in GB and the final three figures (060) might represent the disk space in GB. 2. If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, please note that the default LRO (Large Receive Offload) option must be disabled on the host command line. Please see the Intel release notes for more details. This action can be performed with the following command. `$ sudo ethtool -K <ETH_DEV> lro off` 3. If using IPFE Target Set addresses (TSA). a. Read and understand Disable Port Security in Appendix H, including the warning note. b. Enable the Neutron port security extension.

2
□
	Add DSR OVA image	1. Copy the OVA file to the OpenStack control node.
		`$ scp DSR-7.3.x.x.x.ova admusr@node:~`
		2. Login to the OpenStack control node.
		`$ ssh admusr@node`
		3. In an empty directory unpack the OVA file using **tar**.
		`$ tar xvf DSR-7.3.x.x.x.ova`
		4. One of the unpacked files has a **.vmdk** suffix. This is the VM image file that must be imported.
		DSR-7.3.x.x.x-disk1.vmdk
		5. Source the OpenStack **admin** user credentials.
		`$ .  keystonerc_admin`
		6. Select an informative name for the new image.
		dsr-7.3.x.x.x-original
		7. Import the image using the **glance** utility from the command line.
		`$ glance image-create --name dsr-7.3.x.x.x-original --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file DSR-7.3.x.x.x-disk1.vmdk`
		This process takes about 5 minutes, depending on the underlying infrastructure.

Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

STEP #	This procedure configures networking on virtual machines. 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 □	Name the new VM instance	1. Create an informative name for the new instance: NO1. 2. Examine the network interface recommendations at the bottom of Appendix D Resource Profile.

Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

2
□
	Create and boot the NO VM instance from the glance image	1. Get the following configuration values.
		a. The image ID.
		`$ glance image-list`
		b. The flavor ID.
		`$ nova flavor-list`
		c. The network ID(s)
		`$ neutron net-list`
		d. An informative name for the instance.
		NO1
		NO2
		2. Create and boot the VM instance.
		The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Use one **--nic** argument for each IP/interface. Number of IP/interfaces for each VM type must conform with the interface-to-network mappings described at the bottom of Appendix D Resource Profile.
		Note: IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.
		`$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>`
		3. View the newly created instance using the nova tool.
		`$ nova list  --all-tenants`
		The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

3
□
	Configure VIP (Optional)	1. If more than one NOAM is used, a NOAM VIP is needed. Execute the following commands.
		2. Find the port ID associated with the NOAM instance XMI interface.
		`$ neutron port-list`
		3. Add the VIP IP address to the address pairs list of the NOAM instance XMI interface port.
		`$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>`
		4. If necessary, see Allowed Address Pairs in Appendix H for more information.

Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

4
□
	Configure instance networking	1. Log into the **Horizon** GUI as the DSR tenant user.
		2. Go to the Compute/Instances section.
		3. Click the **Name** field of the newly created instance.
		4. Select the Console tab.
		5. Login as the **admusr**.
		6. Configure the network interfaces, conforming with the interface-to-network mappings described at the bottom of the Appendix D Resource Profile.
		`$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>`
		`$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>`
		Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions.
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly, and then delete it.
		7. Re-run the netAdm command. It creates and configures the interface in one action.
		8. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible via both network and Horizon console.

5 □	Configure NO2 (Optional for small lab deployment)	Repeat steps 1 through 3 for NO2.

Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile

STEP #	This procedure adds network addresses for all virtual machines. 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 □	Name the new VM instance	1. Create an informative name for the new instance:SO1. 2. Examine the network interface recommendations at the bottom of Appendix D Resource Profile.

Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile

2
□
	Create and boot the SO VM instance from the glance image	1. Get the following configuration values.
		a. The image ID.
		`$ glance image-list`
		b. The flavor ID.
		`$ nova flavor-list`
		c. The network ID(s)
		`$ neutron net-list`
		d. An informative name for the instance.
		i. SO1
		ii. SO2
		2. Create and boot the VM instance.
		The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. . Use one "—nic" argument for each IP/interface. Number of IP/interfaces for each VM type must conform with the interface-to-network mappings described at the bottom of Appendix D Resource Profile.
		Note: IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.
		`$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>`
		3. View the newly created instance using the nova tool.
		`$ nova list  --all-tenants`
		The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

3
□
	Configure SOAM VIP (Optional)	1. If more than one SOAM VM is used, a SOAM VIP is needed. Execute the following commands.
		2. Find the port ID associated with the SOAM instance XMI interface.
		`$ neutron port-list`
		3. Add the VIP IP address to the address pairs list of the SOAM instance XMI interface port.
		`$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>`
		4. If necessary, see Allowed Address Pairs in Appendix H for more information.

Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile

3
□
	Configure instance networking	1. Log into the **Horizon** GUI as the DSR tenant user.
		2. Go to the Compute/Instances section.
		3. Click the **Name** field of the newly created instance.
		4. Select the Console tab.
		5. Login as the **admusr**.
		6. Configure the network interfaces, conforming with the interface-to-network mappings described at the bottom of the Appendix D Resource Profile.
		`$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>`
		`$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>`
		Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions.
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly, and then delete it.
		7. Re-run the `netAdm` command. It creates and configures the interface in one action.
		8. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible via both network and Horizon consoles.

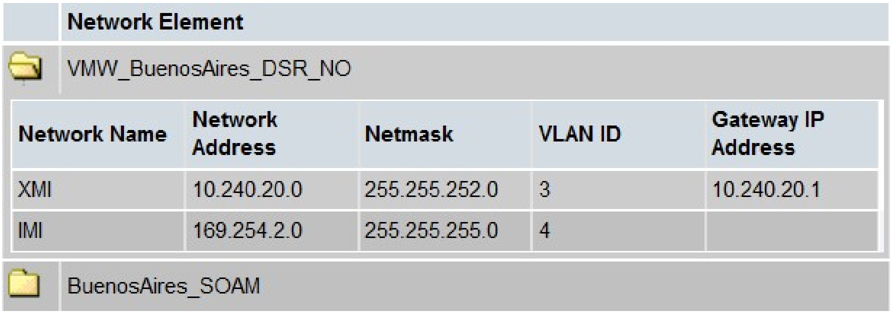
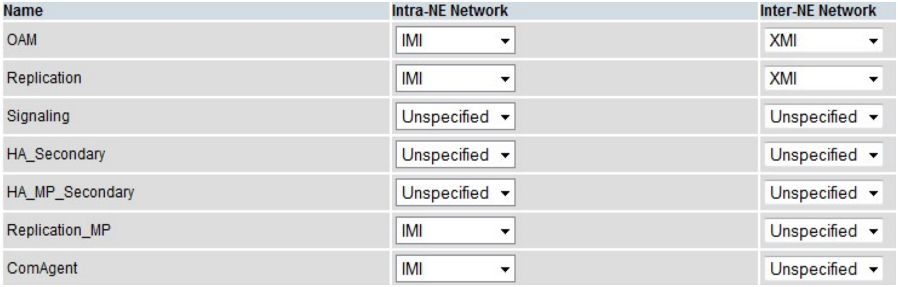
4
□
	Procedure Overview	Repeat steps 1 through 3 for the following VMs. Use unique labels for the VM names. Assign addreses to all desired network interfaces:
		MP(s)
		MP(s) SS7 (optional components)
		IPFE(s)
		NOAM(s)
		SOAM(s)
		SBR s, SBR b (optional components)

4.3 Application Configuration

Procedure 7. Configure the First NOAM NE and Server

S T E P #	This procedure configures the first NOAM virtual machine. 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.

Procedure 7. Configure the First NOAM NE and Server

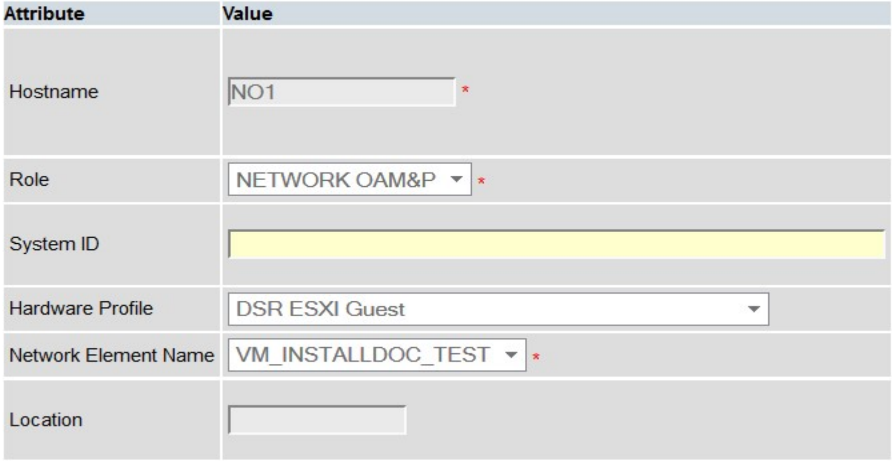
<table>
<tr><td>1
□</td><td><b>NOAM GUI</b>: Login</td><td>In your browser, go to the NOAM xmi IP address and login to the NOAM GUI as the <b>guiadmin</b> user.</td></tr>
<tr><td>2
□</td><td>Create the NOAM Network Element using the XML File</td><td>Navigate to <b>Main Menu->Configuration->Network Elements</b>.
Click <b>Browse</b> and type the pathname of the NOAM network XML file.
Click <b>Upload File</b> to upload the XML file. See the examples in Appendix A Sample Network Element and Hardware Profiles and configure the NOAM network element.
Once the data has been uploaded, you should see a folder appear with the name of your network element. Click on this folder and a list describes the individual networks now configured:

Network Element
VMW_BuenosAires_DSR_NO
<table>
<tr><th>Network Name</th><th>Network Address</th><th>Netmask</th><th>VLAN ID</th><th>Gateway IP Address</th></tr>
<tr><td>XMI</td><td>10.240.20.0</td><td>255.255.252.0</td><td>3</td><td>10.240.20.1</td></tr>
<tr><td>IMI</td><td>169.254.2.0</td><td>255.255.255.0</td><td>4</td><td></td></tr>
</table>
BuenosAires_SOAM</td></tr>
<tr><td>3
□</td><td>Map Services to Networks</td><td>Navigate to <b>Main Menu->Configuration->Services</b>.
Click <b>Edit</b> and set the services as shown in the table below:
<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>OAM</td><td>&lt;IMI Network&gt;</td><td>&lt;XMI Network&gt;</td></tr>
<tr><td>Replication</td><td>&lt;IMI Network&gt;</td><td>&lt;XMI Network&gt;</td></tr>
<tr><td>Signaling</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_MP_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>Replication_MP</td><td>&lt;IMI Network&gt;</td><td>Unspecified</td></tr>
<tr><td>ComAgent</td><td>&lt;IMI Network&gt;</td><td>Unspecified</td></tr>
</table>
For example, if your IMI network is named IMI and your XMI network is named XMI, then your services should config should look like the following:

<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>OAM</td><td>IMI</td><td>XMI</td></tr>
<tr><td>Replication</td><td>IMI</td><td>XMI</td></tr>
<tr><td>Signaling</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_MP_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>Replication_MP</td><td>IMI</td><td>Unspecified</td></tr>
<tr><td>ComAgent</td><td>IMI</td><td>Unspecified</td></tr>
</table>
Click <b>OK</b> to apply the Service-to-Network selections. Dismiss any possible popup notifications.</td></tr>
</table>

Procedure 7. Configure the First NOAM NE and Server

4 □ Insert the 1st NOAM VM

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

Click **Insert** to insert the new NOAM server into servers table (the first or server).

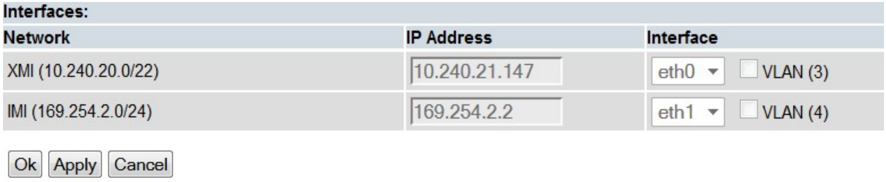


Attribute	Value
Hostname	NO1 *
Role	NETWORK OAM&P *
System ID	
Hardware Profile	DSR ESXI Guest
Network Element Name	VM_INSTALLDOC_TEST *
Location	

Fill in the fields as follows:

Hostname:	<Hostname>
Role:	NETWORK OAM&P
System ID:	<Site System ID>
Hardware Profile:	DSR Guest
or	
Hardware Profile:	DSR Guest
Network Element Name:	[Select **NE** from list]

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



Interfaces:

Network	IP Address	Interface
XMI (10.240.20.0/22)	10.240.21.147	eth0 □ VLAN (3)
IMI (169.254.2.0/24)	169.254.2.2	eth1 □ VLAN (4)

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

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

Add the following NTP servers:

NTP Server	Preferred?
Valid Ntp Server	Yes
Valid Ntp Server	No
Valid Ntp Server	No

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

Procedure 7. Configure the First NOAM NE and Server

5 □	Export the Initial Configuration	Navigate to **Main Menu->Configuration->Servers**. From the GUI screen, select the NOAM server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.
6 □	Copy Configuration File to 1st NOAM Server	Obtain a terminal window to the 1st NOAM server, logging in as the **admusr** user. Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the 1st NOAM to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example: `$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh`
7 □	Wait for Configuration to Complete	The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and prompts the user to reboot the server. If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure. Verify the script completed successfully by checking the following file. `$ sudo cat /var/TKLC/appw/logs/Process/install.log` ***Note***: Ignore the warning about removing the USB key since no USB key is present. No response occurs until the reboot prompt is issued.

8
□
	Set the time zone (optional) and reboot the Server	To change the system time zone, from the command line prompt, execute **set_ini_tz.pl**. The following command example uses the America/New_York time zone.
		Replace, as appropriate, with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix B.
		`$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1`
		`$ sudo init 6`
		Wait for server to reboot.

Procedure 7. Configure the First NOAM NE and Server

9
□
	1st NO Server:
	Verify Server Health
		Login into the NO1 as **admusr**.
		Execute the following command as admusr on the 1st NO server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

Procedure 8. Configure the NOAM Server Group

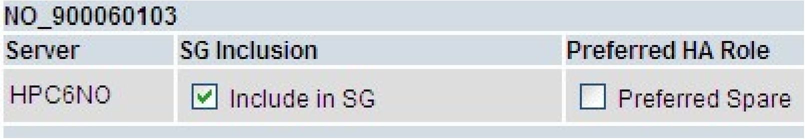
S T E P #	This procedure configures the NOAM server group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **My Oracle Support (MOS)** and ask for assistance.	
1 □	**NOAM GUI**: Login	Establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type **http://<NO1_XMI_IP_Address>** as the URL. Login as the **guiadmin** user. If prompted by a security warming, cllick **Continue to this Website** to proceed.
2 □	Enter NOAM Server Group Data	Using the GUI session on the first NOAM server, navigate to **Main Menu**->**Configuratio**n->**Server Groups**, 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` Click **OK** when all fields are filled in.

Procedure 8. Configure the NOAM Server Group

<table>
<tr>
<td>3
□</td>
<td>Edit the NOAM Server Group</td>
<td>

Navigate to **Main Menu->Configuration->Server Groups**, select the new server group, and click **Edit**.

Select the network element that represents the NOAM.



NO_900060103

Server	SG Inclusion	Preferred HA Role
HPC6NO	☑ Include in SG	□ Preferred Spare

In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the **Include in SG** checkbox.

Leave other boxes unchecked.

Click **OK**.

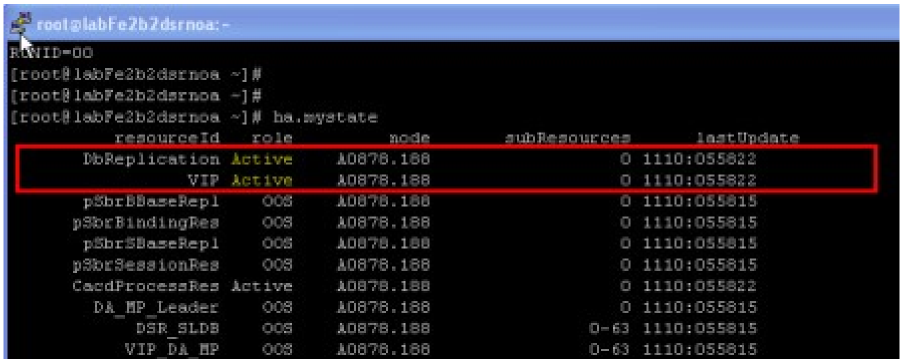
</td>
</tr>
<tr>
<td>4
□</td>
<td>Verify NOAM virtual machine role</td>
<td>

From console window of the first NOAM virtual machine, execute the **ha.mystate** command to verify the **DbReplication** and **VIP** items under the **resourceId** column has a value of **Active** under the **role** column.

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

Press **Ctrl+C** to exit.

Example:



root@labFe2b2dsrnoa:~

```
RUNID=00
[root@labFe2b2dsrnoa ~]#
[root@labFe2b2dsrnoa ~]#
[root@labFe2b2dsrnoa ~]# ha.mystate
              resourceId   role          node          subResources       lastUpdate
           DbReplication Active     A0878.188                     0 1110:055822
                     VIP Active     A0878.188                     0 1110:055822
          pSbrBBaseRepl     OOS     A0878.188                     0 1110:055815
         pSbrBindingRes     OOS     A0878.188                     0 1110:055815
          pSbrSBaseRepl     OOS     A0878.188                     0 1110:055815
         pSbrSessionRes     OOS     A0878.188                     0 1110:055815
         CacdProcessRes Active     A0878.188                     0 1110:055822
           DA_MP_Leader     OOS     A0878.188                     0 1110:055815
               DSR_SLDB     OOS     A0878.188                  0-63 1110:055815
              VIP_DA_MP     OOS     A0878.188                  0-63 1110:055815
```

</td>
</tr>
<tr>
<td>5
□</td>
<td>Restart 1st NOAM virtual machine</td>
<td>

From the NOAM GUI, navigate to **Main Menu**->**Status & Manage**->**Server**.

Select the first NOAM server. Click **Restart**. Click **OK** on the confirmation screen and wait for restart to complete.

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

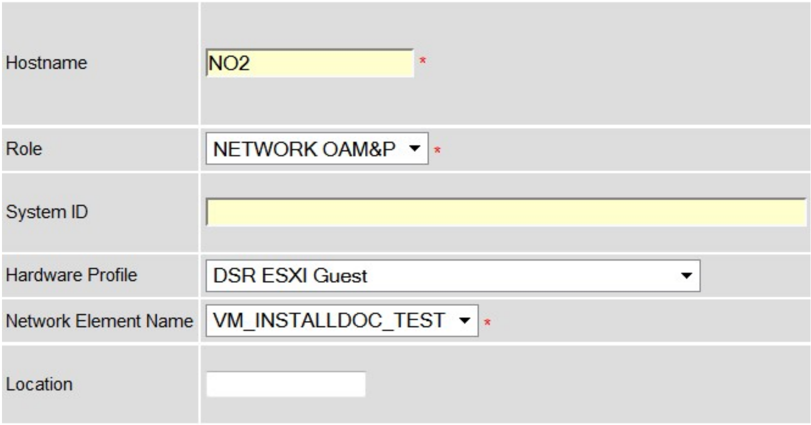
Procedure 9. Configure the Second NOAM Server

S **T** **E** **P** **#**	This procedure configures the second NOAM server. Optional for small lab deployment. 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	If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type **http://<NO1_XMI_IP_Address>** as the URL. Login as the **guiadmin** user.

Procedure 9. Configure the Second NOAM Server

<table>
<tr>
<td>2
□</td>
<td>Insert the 2nd NOAM VM</td>
<td>
Navigate to <b>Main Menu->Configuration->Servers</b>.

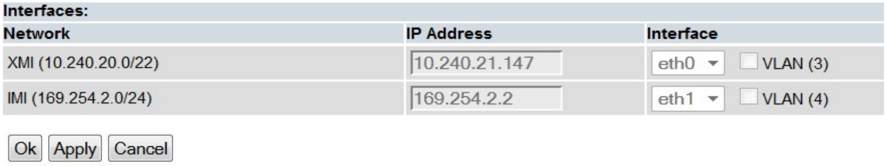
Click <b>Insert</b> to insert the new NOAM server into servers table (the first or server).


<table>
<tr><td>Hostname</td><td>NO2 *</td></tr>
<tr><td>Role</td><td>NETWORK OAM&P *</td></tr>
<tr><td>System ID</td><td></td></tr>
<tr><td>Hardware Profile</td><td>DSR ESXI Guest</td></tr>
<tr><td>Network Element Name</td><td>VM_INSTALLDOC_TEST *</td></tr>
<tr><td>Location</td><td></td></tr>
</table>

Fill in the fields as follows:

<table>
<tr><td>Hostname:</td><td>&lt;Hostname&gt;</td></tr>
<tr><td>Role:</td><td><code>NETWORK OAM&P</code></td></tr>
<tr><td>System ID:</td><td>&lt;Site System ID&gt;</td></tr>
<tr><td>Hardware Profile:</td><td><code>DSR ESXI Guest (VMware)</code></td></tr>
<tr><td>or</td><td></td></tr>
<tr><td>Hardware Profile:</td><td><code>DSR Guest (KVM/OpenStack)</code></td></tr>
<tr><td>Network Element Name:</td><td>[Choose <b>NE</b> list]</td></tr>
</table>

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


Interfaces:
<table>
<tr><th>Network</th><th>IP Address</th><th>Interface</th><th></th></tr>
<tr><td>XMI (10.240.20.0/22)</td><td>10.240.21.147</td><td>eth0</td><td>□ VLAN (3)</td></tr>
<tr><td>IMI (169.254.2.0/24)</td><td>169.254.2.2</td><td>eth1</td><td>□ VLAN (4)</td></tr>
</table>

Fill in the server IP addresses for the XMI network. Select <b>ethX</b> for the interface. Leave the <b>VLAN</b> checkbox unmarked.

Fill in the server IP addresses for the IMI network. Select <b>ethX</b> for the interface. Leave the <b>VLAN</b> checkbox unmarked.

Add the following NTP servers:

<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td>Valid Ntp Server</td><td>Yes</td></tr>
<tr><td>Valid Ntp Server</td><td>No</td></tr>
<tr><td>Valid Ntp Server</td><td>No</td></tr>
</table>

Click <b>OK</b> when you have completed entering all the server data.
</td>
</tr>
<tr>
<td>3
□</td>
<td>Export the initial configuration</td>
<td>From the GUI screen, select the second server and click <b>Export</b> to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.</td>
</tr>
</table>

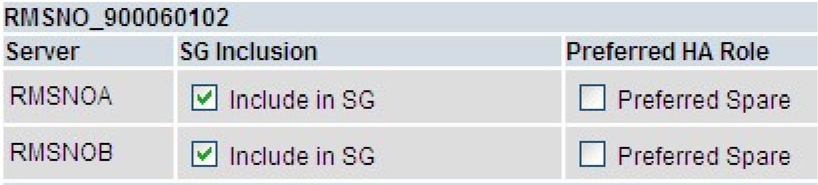
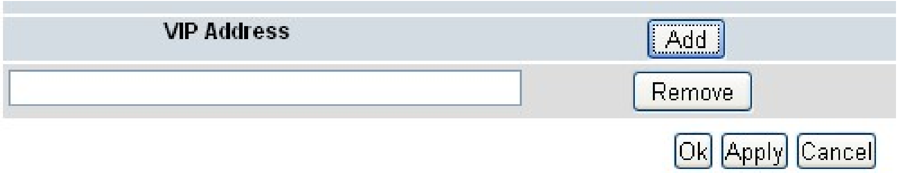
Procedure 9. Configure the Second NOAM Server

4 □	Copy Configuration File to 2nd NOAM Server	Obtain a terminal session to the 1st NOAM as the **admusr** user. Login as **admusr** to the NO1 shell and issue the following commands: `$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh` ***Note***: ipaddr is the IP address of NO2 assigned to its ethx interface associated with the xmi network.
5 □	Wait for Configuration to Complete	Obtain a terminal session to the 2nd NOAM as the **admusr** user. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp directory**, implements the configuration in the file, and prompts the user to reboot the server. If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure. Verify script completed successfully by checking the following file. `$ sudo cat /var/TKLC/appw/logs/Process/install.log` ***Note***: Ignore the warning about removing the USB key since no USB key is present.

6
□
	Set the time zone (optional) and reboot the Server	To change the system time zone, from the command line prompt, execute **set_ini_tz.pl**. The following command example uses the America/New_York time zone.
		Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix B List of Frequently Used Time Zones.
		`$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1`
		`$ sudo init 6`
		Wait for server to reboot.

7
□
	2nd NO Server: Verify Server Health	Login into the NO2 as **admusr** and wait.
		Execute the following command as super-user on the 2ndt NO 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 10. Complete Configuring the NOAM Server Group

STEP #	This procedure finishes configuring th 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 ☐	Edit the NOAM Server Group Data	From the GUI session on the first NOAM server, navigate to **Main Menu->Configuration->Server Groups**. Select the NOAM server group, click **Edit**, and add the second NOAM server to the Server Group by marking the **Include in SG** checkbox for the second NOAM server. Click **Apply.**  RMSNO_900060102 Server | SG Inclusion | Preferred HA Role RMSNOA | ☑ Include in SG | ☐ Preferred Spare RMSNOB | ☑ Include in SG | ☐ Preferred Spare Click **Add** to add a NOAM VIP. Type the VIP Address and click **OK**. 
2 ☐	Wait for Replication	After replication, which initially takes up to 5 minutes, the HA status should be active (**Main Menu->Status & Manage->HA**). ***Note***: This may take up to 5 minutes while the NOAM servers figure out master/slave relationship. Log out of GUI from the first NOAM XMI address.
3 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the NOAM VIP address. Login as user **guiadmin**.
4 ☐	Wait for Remote Database Alarm to Clear	Wait for the alarm ID 10200 "Remote Database re-initialization in progress" to be cleared before proceeding (**Main menu->Alarms & Events->View Active**).
5 ☐	Restart 2nd NOAM virtual machine	Navigate to **Main Menu->Status & Manage->Server** and select the second NOAM server. Click **Restart**. Click **OK** on the confirmation screen. Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the **Appl State** as **Enabled**.
6 ☐	SDS can now be installed (Optional)	If this deployement contains SDS, SDS can now be installed. Refer to document referenced in [6] SDS SW Installation and Configuration Guide, CGBU_010592 /E64816-02.

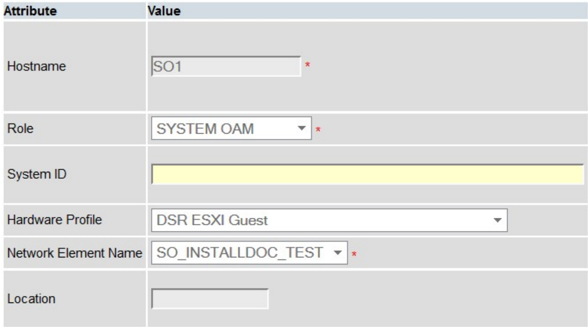
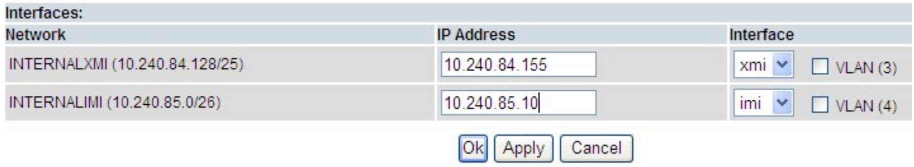
Procedure 11. Configure the SOAM NE

S T E P #	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) ask for assistance.	
1 □	Establish GUI Session on the NOAM VIP	If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as user **guiadmin**.
2 □	Create the SOAM Network Element using an XML File	Make sure to have an SOAM network element XML file available on the PC running the web browser. The SOAM network element XML file is similar to what was created and used in Procedure 9, but defines the SOAM network element. Refer to Appendix A for a sample network element xml file Navigate to **Main Menu->Configuration->Network Elements**. Click **Browse** and type the path and name of the SOAM network XML file. Click **Upload** to upload the XML file and configure the SOAM network element.

Procedure 12. Configure the SOAM Servers

S T E P #	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 □	Establish GUI Session on the NOAM VIP	If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as user **guiadmin**.

Procedure 12. Configure the SOAM Servers

<table>
<tr>
<td>2
□</td>
<td>Insert the 1st SOAM server</td>
<td>
Navigate to <b>Main Menu->Configuration->Servers</b>.
Click <b>Insert</b> to insert the new SOAM server into servers table.

<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>Hostname</td><td>SO1 *</td></tr>
<tr><td>Role</td><td>SYSTEM OAM *</td></tr>
<tr><td>System ID</td><td></td></tr>
<tr><td>Hardware Profile</td><td>DSR ESXI Guest</td></tr>
<tr><td>Network Element Name</td><td>SO_INSTALLDOC_TEST *</td></tr>
<tr><td>Location</td><td></td></tr>
</table>
Fill in the fields as follows:
<table>
<tr><td>Hostname:</td><td>&lt;SO1-Hostname&gt;</td></tr>
<tr><td>Role:</td><td><code>SYSTEM OAM</code></td></tr>
<tr><td>System ID:</td><td>&lt;Site System ID&gt;</td></tr>
<tr><td>Hardware Profile:</td><td><code>DSR ESXI Guest (VMware)</code></td></tr>
<tr><td>or</td><td></td></tr>
<tr><td>Hardware Profile:</td><td><code>DSR Guest (KVM/OpenStack)</code></td></tr>
<tr><td>Network Element Name:</td><td>[Choose <b>NE</b> from list]</td></tr>
</table>
The network interface fields are now available with selection choices based on the chosen hardware profile and network element.

Interfaces:
<table>
<tr><th>Network</th><th>IP Address</th><th>Interface</th></tr>
<tr><td>INTERNALXMI (10.240.84.128/25)</td><td>10.240.84.155</td><td>xmi ☐ VLAN (3)</td></tr>
<tr><td>INTERNALIMI (10.240.85.0/26)</td><td>10.240.85.10</td><td>imi ☐ VLAN (4)</td></tr>
</table>

Fill in the server IP addresses for the XMI network. Select <b>ethX</b> for the interface. Leave the <b>VLAN</b> checkbox unmarked.
Fill in the server IP addresses for the IMI network. Select <b>ethX</b> for the interface. Leave the <b>VLAN</b> checkbox unmarked.
Add the following NTP servers:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td>Valid Ntp Server</td><td>Yes</td></tr>
<tr><td>Valid NTP Server</td><td>No</td></tr>
<tr><td>Valid NTP Server</td><td>No</td></tr>
</table>
Click <b>OK</b> when you have completed entering the server data.
</td>
</tr>
<tr>
<td>3
□</td>
<td>Export the initial configuration</td>
<td>From the GUI screen, select the desired server and click <b>Export</b> to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.</td>
</tr>
<tr>
<td>4
□</td>
<td>Copy Configuration File to the 1st SOAM server</td>
<td>Log in as <b>admusr</b> to the NO1 shell and issue the commands:
<pre>
$ sudo scp
/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh
admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
</pre>
</td>
</tr>
</table>

Procedure 12. Configure the SOAM Servers

5 □	Wait for Configuration to Complete	Obtain a terminal session on the 1st SOAM as the **admusr** user. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the /var/tmp directory, implements the configuration in the file, and prompts the user to reboot the server. If you are on the console wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure. Verify script completed successfully by checking the following file. `$ sudo cat /var/TKLC/appw/logs/Process/install.log` ***Note***: Ignore the warning about removing the USB key since no USB key is present.

6
□
	Set the time zone (optional) and reboot the Server	To change the system time zone, from the command line prompt, execute **set_ini_tz.pl**. The following command example uses the America/New_York time zone.
		Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix B.
		`$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1`
		`$ sudo init 6`
		Wait for server to reboot.

7
□
	1st SOAM Server: Verify Server Health	After the system reboots, login again as **admusr.**
		Execute the following command 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 12. Configure the SOAM Servers

<table>
<tr>
<td>8
□</td>
<td>Insert and Configure the 2nd SOAM server, repeat steps 1 thourgh 7 for 2nd SOAM

<b><i>Note</i></b>: Optional for Non-HA Configuration</td>
<td>Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td>Any valid NTP server address</td><td>Yes</td></tr>
<tr><td>Any valid NTP server address</td><td>No</td></tr>
<tr><td>Any valid NTP server address</td><td>No</td></tr>
</table>
Enter the network data for the 2nd SOAM server, transfer the <b>TKLCConfigData</b> file to the 2nd SOAM server, and reboot the 2nd SOAM server when asked at a terminal window.

Wait approximately 5 minutes for the 2nd SOAM server to reboot.

<b><i>Note</i></b>: For DSR mated sites, repeat this step for additional/spare SOAM server for mated site.</td>
</tr>
</table>

Procedure 13. Configure the SOAM Server Group

<table>
<tr>
<td><b>S
T
E
P
#</b></td>
<td colspan="2">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.

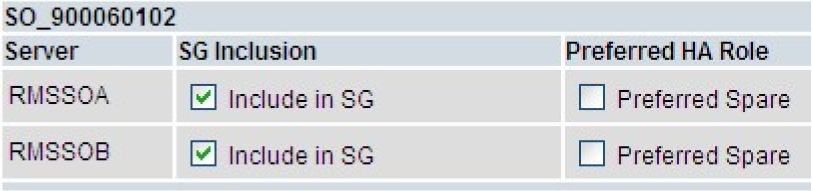
If this procedure fails, contact <b>My Oracle Support (MOS)</b> and ask for assistance.</td>
</tr>
<tr>
<td>1
□</td>
<td>Enter SOAM Server Group Data</td>
<td>From the GUI session on the <b>NOAM VIP</b> address, navigate to <b>Main Menu->Configuration->Server Groups</b>, click <b>Insert</b>, and add the SOAM Server Group name along with the values for the following fields:
<table>
<tr><td>Name:</td><td>[Enter Server Group Name]</td></tr>
<tr><td>Level:</td><td><code>B</code></td></tr>
<tr><td>Parent:</td><td>[Select the <b>NOAM</b> Server Group]</td></tr>
<tr><td>Function:</td><td><code>DSR (Active/Standby Pair)</code></td></tr>
<tr><td>WAN Replication Connection Count:</td><td>Use Default Value</td></tr>
</table>
Click <b>OK</b> when all fields are filled.

<b><i>Note</i></b>: 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.</td>
</tr>
</table>

Procedure 13. Configure the SOAM Server Group

<table>
<tr><td>2
□</td><td>Edit the SOAM Server Group and add VIP</td><td>

Navigate to **Main Menu->Configuration->Server Groups**, select the new **SOAM** server group, and click **Edit**.

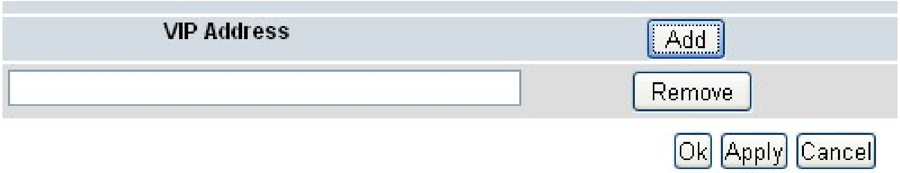


<table>
<tr><th colspan="3">SO_900060102</th></tr>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>RMSSOA</td><td>☑ Include in SG</td><td>□ Preferred Spare</td></tr>
<tr><td>RMSSOB</td><td>☑ Include in SG</td><td>□ Preferred Spare</td></tr>
</table>

Add both SOAM servers to the Server Group Primary Site by marking the **Include in SG** checkbox.

Click **Apply**.

Click **Add** to add a SOAM VIP. Type the **VIP Address** and click **OK**:

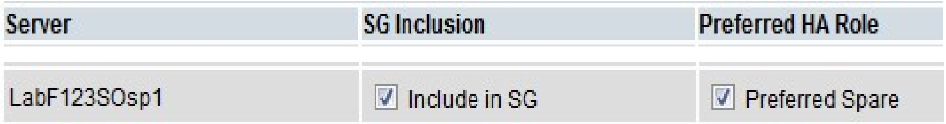


</td></tr>
<tr><td>3
□</td><td>(OPTIONAL)
Prepare Feature Activation where Preferred Spares are Already Present</td><td>

In mated DSR configurations, where a preferred spare is already present upon entering the Active and Standby SOAM servers. Execute **Steps 1-4** from **Appendix C**. Otherwise, skip this step.

</td></tr>
<tr><td>4
□</td><td>(OPTIONAL)
Edit the SOAM Server Group and add Preferred Spares for Site Redundancy</td><td>

If the two site redundancy feature is wanted for the SOAM server group, add a SOAM server located in its server group secondary site by marking the **Include in SG** checkbox. Also mark the **Preferred Spare** checkbox.



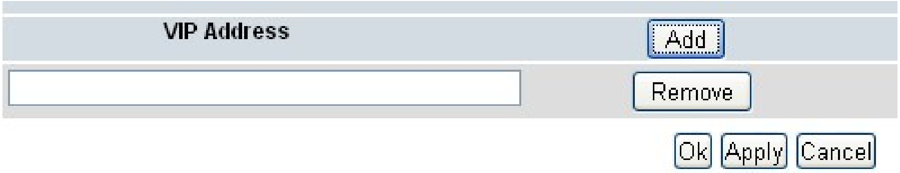
<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>LabF123SOsp1</td><td>☑ Include in SG</td><td>☑ Preferred Spare</td></tr>
</table>

For more information about Server Group Secondary Site or Site Redundancy, see the **Terminology** section.

</td></tr>
<tr><td>5
□</td><td>(OPTIONAL)
Edit the SOAM Server Group and add addional SOAM VIPs</td><td>

Click **Add** to add SOAM VIPs. Type the **VIP Address** and click **OK.**

Note: One VIP applies to the SOAMs at the primary site and one VIP applies to the preferred spare SOAM at the secondary site. Only one SOAM VIP is active at any time, and this is determined by whether a SOAM is active at the primary site or the secondary site.



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

Procedure 13. Configure the SOAM Server Group

6 □	Wait for Replication	After replication, the server status should be active (**Main menu->Status & Manage->HA**). ***Note***: This may take up to 5 minutes while the servers figure out master/slave relationship. Look for the alarm ID 10200 "Remote Database re-initialization in progress" to be cleared before proceeding. (**Main Menu->Alarms->View Active**)
7 □	Restart 1st SOAM server	From the NOAM GUI, navigate to **Main Menu->Status & Manage->Server** and select the **1st SOAM** server. Click **Restart**. Click **OK** to the confirmation popup. Wait for restart to complete. Wait for the Appl State to change to Enabled, and all other columns to Norm.
8 □	Restart 2nd SOAM server	Continuing from the **Main Menu->Status & Manage->Server** menu, select the **2nd SOAM** server. Click **Restart**. Click **OK** to the confirmation popup. Wait for the Appl State to change to Enabled, and all other columns to Norm.
9 □	(OPTIONAL) Restart all Preferred Spare SOAM Servers	If additional preferred spare servers are configured for secondary sites, navigate to **Main Menu->Status & Manage->Server** and select all **Preferred Spare** SOAM servers. Click **Restart**. Click **OK** to the confirmation popup. Wait for the Appl State to change to **Enabled** and all other columns to change to **Norm**.

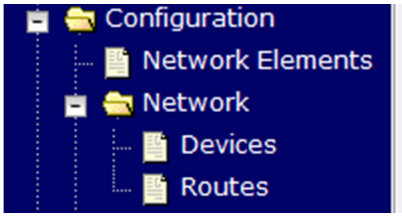
Procedure 14. Activate PCA (PCA Only)

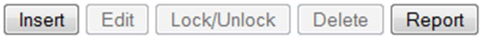
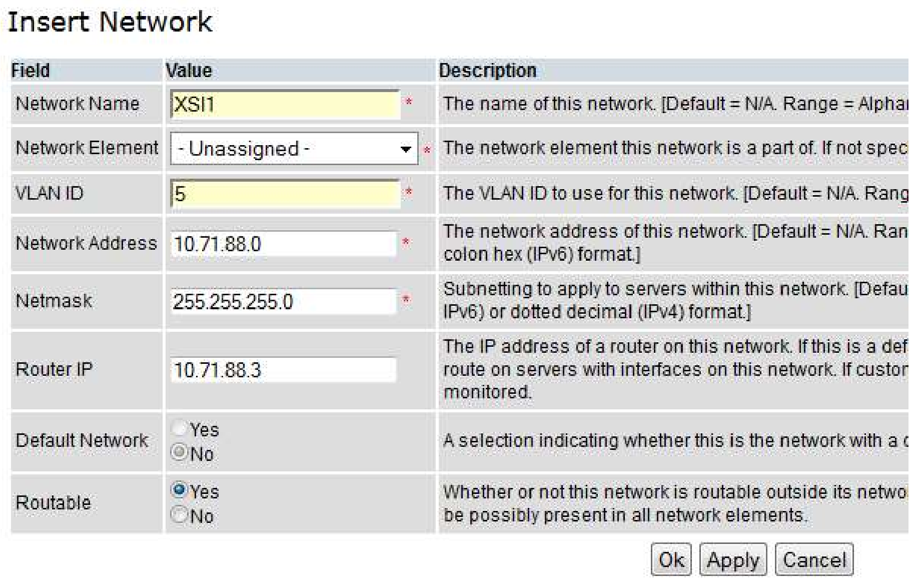
STEP #	This procedure activates PCA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1 □	(PCA Only) Activate PCA Feature	If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) within Appendix A of [2] PCA Configuration, E58667. ***Note***: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.

Procedure 15. Configure the MP Virtual Machines

STEP #	This procedure configures an MP virtual machines (IPFE, SBR, SS7-MP, DA-MP). ***Prerequisite***: **Procedures 7** and **8** have been executed 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 □	Establish GUI Session on the NOAM VIP	If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as user **guiadmin**.

Procedure 15. Configure the MP Virtual Machines

<table>
<tr>
<td>2
□</td>
<td><b>NOAM VIP GUI</b>: Navigate to Signaling Network Configuration Screen</td>
<td>Navigate to <b>Main Menu->Configuration->Network</b>.


Click <b>Insert</b> in the lower left corner.

</td>
</tr>
<tr>
<td>3
□</td>
<td><b>NOAM VIP</b>: Add Signaling Networks</td>
<td>The following screenshot appears:

Insert Network
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Network Name</td><td>XSI1 *</td><td>The name of this network. [Default = N/A. Range = Alpha</td></tr>
<tr><td>Network Element</td><td>- Unassigned - *</td><td>The network element this network is a part of. If not spec</td></tr>
<tr><td>VLAN ID</td><td>5 *</td><td>The VLAN ID to use for this network. [Default = N/A. Rang</td></tr>
<tr><td>Network Address</td><td>10.71.88.0 *</td><td>The network address of this network. [Default = N/A. Ran colon hex (IPv6) format.]</td></tr>
<tr><td>Netmask</td><td>255.255.255.0 *</td><td>Subnetting to apply to servers within this network. [Defau IPv6) or dotted decimal (IPv4) format.]</td></tr>
<tr><td>Router IP</td><td>10.71.88.3</td><td>The IP address of a router on this network. If this is a def route on servers with interfaces on this network. If custor monitored.</td></tr>
<tr><td>Default Network</td><td>○ Yes
● No</td><td>A selection indicating whether this is the network with a c</td></tr>
<tr><td>Routable</td><td>● Yes
○ No</td><td>Whether or not this network is routable outside its netwo be possibly present in all network elements.</td></tr>
</table>

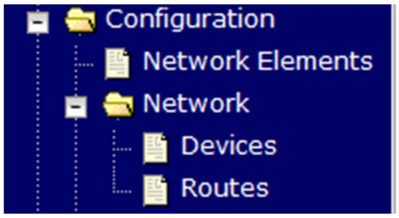
Type the <b>Network Name</b>, <b>VLAN ID</b>, <b>Network Address</b>, <b>Netmask</b>, and <b>Router IP</b> that matches the Signaling network.
<b><i>Note</i></b>: Even if the network does not use VLAN Tagging, you should type the correct VLAN ID here as indicated by the NAPD.
<b><i>IMPORTANT</i>:</b> Leave the Network Element field as Unassigned.
Select <b>No</b> for Default Network.
Select <b>Yes</b> for Routable.
Click <b>OK</b> if you are finished adding signaling networks
<b>-OR-</b>
Click <b>Apply</b> to save this signaling network and repeat this step to enter additional signaling networks.</td>
</tr>
</table>

Procedure 15. Configure the MP Virtual Machines

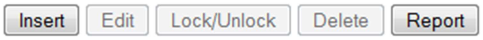
4 □ **NOAM VIP GUI**: [PCA Only]:Navigate to Signaling Network Configuration Screen

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

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

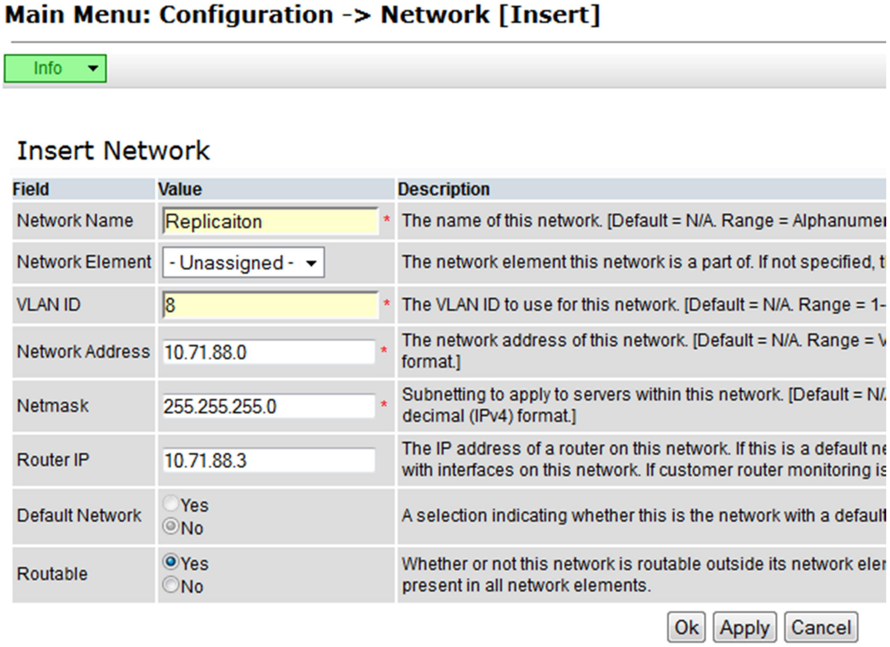


Click **Insert** in the lower left corner.



5 □ **NOAM VIP GUI**: [PCA Only]: Define SBR DB Replication Network

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



Main Menu: Configuration -> Network [Insert]

Insert Network

Field	Value	Description
Network Name	Replicaiton *	The name of this network. [Default = N/A. Range = Alphanume
Network Element	- Unassigned -	The network element this network is a part of. If not specified, t
VLAN ID	8 *	The VLAN ID to use for this network. [Default = N/A. Range = 1-
Network Address	10.71.88.0 *	The network address of this network. [Default = N/A. Range = V format.]
Netmask	255.255.255.0 *	Subnetting to apply to servers within this network. [Default = N/ decimal (IPv4) format.]
Router IP	10.71.88.3	The IP address of a router on this network. If this is a default ne with interfaces on this network. If customer router monitoring is
Default Network	○ Yes ● No	A selection indicating whether this is the network with a default
Routable	● Yes ○ No	Whether or not this network is routable outside its network ele present in all network elements.

Type 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 type the correct VLAN ID here as indicated by the NAPD

IMPORTANT: Leave the Network Element field as Unassigned.

Select **No** for Default Network.

Select **Yes** for Routable.

Click **OK** if you are finished adding signaling networks.

-OR-

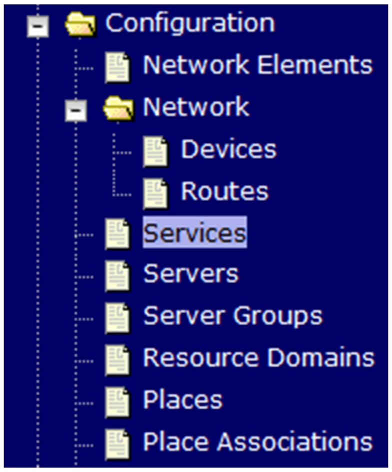
Click **Apply** to save this signaling network and repeat this step to enter additional signaling networks.

Procedure 15. Configure the MP Virtual Machines

6 □ **NOAM VIP GUI**: [PCA Only]: Perform Additional Service to Networks Mapping

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

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



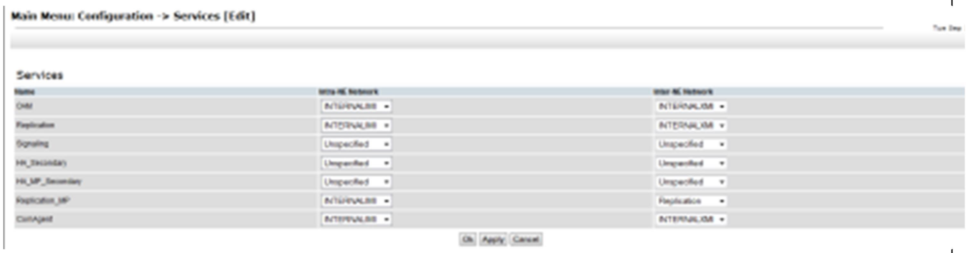
Click **Edit**.

Set the Services as shown in the table below:

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

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

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



Main Menu: Configuration -> Services [Edit]

Services

Name	Intra-NE Network	Inter-NE Network
OAM	INTERNALIMI	INTERNALXMI
Replication	INTERNALIMI	INTERNALXMI
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	INTERNALIMI	Replication
ComAgent	INTERNALIMI	INTERNALXMI

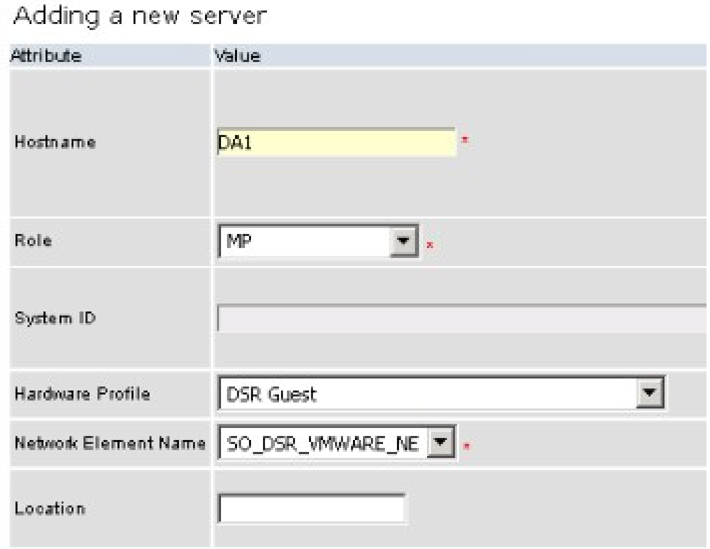
Click **OK** to apply the Service-to-Network selections.

7 □ Insert the MP or IPFE server – Part 1

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

Click **Insert** to add the new MP or IPFE server into servers table. Fill out the following values:

Procedure 15. Configure the MP Virtual Machines

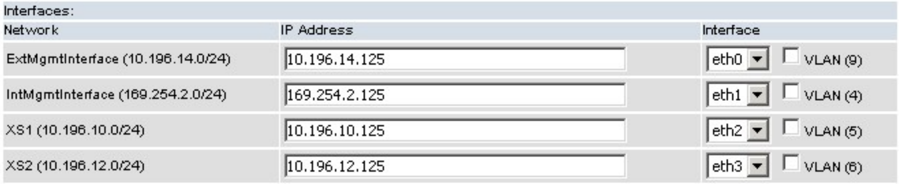


Adding a new server

Attribute	Value
Hostname	DA1 *
Role	MP *
System ID	
Hardware Profile	DSR Guest
Network Element Name	SO_DSR_VMWARE_NE *
Location	

Fill in the fields as follows:

Hostname:	<Hostname>
Role:	`MP`
System ID:	<Site System ID>
Hardware Profile:	`DSR Guest`
Network Element Name:	[Choose **NE** from list]



Interfaces:

Network	IP Address	Interface	
ExtMgmtInterface (10.196.14.0/24)	10.196.14.125	eth0	☐ VLAN (9)
IntMgmtInterface (169.254.2.0/24)	169.254.2.125	eth1	☐ VLAN (4)
XS1 (10.196.10.0/24)	10.196.10.125	eth2	☐ VLAN (5)
XS2 (10.196.12.0/24)	10.196.12.125	eth3	☐ VLAN (6)

For the XMI network, type the MP's XMI IP address. Select the correct interface.

Leave the **VLAN** checkbox unmarked.

For the IMI network, type the MP's IMI IP address. Select the correct interface.

Leave the **VLAN** checkbox unmarked.

For the Replication network, type the MP's **XSI2 IP** address. Select the correct interface. Leave the **VLAN** checkbox unmarked.

For the XSI1 network, type the MP's **XSI1 IP** address. Select the correct interface.

Leave the **VLAN** checkbox unmarked.

For the XSI2 network, type the MP's **XSI2 IP** address. Select the correct interface.

Leave the **VLAN** checkbox unmarked.

Note: If more XSI networks are configured, follow the same method of entry as XSI1 and XSI2. All interfaces need to be added sequentially for any server.

Procedure 15. Configure the MP Virtual Machines

<table>
<tr><td>8
□</td><td>Insert the MP server - Part 2</td><td>Add the following NTP servers:
<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td>Valid NTP server</td><td>Yes</td></tr><tr><td>Valid NTP server</td><td>No</td></tr><tr><td>Valid NTP server</td><td>No</td></tr></table>Click <b>OK</b> when all fields are filled in to finish MP server insertion.</td></tr>
<tr><td>9
□</td><td>Export the initial configuration</td><td>From the GUI screen, select the server that was just inserted and click <b>Export</b> to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.</td></tr>
<tr><td>10
□</td><td>Log onto the MP</td><td>Obtain a terminal window connection on the MP or IPFE server.</td></tr>
<tr><td>11
□</td><td>Copy Configuration File to MP or IPFE server</td><td>From the active NO console login as <b>admusr.</b>
$ sudo scp
/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh
admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
<b><i>Note</i></b>: ipaddr is the XMI IP address of the MP or IPFE.</td></tr>
<tr><td>12
□</td><td>Wait for Configuration to Complete</td><td>Obtain a terminal session on the <b>MP or IPFE</b> as the <b>admusr</b> user.
The automatic configuration daemon looks for the file named <b>TKLCConfigData.sh</b> in the /var/tmp directory, implements the configuration in the file, and prompts the user to reboot the server.
If you are on the console, wait to be prompted to reboot the server, but <b>DO NOT</b> reboot the server, it is rebooted later in this procedure.
Verify script completed successfully by checking the following file.
$ sudo cat /var/TKLC/appw/logs/Process/install.log
<b><i>Note</i></b>: Ignore the warning about removing the USB key since no USB key is present.</td></tr>
<tr><td>13
□</td><td>Set the time zone (optional) and reboot the Server</td><td>To change the system time zone, from the command line prompt, execute <b>set_ini_tz.pl</b>. The following command example uses the America/New_York time zone.
Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix B.
$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl
"America/New_York" >/dev/null 2>&1
$ sudo init 6
Wait for server to reboot.</td></tr>
</table>

Procedure 15. Configure the MP Virtual Machines

<table>
<tr>
<td>14
□</td>
<td>MP or IPFE Server: Verify Server Health</td>
<td>

After the reboot, login as **admusr**.

Execute the following command as super-user on the server and make sure that no errors are returned:

```
$ sudo syscheck
```

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

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

Procedure 15. Configure the MP Virtual Machines

15
□
	(OPTIONAL) Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network	***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.
		Log into the MP as the **admusr** user. (Alternatively, you can log into virtual machines console.)
		Determine <XMI_Gateway_IP> from your SO site network element info.
		Gather the following items:
		<NO_XMI_Network_Address>
		<NO_XMI_Network_Netmask>
		Note: You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the **Main Menu->Configuration->Network Elements** menu.
		[MP console] Create network routes to the NO's XMI(OAM) network:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net`
		`--address=<NO_Site_Network_ID>`
		`--netmask=<NO_Site_Network_Netmask>`
		`--gateway=<MP_XMI_Gateway_IP_Address>`
		`--device=<MP_XMI_Interface>`
		`Route to <MP_XMI_Interface> added.`
		(Optional) [MP console] If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=host`
		`--address=<Customer_NMS_IP>`
		`--gateway=<MP_XMI_Gateway_IP_Address>`
		`--device=<MP_XMI_Interface>`
		`Route to <MP_XMI_Interface> added.`
		Repeat for any existing cusomter NMS stations.
		Delete the existing default route:
		`$  sudo /usr/TKLC/plat/bin/netAdm delete --`
		`route=default --gateway=<MP_XMI_Gateway_IP>  --`
		`device=<MP_XMI_Interface>`
		`Route to <MP_XMI_Interface> removed.`

Procedure 15. Configure the MP Virtual Machines

16
□
	(OPTIONAL, Continued from Previous Step) Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network	[MP Console] Ping active NO XMI IP address to verify connectivity:
		`$ ping <ACTIVE_NO_XMI_IP_Address>`
		`PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.`
		`64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms`
		(Optional) [MP Console] Ping Customer NMS Station(s):
		`$ ping <Customer_NMS_IP>`
		`PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.`
		`64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms`
		If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support.

17 □	Add the signaling interfaces to the MPs and IPFEs	Use the netAdm command to add XSI interfaces. Repeat this step for each signaling interface. Note that KVM/OpenStack users must have added network addresses during the boot invocation ("nova boot") that correspond to the relevant network interfaces. `$ sudo netAdm add --device=ethX --address=<XSI_IP_ADDRESS> \ --netmask=<XSI_NETMASK> --onboot=yes --bootproto=none` ***Note***: ethX is the defined signaling device. i.e., `XMI:eth0/IMI:eth1/XSI1:eth2/XSI2:eth3` ***Note***: When reconfiguring virtual NICs under VMware, the proper procedure is to remove the UDEV rules file (/etc/udev/rules.d/70-persistent-net.rules), shut down the guest and remove the interfaces. Power on the VM, then add the interfaces one by one, in the desrired order of enumeration, each time clicking **OK** to get VMware to instantiate the device.
18 □	Repeat for remaining MPs and IPFEs	**Repeat** this entire procedure for all remaining MP's and IPFE's.

Procedure 16. Configure Places and Assign MP Servers to Places (PCA ONLY)

STEP #

This procedure adds places in the PCA network.

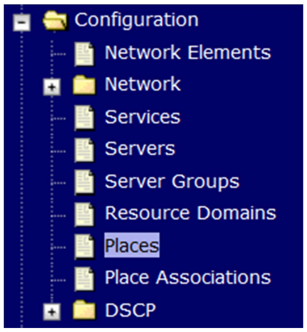
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

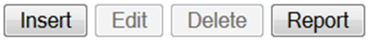
1 □ (PCA Only) Configure Places

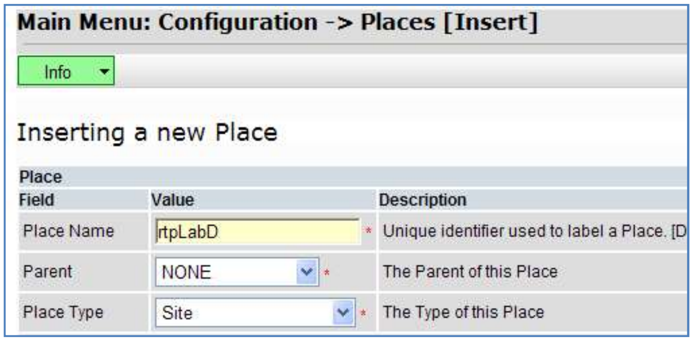
Establish a GUI session on the NOAM by using the XMI VIP address. Login as user **guiadmin**.

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



Click **Insert**.





Main Menu: Configuration -> Places [Insert]

Inserting a new Place

Place

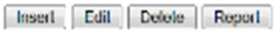
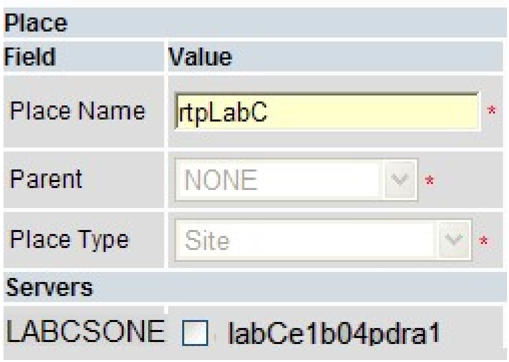
Field	Value	Description
Place Name	rtpLabD *	Unique identifier used to label a Place. [D
Parent	NONE *	The Parent of this Place
Place Type	Site *	The Type of this Place

Place Name:	<Site Name>
Parent:	NONE
Place Type:	Site

Repeat this step for each of the PCA Places (Sites) in the network.

See the Terminology section for more information on Sites & Places.

Procedure 16. Configure Places and Assign MP Servers to Places (PCA ONLY)

2 □	(PCA Only) Configure Place Associations	Select the place configured in step 1 and click **Edit**.  For each place you have defined, select the set of MP servers that are assigned to those places.  Place Field / Value Place Name: rtpLabC * Parent: NONE * Place Type: Site * Servers LABCSONE □ labCe1b04pdra1 Mark all the checkboxes for **PCA DA-MP** and **SBR** servers that are assigned to this place. Repeat this step for all other DA-MP or SBR servers you wish to assign to places. ***Note***: All **PCA DA-MPs, SS7MPs** and **SBR MPs** must be added to the Site Place that corresponds to the physical location of the server.

Procedure 17. Configure the MP Server Group(s) and Profiles

S T E P #	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.

Procedure 17. Configure the MP Server Group(s) and Profiles

1 □ Enter MP or IPFE Server Group Data

From the GUI session on the NOAM VIP address, mavigate to **Main Menu->Configuration->Server Groups**, click **Insert** and fill out the following fields:

Server Group Name:	[Server Group Name]
Level:	C
Parent:	[SOAM Server Group That is Parent To this MP]
Function:	Select the Proper Function for this MP Server Group:

Server Group Function	MPs Will Run	Redundancy Model
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active Per SG
DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP/Per SG
Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP/Per SG
IP Front End	IPFE application	Multiple MPs active per SG. Each TSA may be hosted by any one of the IPFEs.
Policy & Charging SBR	Policy and Charging Session/or Policy Binding Function	1Active MP, 1 Standby MP, 1 Optional Spare Per SG
SS7-IWF	MAP IWF Application	1 Active MP Per SG

For PCA application:

- Online Charging function(only)

  At least one MP Server Group with the **Policy and Charging SBR** function must be configured.

  At least one MP Server Group with the **DSR (multi-active cluster**) function must be configured.

- Policy DRA function

  At least two MP Server Groups with the **Policy and Charging SBR** function must be configured. One stores session data and one stores binding data.

  At least one MP Server Group with the **DSR (multi-active cluster**) function must be configured

WAN Replication Connection Count:

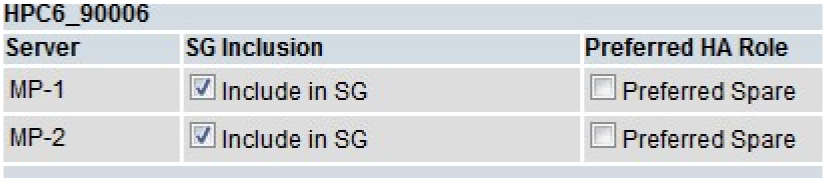
For non-Policy and Charging SBR Server Groups:	Default Value
For Policy and Charging Server Groups:	8

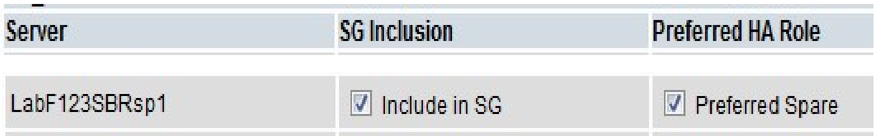
For the PCA application, the following types of MP Server Groups must be configured:

DA-MP (Function: DSR (multi-active cluster))
SBR (Function: Policy and Charging SBR)
IPFE (Function: IP Front End)

Click **OK** when all fields are filled in.

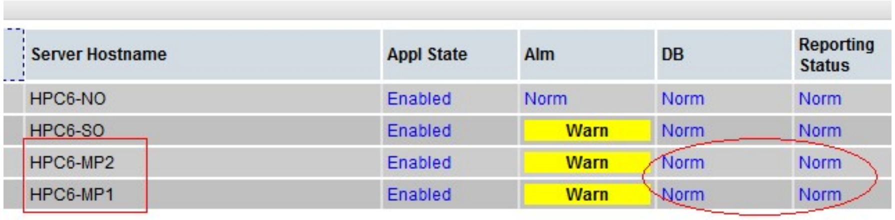
Procedure 17. Configure the MP Server Group(s) and Profiles

<table>
<tr><td>2
□</td><td>Repeat for Addional Server Groups</td><td>Repeat step 1 for any remaining MP and IPFE server groups you wish to create. For instance, when installing an IPFE, you need to create an IP front end server group for each IPFE server.</td></tr>
<tr><td>3
□</td><td>Edit the MP Server Groups to include MPs</td><td>Navigate to <b>Main Menu</b>-><b>Configuration</b>-><b>Server Groups</b>, select a server group that you just created, and click <b>Edit.</b>
Select the network element representing the MP server group you wish to edit.
Mark the <b>Include in SG</b> checkbox for every MP server you wish to include in this server group. Leave other checkboxes blank.

<table>
<tr><th colspan="3">HPC6_90006</th></tr>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>MP-1</td><td>☑ Include in SG</td><td>□ Preferred Spare</td></tr>
<tr><td>MP-2</td><td>☑ Include in SG</td><td>□ Preferred Spare</td></tr>
</table>

<b><i>Note</i></b>: Each <b>IPFE and SS7-MP</b> server should be in it’s own server group.
Click <b>OK</b>.</td></tr>
<tr><td>4
□</td><td>(OPTIONAL)
(PCA ONLY)
Edit the MP Server Group and add Preferred Spares for Site Redundancy</td><td>If two site redundancy for the Policy and Charging SBR Server Group is wanted, add a MP server that is physically located in a separate site(location) to the server group by marking the <b>Include in SG</b> checkbox and also mark the <b>Preferred Spare</b> checkbox.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>LabF123SBRsp1</td><td>☑ Include in SG</td><td>☑ Preferred Spare</td></tr>
</table>

For more information about site redundancy for Policy and Charging SBR Server Groups, see the <b>Terminology</b> section.
Click <b>OK</b> to save</td></tr>
<tr><td>5
□</td><td>Repeat For Addional Server Groups</td><td>Repeat Steps 1 - 4 for any remaining MP and IPFE server groups you need to create.</td></tr>
</table>

Procedure 17. Configure the MP Server Group(s) and Profiles

<table>
<tr><td>6
□</td><td>Wait for Replication to complete on all MPs</td><td>
Navigate to <b>Main Menu->Status & Manage->Server</b>.
Identify all the MP servers in the <b>Server Hostname</b> column. Wait for the corresponding <b>DB</b> and <b>Reporting Status</b> columns of those MPs to say <b>Norm</b>. This may take up to 5 or 10 minutes.

<table>
<tr><th>Server Hostname</th><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th></tr>
<tr><td>HPC6-NO</td><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>HPC6-SO</td><td>Enabled</td><td>Warn</td><td>Norm</td><td>Norm</td></tr>
<tr><td>HPC6-MP2</td><td>Enabled</td><td>Warn</td><td>Norm</td><td>Norm</td></tr>
<tr><td>HPC6-MP1</td><td>Enabled</td><td>Warn</td><td>Norm</td><td>Norm</td></tr>
</table>
If only relay traffic is run, engineering suggests using the VM:Relay profile for all DA-MPs in a cloud deployed DSR.
For DSR applications, following are the recommended DA-MP profiles:
<table>
<tr><th>Profile Name</th><th>Description</th></tr>
<tr><td>VM:Relay</td><td>VMs running relay application</td></tr>
<tr><td>VM:Database</td><td>VMs running a database application (e.g., FABR, RBAR)</td></tr>
<tr><td>VM:10K_MPS</td><td>VMs running a session application (e.g., PCA)</td></tr>
</table>
</td></tr>
<tr><td>7
□</td><td>Wait for Remote Database Alarm to Clear</td><td>
Wait for the alarm "10200: Remote Database re-initialization in progress" to be cleared. (<b>Main Menu</b>-&gt;<b>Alarms & Events</b>-&gt;<b>Active Alarms</b>)
This should happen shortly after you have verified the <b>“Norm”</b> DB status in the previous step.
</td></tr>
</table>

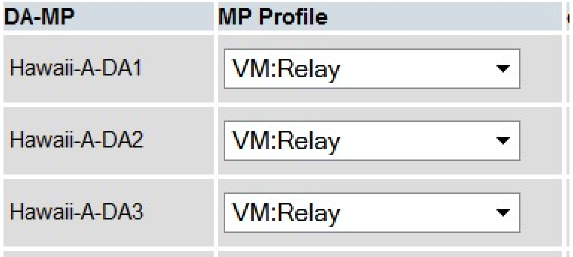
Procedure 17. Configure the MP Server Group(s) and Profiles

<table>
<tr>
<td>8
□</td>
<td>Assign Profiles to DA-MPs from SOAM GUI</td>
<td>

Log onto the GUI of the active SOAM server as **guiadmin** user.

From the SO GUI, navigate to **Main Menu->Diameter Common->MPs->Profiles Assignments**.

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



<table>
<tr><th>DA-MP</th><th>MP Profile</th></tr>
<tr><td>Hawaii-A-DA1</td><td>VM:Relay ▾</td></tr>
<tr><td>Hawaii-A-DA2</td><td>VM:Relay ▾</td></tr>
<tr><td>Hawaii-A-DA3</td><td>VM:Relay ▾</td></tr>
</table>

For each MP, select the proper profile assignment based on the MP’s type and the function it serves:

<table>
<tr><th>Profile Name</th><th>Description</th></tr>
<tr><td>VM:Relay</td><td>VM DA-MP VM running relay application</td></tr>
<tr><td>VM:Database</td><td>VM DA-MP VM running a database application (e.g., FABR, RBAR)</td></tr>
<tr><td>VM:10K_MPS</td><td>VM DA-MP VM running a session application (e.g., PCA)</td></tr>
</table>

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

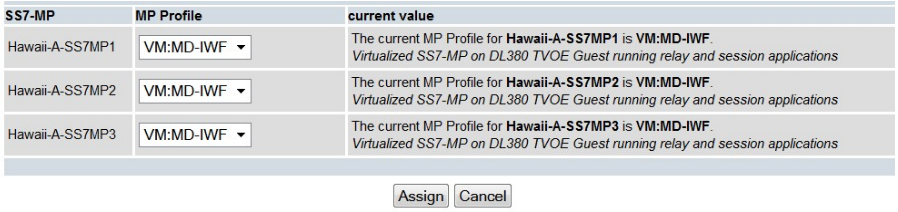
When finished, click **Assign**.

</td>
</tr>
<tr>
<td>9
□</td>
<td>Assign Profiles to SS7-MPs from SOAM GUI</td>
<td>

Log onto the GUI of the active SOAM server as **guiadmin** user

From the SO GUI, navigate to **Main Menu->Diameter->Configuration->DA-MPs->Profiles Assignments**.

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



<table>
<tr><th>SS7-MP</th><th>MP Profile</th><th>current value</th></tr>
<tr><td>Hawaii-A-SS7MP1</td><td>VM:MD-IWF ▾</td><td>The current MP Profile for <b>Hawaii-A-SS7MP1</b> is <b>VM:MD-IWF</b>.
<i>Virtualized SS7-MP on DL380 TVOE Guest running relay and session applications</i></td></tr>
<tr><td>Hawaii-A-SS7MP2</td><td>VM:MD-IWF ▾</td><td>The current MP Profile for <b>Hawaii-A-SS7MP2</b> is <b>VM:MD-IWF</b>.
<i>Virtualized SS7-MP on DL380 TVOE Guest running relay and session applications</i></td></tr>
<tr><td>Hawaii-A-SS7MP3</td><td>VM:MD-IWF ▾</td><td>The current MP Profile for <b>Hawaii-A-SS7MP3</b> is <b>VM:MD-IWF</b>.
<i>Virtualized SS7-MP on DL380 TVOE Guest running relay and session applications</i></td></tr>
</table>

For each SS7 MP, select the proper profile assignment based on the SS7 MP’s type and the function it serves:

<table>
<tr><th>Profile Name</th><th>Description</th></tr>
<tr><td>VM:MD-IWF</td><td>VM Running MAP-IWF functions</td></tr>
</table>

When finished, click **Assign**.

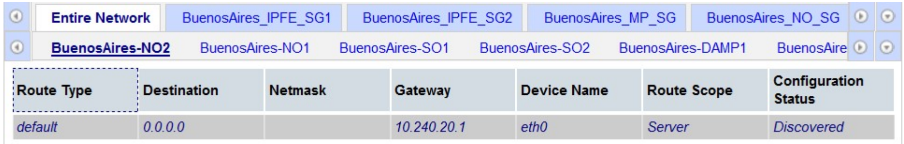
</td>
</tr>
</table>

Procedure 17. Configure the MP Server Group(s) and Profiles

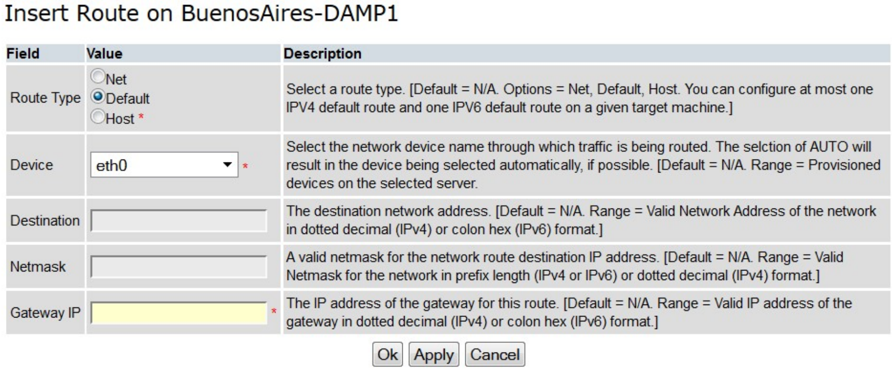
10 □	Restart MP virtual machines	From the NOAM GUI, navigate to **Main Menu->Status & Manage->Server**. For each MP server: • Select the MP server. • Click **Restart**. • Click **OK** on the confirmation screen. Wait for the message which tells you that the restart was successful. **Policy and Charging DRA Installations**: You may continue to see alarms related to ComAgent until you complete PCA configuration by finishing Procedure 30.

4.4 Configure Signaling Network Routes

Procedure 18. Configure the Signaling Network Routes

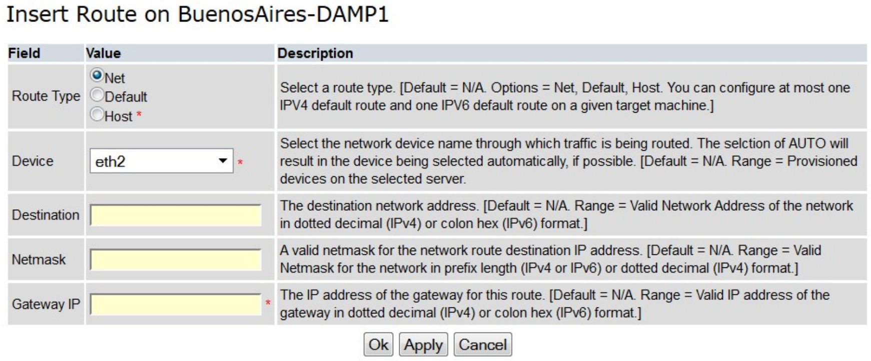
S T E P #	This procedure configures signaling network routes on MP-type servers (DA-MP, IPFE, SBR, SS7-MP, etc.). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1 □	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the NOAM VIP address. Login as user **guiadmin**.
2 □	**NOAM VIP**: Navigate to Routes Configuration Screen	Navigate to **Main Menu->Configuration->Network->Routes**. Select the first MP Server you see listed on the first row of tabs as shown, then click the **Entire Server Group** link. Initially, no routes should be displayed.  Entire Network BuenosAires_IPFE_SG1 BuenosAires_IPFE_SG2 BuenosAires_MP_SG BuenosAires_NO_SG BuenosAires-NO2 BuenosAires-NO1 BuenosAires-SO1 BuenosAires-SO2 BuenosAires-DAMP1 BuenosAire Route Type / Destination / Netmask / Gateway / Device Name / Route Scope / Configuration Status default / 0.0.0.0 / / 10.240.20.1 / eth0 / Server / Discovered
3 □	NOAM VIP: Add Route	Click **Insert** at the bottom of the screen to add additional routes.

Procedure 18. Configure the Signaling Network Routes

<table>
<tr>
<td>4
□</td>
<td><b>NOAM VIP: (Optional)</b> Add Default Route for MPs Going Through Signaling Network Gateway</td>
<td>
<b>***OPTIONAL -</b> Only execute this step if you performed (OPTIONAL) Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network -- which removed the XMI gateway default route on MPs.
If your MP servers no longer have a default route, then you can now insert a default route here which uses one of the signaling network gateways.

Insert Route on BuenosAires-DAMP1
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Route Type</td><td>○ Net
● Default
○ Host *</td><td>Select a route type. [Default = N/A. Options = Net, Default, Host. You can configure at most one IPV4 default route and one IPV6 default route on a given target machine.]</td></tr>
<tr><td>Device</td><td>eth0 *</td><td>Select the network device name through which traffic is being routed. The selction of AUTO will result in the device being selected automatically, if possible. [Default = N/A. Range = Provisioned devices on the selected server.</td></tr>
<tr><td>Destination</td><td></td><td>The destination network address. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr>
<tr><td>Netmask</td><td></td><td>A valid netmask for the network route destination IP address. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.]</td></tr>
<tr><td>Gateway IP</td><td>*</td><td>The IP address of the gateway for this route. [Default = N/A. Range = Valid IP address of the gateway in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr>
</table>

<table>
<tr><td>Route Type:</td><td><code>Default</code></td></tr>
<tr><td>Device:</td><td>Select the signaling device directly attached to the network where the XSI default gateway resides.</td></tr>
<tr><td>Gateway IP:</td><td>The XSI gateway you wish to use for default signaling network access.</td></tr>
</table>
Click <b>OK</b>.
</td>
</tr>
</table>

Procedure 18. Configure the Signaling Network Routes

<table>
<tr>
<td>5
□</td>
<td><strong>NOAM VIP:</strong> Add Network Routes for Diameter Peers</td>
<td>Use this step to add IP and/or IPv6 routes to diameter peer destination networks. The goal here is to ensure that diameter traffic uses the gateway(s) on the signaling networks.

Insert Route on BuenosAires-DAMP1
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Route Type</td><td>● Net
○ Default
○ Host *</td><td>Select a route type. [Default = N/A. Options = Net, Default, Host. You can configure at most one IPV4 default route and one IPV6 default route on a given target machine.]</td></tr>
<tr><td>Device</td><td>eth2 *</td><td>Select the network device name through which traffic is being routed. The selction of AUTO will result in the device being selected automatically, if possible. [Default = N/A. Range = Provisioned devices on the selected server.</td></tr>
<tr><td>Destination</td><td></td><td>The destination network address. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr>
<tr><td>Netmask</td><td></td><td>A valid netmask for the network route destination IP address. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.]</td></tr>
<tr><td>Gateway IP</td><td>*</td><td>The IP address of the gateway for this route. [Default = N/A. Range = Valid IP address of the gateway in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr>
</table>

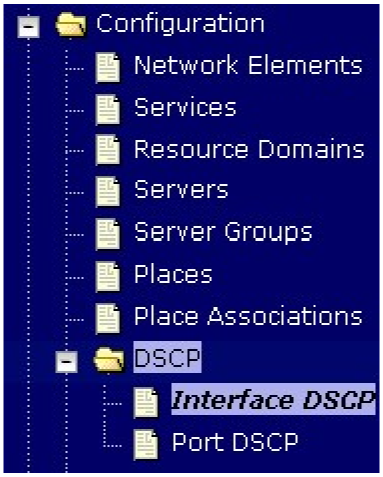
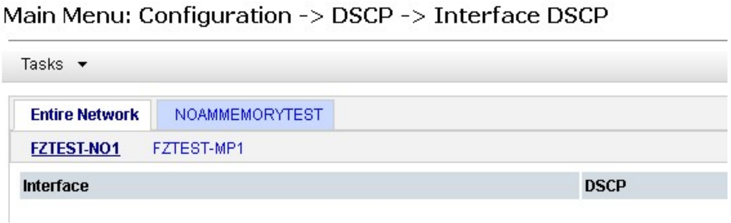
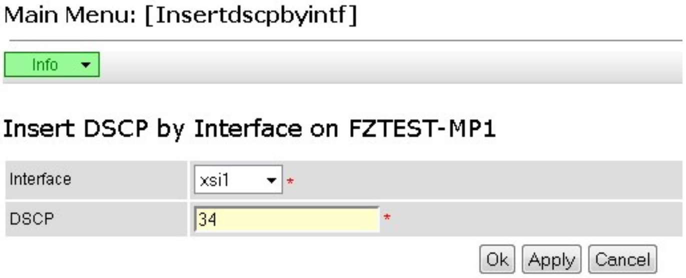
Route Type: Net
Device: Select the appropriate signaling interface that is used to connect to that network
Destination: Type the <strong>Network ID</strong> of network to which the peer node is connected to
Netmask: Type the corresponding Netmask
Gateway IP: Type the <strong>IP</strong> of the customer gateway.
If you have more routes to enter, click <strong>Apply</strong> to save the current route entry and repeat this step to enter more routes.
If you are finished entering routes, click <strong>OK</strong> to save the latest route and leave this screen.</td>
</tr>
<tr>
<td>6
□</td>
<td>Repeat steps 2-5 for all other MP server groups</td>
<td>The routes entered in this procedure should now be configured on *all* MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from 2, but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups.</td>
</tr>
</table>

4.5 Configure DSCP (Optional)

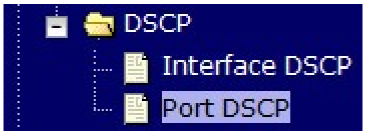
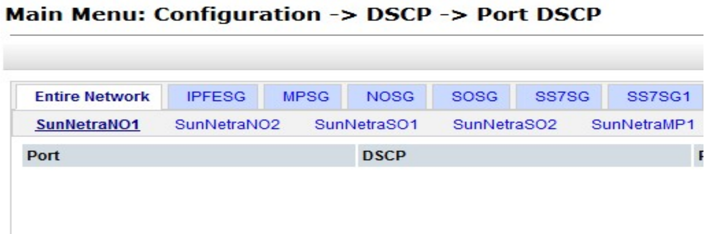
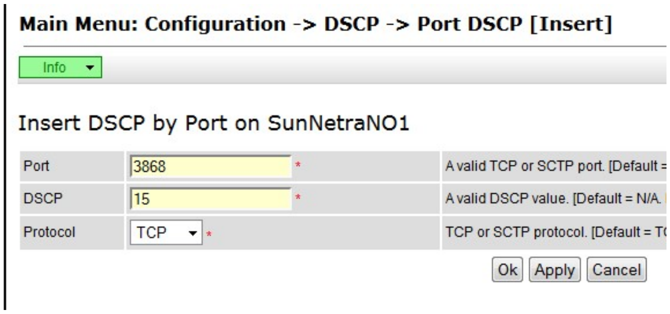
Procedure 19. Configure DSCP Values for Outgoing Traffic (Optional)

<table>
<tr>
<td><strong>S
T
E
P
#</strong></td>
<td colspan="2">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.
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>Establish GUI Session on the NOAM VIP</td>
<td>Establish a GUI session on the NOAM by using the NOAM VIP address. Login as user <strong>guiadmin</strong>.</td>
</tr>
</table>

Procedure 19. Configure DSCP Values for Outgoing Traffic (Optional)

2 □	**NOAM VIP**: Option 1: Configure Interface DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to **Main Menu->Configuration->DSCP->Interface DSCP**.  Configuration Network Elements Services Resource Domains Servers Server Groups Places Place Associations DSCP Interface DSCP Port DSCP Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with **Entire Network** selected; or limit yourself to a particular server group by clicking on that server group name's tab). Click **Insert**. Main Menu: Configuration -> DSCP -> Interface DSCP Tasks ▾ Entire Network | NOAMMEMORYTEST FZTEST-NO1 FZTEST-MP1 Interface | DSCP Select the network interface from the list, and then type the **DSCP** value you wish to have applied to packets leaving this interface. Main Menu: [Insertdscpbyintf] Info ▾ Insert DSCP by Interface on FZTEST-MP1 Interface: xsi1 ▾ * DSCP: 34 * Ok Apply Cancel Click **OK** if there are no more interfaces on this server to configure, or **Apply** to finish this interface and continue on with more interfaces by selecting them from the drop down and typing their **DSCP** values.

Procedure 19. Configure DSCP Values for Outgoing Traffic (Optional)

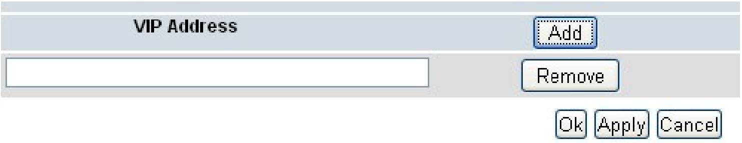
3 □	**NOAM VIP**: Option 2: Configure Port DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to **Main Menu->Configuration->DSCP->Port DSCP**.  Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with "Entire Network" selected; or limit yourself to a particular server group by clicking on that server group name's tab). Click **Insert**.  Main Menu: Configuration -> DSCP -> Port DSCP Entire Network IPFESG MPSG NOSG SOSG SS7SG SS7SG1 SunNetraNO1 SunNetraNO2 SunNetraSO1 SunNetraSO2 SunNetraMP1 Port DSCP Enter the source port, DSCP value, and select the transport protocol.  Main Menu: Configuration -> DSCP -> Port DSCP [Insert] Info Insert DSCP by Port on SunNetraNO1 Port 3868 * A valid TCP or SCTP port. [Default = DSCP 15 * A valid DSCP value. [Default = N/A. Protocol TCP * TCP or SCTP protocol. [Default = T Ok Apply Cancel Click **OK** if there are no more port DSCPs on this server to configure, or **Apply** to finish this port entry and continue entering more **port DSCP mappings**.
4 □	Repeat for additional servers	Repeat steps 2-3 for all remaining servers.

Procedure 20. Add VIP for Signaling Networks (Active/Standby Configurations ONLY)

S T E P #	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.

Procedure 20. Add VIP for Signaling Networks (Active/Standby Configurations ONLY)

1
□
	Configure VIP (OpenStack only)	1. **If no IPFE TSA is used, execute the following commands. If IPFE TSA addreses were configured in Procedure 6 step 5, the following steps are redundant and should not be performed**.
		2. Login to the OpenStack control node as admusr.
		3. Find the port id associated with the instance XSI interface corresponding to the VIP IP address..
		`$ neutron port-list`
		4. Add the VIP IP address to the address pairs list of the corresponding instance XSI interface port.
		`$ neutron port-update <Port ID> -- allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>`
		If necessary, see Allowed Address Pairs in Appendix I for more information.

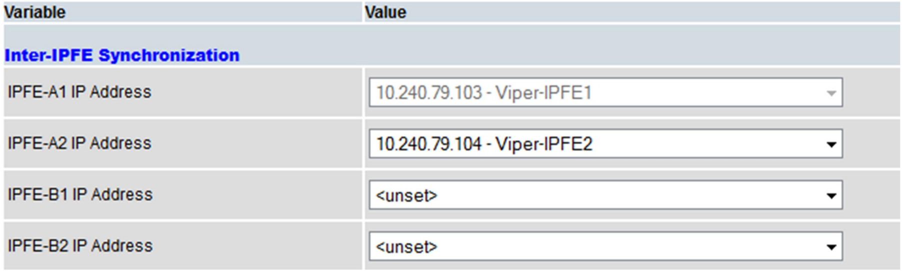
2 □	Edit the MP Server Group and add VIPs (ONLY FOR 1+1)	***Note***: **If your MPs are in a DSR multi-active cluster server group configuration (n+0), then skip this step**. ***Note***: Be sure you have performed Procedure 6, steps 5 and 6 correctly (VIP configuration). 1. Navigate to **Main Menu->Configuration->Server Groups**, select the MP server group, and click **Edit**. 2. Click **Add** to add the VIP for XSI1. 3. Type the VIP of **int-XSI-1** and click **Apply**. 4. Click **Add** again to add the VIP for XSI2. 5. Type the VIP of **int-XSI-2** and click **Apply**. 6. If more Signaling networks exists, add their corresponding VIP addresses. 7. Click **OK**. 

4.6 Configure IP Front End (Optional)

Procedure 21. IP Front End (IPFE) Configuration

S T E P #	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.

Procedure 21. IP Front End (IPFE) Configuration

1 □	**SOAM VIP**: Configuration of replication IPFE association data	Log into the **SOAM VIP** GUI as **guiadmin** user. Navigate to **Main Menu->IPFE->Configuration->Options**. Type the IP address of the **1st IPFE** in **the IPFE-A1 IP Address** field and the IP address of the **2nd IPFE** in the **IPFE-A2 IP Address** field. If applicable, type the address of the **3rd** and **4th** IPFE servers in **IPFE-B1 IP Address** and **IPFE-B2 IP Address** fields.  Variable — Value Inter-IPFE Synchronization IPFE-A1 IP Address — 10.240.79.103 - Viper-IPFE1 IPFE-A2 IP Address — 10.240.79.104 - Viper-IPFE2 IPFE-B1 IP Address — <unset> IPFE-B2 IP Address — <unset> ***Note***: It is recommended that the address reside on the **IMI (Internal Management Interface)** network. ***Note***: **IPFE-A1** and **IPFE-A2** must have connectivity between each other via these addresses. The same applies with **IPFE-B1** and **IPFE-B2**.
2 □	**SOAM VIP**: Configuration of IPFE Target sets	Login to the **SOAM VIP** GUI as **guiadmin** user. Navigate to **Main Menu->IPFE->Configuration->Target Sets**. Click either **Insert IPv4** or **Insert IPv6**, depending on the IP version of the target set you plan to use. This screen displays the following configurable settings: **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 is treated as a new connection and does 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,navigate to **Main Menu->IPFE->Configuration->Options**, Monitoring Protocol must be set to **Heartbeat** so that the application servers can provide the load information the IPFE uses to select the **least-loaded** server for connections. ***Note***: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatability scenarios. **(Optional):** If you have selected the **Least Load algorithm**, then 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

Procedure 21. IP Front End (IPFE) Configuration

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 **Main Menu ->Diameter->Configuration->Configuration Sets->Capacity Configuration**. 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.

Primary Public IP Address: IP address for the target set.

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 multihomed SCTP or Both TCP and SCTP, provide a Secondary IP Address.

Note: A secondary address is required to support **SCTP multihoming**. A secondary address can support **TCP**, but the **TCP** connections are not multihomed.

Note: If **SCTP multihoming** 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 multihoming**, a description, and a weight for the application server.

Note: The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also match the IP version of the target set address (IPv4 or IPv6). If the **Secondary Public IP Address** is configured, it must reside on the **same** application server as the first IP address.

Note: If all application servers have an equal **weight** (e.g., 100, which is the default), they have an equal chance of being selected. Application servers with larger **weights** have a greater chance of being selected.

Click **Add** to add more application servers (up to 16).

Click **Apply**.

Procedure 21. IP Front End (IPFE) Configuration

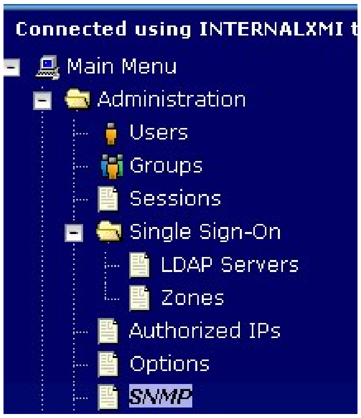
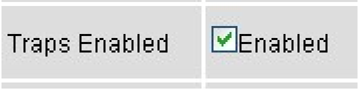
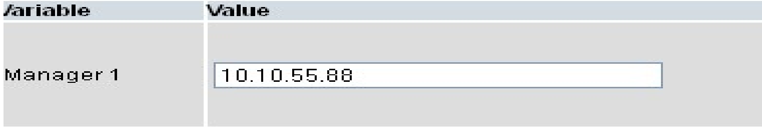
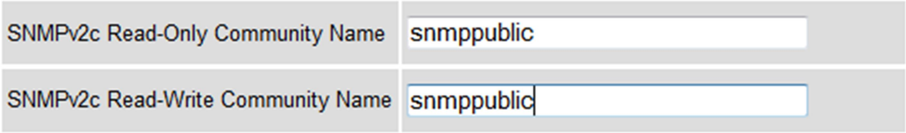
3 □	**SOAM VIP**: Repeat for additional Configuration of IPFE Target sets	Repeat for **step 9** for each target set (up to 16). At least one target set must be configured.

4.7 SNMP Configuration (Optional)

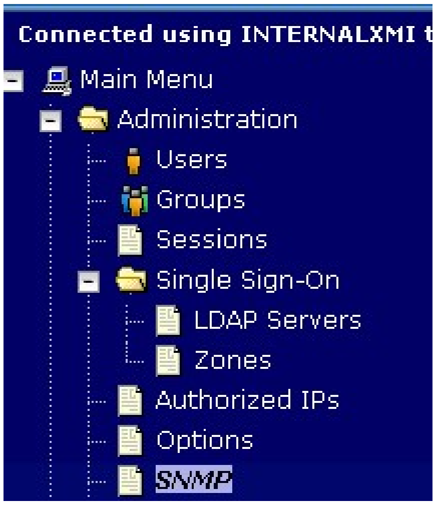
Procedure 22. Configure SNMP Trap Receiver(s) (OPTIONAL)

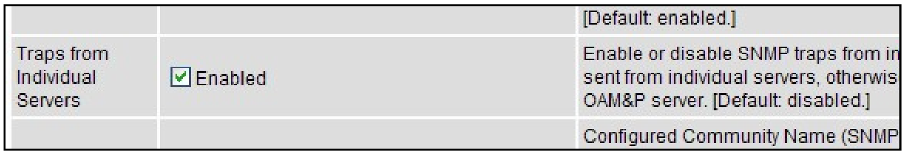
S T E P #	This procedure configures forwarding of SNMP. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

Procedure 22. Configure SNMP Trap Receiver(s) (OPTIONAL)

1 □	**NOAM VIP**: Configure System-Wide SNMP Trap Receiver(s)	Using a web browser, log onto the NOAM VIP as **guiadmin** user. Navigate to **Main Menu**->**Administration**->**SNMP**.  Connected using INTERNALXMI t Main Menu Administration Users Groups Sessions Single Sign-On LDAP Servers Zones Authorized IPs Options SNMP Verify the **Traps Enabled** checkbox is marked:  Traps Enabled ☑Enabled Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the the NOAM's XMI network. Continue to fill in additional secondary manager IPs in the corresponding slots if desired.  /ariable Value Manager 1 10.10.55.88 Type the **SNMP Community Name**.  SNMPv2c Read-Only Community Name snmppublic SNMPv2c Read-Write Community Name snmppublic Leave all other fields at their default values. Click **OK**.

Procedure 22. Configure SNMP Trap Receiver(s) (OPTIONAL)

<table>
<tr>
<td>2
□</td>
<td><b>NOAM VIP:</b>
Enable Traps from Individual Servers <b>(OPTIONAL)</b></td>
<td>
<p><b><i>Note</i></b>: By default SNMP traps from MPs are aggregated and then displayed at the active NOAM. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure.</p>
<p>This procedure requires all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable.</p>
<p>Using a web browser, log into the NOAM VIP as <b>guiadmin</b> user. Navigate to <b>Main Menu</b>-><b>Administration</b>-><b>SNMP</b>.</p>


<p>Make sure the <b>Enabled</b> checkbox is marked, if not, mark it as shown below:</p>

<table>
<tr><td></td><td></td><td>[Default: enabled.]</td></tr>
<tr><td>Traps from Individual Servers</td><td>☑ Enabled</td><td>Enable or disable SNMP traps from in sent from individual servers, otherwis OAM&P server. [Default: disabled.]</td></tr>
<tr><td></td><td></td><td>Configured Community Name (SNMP</td></tr>
</table>
<p>Click <b>Apply</b> and verify the data is committed.</p>
</td>
</tr>
</table>

4.8 Create iDIH Virtual Machines (VMware)

Procedure 23. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<table>
<tr>
<td><b>S
T
E
P
#</b></td>
<td colspan="2">
<p>This procedure creates the iDIH Oracle, Mediation, and Application guest.</p>
<p>Needed material:</p>
<ul><li>iDIH Oracle OVA, iDIH Mediation OVA, and iDIH Application OVA.</li></ul>
<p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p>
<p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
</td>
</tr>
<tr>
<td>1
□</td>
<td>Add the iDIH Oracle OVA to VMware</td>
<td>
<ol>
<li>Launch the VMware client of your choice.</li>
<li>Add the <b>iDIH Oracle OVA</b> image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.</li>
</ol>
</td>
</tr>
</table>

Procedure 23. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

2 □	Create the Oracle VM, from the OVA image	1. Browse the library or repository that you placed the **iDIH Oracle OVA** image. 2. Deploy the OVA Image using vSphere Client or the vSphere Web Client. 3. Name the **iDIH Oracle VM** and select the datastore.
3 □	Configure resources for the iDIH Oracle VM	1. Configure the **iDIH Oracle VM** per the Resource Profile in Appendix D for the **iDIH Oracle VM** using the vSphere Client or the vSphere Web Client. 2. Record the Ethernet addresses associated with each interface and the virtual network it is associated with.
4 □	Power on the iDIH Oracle VM	Use the vSphere client or vSphere web client to Power on the **iDIH Oracle VM**.
5 □	Procedure Overview	Repeat Steps 1 through 4 for the following VMs. Use Unique labels for the VM Names: iDIH Application iDIH Mediation

4.9 Create iDIH Virtual Machines (KVM/OpenStack)

Procedure 24. (KVM/OpenStack only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

S T E P #	This procedure creates the iDIH Oracle, Mediation, and Application guest. Needed material: • iDIH Oracle OVA, iDIH Mediation OVA and iDIH Application OVA 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.

Procedure 24. (KVM/OpenStack only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

1
□
	Add the iDIH Oracle OVA to KVM/OpenStack	1. Copy the OVA file to the OpenStack control node.
		`$ scp oracle-7.3.x.x.x.ova admusr@node:~`
		2. Login to the OpenStack control node.
		`$ ssh admusr@node`
		3. In an empty directory unpack the OVA file using “tar”
		`$ tar xvf oracle-7.3.x.x.x.ova`
		4. One of the unpacked files has a **.vmdk** suffix. This is the VM image file that must be imported.
		oracle-7.3.x.x.x-disk1.vmdk
		5. Source the OpenStack “admin” user credentials.
		`$ .  keystonerc_admin`
		6. Select an informative name for the new image.
		dsr-7.3.x.x.x-original
		7. Import the image using the “glance” utility from the command line.
		`$ glance image-create --name oracle-7.3.x.x.x-original --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file oracle-7.3.x.x.x-disk1.vmdk`
		This process takes about 5 minutes, depending on the underlying infrastructure.

2 □	Name the new VM instance	1. Create an informative name for the new instance: “iDIH-Oracle”. 2. Examine the network interface recommendations at the bottom of the Resource Profile in Appendix D. Network ports must be created for each recommended interface.

Procedure 24. (KVM/OpenStack only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

3
□
	Create and boot the iDIH VM instance from the glance image	1. Get the following configuration values.
		The image ID.
		`$ glance image-list`
		The flavor ID.
		`$ nova flavor-list`
		The network ID(s)
		`$ neutron net-list`
		An informative name for the instance.
		iDIH-Oracle
		iDIH-Mediation
		iDIH-Application
		2. Create and boot the VM instance.
		The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Number of IP/interfaces for each VM type must conform with the interface-to-network mappings described at the bottom of Appendix D Resource Profile.
		Note: IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.
		`$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>`
		3. View the newly created instance using the nova tool.
		`$ nova list  --all-tenants`
		The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

Procedure 24. (KVM/OpenStack only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

4
□
	Configure instance networking	1. Log into the **Horizon** GUI as the DSR tenant user.
		2. Go to the Compute/Instances section.
		3. Click the **Name** field of the newly created instance.
		4. Select the Console tab.
		5. Login as the **admusr**.
		6. Configure the network interfaces, conforming with the interface-to-network mappings described at the bottom of the Appendix D Resource Profile.
		`$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>`
		`$ sudo netAdm add --onboot=yes --device=eth1 --address=<imi ip> --netmask=<imi net mask>`
		`$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>`
		Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions.
		`$ sudo netAdm set --onboot=yes --device= ethX --address=<imi ip> --netmask=<imi net mask>`
		8. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible via both network and Horizon console.

5 □	Procedure Overview	Repeat steps 1 through 4 for the following VMs. Use Unique labels for the VM names: iDIH-Application iDIH-Mediation

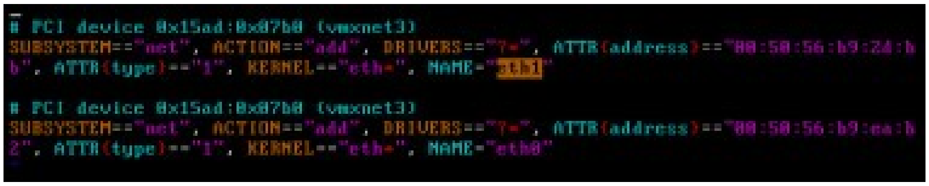
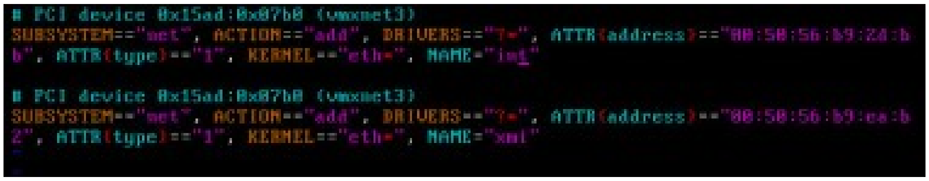
4.10 Configure iDIH Virtual Machines

Procedure 25. Configure iDIH VM Networks (Optional)

STEP#	This procedure configures the iDIH guest VM external management networks. 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 the Oracle VM Console	Access the iDIH Oracle VM console. Login as **admusr**.

Procedure 25. Configure iDIH VM Networks (Optional)

2 ☐	Trigger net rules file creation	Run the udevadm command to recreate net rules file. `$ sudo udevadm trigger --subsystem-match=net`

3
☐
	Modify the Ethernet interface names in the net rules file	Login to the **iDIH Oracle VM** console as **admusr**.
		Update the net rules file replace the default interfaces names ethX with xmi and int interfaces names. Be sure to use the MAC addresses recorded in the previous procedure to determine which interfaces should be named xmi and int. The mediation guest also requires the user to rename a third interface ethX as imi.
		`$ sudo vi  /etc/udev/rules.d/70-persistent-net.rules`
		
		`# PCI device 0x15ad:0x07b0 (vmxnet3)`
		`SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:50:56:b9:24:b`
		`b", ATTR{type}=="1", KERNEL=="eth*", NAME="eth1"`
		`# PCI device 0x15ad:0x07b0 (vmxnet3)`
		`SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:50:56:b9:ea:b`
		`2", ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"`
		
		`# PCI device 0x15ad:0x07b0 (vmxnet3)`
		`SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:50:56:b9:24:b`
		`b", ATTR{type}=="1", KERNEL=="eth*", NAME="int"`
		`# PCI device 0x15ad:0x07b0 (vmxnet3)`
		`SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:50:56:b9:ea:b`
		`2", ATTR{type}=="1", KERNEL=="eth*", NAME="xmi"`
		Reboot the guest.
		`$ sudo init 6`

4
☐
	(VMware only)
	As admusr on the Oracle VM configure the xmi and int networks with netAdm
		Login to the **iDIH Oracle VM** console as **admusr**.
		Configure the xmi network ip address and netmask.
		`$ sudo netAdm add --device=xmi --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
		Configure the default gateway.
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External Management Network> --device=xmi`
		Configure the int network ip address and netmask.
		`$ sudo netAdm add --device=int --address=10.254.254.2 --netmask=255.255.255.224 --onboot=yes --bootproto=none`
		Note: oracle guest internal ip=10.254.254.2, the mediation guest internal ip = 10.254.254.3 and the application internal ip address= 10.254.254.4. The netmasks for all is 255.255.255.224.

Procedure 25. Configure iDIH VM Networks (Optional)

5
□
	(KVM/Openstack only)
	As admusr on the Oracle VM configure the int network with netAdm
		Login to the **iDIH Oracle VM** console as **admusr**.
		Configure the int network ip address and netmask.
		`$ sudo netAdm add --device=int --address=10.254.254.2 --netmask=255.255.255.224 --onboot=yes --bootproto=none`
		The xmi network should already exist, but it can be created by the following command.
		`$ sudo netAdm add --device=xmi --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
		The default gateway should already exist but can be created by the following command.
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External Management Network> --device=xmi`
		Note: oracle guest internal ip=10.254.254.2, the mediation guest internal ip = 10.254.254.3 and the application internal ip address= 10.254.254.4. The netmasks for all is 255.255.255.224.

6 □	As admusr on the Oracle VM configure NTP and the Oracle VM hostname	On the Oracle VM console launch the platform configuration menu. `$ sudo su – platcfg` From the platform configuration menu configure ntpserver1 with the ip address supplied for NTP **Network Configuration->NTP->Edit->ntpserver1** Click **Yes** when asked to restart NTP. Exit the network configuration menu. Configure the Oracle VM hostname. **Server Configuration->Hostname->Edit**. ***Note***: Typically we select hostname identify the host as iDIH application, iDIH mediation and iDIH oracle. Exit the platform configuration menu.
7 □	Procedure Overview	Repeat Steps 1 through 5 for the following VMs. Use Unique labels for the VM Names: iDIH Mediation iDIH Application

Procedure 26. Run Post Installation scripts on iDIH VMs (Optional)

S T E P #	This procedure runs post installation scripts on the iDIH VMs. Prerequisite: Procedure 25 has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

Procedure 26. Run Post Installation scripts on iDIH VMs (Optional)

1 □	Log into the iDIH Oracle VM Console	Access the iDIH Oracle VM console. Login as **admusr**.
2 □	Run the iDIH Oracle post installation script	Wait for the software upgrades to complete on all iDIH Virtual machines. As **admusr** on the **iDIH Oracle VM** console run the Oracle post installation script. `$ sudo /opt/xIH/oracle/configureOracle.sh` ***Note***: The Oracle post installation script runs for an hour or longer depending on the Oracle version and patch level. Wait for it to complete before the next step is executed.
3 □	Log into the iDIH Mediation VM Console as admusr	Access the iDIH Mediation VM console. Login as **admusr**.
4 □	Configure the iDIH Mediation VM IMI network	Login to the **iDIH Mediation VM** console as **admusr**. Configure the Mediation internal management network. `$ sudo netAdm add--device=imi --address=<IP Address in Internal Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
5 □	Run the iDIH Medation VM post installation script	The Oracle post installation script must come to completion before the Medation post installation script is run. As **admusr** on the **iDIH Medation VM** console run the Medation post installation script. `$ sudo /opt/xIH/mediation/install.sh` ***Note***: The Mediation post installation script runs for 15 minutes. Wait for it to complete before the next step is executed. ***Note***: It is assumed network configuration and functionality is correct prior to installation. If you encounter an issue of the mediation post installation script **/opt/xIH/mediation/install.sh** hanging at the beginning as shown below, but you are still able to ssh to 10.254.254.2, make sure the internal interface(int) MTU has the correct setting - 1500 MTU. If yes, MTU size adjustment may be needed. For verification, connect to oracle using sqlplus using the following commands: Log into the Mediation server as **admusr**. Execute the command **sudo su - tekelec**. Execute the command **sqlplus /@NSP**. The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Procedure 26. Run Post Installation scripts on iDIH VMs (Optional)

6 □	Log into the iDIH Application VM Console as admusr	Access the iDIH Application VM console. Login as **admusr**.
7 □	Run the iDIH Application post installation script	The Mediation post installation script must come to completion before the Application post installation script is run. As **admusr** on the **iDIH Application VM** console run the Application post installation script. `$ sudo /opt/xIH/apps/install.sh` ***Note***: The Application post installation script runs for 45 minutes. Wait for it to complete before the next step is executed.

8
□
	Set Mediation hostname	As **tekelec** on the **iDIH Mediation VM** console run the following commands.
		`$ sudo su – tekelec`
		`` $ med:/usr/TKLC/xIH iset -fnodeName=`hostname` -fhostName=`hostname` NodeInfo where 1=1 ``

9 □	Restart each of the iDIH guests from their consoles	The Application post installation script must come to completion before the any of the Virtual Machines are restarted. As **admusr** on the **iDIH Mediation VM** run init command to **restart** the MediationVirtual Machine. `$ sudo init 6` As **admusr** on the **iDIH Application VM** run the init command to **restart** the Application Virtual Machine. `$ sudo init 6` As **admusr** on the **iDIH Oracle VM** run the init command to **restart** the Oracle Virtual Machine. `$ sudo init 6`
10 □	Run the iDIH healthcheck script on each of the iDIH virtual machines	Once all of the iDIH Virtual Machines have restarted. Run the healtcheck scripts on each iDIH Virtual Machine. As **admusr** on the **iDIH Oracle VM** console run the **healthcheck script** and verify the results. Ignore the NTP message stating the **tvoe-host** is **not integrated**. `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` As **admusr** on the **iDIH Application VM** console run the **healthcheck script** and verify the results. Ignore the NTP message stating **tvoe-host** is not **integrated**. `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` As **admusr** on the **iDIH Medation VM** console run the **healthcheck script** and verify results. Ingnore the NTP message stating tvoe-host is not integrated. `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` ***Note***: Ignore NTP message stating the **tvoe-host** is **not integrated.**

Procedure 27. Integrate iDIH into DSR (Optional)

S T E P #

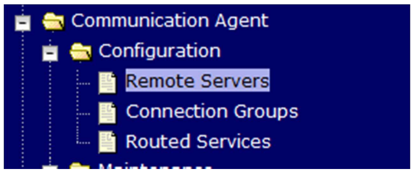
This procedure configures the iDIH connections to DSR.

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

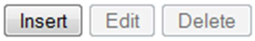
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1 □ Configure the iDIH ComAgent Connection on the NOAM

Navigate to **Main Menu->Communcation Agent->Configuration->Remote Servers**.



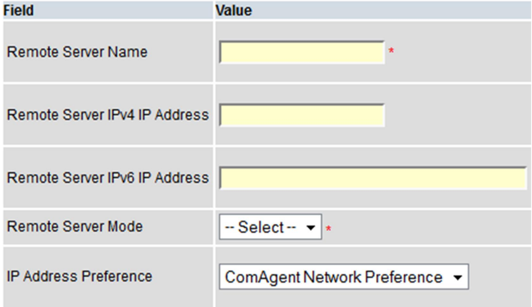
Click **Insert**.



Add the iDIH Mediation Server.

For the **Remote Server IP Address** field, type the **IMI IP address** of the iDIH Mediation server.

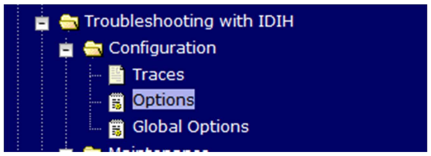
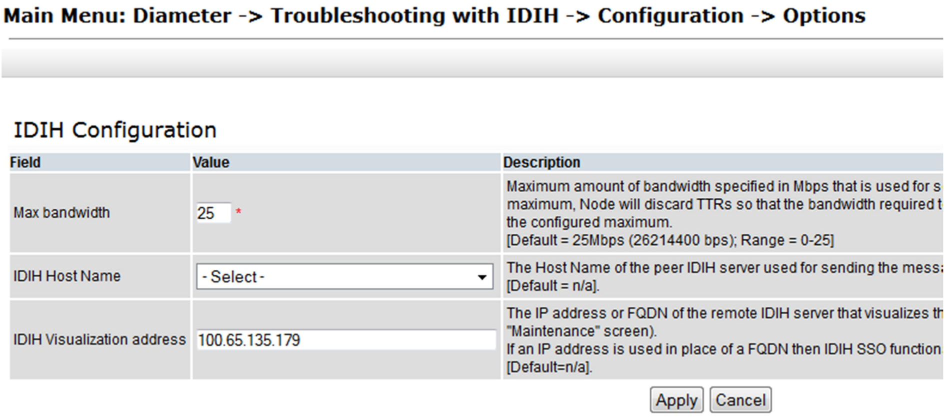
For the **IP Address Preference** field, selct the **IP protocol preference** (if IPv6 and IPv4 are configured).



Field	Value
Remote Server Name	*
Remote Server IPv4 IP Address	
Remote Server IPv6 IP Address	
Remote Server Mode	-- Select -- *
IP Address Preference	ComAgent Network Preference

Set the **Remote Server Mode** to **Server**.

Procedure 27. Integrate iDIH into DSR (Optional)

2 □	Configure the Troubleshooting with iDIH on the SOAM	Navigate to **Main Menu->Diameter->Troubleshooting with iDIH->Configuration->Options**.  Troubleshooting with IDIH Configuration Traces Options Global Options Type the fully qualified iDIH host name (or IP address) in the iDIH **Visualization Address field**:  Click **Apply**.

Main Menu: Diameter -> Troubleshooting with IDIH -> Configuration -> Options

IDIH Configuration

Field	Value	Description
Max bandwidth	25 *	Maximum amount of bandwidth specified in Mbps that is used for s maximum, Node will discard TTRs so that the bandwidth required t the configured maximum. [Default = 25Mbps (26214400 bps); Range = 0-25]
IDIH Host Name	- Select -	The Host Name of the peer IDIH server used for sending the mess [Default = n/a].
IDIH Visualization address	100.65.135.179	The IP address or FQDN of the remote IDIH server that visualizes th "Maintenance" screen). If an IP address is used in place of a FQDN then IDIH SSO function [Default=n/a].

Procedure 28. iDIH Application Final Configuration (Optional)

S T E P #	This procedure finalizes iDIH 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 □	Log into the Application Virtual Machine Console as admusr	Access the **iDIH Application VM** console via the **VMware** client of your choice. Login as **admusr**.

Procedure 28. iDIH Application Final Configuration (Optional)

2
□
	As admusr on the Application VM sudo to the tekelec user. And run trda configuration script	Sudo to the the tekelec user.
		`[admusr@thunderbolt-app ~]$ sudo su - tekelec`
		`/usr/TKLC/xIH/profiles/xih-apps.sh`
		`Loading component profile /usr/TKLC/xIH/profiles/xih-apps.sh...`
		As tekelec user execute the trda-config.sh script and supply the xmi vip address for the SOAM when prompted.
		`thunderbolt-app:/usr/TKLC/xIH ./apps/trda-config.sh`
		`dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-adapter.properties to UNIX format ...`
		`Please enter DSR SOAM server VIP address:`

4.11 Post-Install Activities

Procedure 29. Configure ComAgent Connections

STEP #	This procedure configures ComAgent connections on DSR 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 □	Configure ComAgent	Refer to [14] Full Address Based Resolution (FABR) User's Guide, E53470 for the steps required to configure **ComAgent**

Procedure 30. Complete PCA Configuration (Optional)

STEP #	This procedure completes PCA configuration. **Prerequisite:** PCA 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 □	Complete PCA Configuration	Refer to Section PCA Configuration of [2] PCA Configuration, E58667 for the steps required to complete PCA configuration.

Procedure 31. Backups and Disaster Prevention

STEP #	This procedure provides instruction on backups and disaster prevention. **Prerequisite:** DSR and optional sub-systems are installed 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.

Procedure 31. Backups and Disaster Prevention

1 □	Backups	The preferred method of backing up cloud system VM instances is by snapshotting. Once the DSR and optional sub-systems are installed and configured, but before adding traffic , use the appropriate cloud tool such as the VMware Manager or the OpenStack Horizon GUI, to take snapshots of critical VM instances. It is particularly important to snapshot the control instances, such as the NOAM and SOAM.

Procedure 32. (KVM/OpenStack Only) Configure IPFE Target Set Addresses (n)

S T E P #	This procedure configures Target Set addresses on IPFE and MP instances. 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
□
	IPFE with TSA only. Remove port security on TSA XMI network interfaces on IPFE and MP instances	***Prerequisite***: **Enable the Neutron port_security extension** first. We require this extension to disable the Neutron anti-spoofing filter rules for a given port. Refer to section H-6 in Appendix H where this is discussed.
		If using IPFE with Target Set addresses.
		1. Determine the TSA IP address as used in section 4.6, i.e., Procedure 21 Step 2.
		2. Determine the corresponding XSI interface IP address as used in section 4.6, i.e., Procedure 21 Step 2.
		3. Log into the OpenStack control node as the admusr.
		4. Source the tenant user credentials.
		5. Determine security groups associated with the IPFE instance.
		`$ nova list-secgroup <VM instance ID>`
		Note: <VM instance ID> can be queried from the output of “nova list” command in the ID column for the given VM.
		6. Save the ID and names of the listed security groups for later use.
		7. Remove all listed security groups.
		`$ nova remove-secgroup <VM instance ID> <Security group ID>`
		Note: Use the <VM instance ID> and <Security group ID> as noted down in the step-6 above.
		Alternatively, we can use following syntax although:
		`$ nova remove-secgroup <VM instance name> <Security group name>`
		8. Determine the port ID of the XSI interface IP address from step 2 above.
		`$ neutron port-list -F id -F fixed_ips | grep <instance IP on TSA/XSI network>`
		Note: <port ID> is the value in first column of the output to this command.

Procedure 32. (KVM/OpenStack Only) Configure IPFE Target Set Addreses (n)

		9. Disable port security for the port found in step 7.
		`$ neutron port-update <Port ID> --port-security-enabled=false`
		10. Re-enable port security for all the interfaces not on the TSA/XSI port used in step 9, including XMI, IMI and others.
		Determine the port IDs of the instance IP addresses not associated with the TSA/XSI network.
		`$ neutron port-list -F id -F fixed_ips | grep <instance IP not on TSA/XSI network>`
		For each of the non TSA/XSI instance ports perform the following command for each of the security groups from step 6.
		`$ neutron port-update <Port ID> --security-group <Security group ID>>`
		Note: Use the <Security Group ID> as noted down in the step-6 above.

Appendix A. Sample Network Element and Hardware Profiles

To enter all the network information for a network element into an Appworks-based system, 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 NOAM network element XML file has. It is easy to accidentally create different network names for NOAM and SOAM network elements, and then the mapping of services to networks are not possible.

```xml
<?xml version="1.0"?>
<networkelement>
    <name>NE</name>
    <networks>
        <network>
            <name>XMI</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>IMI</name>
            <vlanId>4</vlanId>
            <ip>10.3.0.0</ip>
            <mask>255.255.255.0</mask>
            <nonRoutable>true</nonRoutable>
        </network>
    </networks>
</networkelement>
```

Figure 2: Example Network Element XML File

The server hardware information is needed to configure the Ethernet interfaces on the servers. This server hardware profile data XML file is used for Appworks deployments. It is supplied to the NOAM server so that the information can be pulled in by Appworks 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>DSR ESXI Guest</serverType>
    <available>
        <device>eth0</device>
        <device>eth1</device>
        <device>eth2</device>
        <device>eth3</device>
        <device>eth4</device>
    </available>
    <devices>
        <device>
            <name>eth0</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth1</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth2</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth3</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth4</name>
            <type>ETHERNET</type>
        </device>
    </devices>
</profile>
```

Figure 3: Example Server Hardware Profile XML File – Virtual Guest on KVM/OpenStack

Appendix B. 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 timezone.

Table 5. List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time - Arizona	UTC-07
America/Los_Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09

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

Appendix C. Multi-Site Feature Activation

Procedure C-1. Multi-Site Feature Activation

STEP #	This procedure activates optional features in multi-site configurations for spare 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 □	**ACTIVE SOAM**: Prepare SOAM for optional feature activation	Establish an SSH session to the Active SOAM, login as **admusr.** Execute the following command: `$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"` ***Note***: Before running the irem command, collect information on which DSR applications are already activated.
2 □	**ACTIVE SOAM**: Verify preparation	Execute the following command to verify preparation of optional feature activation: `$  iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"` ***Note***: There should be no output of this command, if there is, verify the correct entry of the command in **step 1**.
3 □	**ACTIVE NOAM**: Activate Optional Features	Establish an SSH session to the Active NOAM Login as **admusr.** Follow references [2], [3], [4], [5], and [7] to activate any features that were previously activated.

Appendix D. Resource Profile

VM Name	VM Purpose	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Notes
DSR NOAM	Network Operation, Administration, and Maintenance	2	4	4	6	60	
DSR SOAM	Site Operation, Administration and Maintenance	2	4	4	6	60	

VM Name	VM Purpose	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Notes
DA MP	Diameter Agent Message Processor	2	9 (24 for IWF)	8	16 (24 for IWF)	60	The 24 GB RAM requirement is a minimum if the DA-MP VM is used with the IWF
IPFE	IP Front End			4	16	60	
SS7 MP	SS7 Message Processor for MAP Diameter			8	24	60	The 24 GB RAM requirement is a hard minimum for SS7
SBR(s)	Subscriber Binding Repository (session) for Policy DRA			12	16	60	To support 5M sessions
SBR(b)	Subscriber Binding Repository (binding) for Policy DRA			12	16	60	
iDIH Application	Integrated Diameter Intelligence Hub web server			4	8	64	
iDIH Mediation	Integrated Diameter Intelligence Hub mediation server			4	8	64	
iDIH DB	Integrated Diameter Intelligence Hub DB server			4	8	120(system) + 100 (DB)	Storage for DB Disk may be increased

VM Name	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3)	Signaling D (XSI4)	Replication (SBR Rep)	DIH Internal
DSR NOAM	eth0	eth1						
DSR SOAM	eth0	eth1						

VM Name	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3)	Signaling D (XSI4)	Replication (SBR Rep)	DIH Internal
DA-MP	eth0	eth1	eth2	eth3	eth4	eth5	eth6	
IPFE	eth0	eth1	eth2	eth3	eth4	eth5		
SS7 MP	eth0	eth1	eth2	eth3	eth4	eth5	eth6	
SBRB	eth0	eth1					eth2	
SBRS	eth0	eth1					eth2	
iDIH App	xmi							int
iDIH Med	xmi	imi						int
iDIH DB	xmi							int

Note: The Ethernet interfaces define in the table are there as a guidline. Interfaces can be ordered as preferred. I.E. eth1 or eth2 could be associated with XMI if desired.

Appendix E. Common KVM/Openstack Tasks

Procedure E-1. Create a Network Port

1
□
	Create the network ports for the NO network interfaces	1. Each network interface on an instance must have an associated network port.
		An instance usually has at least eth0 and eth1 for a public and private network respectively.
		Some configurations require 6 or more interfaces and corresponding network ports.
		2. Determine the IP address for the interface.
		For eth0, the IP might be 10.x.x.157.
		For eth1, the IP might be 192.168.x.157
		3. Identify the neutron network ID associated with each IP/interface using the **neutron** command line tool.
		`$ neutron net-list`
		4. Identify the neutron subnet ID associated with each IP/interface using the **neutron** command line tool.
		`$ neutron subnet-list`
		5. Create the network port using the **neutron** command line tool, being sure to choose an informative name. Note the use of the subnet ID and the network ID (final argument).
		Port names are usually a combination of instance name and network name.
		NO1-xmi
		SO2-imi
		MP5-xsi2
		The ports must be owned by the DSR tenant user, not the admin user. Either source the credentials of the DSR tenant user or use the DSR tenant user ID as the value for the “—tenant-id” argument.
		`$ . keystonerc_dsr_user`
		`$ keystone user-list`
		`$ neutron port-create --name=NO1-xmi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>`
		`$ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>`
		View your newly created ports using the neutron tool.
		`$ neutron port-list`

Procedure E-2. Create and Boot OpenStack Instance

1
□
	Create a VM instance from a glance image	4. Get the following configuration values.
		The image ID.
		`$ glance image-list`
		The flavor ID.
		`$ nova flavor-list`
		The network ID(s)
		`$ neutron net-list`
		An informative name for the instance.
		NO1
		SO2
		MP5
		5. Create and boot the VM instance.
		The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Number of IP/interfaces for each VM type must conform with the interface-to-network mappings described at the bottom of Appendix D Resource Profile.
		Note: IPv6 addresses should use the “v6-fixed-ip” argument instead of “v4-fixed-ip”.
		`$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> InstanceName`
		View the newly created instance using the nova tool.
		`$ nova list  --all-tenants`
		The VM takes approximately 5 minutes to boot. At this point, the VM has no configured network interfaces and can only be accessed by the Horizon console tool.

Procedure E-3. Configure Networking for OpenStack Instance

1 □

Configure the network interfaces and hostname.

1. Log into the **Horizon** GUI as the DSR tenant user.
2. Go to the Compute/Instances section.
3. Click on the **Name** field of the newly created instance.
4. Select the Console tab.
5. Login as the **admusr**.
6. Select an informative hostname for the new VM instance.

   NO1
   SO2
   MP5
7. Configure the network interfaces, conforming with the interface-to-network mappings described at the bottom of the Appendix D Resource Profile.

   ```
   $ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>
   ```

   ```
   $ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>
   ```

   Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.

   If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions.

   ```
   $ cd /etc/sysconfig/network-scripts
   ```

   ```
   $ sudo mv ifcfg-ethX /tmp
   ```

   Keep ifcfg-ethX in /tmp until ethX is working correctly, then delete it.

   e. Re-run the `netAdm` command. It creates and configures the interface in one action.
8. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.

   ```
   $ sudo init 6
   ```

The new VM should now be accessible via both network and Horizon console.

Appendix F. Firewall Ports

Flow Description	Purpose	Protocol/Port	IP Protocol Version
ICMP echo to OA	plat management	ICMP	IPv4, IPV6
OpenHPI MGMT and Communication	plat management	TCP:443	IPv4, IPVv6
virtual guest discovery via libvirt	control	TCP:22	IPv4 , IPv6
NTP flow for time sync	plat management	UDP:123	IPv4 , IPv6
SSH & SFTP access into PM&C	plat management	TCP:22	IPv4 , IPv6
PM&C GUI Access	plat management	TCP: 80 TCP: 443	IPv4, IPv6
Server Install (time)	control	TCP:37	IPv4

Flow Description	Purpose	Protocol/Port	IP Protocol Version
Server Install (http)	control	TCP: 80	IPv4
Server Install (SNMP)	control	UDP:162	IPv4 , IPv6
Server Upgrade (nfs)	control	UDP: 111 TCP: 886 TCP: 2049 UDP/TCP: 4000-4003	IPv4
NTP flow for time sync	control	UDP:123	IPv4 , IPv6
hostname resolution (dns)	plat management	UDP/TCP: 53	IPv4, IPv6
LightWieght Directory Access Protocol (LDAP)	plat management	UDP/TCP: 389	IPv4, IPv6

Appendix G. Disable/Enable DTLS

Oracle's SCTP Datagram Transport Layer Security (DTLS) has SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers installing DSR 7.1/7.1.1/7.2/7.3 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 the following procedure to disable DTLS:

Procedure G-1. Disable DTLS

STEP #	This procedure disables DTLS. 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 □	**MP Server**: Login	Establish an SSH session to the MP server. Login as **admusr.**
2 □	**MP Server**: Disable SCTP Auth Flag	Execute the following command to disable the SCTP Auth Flag: ***Note***: It is recommended to copy and paste directly as listed below to avoid errors. `$ sudo sysctl -w net.sctp.auth_enable=0`

3
□
	MP Server: Verify SCTP Auth Flag is Disabled	Execute the following command to verify the SCTP Auth Flag is disabled:
		Note: It is recommended to copy and paste directly as listed below to avoid errors.
		`$ sudo sysctl -a | grep net.sctp.auth_enable`
		The following output is expected:
		`net.sctp.auth_enable = 0`

Procedure G-1. Disable DTLS

4 □	**MP Server**: Make SCTP Auth Flag changes Persistent	Execute the following command to make the SCTP Auth Flag changes persistent: ***Note***: It is recommended to copy and paste directly as listed below to avoid errors. `$ sudo sed -i 's/sysctl -w net.sctp.auth_enable=1/sysctl -w net.sctp.auth_enable=0/g' /etc/dpi_init`

5
□
	MP Server: Verify Auth Flag is Disabled	Execute the following command to verify the SCTP Auth Flag has been disabled:
		Note: It is recommended to copy and paste directly as listed below to avoid errors.
		`$ sudo grep net.sctp.auth_enable /etc/dpi_init`
		The following output should be displayed:
		`sysctl -w net.sctp.auth_enable=0`

6 □	**Additional MP Servers**: Repeat	Repeat for all remaining MP servers.

If DTLS connections are to be configured AFTER DTLS has been disabled as performed in **Procedure S.1**, then the procedure below for Enabling DTLS needs to be followed before DTLS connections are configured.

Procedure G-2. Enable DTLS

STEP #	This procedure enables DTLS. 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 □	**MP Server**: Login	Establish an SSH session to the MP server. Login as **admusr.**
2 □	**MP Server**: Enable SCTP Auth Flag	Execute the following command to Enable the SCTP Auth Flag: ***Note***: It is recommended to copy and paste directly as listed below to avoid errors. `$ sudo sysctl -w net.sctp.auth_enable=1`

3
□
	MP Server: Verify SCTP Auth Flag changes	Execute the following command to verify the SCTP Auth Flag changes:
		Note: It is recommended to copy and paste directly as listed below to avoid errors.
		`$ sudo sysctl -a | grep net.sctp.auth_enable`
		The following output is expected:
		`net.sctp.auth_enable = 1`

4 □	**MP Server**: Make SCTP Auth Flag Changes persistent	Execute the following command to make the SCTP Auth Flag changes persistent: ***Note***: It is recommended to copy and paste directly as listed below to avoid errors. `$ sudo sed -i 's/sysctl -w net.sctp.auth_enable=0/sysctl -w net.sctp.auth_enable=1/g' /etc/dpi_init`

Procedure G-2. Enable DTLS

5
□
	MP Server: Verify Auth Flag changes	Execute the following command to verify the SCTP Auth Flag has been disabled:
		Note: It is recommended to copy and paste directly as listed below to avoid errors.
		`$ sudo grep net.sctp.auth_enable /etc/dpi_init`
		The following output should be displayed:
		`sysctl -w net.sctp.auth_enable=1`

6 □	**Additional MP Servers**: Repeat	Repeat for all remaining MP servers.

Appendix H. Application VIP Failover Options (OpenStack)

H-1. Application VIP Failover Options

Within an OpenStack cloud environment there are several options for allowing applications to manage their own virtual IP (VIP) addresses as is traditionally done in telecommunications applications. This document describes two of those options:

- Allowed address pairs
- Disable port security

Each of these options is covered in the major sub-sections that follow. The last major sub-section discusses how to utilize application managed virtual IP addresses within an OpenStack VM instance.

Both of these options effectively work around the default OpenStack Networking (Neutron) service anti-spoofing rules that ensure that a VM instance cannot send packets out a network interface with a source IP address different from the IP address Neutron has associated with the interface. In the Neutron data model, the logical notion of networks, sub-networks and network interfaces are realized as networks, subnets, and ports as shown in the following figure:

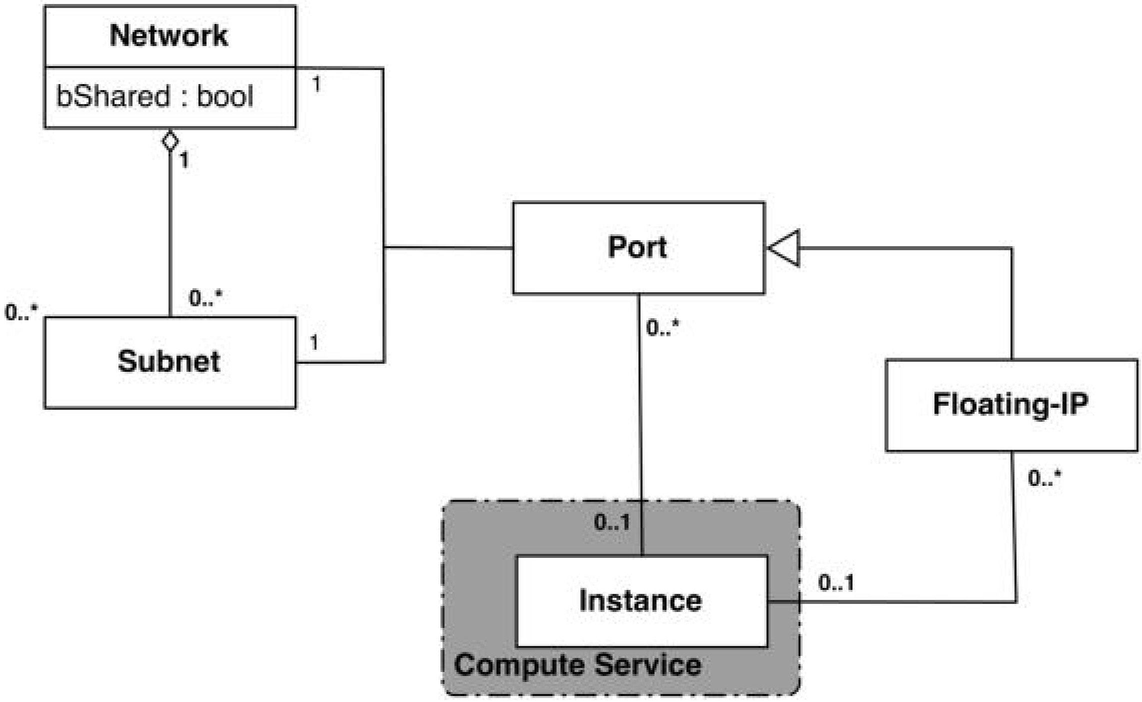


Figure 2. Neutron High-Level Data Model

Note how a port in the Neutron data model maps to at most one VM instance where internal to the VM instance, the port ise represented as an available network device such as eth0. VM instances can have multiple network interfaces in which case there are multiple Neutron ports associated with the VM instance, each with different MAC and IP addresses.

Each Neutron port by default has one MAC Address and one IPv4 or IPv6 address associated with it. The IP address associated with a port can be assigned in two ways:

- Automatically by Neutron when creating a port to fulfill an OpenStack Compute (Nova) service request to associate a network interface with a VM instance to be instantiated OR
- Manually by a cloud administrator when creating or updating a Neutron port

The anti-spoofing rules are enforced at the Neutron port level by ensuring that the source IP address of outgoing packets matches the IP address Neutron has associated with the corresponding port assigned to the VM instance. By default if the source IP address in the outgoing packet does not match the IP address associated with the corresponding Neutron port then the packet is dropped.

These anti-spoofing rules clearly create a complication for the use of application managed virtual IP addresses since Neutron is not going to know about the VIPs being applied by the application to VM instance network interfaces without some interaction between the application (or a higher level management element) and Neutron. Which is why the two options in this document either fully disable the port security measures within Neutron, including the anti-spoofing rules, or expand the set of allowable source IP addresses to include the VIPs that may be used by the application running within a VM instance.

Note that for both of the options described in the following sub-sections, there is a particular Neutron service extension or feature that must be enabled for the option to work. For one option (allowed address pairs) the required Neutron extension is enabled in most default deployments whereas for the other option (allow port security to be disabled) it is not.

Within this document when describing how to use either of these two options, there is example command line operations that interact with the OpenStack Neutron service via its command line utility, simply named `neutron`. However, be aware that all of the operations performed using the `neutron` command line utility can also be performed through the Neutron REST APIs, see the Networking v2.0 API documentation for more information.

H-2. Allowed Address Pairs

This section describes an option that extends the set of source IP addresses that can be used in packets being sent out a VM instance's network interface (which maps to a Neutron port). This option utilizes a Neutron capability, called the allowed-address-pairs extension, which allows an entity (cloud administrator, management element, etc.) to define additional IP addresses to be associated with a Neutron port. In this way, if an application within the VM instance sends an outgoing packet with one of those additional IP addresses, then Neutron anti-spoofing rules enforcement logic does not drop those packets. The Neutron allowed-address-pairs extension is available starting with the OpenStack Havana release.

The three sub-sections that follow describe the OpenStack configuration requirements for this option, how to utilize this option after a VM instance has already booted, and how to utilize this option before a VM instance has booted.

H-3. OpenStack Configuration Requirements

The Neutron allowed-address-pairs extension needs to be enabled for this option to work. For most OpenStack cloud deployments this extension should be enabled by default but to check, run the following command (after sourcing the appropriate user credentials file):

```
   # neutron ext-list
+-----------------------+-----------------------------------------------+
| alias                 | name                                          |
+-----------------------+-----------------------------------------------+
| security-group        | security-group                                |
| l3_agent_scheduler    | L3 Agent Scheduler                            |
| net-mtu               | Network MTU                                   |
| ext-gw-mode           | Neutron L3 Configurable external gateway mode |
| binding               | Port Binding                                  |
| provider              | Provider Network                              |
| agent                 | agent                                         |
| quotas                | Quota management support                      |
| subnet_allocation     | Subnet Allocation                             |
| dhcp_agent_scheduler  | DHCP Agent Scheduler                          |
| l3-ha                 | HA Router extension                           |
| multi-provider        | Multi Provider Network                        |
| external-net          | Neutron external network                      |
| router                | Neutron L3 Router                             |
| allowed-address-pairs | Allowed Address Pairs                         |
| extraroute            | Neutron Extra Route                           |
| extra_dhcp_opt        | Neutron Extra DHCP opts                       |
| dvr                   | Distributed Virtual Router                    |
+-----------------------+-----------------------------------------------+
```

The allowed-address-pairs extension should appear in the list of extensions as shown in the bold line above.

H-4. After a VM Instance has been Booted: Allowed Address Pairs

If a VM instance has already been booted, i.e. instantiated, and you need to associate one or more additional IP addresses with the Neutron port assigned to the VM instance then you need to execute a command of the following form:

```
# neutron port-update <Port ID> --allowed_address_pairs list=true
type=dict ip_address=<VIP address to be added>
```

where the bolded items have the following meaning:

- <Port ID>

  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence like "`$(neutron port-show -f value -F id <Port Name>)`" to replace the <Port ID> placeholder.

- <VIP address to be added>

  Identifies the IP address, a virtual IP address in this case, that should additionally be associated with the port where this can be a single IP address, e.g. 10.133.97.135/32, or a range of IP addresses as indicated by a value such as 10.133.97.128/30.

So for example if you wanted to indicate to Neutron that the allowed addresses for a port should include the range of addresses between 10.133.97.136 to 10.133.97.139 and the port had an ID of 8a440d3f-4e5c-4ba2-9e5e-7fc942111277 then you would type the following command:

```
# neutron port-update 8a440d3f-4e5c-4ba2-9e5e-7fc942111277 --
allowed_address_pairs list=true type=dict ip_address=10.133.97.136/30
```

H-5. Before a VM Instance has been Booted: Allowed Address Pairs

If you want to associate additional allowed IP addresses with a port before it is associated with a VM instance then you need to first create the port and then associate one or more ports with a VM instance when it is booted. The command to create a new port with defined allowed address pairs is of the following form:

```
# neutron port-create --name <Port Name> --fixed-ip subnet-id=$(neutron
subnet-show -f value -F id <Subnet name>),ip_address=<Target IP address>
$(neutron net-show -f value -F id <Network name>) --allowed_address_pairs
list=true type=dict ip_address=<VIP address to be added>
```

where the bolded items have the following meaning:

- <Port Name>

  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the "`--name` **`<Port Name>`**" portion of the command is completely optional.

- <Subnet name>

  The name of the subnet to which the port should be added.

- <Target IP address>

  The unique IP address to be associated with the port.

- <Network Name>

  The name of the network with which the port should be associated.

- <VIP address to be added>

  This parameter value has the same meaning as described in the previous section.

So for example if you wanted to indicate to Neutron that a new port should have an IP address of 10.133.97.133 on the 'ext-subnet' subnet with a single allowed address pair, 10.133.97.134, then you would type a command similar to the following:

```
# neutron port-create -name foo --fixed-ip subnet-id=$(neutron subnet-show
-f value -F id ext-subnet),ip_address=10.133.97.133 $(neutron net-show -f
value -F id ext-net) --allowed_address_pairs list=true type=dict
ip_address=10.133.97.134/32
```

Once the port or ports with the additional allowed addresses have been created, when you boot the VM instance use a nova boot command similar to the following:

```
# nova boot --flavor m1.xlarge --image testVMimage --nic port-id=$(neutron
port-show -f value -F id <Port Name>) testvm3
```

where the flavor, image, and VM instance name values need to be replaced by values appropriate for your VM. If the port to be associated with the VM instance is not named, then you need to obtain the port's ID using the neutron port-list command and replace the "`$(neutron port-show -f value -F id <Port Name>)`" sequence in the above command with the port's ID value.

H-6. Disable Port Security

This section describes an option that rather than extending the set of source IP addresses that are associated with a Neutron port, as is done with the allowed-address-pairs extension, simply disables the Neutron anti-spoofing filter rules for a given port. This option allows all IP packets originating from the VM instance to be propagated no matter whether the source IP address in the packet matches the IP address associated with the Neutron port or not. This option relies upon the Neutron port_security extension that is available starting with the OpenStack Kilo release.

The three sub-sections that follow describe the OpenStack configuration requirements for this option, how to utilize this option after a VM instance has already booted, and how to use this option before a VM instance has booted.

OpenStack Configuration Requirements

The Neutron port_security extension needs to be enabled for this method to work. For the procedure to enable the port_security extension see:

ML2 Port Security Extension Wiki page

Note: Enabling the port_security extension when there are already existing networks within the OpenStack cloud causes all network related requests into Neutron to fail due to a known bug in Neutron. There is a fix identified for this bug that is part of the Liberty release and is scheduled to be backported to the Kilo 2015.1.2 release. In the mean time, this option is only non-disruptive when working with a new cloud deployment where the cloud administrator can enable this feature before any networks and VM instances that use those networks are created. The port_security extension can be enabled in an already deployed OpenStack cloud, but all existing networks, subnets, ports, etc., need to be deleted before enabling the port_security extension. This typically means all VM instances also need to be deleted as well, but a knowledgeable cloud administrator **may** be able to do the following to limit the disruption of enabling the port_security extension:

- Record the current IP address assignments for all VM instances,
- Remove the network interfaces from any existing VM instances,
- Delete the Neutron resources,
- Enable the port_security extension,
- Re-create the previously defined Neutron resources (networks, subnets, ports, etc.), and then
- Re-add the appropriate network interfaces to the VMs.

Depending on the number of VM instances running in the cloud, this procedure may or may not be practical.

H-7. After a VM Instance has been Booted: Port Security

If you need to disable port security for a port after it has already been associated with a VM instance, then you need to execute one or both of the following commands to use the port_security option. First, if the VM instance with which the existing port is associated has any associated security groups (run `nova list-secgroup <VM instance name>` to check), then you first need to run a command of the following form for each of the security group(s) associated with the VM instance:

```
# nova remove-secgroup <VM instance name> <Security group name>
```

where the bolded item has the following meaning:

- <VM instance name>

  Identifies the name of the VM instance for which the identified security group name should be deleted.

- <Security group name>

  Identifies the name of the security group that should be removed from the VM instance.

So for example if you wanted to remove the default security group from a VM instance named ‘testvm4’ then you would type a command similar to the following:

```
# nova remove-secgroup testvm4 default
```

Once any security groups associated with VM instance to which the Neutron port is assigned have been removed, then the Neutron port(s) associated with the target VM instance need to be updated to disable port security on those ports. The command to disable port security for a specific Neutron port is of the form:

```
# neutron port-update <Port ID> -- port-security-enabled=false
```

where the bolded item has the following meaning:

- <Port ID>

  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence such as “`$(neutron port-show –f value –F id <Port Name>)`”.

So for example if you wanted to indicate to Neutron that port security should be disabled for a port with an ID of 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 then you would type the following command:

```
# neutron port-update 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 --port-
security-enabled=false
```

If the port-update command succeeds, within the VM instance with which the 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 port is associated, application managed VIPs can now be added to the network interface within the VM instance associated with the port and network traffic using that VIP address should now propagate.

H-8. Before a VM Instance has been Booted: Port Security

If you want to disable port security for a port before it is associated with a VM instance, then you need to first create the port at which time you can specify that port security should be disabled. The command to create a new port with port security disabled is of the following form:

```
# neutron port-create --name <Port Name> --port-security-enabled=false --
fixed-ip subnet-id=$(neutron subnet-show –f value –F id <Subnet
name>),ip_address=<Target IP address> $(neutron net-show –f value –F id
<Network name>)
```

where the bolded items have the following meaning:

- <Port Name>

  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the "`--name` **`<Port Name>`**" portion of the command is completely optional.

- <Subnet name>

  The name of the subnet to which the port should be added.

- <Target IP address>

  The unique IP address to be associated with the port.

- <Network Name>

  The name of the network with which the port should be associated.

So for example if you wanted to indicate to Neutron that a new port should have port security disabled and an IP address of 10.133.97.133 on the 'ext-subnet' subnet then you would type a command similar to the following:

```
# neutron port-create -name foo --port-security-enabled=false --fixed-ip
subnet-id=$(neutron subnet-show -f value -F id ext-
subnet),ip_address=10.133.97.133 $(neutron net-show -f value -F id ext-
net)
```

Once the port or ports with port security disabled have been created, when you boot the VM instance, you need to execute a command similar to the following:

```
# nova boot --flavor m1.xlarge --image testVMimage --nic port-id=$(neutron
port-show -f value -F id <Port Name>) testvm3
```

where the flavor, image, and VM instance name values need to be replaced by values appropriate for your VM. If the port to be associated with the VM instance is not named, then you need to obtain the port's ID using the neutron port-list command and replace the "`$(neutron port-show -f value -F id <Port Name>)`" sequence in the above command with the port's ID value.

H-9. Managing Application Virtual IP Addresses within VM Instances

Once either of the previously described options is in place to enable applications to manage their own virtual IP addresses, there should be no modifications required to how the application already manages its VIPs in a non-virtualized configuration. There are many ways that an application can add or remove virtual IP addresses but as a reference point, here are some example command line operations to add a virtual IP address of 10.133.97.136 to the eth0 network interface within a VM and then send four gratuitous ARP packets to refresh the ARP caches of any neighboring nodes:

```
# ip address add 10.133.97.136/23 broadcast 10.133.97.255 dev eth0 scope
global

# arping -c 4 -U -I eth0 10.133.97.136
```

As the creation of virtual IP addresses typically coincides with when an application is assigned an active role, the above operations would be performed both when an application instance first receives an initial active HA role or when an application instance transitions from a standby HA role to the active HA role.

Appendix I. 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.