Oracle® Communications

Diameter Signaling Router

Cloud Installation Guide

Release 8.2

E88973-03

July 2018

Oracle Communications Diameter Signaling Router Cloud Installation Guide, Release 8.2

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

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

See more information on My Oracle Support (MOS) in Appendix K.

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

This document installs the Diameter Signaling Router (DSR) 8.2 and IDIH 8.2 applications on a supported Cloud platform

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.

1.1 References

[1] Communication Agent Configuration Guide

[2] DSR PCA Activation Guide

[3] DSR Meta Administration Feature Activation Procedure

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

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

[6] SDS SW Installation and Configuration Guide

[7] MAP-Diameter IWF Feature Activation Procedure

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

[9] Communication Agent User's Guide

[10] Diameter User's Guide

[11] Mediation User's Guide

[12] Range Based Address Resolution (RBAR) User's Guide

[13] Full Address Based Resolution (FABR) User's Guide

[14] IP Front End (IPFE) User's Guide

[15] DSR Alarms and KPIs Reference

[16] Measurements Reference

[17] Diameter Common User's Guide

[18] Map-Diameter IWF User's Guide

[19] Gateway Location Application (GLA) User's Guide

[20] DSR Security Guide

[21] DSR IPv6 Migration Guide

[22] DSR DTLS Feature Activation Procedure

[23] DSR RADIUS Shared Secret Encryption Key Revocation MOP MO008572

[24] DCA Framework and Application Activation and Deactivation Guide

[25] Oracle VM Concepts Guide, Release 3.4

[26] Networking v2.0 API documentation

[27] DSR Cloud Benchmarking Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
CD	Compact Disk
DA-MP	Diameter Agent Message Processor
DSCP	Differentiated Services Code Point
DSR	Diameter Signaling Router
ESXi	Elastic Sky X Integrated
FABR	Full Address Based Resolution
iDIH	Integrated Diameter Intelligence Hub
IPFE	IP Front End
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 (for example, TPD)
OVA	Open Virtualization Archive
OVM-M	Oracle VM Manager
OVM-S	Oracle VM Server
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
SSO	Single Sign On
TPD	Tekelec Platform Distribution
TSA	Target Set Address
VIP	Virtual IP
VM	Virtual Machine
vSTP	Virtual Signaling Transfer Point

1.3 Terminology

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

Table 2. Terminology

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

Term	Definition
Site	Applicable for various applications, a site is type of **place**. A place is configured object that allows servers to be associated with a physical location. A site place allows servers to be associated with a physical site. For example, sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one site when the server is configured. For the Policy and 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.
Two Site Redundancy	Two site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy and Charging Mated Sites Place Association containing two sites. Two site redundancy is a feature provided by server group configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in two geographically separate sites (locations). This feature ensures there is always a functioning active server in a server group even if all the servers in a single site fail.

2. Installation Overview

This section provides a brief overview of the recommended methods for installing the source release software that is installed and running on a Cloud to the target release software.

2.1 Required Materials

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

2.2 Installation Overview

This section describes the overall strategy to employ for a single or multi-site DSR and iDIH installation. It also lists the procedures required for installation with estimated times. Section 2.2.1 discusses the overall installation strategy and includes an installation flowchart to determine exactly which procedures should be run for an installation. Section 2.2.3 lists the steps required to install a DSR system. The later sections expand on the information from the matrix and provide a general timeline for the installation. Additionally, basic firewall port information is included in Appendix F Firewall Ports. It should also be noted that some procedures are cloud platform dependent and not all procedures are performed on all cloud platforms.

2.2.1 Installation Strategy

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

1. An overall installation requirement is decided upon. The following data are collected:
    - The total number of sites
    - The number of virtual machines at each site and their role(s)

  - What time zone should be used across the entire collection of DSR sites?
  - Will SNMP traps be viewed at the NOAM or will an external NMS be used? (Or both?)

2. A site survey (NAPD) is conducted with the customer to determine exact networking and site details.

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

DSR currently supports the following installation strategies:

- DSR installation without using HEAT templates

  [Figure 1] illustrates the overall process that each DSR installation involves. In summary, this involves creation of guests and configures each guest role based on Resource Profile and Configure Network.

- DSR installation using HEAT templates (OpenStack only)

  [Figure 2] illustrates the overall process that each DSR installation involves using the Heat Templates. In summary, this involves creation of parameter files, environment files, template files, DSR Topology Configuration xml and deploys DSR using open stack CLI commands.

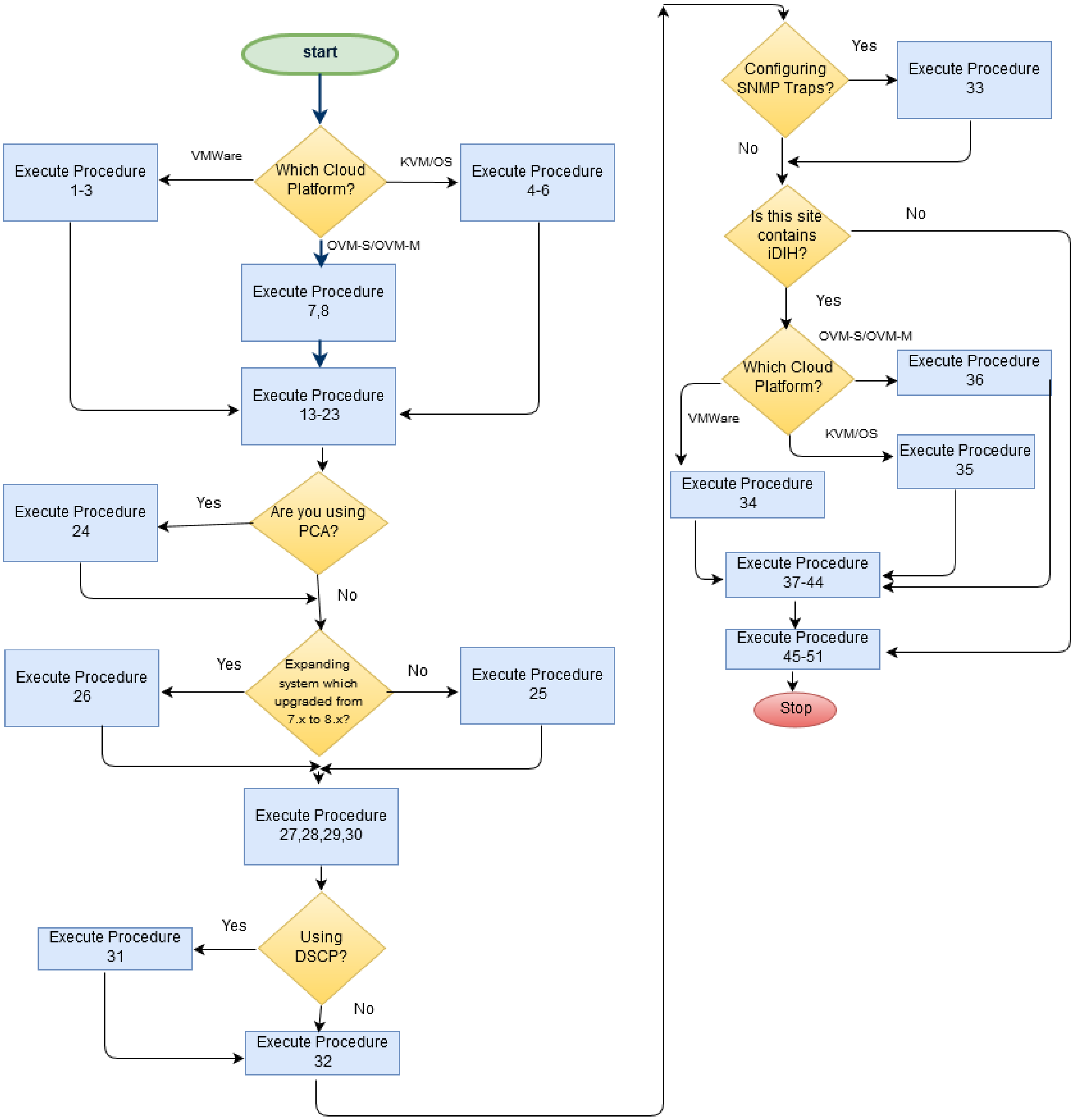


Figure 1: DSR Single Site Installation Procedure Map Without Using HEAT Templates

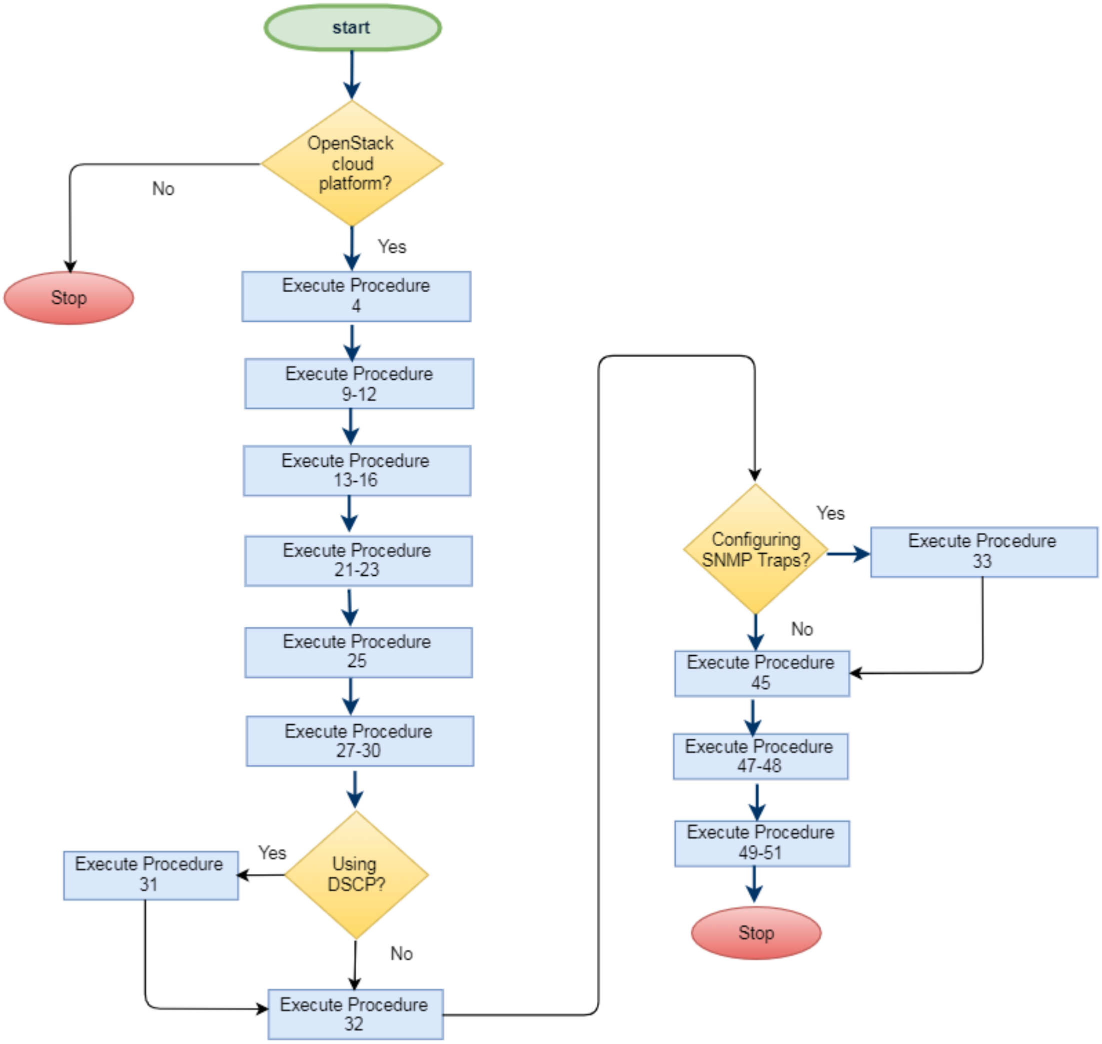


Figure 2: DSR Installation Procedure Map Using HEAT Templates

2.2.2 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 DSR Application Servers (NOAM, SOAM, MPs of all types) in a DSR installation.

DSR application servers can be configured to:

1. Send all their SNMP traps to the NOAM by 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.

2.2.3 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 are to be executed in the order they are listed.

- If installation strategy is **Install DSR without using HEAT templates**, then follow Table 3.
- If installation strategy is **Install DSR using HEAT templates**, then follow Table 4.

Table 3. Installation Overview Without Using HEAT Templates

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 1 or Procedure 4 or Procedure 7	Import DSR OVA	5	5
Procedure 2 or Procedure 5	Configure DSR NOAM guest role based on resource profile	10	15
Procedure 3 or Procedure 6	Configure DSR remaining guests role based on resource profile	40	55
Procedure 13	Configure the First NOAM NE and Server	25	80
Procedure 14	Configure the NOAM Server Group	15	95
Procedure 15	Configure the Second NOAM Server	15	110
Procedure 16	Complete Configuring the NOAM Server Group	10	120
Procedure 17 (Optional)	Configure the DR NOAM NE and Server (Optional)	25	145
Procedure 18 (Optional)	Configure the DR NOAM Server Group (Optional)	15	160
Procedure 19 (Optional)	Configure the Second DR NOAM Server (Optional)	15	175
Procedure 20 (Optional)	Complete Configuring the DR NOAM Server Group (Optional)	10	185
Procedure 21	Configure the SOAM NE	15	200
Procedure 22	Configure the SOAM Servers	10	210
Procedure 23	Configure the SOAM Server Group	10	220
Procedure 24	Activate PCA/DCA (PCA/DCA Only)	10	230
Procedure 25	Configure the MP Virtual Machines	5	235
Procedure 26 (Optional)	Configure the MP Virtual Machines (Optional)	10	245
Procedure 27	Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)	10	255
Procedure 28	Configure the MP Server Group(s) and Profiles	5	260
Procedure 29 (Optional)	Configure the Signaling Devices (Optional)	10	270
Procedure 30	Configure the Signaling Network Routes	20	290
Procedure 31 (Optional)	Configure DSCP Values for Outgoing Traffic (Optional)	5	295

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 32	IP Front End (IPFE) Configuration	45	340
Procedure 33 (Optional)	Configure SNMP Trap Receiver(s) (Optional)	15	355
Procedure 34	(VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)	10	365
Procedure 35	(KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)	10	375
Procedure 36	(OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each	10	385
Procedure 37 (Optional)	Configure iDIH VM Networks (Optional)	10	395
Procedure 38 (Optional)	Run Post Installation Scripts on iDIH VMs (Optional)	25	420
Procedure 39 (Optional)	Configure DSR Reference Data Synchronization for iDIH (Optional)	30	450
Procedure 40 (Optional)	iDIH Configuration: Configuring the SSO Domain (Optional)	10	460
Procedure 41 (Optional)	Integrate iDIH into DSR (Optional)	10	470
Procedure 42 (Optional)	iDIH Configuration: Configure the Mail Server (Optional)	10	480
Procedure 43	iDIH Configuration: Configure SNMP Management Server (Optional)	20	500
Procedure 44 (Optional)	iDIH Configuration: Change Network Interface (Optional)	30	530
Procedure 45	Configure ComAgent Connections	15	545
Procedure 46	Complete PCA Configuration (Optional)	5	550
Procedure 47	Backups and Disaster Prevention	15	565
Procedure 48	(KVM/OpenStack Only) Configure Port Security	10	575
Procedure 49	Enable/Disable DTLS (SCTP Diameter Connections Only)	10	585
Procedure 50	Shared Secret Encryption Key Revocation (RADIUS Only)	10	595
Procedure 51	DSR Performance Tuning	10	600

Note: Refer section 3 Software Installation Procedure for detailed procedures.

Table 4: Installation Procedures Using HEAT Templates

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 4	Import DSR OVA	5	5
Procedure 10	Create OpenStack Parameter File for NOAM	10	15
Procedure 11	Create OpenStack Parameter File for Signaling	15	30
Procedure 12	Deploy HEAT Templates	15	45
Procedure 13	Configure the First NOAM NE and Server	10	55
Procedure 14	Configure the NOAM Server Group	25	80
Procedure 15	Configure the Second NOAM Server	15	95
Procedure 16	Complete Configuring the NOAM Server Group	15	110
Procedure 21	Configure the SOAM NE	10	120
Procedure 22	Configure the SOAM Servers	15	135
Procedure 23	Configure the SOAM Server Group	10	145
Procedure 24	Activate PCA/DCA (PCA/DCA Only)	10	155
Procedure 25	Configure the MP Virtual Machines	5	160
Procedure 27	Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)	10	170
Procedure 28	Configure the MP Server Group(s) and Profiles	5	175
Procedure 29 (Optional)	Configure the Signaling Devices (Optional)	10	185
Procedure 30	Configure the Signaling Network Routes	20	205
Procedure 31 (Optional)	Configure DSCP Values for Outgoing Traffic (Optional)	5	210
Procedure 32	IP Front End (IPFE) Configuration	15	225
Procedure 33 (Optional)	Configure SNMP Trap Receiver(s) (Optional)	15	240
Procedure 45	Configure ComAgent Connections	20	260
Procedure 47	Backups and Disaster Prevention	15	275
Procedure 48	(KVM/OpenStack Only) Configure Port Security	30	305
Procedure 49	Enable/Disable DTLS (SCTP Diameter Connections Only)	15	320
Procedure 50	Shared Secret Encryption Key Revocation (RADIUS Only)	10	330
Procedure 51	DSR Performance Tuning	10	340

Note: Refer section 4 Software Installation Using HEAT Templates (OpenStack) for detailed procedures.

2.3 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 5 for the post-DSR installation configuration documentation needed for their components.

Table 5. Post-DSR Installation Configuration Step

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
MAP-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure
Policy and Charging Application (PCA)	PCA Activation Procedure
Host Intrusion Detection System (HIDS)	DSR Security Guide, Section 3.2
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Procedures

3. 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 Privileges to add OVA's to catalog (VMware only)
- KVM/OpenStack admin and tenant privileges
- OVM-S/OVM-M credentials and privileges, OVM-M cli tool must be installed and is accessible

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.

IPv6

IPv6 configuration of XMI and IMI networks has been introduced in DSR 7.1. Standard IPv6 formats for IPv6 and prefix can be used in all IP configuration screens, which enable the DSR to be run in an IPv6 only environment. When using IPv6 for XMI and management, you must place the IPv6 address in brackets (highlighted in red below), example as followed:

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

If a dual-stack (IPv4 and IPv6) network is required, configure the topology with IPv4 first, and then **migrate** to IPv6. Reference [21] DSR IPv6 Migration Guide for instructions on how to accomplish this migration.

3.1 Create DSR Guests (VMware)

Procedure 1. (VMware) Import DSR OVA

STEP #	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 and Configure Network

STEP #	This procedure configures networking on VMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, My Oracle Support (MOS) and ask for assistance.	
1. □	Create the NOAM1 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 **vSphere Web Client**. 3. Name the **NOAM1 VM** and select the data store.
2. □	Configure resources for the NOAM1 VM	Configure the NOAM1 per the resource profiles defined in [27] DSR Cloud Benchmarking Guide for the **DSR NOAM** using the **vSphere Client** or **vSphere Web Client**.
3. □	Power on NOAM1	Use the **vSphere Client** or **vSphere Web Client** to power on the NOAM1 VM.

4.
□
	Configure NOAM1	1. Access the **NOAM1 VM** console using the **vSphere Client** or **vSphere Web Client**.
		2. Login as the **admusr** user.
		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. Ping the XMI gateway for network verification.
		`$ ping -c3 <Gateway of External Management Network>`

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

5. □	Configure NOAM2	Repeat this procedure for the NOAM2 VM.

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

S T E P #	This procedure adds network addresses for all VMs. ***Note***: This procedure provides an example for creating an SOAM. Follow the same steps to create other guests with their respective VM names and profiles. 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 SOAM1 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 **vSphere Web Client**. 3. Name the **SOAM1 VM** and select the data store.
2. □	Configure resources for the SOAM1 VM	Configure the **SOAM1 VM** per the resource profiles defined in [27] DSR Cloud Benchmarking Guide for the **DSR SO** using the **vSphere Client** or **vSphere Web Client**. Interfaces must be added per the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
3. □	Power on SOAM1 VM	1. Power on the **DSR SOAM1 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** using the **vSphere Client** or **vSphere Web Client**.
		2. Login as the **admusr** user.
		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. □	Verify network connectivity	1. Access the **SOAM1 VM console** using the **vSphere Client** or **vSphere Web Client**. 2. Login as the **admusr** user. 3. Ping the NOAM1. `$ ping -c3 <IP Address in External Management Network>`

Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile and Configure 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)
		SOAM(s)
		Session SBRs, Binding SBR (Optional Components)
		DR NOAMs (Optional Components)

3.2 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 resource profiles defined in [27] DSR Cloud Benchmarking Guide 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 the Disable Port Security procedure in Appendix G.6, including the warning note. b. Enable the Neutron port security extension. ***Note***: This step is **NOT** applicable for HEAT deployment.

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

2.
□
	Add DSR OVA image	1. Copy the OVA file to the OpenStack control node.
		`$ scp DSR-x.x.x.x.x.ova admusr@node:~`
		2. Log into the OpenStack control node.
		`$ ssh admusr@node`
		3. In an empty directory, unpack the OVA file using **tar**.
		`$ tar xvf DSR-x.x.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-x.x.x.x.x-disk1.vmdk
		5. Source the OpenStack **admin** user credentials.
		`$ .  keystonerc_admin`
		6. Select an informative name for the new image.
		dsr-8.2.x.x.x-original
		7. Import the image using the **glance** utility from the command line.
		`$ glance image-create --name dsr-x.x.x.x-original --visibility public --protected false --progress --container-format bare --disk-format vmdk --file DSR-x.x.x.x-disk1.vmdk`
		This process takes about 5 minutes depending on the underlying infrastructure.
		8. (Optional – Steps 8 and 9 are not needed if VMDK is used.) Convert VMDK to QCOW2 format.
		Use the qemu-img tool to create a qcow2 image file using this command.
		`qemu-img convert -f vmdk -O qcow2 <VMDK filename> <QCOW2 filename>`
		For example:
		`qemu-img convert -f vmdk -O qcow2 DSR-82_12_0.vmdk DSR-82_12_0.qcow2`
		Install the qemu-img tool (if not already installed) using this yum command.
		`sudo yum install qemu-img`
		9. Import the coverted qcow2 image using the **glance** utility from the command line.
		`$ glance image-create --name dsr-x.x.x-original --is-public True --is-protected False --progress  --container-format bare --disk-format qcow2 --file DSR-x.x.x-disk1.qcow2`
		This process takes about 5 minutes depending on the underlying infrastructure.

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

S T E P #	This procedure configures networking on VMs. 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: **NOAM1**. 2. Examine the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.

2.
□
	Create and boot the NOAM 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.
		NOAM1
		NOAM2
		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 OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		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 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

3.
□
	Configure NOAM VIP (Optional)	***Note***: Refer to Application VIP Failover Options (OpenStack) in Appendix G for more information on VIP.
		If an NOAM VIP is needed, execute the following commands:
		1. Find the port ID associated with the NOAM instance XMI interface.
		`$ neutron port-list`
		2. 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. □	Check if interface is configured	If DHCP is enabled on the Neutron subnet, VM configures the VNIC with the IP address provided in step 2. To verify, ping the XMI IP address provided with the **nova boot** command from step 2.: `$ ping <XMI-IP-Provided-During-Nova-Boot>` If the ping is successful, ignore step 5. to configure the interface manually.

5.
□
	Manually configure interface, if not already done (Optional)	***Note***: If the instance is already configured with an interface and has successfully pinged (step 4.), then **ignore** this step to configure the interface manually.
		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** user.
		6. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		`$ 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>`
		Verify network connectivity by pinging Gateway of XMI network.
		`$ ping -c3 <XMI Gatewau>`
		Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
		7. Reboot the NOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible using both network and Horizon consoles.

6. □	Configure NOAM2	Repeat steps 1 through 5 for NOAM2.

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

STEP #	This procedure adds network addresses for all VMs. ***Note***: This procedure provides an example for creating an SOAM. Follow the same steps to create other guests with their respective VM names and profiles. 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: **SOAM1**. 2. Examine the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.

2.
□
	Create and boot the SOAM 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.
		SOAM1
		SOAM2
		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 OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		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 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

3.
□
	Configure SOAM VIP (Optional)	***Note***: Refer to Allowed Address Pairs in Appendix G.2 for more information on VIP.
		If an SOAM VIP is needed, execute the following commands:
		1. Find the port ID associated with the SOAM instance XMI interface.
		`$ neutron port-list`
		2. 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. □	Check if interface is configured	If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address provided in step 2 above. To verify, ping the XMI IP address provided with nova boot… command (step 2): `$ ping <XMI-IP-Provided-During-Nova-Boot>` If the ping is successful, ignore step 5 to configure the interface manually.

5.
□
	Manually configure interface, if not already done (Optional)	***Note***: If the instance is already configured with an interface and successfully pinging (step 4), then **ignore** this step to configure the interface manually.
		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** user.
		6. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		`$ 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>`
		Verify network connectivity by pinging Gateway of XMI network.
		`$ ping -c3 <XMI Gatewau>`
		Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
		7. Reboot the SOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible using both network and Horizon consoles.

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

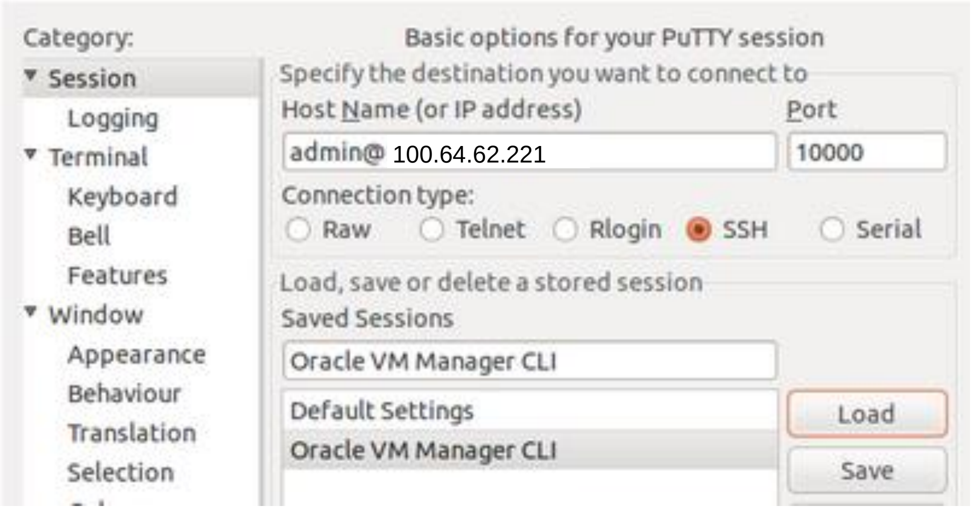
6. □	Verify network connectivity	1. Access the **SOAM1 VM console** using the openstack. 2. Login as the **admusr** user. 3. Ping the NOAM1. `$ ping -c3 <IP Address in External Management Network>`

7.
□
	Procedure overview	Repeat steps 1 through 6 for the following VMs. Use unique labels for the VM names. Assign addresses to all desired network interfaces:
		MP(s)
		MP(s) SS7 (Optional Components)
		IPFE(s)
		MP vSTP (For vSTP configuration) (Optional Components)
		SOAM(s)
		Session SBRs, Binding SBR (Optional Components)
		DR NOAMs (Optional Components)

3.3 Create DSR Guests (OVM-S/OVM-M)

Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

STEP #		
	This procedure imports the DSR image. This procedure requires values for these variables: • <OVM-M IP> = IP address to access a sh prompt on the OVM server • <URL to OVA> = link to a source for downloading the product image (.ova) • <MyRepository name> = name of the repository in the OVM to hold the product image (.ova) Execution of this procedure discovers and uses the values of these variables: • <Virtual Appliance OVA ID> • <OVA VM name_vm_vm> • <OVM network id for (each subnet)> • <OVM network name for (each subnet)> 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.
□
	Preparation: Access command line of OVM	Refer to Common OVM Manager Tasks (CLI) in Appendix D for setting up the platform.
		1. Get the site-specific values for these variables (overwrite example).
		<OVM-M IP> = `100.64.62.221`
		2. Use the respective value for <OVM-M IP> into the command.
		`ssh -l admin <OVM-M IP> -p 10000`
		Example:
		`ssl -l admin 100.64.62.221 -p 10000`
		Alternatively, use a terminal emulation tool like putty.
		
		Host Name (or IP address): admin@ 100.64.62.221
		Port: 10000
		Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
		Saved Sessions: Oracle VM Manager CLI
		Default Settings
		Oracle VM Manager CLI

Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Basic options for your PuTTY session
Specify the destination you want to connect to
Load, save or delete a stored session
Load
Save

Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

2.
□
	OVM-M CLI: Import the VirtualAppliance/ OVA	1. Get the site-specific values for these variables (overwrite example).
		<URL to OVA> = `http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		<MyRepository name> = `XLab Utility Repo01`
		2. Use the respective values for <MyRepository name> and <URL to OVA> into the command.
		`OVM> importVirtualAppliance Repository name=’<MyRepository name>’ url="<URL to OVA>”`
		Example:
		`OVM> importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		3. Execute the command and validate success.
		4. Examine the screen results to find site-specific text for variables in these locations:
		Command: `importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`Status: Success`
		`Time: 2017-04-18 15:23:31,044 EDT`
		`JobId: 1492543363365`
		`Data:`
		`  id: 1128a1c6ce name: DSR-8.2.0.0.0_82.4.0.ova`
		5. Use the respective values for values for these variables (overwrite example).
		<Virtual Appliance OVA ID> = `1128a1c6ce`

Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

3.
□
	OVM-M CLI:
	Get the virtual appliance ID
		The virtual appliance OVA ID is used in later steps.
		1. Get the site-specific text for these variables (overwrite example).
		<Virtual Appliance OVA ID> = `1128a1c6ce`
		2. Use the respective values for <Virtual Appliance OVA ID> into the command.
		`OVM> show VirtualAppliance id=<Virtual Appliance OVA id>`
		Example:
		`OVM> show VirtualAppliance id=1128a1c6ce`
		3. Execute the command and validate success.
		4. Examine the screen results to find site-specific text for variables in these locations:
		Command: `show VirtualAppliance id=1128a1c6ce`
		`Status: Success`
		`Time: 2017-04-18 15:23:53,534 EDT`
		`Data:`
		`  Origin = http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`  Repository = 0004fb0000030000da5738315337bfc7  [XLab Utility Repo01]`
		`  Virtual Appliance Vm 1 = 11145510c0_vm_vm [vm]`
		`  Virtual Appliance VirtualDisk 1 = 11145510c0_disk_disk1 [disk1]`
		`  Id = 11145510c0  [DSR-8.2.0.0.0_82.4.0.ova]`
		`  Name = DSR-8.2.0.0.0_82.4.0.ova`
		`  Description = Import URL: http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`  Locked = false`
		5. Use the respective values for these variables (overwrite example).
		<OVA VM name_vm_vm> = `11145510c0_vm_vm`

Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

4. □ **OVM-M CLI:** Determine the OVM network IDs (established during the platform installation)

```
OVM> list Network
```

1. Execute the command and validate success.
2. Examine the screen results to find the find site-specific OVM values for each subnet:
   - <OVM network ID>
   - <OVM network name>
3. Note the entire screen results. Refer to this data in later steps.

```
Command: list network
Status: Success
Time: 2017-04-19 18:51:42,494 EDT
Data:
  id:10486554b5  name:XSI-7 (10.196.237.0/25)
  id:10f4d5744c  name:XMI-11 (10.75.159.0/25)
  id:10775cf4e5  name:IDIH Internal
  id:102e89a481  name:IMI Shared (169.254.9.0/24)
  id:c0a80500  name:192.168.5.0
  id:10d8de6d9a  name:XSI-6 (10.196.236.128/25)
  id:10806a91fb  name:XSI-8 (10.296.237.128/25)
  id:10a7289add  name:Control DHCP
  id:1053a604f0  name:XSI-5 (10.196.236.0/25)
  id:10345112c9  name:XMI-10 (10.75.158.128/25
```

4. Use the respective values for network ID variables (change the examples in this table according to the values).

	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3-16)	Replication (SBR Rep)	DIH Internal
<OVM network name>	XMI-10	IMI Shared	XSI-5	XSI-6	XSI-7	DIH Internal	XMI-10
<OVM network ID>	10345112c9	102e89a481	1053a604f0	10d8de6d9a		10486554b5	10775cf4e5

3.4 Configure Virtual Machines

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

STEP #	This procedure creates virtual machines. Repeat this procedure for each DSR VM guest that needs to be created. This procedure requires values for these variables: • <OVA VM name_vm_vm> • <ServerPool name> • <VM name> • <OVM network ID for XMI> • <OVM network ID for IMI> • <OVM network ID for XSI#> where # is a numeric from 1-16, for the signaling networks • <OVM network ID for Replication XSI#> • <URL for OVM GUI> • <VM IP in XMI> from the NAPD • <Gateway for XMI> from the NAPD • <NetMask for XMI> from the NAPD Execution of this procedure discovers and uses the values of these variables: • <VM ID> • <vCPUs Production> • <VNIC 1 ID> • <interface name> defined in [27] DSR Cloud Benchmarking Guide 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.
□
	OVM-M CLI: Create a VM for each guest from the VM in the OVA virtual appliance	1. Get the site-specific text for these variables (overwrite example).
		<OVA VM name_vm_vm> = `11145510c0_vm_vm`
		2. Use the respective values for <OVA VM name> into the command.
		`OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=<OVA VM name>`
		Example:
		`OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm`
		3. Execute the command and validate success.
		4. Examine the screen results to find site-specific text for variables in these locations:
		Command: `createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm`
		`Status: Success`

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

		`Time: 2017-04-18 16:02:09,141 EDT`
		`JobId: 1492545641976`
		`Data:`
		`  id: 0004fb00000600004a0e02bdf9fc1bcd name:DSR-8.2.0.0.0_82.4.0.ova_vm`
		5. Use the respective values for these variables (overwrite example).
		<VM ID> = `0004fb00000600004a0e02bdf9fc1bcd`

2.
□
	OVM-M CLI: Add the VM to the server pool	1. Get the site-specific text for these variables (overwrite example).
		<VM ID> = `0004fb00000600004a0e02bdf9fc1bcd`
		<ServerPool name> = `XLab Pool 01`
		2. Use the respective values for <VM ID> and <ServerPool name> into the command.
		`OVM> add Vm id=<VM id> to ServerPool name=”<ServerPool name>”`
		Example:
		`OVM> add Vm id=0004fb00000600004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"`
		3. Execute the command and validate success.
		Command: `add Vm id=0004fb0000060000beb93da703830d3c to ServerPool name="XLab Pool 01"`
		`Status: Success`
		`Time: 2017-04-19 21:05:10,950 EDT`
		`JobId: 1492650310802`
		Note: Refer to the Server Pool section in Appendix D.2 for more information.

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

3. □ **OVM-M CLI**: Edit VM to apply required profile/ resources

1. Get the site-specific text for these variables (overwrite example).

   <VM ID> = `0004fb00000600004a0e02bdf9fc1bcd`

   <VM name > = `na-noam-na-2a`

   <vCPUs Production> = `4`

2. Refer to [27] DSR Cloud Benchmarking Guide for recommended resource.

VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production
Type of guest host	#	#	#	#	#

3. Use the respective values for <VM ID>, <VM name>, and <vCPUs Production> into the command.

```
OVM> edit Vm id=<VM id> name=<VM name> memory=6144
memoryLimit=6144 cpuCountLimit=<vCPUs Production>
cpuCount=<vCPUs Production> domainType=XEN_HVM
description="<VM name>"
```

   Example:

```
OVM> edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-
noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4
cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"
```

4. Execute the command and validate success.

   Command: `edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"`

```
Status: Success

Time: 2017-04-18 17:55:25,645 EDT

JobId: 1492552525477
```

Now, the VM has a name and resources.

4. □ **OVM-M CLI**: Determine VNIC ID

1. Get the site-specific text for these variables (overwrite example).

   <VM name> = `na-noam-na-2a`

2. Use the respective value for <VM name> into the command.

```
OVM> show Vm name=<VM name>
```

   Example:

```
OVM> show Vm name=na-noam-na-2a
```

3. Execute the command and validate success.

4. Examine the screen results to find site-specific text for variables in these locations:

```
Status = Stopped

Memory (MB) = 6144

Max. Memory (MB) = 6144
```

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

```
Processors = 4

Max. Processors = 4

Priority = 50

Processor Cap = 100

High Availability = No

Operating System = Oracle Linux 6

Mouse Type = PS2 Mouse

Domain Type = Xen HVM

Keymap = en-us

Start Policy = Use Pool Policy

Origin = http://10.240.155.70/iso/DSR/8.2/ova/DSR-
8.2.0.0.0_82.4.0.ova

Disk Limit = 4

Huge Pages Enabled = No

Config File Absolute Path =
192.168.5.5:/storage/ovm01/repository/VirtualMachines/0004fb
00000600004a0e02bdf9fc1bcd/vm.cfg

Config File Mounted Path =
/OVS/Repositories/0004fb0000030000da5738315337bfc7/VirtualMa
chines/0004fb00000600004a0e02bdf9fc1bcd/vm.cfg

Server Pool = 0004fb00000200009148c8926d307f05  [XLab Pool
01]

Repository = 0004fb0000030000da5738315337bfc7  [XLab Utility
Repo01]

Vnic 1 = 0004fb0000070000091e1ab5ae291d8a [Template Vnic]

VmDiskMapping 1 = 0004fb0000130000a1996c6074d40563  [Mapping
for disk Id (79def426328a4127b5bf9f7ae53d3f48.img)]

VmDiskMapping 2 = 0004fb00001300002db3d4b67a143ab5  [Mapping
for disk Id (EMPTY_CDROM)]

Restart Action On Crash = Restart

Id = 0004fb00000600004a0e02bdf9fc1bcd  [na-noam-na-2a]

Name = na-noam-na-2a

Description = na-noam-na-2a

Locked = false

DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV
guest)]
```

5. Use the respective values for these variables (overwrite example).

   <Vnic 1 ID> = `0004fb0000070000091e1ab5ae291d8a`

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

<table>
<tr>
<td>5.
□</td>
<td>Determine network interfaces for the type of guest host</td>
<td>Refer to [27] DSR Cloud Benchmarking Guide to learn which network interfaces need to be configured for each guest type. The table looks like this:
<table>
<tr><th></th><th>OAM (XMI)</th><th>Local (IMI)</th><th>Sig A (XSI1)</th><th>Sig B (XSI2)</th><th>Sig C (XSI3-16)</th><th>Rep (SBR)</th><th>DIH Internal</th></tr>
<tr><td>Type of guest host</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td></tr>
</table>

<b><i>Note</i></b>: The VNICs need to be created in the correct order so the interfaces are associated with the correct network.</td>
</tr>
<tr>
<td>6.
□</td>
<td><b>OVM-M CLI</b>: Attach XMI VNIC (if required by guest host type)</td>
<td><b>Add (attach) VNIC ID of the XMI network to VM</b>:
1. Get the site-specific text for these variables (overwrite example)
<VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a
<OVM network ID for XMI> = 10345112c9
2. Use the respective values for <VNIC 1 ID> and <OVM network ID for XMI> into the command
OVM> add Vnic ID=<Vnic 1 ID> to Network name=<OVM network ID for XMI>
Example:
OVM> add Vnic ID=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9
3. Execute the command and validate success.
Command: add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9
Status: Success
Time: 2017-04-19 19:08:59,496 EDT
JobId: 1492643339327</td>
</tr>
</table>

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

7.
□
	OVM-M CLI: Create and attach IMI VNIC (if required by guest host type)	**Create VNIC ID on the IMI network and attach to VM**:
		1. Get the site-specific text for these variables (overwrite example).
		<VM name> = `na-noam-na-2a`
		<OVM network ID for IMI> = `102e89a481`
		2. Use the respective values for <OVM network ID for IMI> and <VM name> into the command.
		`OVM> create Vnic network=<OVM network ID for IMI> name=<VM name>-IMI on VM name=<VM name>`
		Example:
		`OVM> create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a`
		3. Execute the command and validate success.
		Command: `create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a`
		`Status: Success`
		`Time: 2017-04-19 21:21:57,363 EDT`
		`JobId: 1492651317194`
		`Data:`
		`id:0004fb00000700004f16dc3bfe0750a7  name:na-noam-na-2a-IMI`

8.
□
	OVM-M CLI: Create and attach XSI VNIC(s) (if required by guest host type)
	Note: Repeat this step if the VM will have multiple signaling networks, specifying the number of the network
		Create VNIC ID on the XSI network(s) and attach to VM:
		1. Get the site-specific text for these variables (overwrite example).
		<VM name> = `hostname`
		<OVM network ID for XSI#> = `1053a604f0`
		<#> = `the number of the XSI network [1-16]`
		2. Use the respective values for <OVM network ID for XSI#> and <VM name> into the command.
		`OVM> create Vnic network=<OVM network id for XSI#> name=<VM name>-XSI<#> on Vm name=<VM name>`
		Example:
		`OVM> create Vnic network=1053a604f0 name=hostname-XSI1 on Vm name=hostname`
		3. Execute the command and validate success.

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

9.
□
	OVM-M CLI: Create and attach replication VNIC (if required by guest host type)	**Create VNIC ID on the Replication network and attach to VM**:
		1. Get the site-specific text for these variables (overwrite example).
		<VM name> = `hostname`
		<OVM network ID for Replication XSI#> = `10486554b5`
		<OVM network name for Replication XSI#> = `XSI7`
		<#> = `the number of the XSI Replication network [1-16]`
		2. Use the respective values for <OVM network ID for Replication XSI#>, <OVM network name for Replication XSI#>, and <VM name> into the command.
		`OVM> create Vnic network=<OVM network id for Replication XSI#> name=<VM name>-<OVM network name for Replication XSI#> on Vm name=<VM name>`
		Example:
		`OVM> create Vnic network=10486554b5 name= hostname-XSI7 on Vm name=hostname`
		3. Execute the command and validate success.

10.
□
	OVM-M CLI: Start VM	1. Get the site-specific text for these variables (overwrite example).
		<VM name> = `na-noam-na-2a`
		2. Use the respective values for <VM name> into the command.
		`OVM> start Vm name=<VM name>`
		Example:
		`OVM> start Vm name=na-noam-na-2a`
		3. Execute the command and validate success.
		Command: `start Vm name=na-noam-na-2a`
		`Status: Success`
		`Time: 2017-04-19 19:29:35,376 EDT`
		`JobId: 1492644568558`

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

11.
□
	OVM-M GUI: Configure the XMI network interface for this VM	1. Get the site-specific text for these variables (overwrite example).
		<URL for OVM GUI> = https://100.64.62.221:7002/ovm/console/faces/resource/resourceView.jspx
		<interface name> = from the table in [27] DSR Cloud Benchmarking Guide
		<VM IP in XMI> = from the NAPD
		<Gateway for XMI> = from the NAPD
		<NetMask for XMI> = from the NAPD
		2. Access the CLI of the console for the VM:
		3. Log into the **OVM-M** GUI by typing the **<URL for OVM GUI>** into a browser.
		a. Navigate to the Servers and VMs tab.
		b. Expand and select the <ServerPool name>.
		c. From the **Perspective** list, select **Virtual Machines**.
		d. Select the <VM name> from the rows listed, and click the **Launch Console** icon.
		e. In the Console window, log into the VM as the admusr.
		4. Use the respective values for <interface name>, <VM IP in XMI>, <Gateway for XMI>, and <NetMask for XMI> into the commands
		XMI:
		`$ sudo netAdm set --onboot=yes --device=<interface name>  --address=<VM IP in XMI> --netmask=<NetMask for XMI>`
		`$ sudo netAdm add --route=default --device=<interface name> -gateway=<Gateway for XMI>`
		Example:
		`$ sudo netAdm set --onboot=yes --device=eth0 --address=10.75.158.189 --netmask=255.255.255.128`
		Example:
		`$ sudo netAdm add --route=default --device=eth0 --gateway=10.75.158.129`
		5. Execute the command and validate success
		6. Verify network connectivity by pinging Gateway of network
		`$ ping -c3 <Gateway for XMI>`
		7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible using both network and console.

4. Software Installation Using HEAT Templates (OpenStack)

4.1 Prepare OpenStack Template and Environment files

Procedure 9. Prepare OpenStack Templates and Environment Files for NOAM/Signaling Stacks

S T E P #	This procedure gathers required templates and environment files to provide while deploying NOAM/signaling stacks. **Prerequisite**: All the respective infrastructures has to be up and running. 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. □	Login to Oracle document repository - OTN	Log into the Oracle Document Repository at http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html
2. □	Select the DSR Release	Select the respective release folder. For example, Release 8.2.x.
3. □	Download HEAT templates	Download the **HEAT Templates** zip file under **Cloud Installation and Upgrade** section.
4. □	Unzip the HEAT templates to a folder	1. Create a new folder with any name for storing the HEAT templates under the home directory. Example : /home/heat_templates 2. Store the downloaded HEAT templates zip file in the folder. Example : /home/heat_templates/exampleHeat.zip 3. Unzip the downloaded heat templates. unzip /home/heat_templates/exampleHeat.zip

Procedure 9. Prepare OpenStack Templates and Environment Files for NOAM/Signaling Stacks

5. □	Determine the template and environment files	Below are possible deployment use cases of DSR. The HEAT templates contain files for all scenarios. Determine the appropriate template and environment files with respect to your requirement. ***Note***: Currently, SS7 MPs are not supported. All SS7 related parameters should be provided as default values, refer to Appendix J.2 Example Parameter File.

Deployment Use Case	Template Files	Environment Files
Dynamic IP - With VIP	**NOAM Template** dsrNetworkOam_provider.yaml **Signaling Template** dsrSignalingNode_provider.yaml	dsrResources_provider.yaml
Dynamic IP - Without VIP	**NOAM Template** dsrNetworkOamNoVip_provider.yaml **Signaling Template** dsrSignalingNodeNoVip_provider.yaml	dsrResourcesNoVip_provider.yaml
Fixed IP - With VIP	**NOAM Template** dsrNetworkOam_fixedIps.yaml **Signaling Template** dsrSignalingNode_fixedIps.yaml	dsrResources_fixedIps.yaml
Fixed IP - Without VIP	**NOAM Template** Yet to be created **Signaling Template** Yet to be created.	Yet to be created
Dynamic IP - With IDIH Nodes	**NOAM Template** dsrNetworkOam_provider.yaml **Signaling Template** dsrSignalingNodeIdih_provider.yaml	idihResources_provider.yaml
Fixed IP - With IDIH Nodes	**NOAM Template** dsrNetworkOam_fixedIps.yaml **Signaling Template** dsrSignalingNodeIdih_fixedIps.yaml	dsrResourcesIdih_fixedIps.yaml

4.2 Create OpenStack Parameters Files

Procedure 10. Create OpenStack Parameter File for NOAM

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">This procedure instructs how to manually create input parameters file to be provided while deploying NOAM stacks.
<b>Prerequisit</b>e: All the respective infrastructures has to be up and running
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>Login to OpenStack server CLI</td><td>Log into the OpenStack server though command line.</td></tr>
<tr><td>2.
□</td><td>Create the parameter file</td><td>1. Go to the folder created in Procedure 9, step 4. for storing the templates.
2. Create an empty NOAM parameter file in this folder following this naming convention to identify the purpose of the file.
<DSR Name>_<Site Name>_NetworkOam_Params.yaml
For example:
dsrCloudInit_Site00_NetworkOam_Params.yaml</td></tr>
<tr><td>3.
□</td><td>Sample file</td><td>Refer to Appendix J.1 Example Template File for a sample file with values.
<b><i>Note</i></b>: It is important to keep the example file ready since this helps you understand the use of each key value pair described in the next step while creating the parameter file.</td></tr>
<tr><td>4.
□</td><td>Populate the parameters file</td><td>Refer to Appendix J.1 Example Template File to create the parameter file in YAML format.
<b><i>Note</i></b>: Follow these guidelines while working with the YAML files.
• The file must end with .yaml extension.
• YAML must be case-sensitive and indentation-sensitive.
• YAML does not support the use of tabs. Instead of tabs, it uses spaces.
• This file is in YAML format and it contains <b>key:value</b> pairs.
• The first key should be <b>parameters:</b> and then the remaining required key/value pairs for the topology.
This table lists all required key:value pairs.
<table>
<tr><th>Key Name</th><th>Type</th><th>Description</th></tr>
<tr><td>numPrimaryNoams</td><td>number</td><td>The number of NOAMs that receive and load DSR topology information.
<b><i>Note</i></b>: In DSR 8.2, use 1 as valid value.
This NOAM represents active NOAM.</td></tr>
</table>
</td></tr>
</table>

Procedure 10. Create OpenStack Parameter File for NOAM

numNoams	number	The number of NOAMs in the DSR topology other than primary NOAM. ***Note***: In DSR 8.2, use 1 as valid value. This NOAM represents standby NOAM.
noamImage	string	The VM image for the NOAM. ***Note***: This image is used for both active and standby NOAMs.
noamFlavor	string	The flavor that defines the VM size for the NOAM. ***Note***: This flavor is used for both active and standby NOAMs.
primaryNoamVmNames	comma_delimited_list	List of Primary NOAM VM names ***Note***: Number of VMnames must be equal to the numPrimaryNoams value.
noamVmNames	comma_delimited_list	List of NOAM VM names other than primary NOAM VMs. ***Note***: Number of VMnames must be equal to the numNoams value.
noamAZ	string	The availability zone into which NOAM servers should be placed. ***Note***: In DSR 8.2, all NOAM servers are placed in the same availability zone.
noamSG	string	The server group where NOAMs at this site belong.
xmiPublicNetwork	string	External management interface.
imiPrivateNetwork	string	Internal management interface.
imiPrivateSubnet	string	Name of the the IMI network.
imiPrivateSubnetCidr	string	The address range for the subnet.
ntpServer	string	IP of the NTP server.
Note: The below 3 keys are ONLY applicable for fixed IP scenario.		

Procedure 10. Create OpenStack Parameter File for NOAM

primaryNoamXmiIps	comma_delimited_list	Previously reserved IP for the primary NOAM to talk to external devices.
noamXmiIps	comma_delimited_list	Previously reserved IP for non-primary NOAMs to talk to external devices.
noamVip	string	VIP for NOAMs.

Procedure 11. Create OpenStack Parameter File for Signaling

S T E P #	This procedure manually creates the input parameters file to provide while deploying signaling stacks. **Prerequisite**: All the respective infrastructures has to be up and running. 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 OpenStack server CLI	Log into the OpenStack CLI.
2. □	Create the parameter file	1. Go to the folder created in Procedure 9, step 4. for storing the templates. 2. Create an empty signaling parameter file in this folder following this naming convention to identify the purpose of the file. <DSR Name>_<Site Name>_SignalingNode_Params.yaml For example: dsrCloudInit_Site00_SignalingNode_Params.yaml
3. □	Sample file	Refer to Appendix J.1 Example Template File for a sample file with values. ***Note***: It is important to keep the example file ready since this helps you understand the use of each key value pair described in the next step while creating the parameter file.
4. □	Populate the parameters file	Refer to Appendix J.1 Example Template File to create the parameter file in YAML format. ***Note***: Follow these guidelines while working with the YAML files. • The file must end with .yaml extension. • YAML must be case-sensitive and indentation-sensitive. • YAML does not support the use of tabs. Instead of tabs, it uses spaces. • This file is in YAML format and it contains **key:value** pairs. • The first key should be **parameters:** and then the remaining required key/value pairs for the topology. This table lists all required key:value pairs.

Key Name	Type	Description
numSoams	number	The number of SOAMs at this signaling node.
soamImage	string	The VM image for an SOAM.

Procedure 11. Create OpenStack Parameter File for Signaling

soamFlavor	string	The flavor that defines the VM size for an SOAM.
soamVmNames	comma_delimited_list	List of SOAM VM names.
soamAZ	string	The availability zone into which SOAM servers should be placed ***Note***: In DSR 8.2, all SOAM servers are placed in the same availability zone
soamSG	string	Server group for the SOAM VMs.
numDas	number	The number of DAs at this signaling node.
daImage	string	The VM image for a DA.
daFlavor	string	The flavor that defines the VM size for a DA.
daVmNames	comma_delimited_list	List of DA VM names.
daAZ	string	The availability zone into which DA servers should be placed. ***Note***: In DSR 8.2, all DA-MP servers are placed in the same availability zone.
daSG	string	Server group for the DA VMs.
daProfileName	string	The MP profile to be applied to all DAs. Possible values are: VM_Relay, VM_Database, VM_MDIWF, VM_6K_Mps, VM_8K_Mps, VM_10K_Mps, VM_12K_Mps, VM_14K_Mps, VM_16K_Mps, VM_18K_Mps, VM_21K_Mps, VM_24K_Mps, VM_27K_Mps, VM_30K_Mps
numIpfes	number	The number of IPFEs at this signaling node.
ipfeImage	string	The VM image for an IPFE.
ipfeFlavor	string	The flavor that defines the VM size for an IPFE.
ipfeVmNames	comma_delimited_list	List of IPFE VM names.
ipfeAZ	string	The availability zone into which IPFE servers should be placed. ***Note***: In DSR 8.2, all IPFE servers are placed in the same availability zone.

Procedure 11. Create OpenStack Parameter File for Signaling

ipfeSGs	comma_delimited_list	Server group for each IPFE VM.
numStps	number	The number of STPs at this signaling node.
stpImage	string	The VM image for an STP.
stpFlavor	string	The flavor that defines the VM size for an STP.
stpVmNames	comma_delimited_list	List of STP VM names.
stpAZ	string	The availability zone into which STP servers should be placed. ***Note***: In DSR 8.2, all STP servers are placed in the same availability zone.
stpSG	string	Server group for the STP VMs.
xmiPublicNetwork	string	External management interface.
imiPrivateNetwork	string	Internal management interface.
imiPrivateSubnet	string	Name of the IMI network.
imiPrivateSubnetCidr	string	The address range for the subnet.
xsiPublicNetwork	string	External signaling interface.
primaryNoamVmName	string	Name of NOAM VM that the config XML was loaded onto ***Note***: NOT used in 8.2. In DSR 8.2, user should NOT provide any value to this key.
noamXmiIps	comma_delimited_list	The XMI IPs for all NOAM servers, excluding VIPs. ***Note***: NOT used in 8.2. In DSR 8.2, user should NOT provide any value to this key.
ntpServer	string	IP of the NTP server.
Note: The below keys are ONLY applicable for the fixed IP scenario with or without IDIH nodes.		
soamXmiIps	comma_delimited_list	Previously reserved IP for non-primary SOAMs to talk to external devices.
soamVip	string	VIP for SOAMs.

Procedure 11. Create OpenStack Parameter File for Signaling

daXmiIps	comma_delimited_list	Previously reserved IP for DA MP to talk to external devices.
daXsiIps	comma_delimited_list	Previously reserved IP for DA MP to talk to signaling devices.
ipfeXmiIps	comma_delimited_list	Previously reserved IP for IPFE to talk to external devices.
ipfeXsiIps	comma_delimited_list	Previously reserved IP for IPFE to talk to signaling devices.
ss7XmiIps	comma_delimited_list	Previously reserved IP for SS7 to talk to external devices.
ss7XsiIps	comma_delimited_list	Previously reserved IP for SS7 to talk to signaling devices.
stpXmiIps	comma_delimited_list	Previously reserved IP for STP to talk to external devices.
stpXsiIps	comma_delimited_list	Previously reserved IP for STP to talk to signaling devices.
ipfeXsiPublicIp	string	Reserved single IP address on signaling network to which remote diameter hosts route packets for load balancing over set of message processors.
stpSctpPorts	comma_delimited_list	The SCTP ports to be associated with STP. ***Note***: If there is no STP in topology then provide empty list, for example, [ ] ***Note***: Open these ports beforehand on which STP connections are going to be created while doing configuration.
These two parameters are applicable for TCP/SCTP to use with the Diameter connection. ***Note***: Open these ports beforehand on which Diameter connections are going to be created while doing Diameter configuration.		
diameterTcpPorts	comma_delimited_list	The TCP ports to be associated with. If this parameter is not provided, then default ports are assigned.
diameterSctpPorts	comma_delimited_list	The SCTP ports to be associated with. If this parameter is not provided, then default ports are assigned.
Note: The below keys are applicable only for scenarios that include IDIH nodes.		

Procedure 11. Create OpenStack Parameter File for Signaling

idihAppImage	string	The VM image for the IDIH application VM.
idihAppFlavor	string	The flavor that defines the size for the IDIH application VM.
idihAppVmName	string	The IDIH Mediation VM name.
idihMedImage	string	The flavor that defines the size for the IDIH Mediation VM.
idihMedVmName	string	The IDIH Mediation VM name.
idihDbImage	string	The VM image for the IDIH database VM.
idihDbFlavor	string	The flavor that defines the size for the IDIH database VM.
idihDbVmName	string	The IDIH database VM name.
idihAZ	string	The availability zone into which IDIH VMs should be placed.
idihIntPrivateNetwork	string	Name of the internal tenant network (that is created) for communication between IDIH VMs.
idihIntPrivateSubnet	string	Name of the subnet (that is created) on the IDIH internal tenant network (idihIntPrivateNetwork).

Note: The below keys are applicable only for the fixed IP scenario with IDIH nodes.

idihDbXmiIp	string	Previously reserved IP for IDIH-DB to talk to external devices.
idihMedXmiIp	string	Previously reserved IP for IDIH-Mediation to talk to external devices.
idihAppXmiIp	string	Previously reserved IP for IDIH-Application to talk to external devices.

Note: At least one is mandatory (either TCP/SCTP parameter). Refer to this table to determine the valid combinations for SCTP/TCP port configurations.

diameterTcpPorts	diameterSctpPorts	Is Valid?
[]	[]	NO
[“”]	[“”]	NO
[“<port(s)>”]	[]	YES
[]	[“<port(s)>”]	YES
[“<port(s)>”]	[“<port(s)>”]	YES

Note: Repeat steps 2 and 3 of this procedure for each additional site.

4.3 Deploy HEAT Templates

Procedure 12. Deploy HEAT Templates

S T E P #	This procedure instructs how to deploy HEAT templates to create NOAM and Signaling stacks. **Prerequisite**: All the respective infrastructures has to be up and running. The required input files are all available. 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. □	Login to OpenStack server CLI	Log into the OpenStack CLI.
2. □	Prepare the input files required for the deployment	To create NOAM and signaling stacks, provide these input files as parameters while deploying the HEAT templates. **Template Files** With respect to the deployment scenario decided in Procedure 9, step 2. , the template files for NOAM and signaling stacks have been already determined. **Environment Files** With respect to the deployment scenario decided in Procedure 9, step 2. , the environment files for NOAM and signaling stacks have been already determined. **Parameter Files** The parameter file for NOAM has already been created in Procedure 10. The parameter file for signaling has already been created in Procedure 11.

3.
□
	Deploy NOAM stack	Execute the OpenStack command to create NOAM stack using the three input files. Make sure the template and environment files are selected with respect to NOAM stack as per in Procedure 9, step 2.
		`openstack stack create -e <EnvironmentFileForNOAM.yaml>  -e <ParameterFileForNOAM.yaml> -t <TemplateFileForNOAM> <NOAMStackName>`
		Example for VIP scenario:
		`$ openstack stack create -e dsrResources_provider.yaml  -e SinglesiteProvider_Site00_NetworkOam_Params.yaml -t dsrNetworkOam_provider.yaml SinglesiteProvider_Site00_NetworkOam`

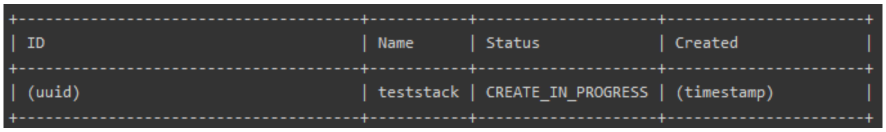
4.
□
	Deploy signaling stack	Execute the OpenStack command to create signaling stack using the three input files. Make sure the template and environment files are selected with respect to signaling stack as per in Procedure 9, step 2.
		`openstack stack create -e <EnvironmentFileForSignaling.yaml>  -e <ParameterFileForSignaling.yaml> -t <TemplateFileForSignaling> <SignalingStackName>`
		Example for VIP scenario:
		`$ openstack stack create -e dsrResources_provider.yaml  -e SinglesiteProvider_Site00_SignalingNode_Params.yaml -t dsrSignalingNode_provider.yaml SinglesiteProvider_Site00_Signaling`

Procedure 12. Deploy HEAT Templates

5. □ Verify the stack creation status

1. Execute this command to see the stack creation status.

```
$ openstack stack show <stackname>
```

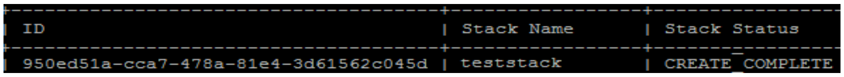


```
+------------------------------------+-----------+-------------------+----------------------+
| ID                                 | Name      | Status            | Created              |
+------------------------------------+-----------+-------------------+----------------------+
| (uuid)                             | teststack | CREATE_IN_PROGRESS | (timestamp)         |
+------------------------------------+-----------+-------------------+----------------------+
```

It takes about 2 minutes to complete the creation.

2. Execute the command again to verify the status.

```
$ openstack stack show <stackname>
```

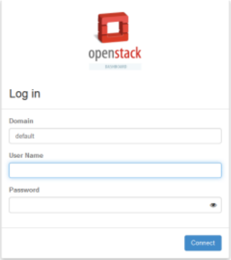


```
+--------------------------------------+-------------------+------------------
| ID                                   | Stack Name        | Stack Status
+--------------------------------------+-------------------+------------------
| 950ed51a-cca7-478a-81e4-3d61562c045d | teststack         | CREATE_COMPLETE
```

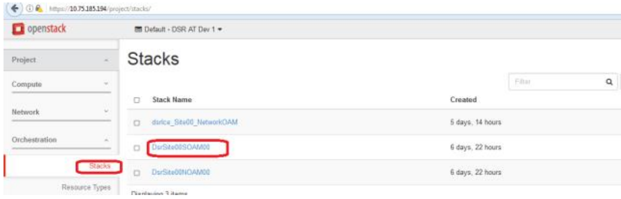
Procedure 12. Deploy HEAT Templates

6. □ Retrieve required IPs from created stacks

1. Log into the OpenStack GUI with valid credentials.



2. Navigate to **Project > Orchestration** and click **Stacks**.

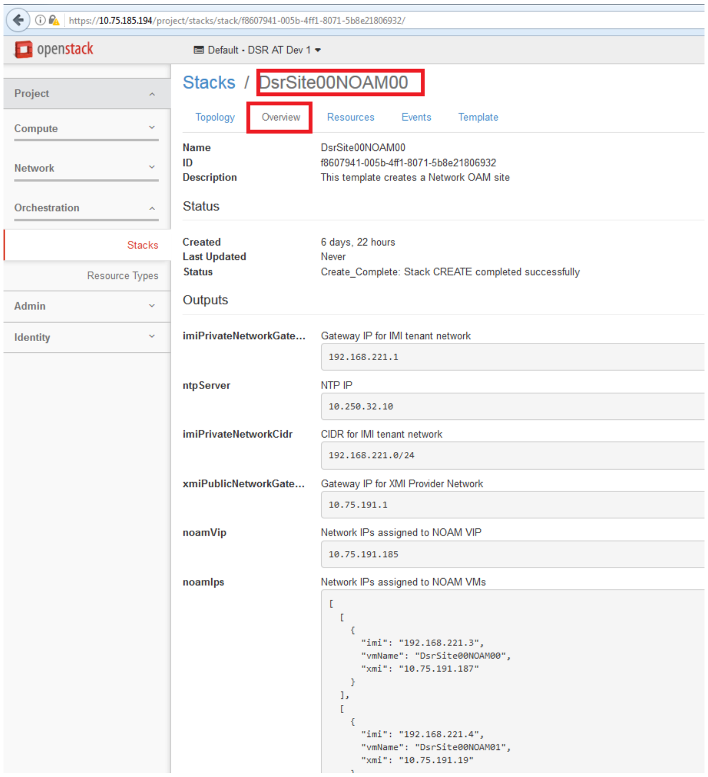


Stacks

Stack Name	Created
dsrlce_Site00_NetworkOAM	5 days, 14 hours
DsrSite00SOAM00	6 days, 22 hours
DsrSite00NOAM00	6 days, 22 hours

Displaying 3 items

3. Select the stack you created (<stackname>) and click **Overview** to see the IP details of the stack.



Name DsrSite00NOAM00
ID f8607941-005b-4ff1-8071-5b8e21806932
Description This template creates a Network OAM site

Status

Created 6 days, 22 hours
Last Updated Never
Status Create_Complete: Stack CREATE completed successfully

Outputs

imiPrivateNetworkGate... Gateway IP for IMI tenant network

```
192.168.221.1
```

ntpServer NTP IP

```
10.250.32.10
```

imiPrivateNetworkCidr CIDR for IMI tenant network

```
192.168.221.0/24
```

xmiPublicNetworkGate... Gateway IP for XMI Provider Network

```
10.75.191.1
```

noamVip Network IPs assigned to NOAM VIP

```
10.75.191.185
```

noamIps Network IPs assigned to NOAM VMs

```
[
  [
    {
      "imi": "192.168.221.3",
      "vmName": "DsrSite00NOAM00",
      "xmi": "10.75.191.187"
    }
  ],
  [
    {
      "imi": "192.168.221.4",
      "vmName": "DsrSite00NOAM01",
      "xmi": "10.75.191.19"
```

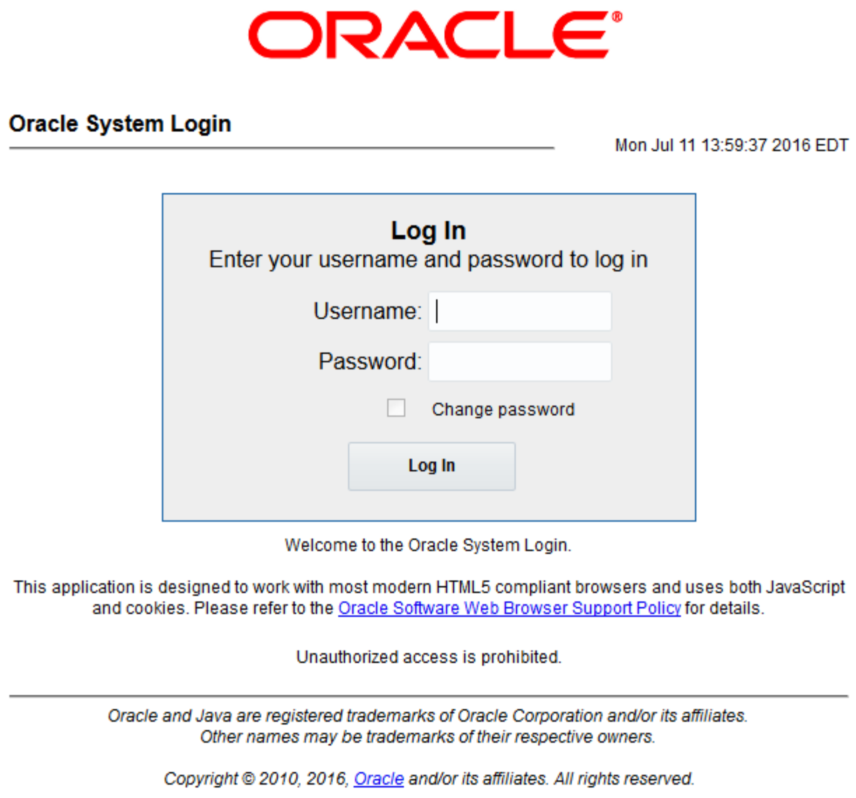
Note:

- All NOAM IP information displays in the NOAM stack (<NOAMStackName>).
- All signaling IP information displays in the signaling stack (<SignalingStackName>).

4. Retrieve the IP details for DSR configuration.

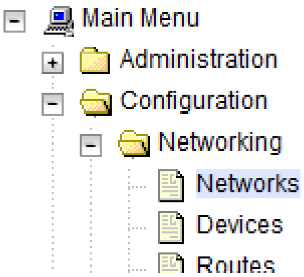
5. Application Configuration

Procedure 13. Configure the First NOAM NE and Server

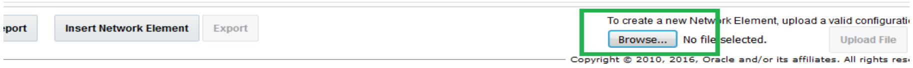
STEP #	This procedure configures the first NOAM VM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**NOAM GUI**: Login	Establish a GUI session as the **guiadmin** user on the NOAM server by using the XMI IP address.  ORACLE® **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 13. Configure the First NOAM NE and Server

<table>
<tr>
<td>2.
□</td>
<td><b>NOAM GUI</b>: Create the NOAM network element using the XML file</td>
<td>
1. Navigate to <b>Configuration > Networking > Networks</b>.

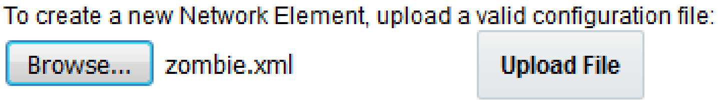


2. Click <b>Browse</b> and type the pathname of the NOAM network XML file.



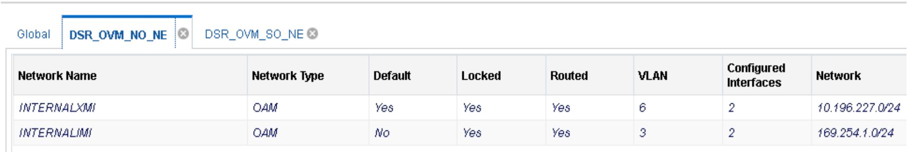
To create a new Network Element, upload a valid configurati
No file selected.
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights res

3. 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.



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

4. Once the data has been uploaded, you should see a tabs display with the name of your network element. Click on this tab which describes the individual networks that are now configured.



<table>
<tr><th>Network Name</th><th>Network Type</th><th>Default</th><th>Locked</th><th>Routed</th><th>VLAN</th><th>Configured Interfaces</th><th>Network</th></tr>
<tr><td>INTERNALXMI</td><td>OAM</td><td>Yes</td><td>Yes</td><td>Yes</td><td>6</td><td>2</td><td>10.196.227.0/24</td></tr>
<tr><td>INTERNALIMI</td><td>OAM</td><td>No</td><td>Yes</td><td>Yes</td><td>3</td><td>2</td><td>169.254.1.0/24</td></tr>
</table>
</td>
</tr>
</table>

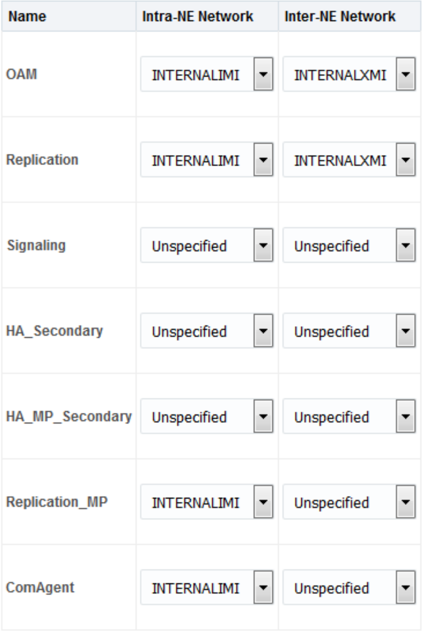
Procedure 13. Configure the First NOAM NE and Server

3. □ **NOAM GUI**: Map services to networks

1. Navigate to **Configuration > Networking > Services**.
2. Click **Edit** and set the services as shown in the table below:

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

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

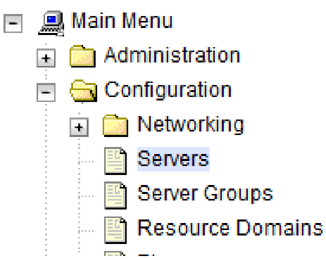


Name	Intra-NE Network	Inter-NE Network
OAM	INTERNALIMI	INTERNALXMI
Replication	INTERNALIMI	INTERNALXMI
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	INTERNALIMI	Unspecified
ComAgent	INTERNALIMI	Unspecified

3. Click **OK** to apply the Service-to-Network selections. Dismiss any possible popup notifications.

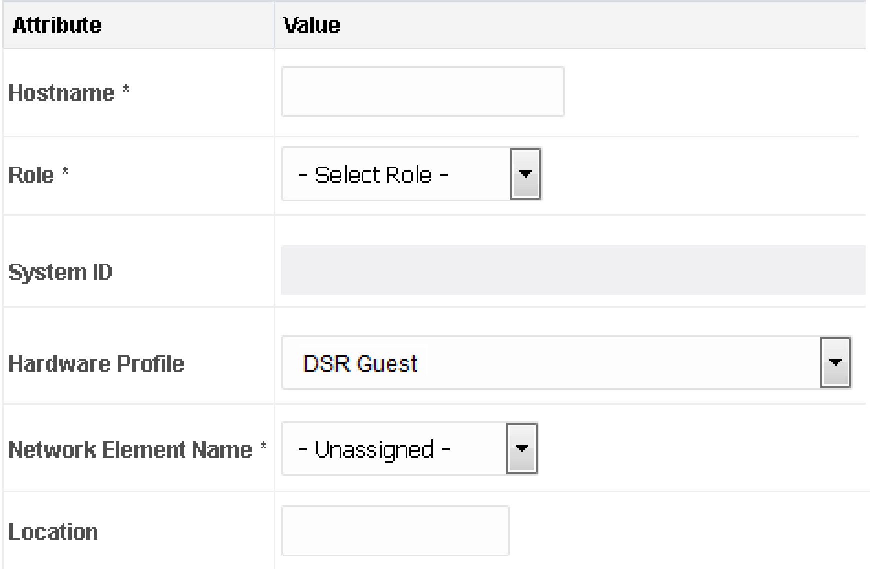
4. □ **NOAM GUI**: Insert the 1st NOAM VM

1. Navigate to **Configuration > Servers**.



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

Procedure 13. Configure the First NOAM NE and Server



Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

3. Fill in the fields as follows:

   Hostname: <Hostname>

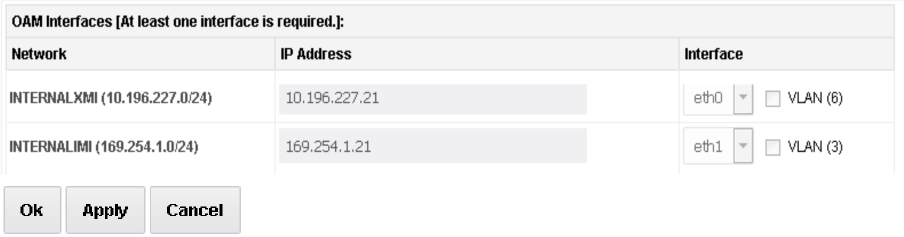
   Role: NETWORK OAM&P

   System ID: <Site System ID>

   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.



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 □ VLAN (3)

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

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

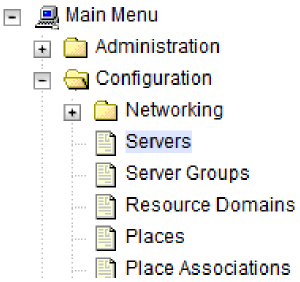
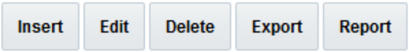
6. Add the following NTP servers:

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

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

Note: Properly configure the NTP on the controller node to reference lower stratum NTP servers.

Procedure 13. Configure the First NOAM NE and Server

5. □	**NOAM GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. 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.
□
	NOAM Server: Copy configuration file to 1st NOAM server	1. Obtain a terminal window to the 1st NOAM server, logging in as the **admusr** user.
		2. Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the 1st NOAM to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		`$ sudo cp`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh`
		`/var/tmp/TKLCConfigData.sh`

7. □	**First SOAM Server**: 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.
□
	First SOAM Server: 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.

Procedure 13. Configure the First NOAM NE and Server

9.
□
	First NOAM Server: Verify server health	1. Log into the NOAM1 as the **admusr** user.
		2. Execute the following command as admusr on the 1st NOAM 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`

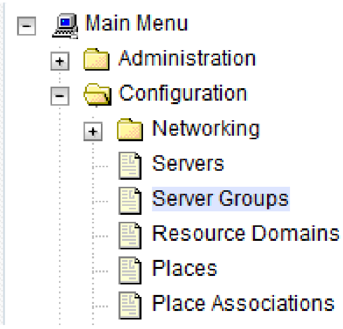
Procedure 14. Configure the NOAM Server Group

STEP #	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, click **Continue to this Website** to proceed.

Procedure 14. Configure the NOAM Server Group

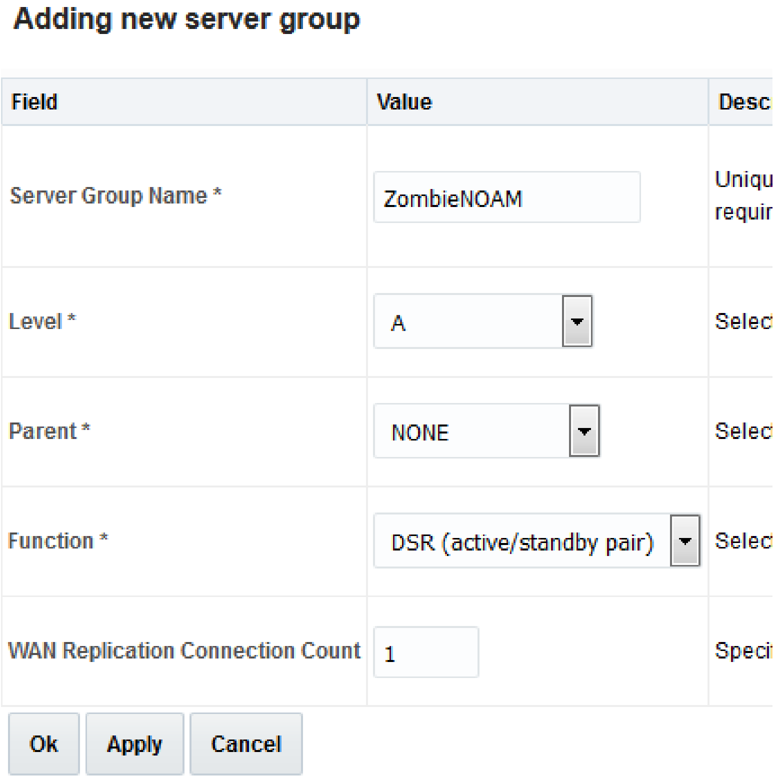
2. □ **NOAM GUI**: Enter NOAM server group data

1. Navigate to **Configuration > Server Groups**.



2. Click **Insert** and fill in 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



Adding new server group

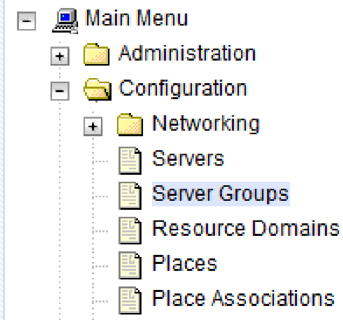
Field	Value	Desc
Server Group Name *	ZombieNOAM	Uniqu requir
Level *	A	Selec
Parent *	NONE	Selec
Function *	DSR (active/standby pair)	Selec
WAN Replication Connection Count	1	Speci

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

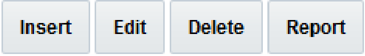
Procedure 14. Configure the NOAM Server Group

3. □ **NOAM GUI**: Edit the NOAM Server Group

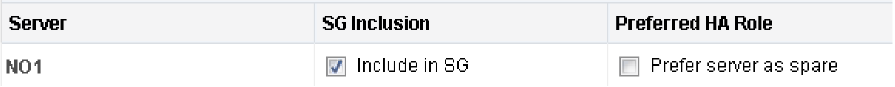
1. Navigate to **Configuration > Server Groups**.



2. Select the new server group and click **Edit**.



Select the network element that represents the NOAM.



Server	SG Inclusion	Preferred HA Role
NO1	☑ Include in SG	□ Prefer server as spare

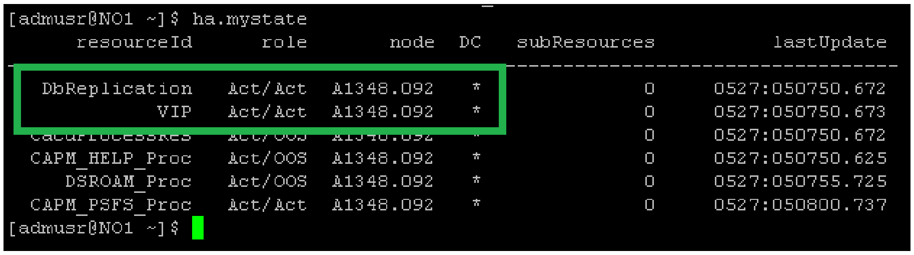
3. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the **Include in SG** checkbox.
4. Leave other boxes unchecked.
5. Click **OK**.

4. □ **NOAM Server**: Verify NOAM VM role

1. From console window of the first NOAM VM, 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.

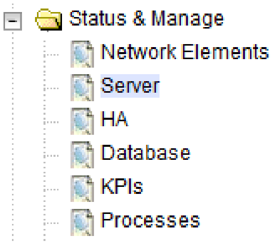
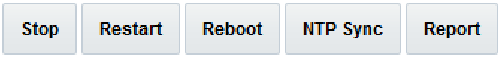
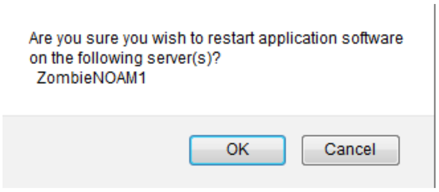
   You may have to wait a few minutes for it to be in that state.
2. Press **Ctrl+C** to exit.

   Example:



```
[admusr@NO1 ~]$ ha.mystate
      resourceId        role         node  DC   subResources          lastUpdate
-----------------------------------------------------------------------------------
     DbReplication    Act/Act   A1348.092   *              0     0527:050750.672
               VIP    Act/Act   A1348.092   *              0     0527:050750.673
    CacdProcessRes    Act/OOS   A1348.092   *              0     0527:050750.672
    CAPM_HELP_Proc    Act/OOS   A1348.092   *              0     0527:050750.625
       DSROAM_Proc    Act/OOS   A1348.092   *              0     0527:050755.725
    CAPM_PSFS_Proc    Act/Act   A1348.092   *              0     0527:050800.737
[admusr@NO1 ~]$
```

Procedure 14. Configure the NOAM Server Group

5. □	**NOAM GUI**: Restart 1st NOAM VM	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first NOAM server. Click **Restart**.  3. Click **OK** on the confirmation screen and wait for restart to complete. Are you sure you wish to restart application software on the following server(s)? ZombieNOAM1

6.
□
	NOAM Server: Set sysmetric thresholds for VMs.
	Note: These commands disable the message rate threshold alarms
		From console window of the first NOAM VM, execute the **iset** commands as **admusr**.
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RoutingMsgRate' and function='DIAM'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxRbarMsgRate' and function='RBAR'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxFabrMsgRate' and function='FABR'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxCpaMsgRate' and function='CPA'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxDmiwfMsgRate' and function='DM-IWF'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxMdIwfIngressMsgRate' and function='MD-IWF'"`

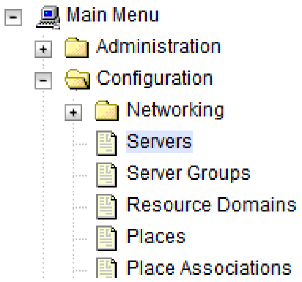
Procedure 15. Configure the Second NOAM Server

S T E P #	This procedure configures the second NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**NOAM GUI**: Login	1. If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type **http://<NO1_XMI_IP_Address>** as the URL. 2. Login as the **guiadmin** user.

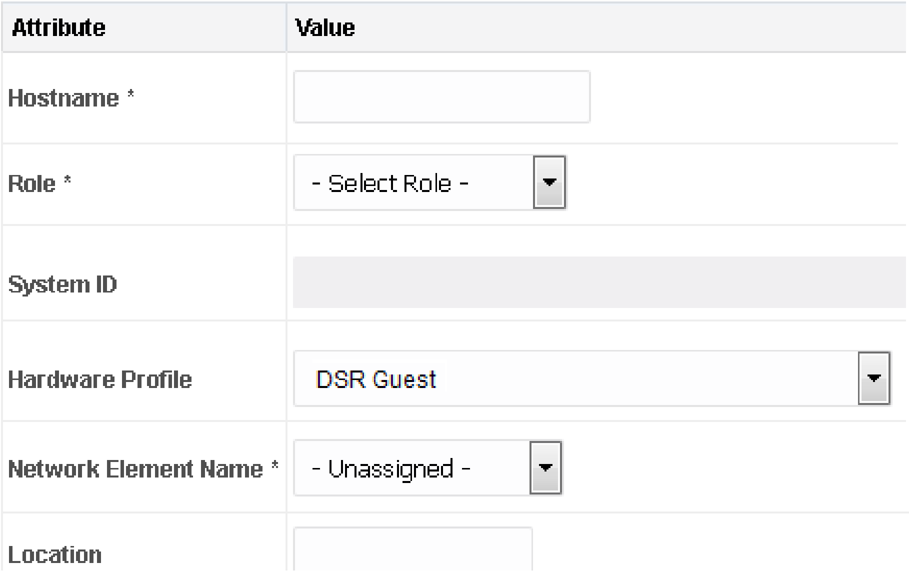
Procedure 15. Configure the Second NOAM Server

2. □ **NOAM GUI**: Insert the 2nd NOAM VM

1. Navigate to **Configuration > Servers**.



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

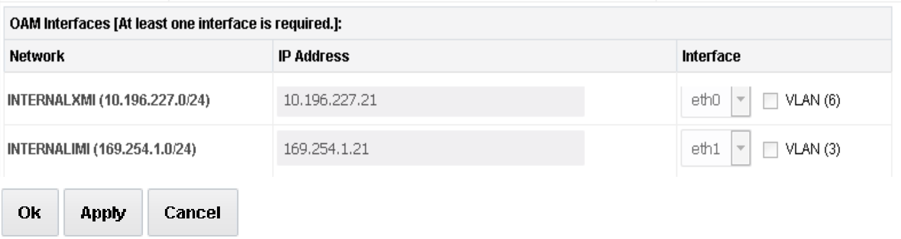


Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

3. Fill in the fields as follows:

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

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

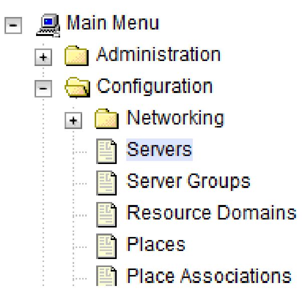


OAM Interfaces [At least one interface is required.]:

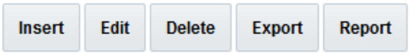
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 □ VLAN (3)

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

Procedure 15. Configure the Second NOAM Server

<table>
<tr><td></td><td></td><td>5. Fill in the server IP addresses for the IMI network. Select <b>ethX</b> for the interface. Leave the <b>VLAN</b> checkbox unmarked.
6. 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>7. Click <b>OK</b> when you have completed entering all the server data.
<b><i>Note</i></b>: Properly configure the NTP on the controller node to reference lower stratum NTP servers.</td></tr>
<tr><td>3.
□</td><td><b>NOAM GUI</b>: Export the initial configuration</td><td>1. Navigate to <b>Configuration > Servers</b>.


Main Menu
Administration
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. From the GUI screen, select server just configured 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><b>First NOAM Server</b>: Copy configuration file to 2nd NOAM server</td><td>1. Obtain a terminal session to the 1st NOAM as the <b>admusr</b> user.
2. Login as the <b>admusr</b> user to the NO1 shell and issue the following commands:
<code>$ sudo scp</code>
<code>/var/TKLC/db/filemgmt/TKLCConfigData.<hostname&gt;.sh</code>
<code>admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh</code>
<b><i>Note</i></b>: ipaddr is the IP address of NOAM2 assigned to its ethx interface associated with the xmi network.</td></tr>
</table>

Procedure 15. Configure the Second NOAM Server

5. □	**Second NOAM Server**: Wait for configuration to complete	1. 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. 2. 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. 3. 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. □	**Second NOAM Server**: Reboot the server	Obtain a terminal session to the 2nd NOAM as the **admusr** user. `$ sudo init 6` Wait for server to reboot.

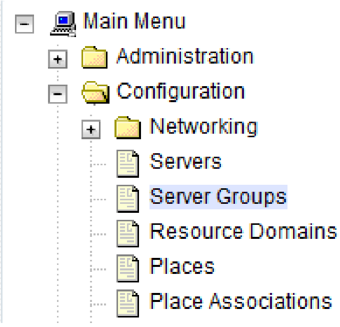
7.
□
	Second NOAM Server: Verify server health	1. Log into the NOAM2 as **admusr** and wait.
		2. Execute the following command as super-user on the 2ndt NO server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`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 16. Complete Configuring the NOAM Server Group

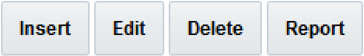
STEP #	
	This procedure finishes configuring the NOAM Server Group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. □ **NOAM GUI**: Edit the NOAM Server Group Data

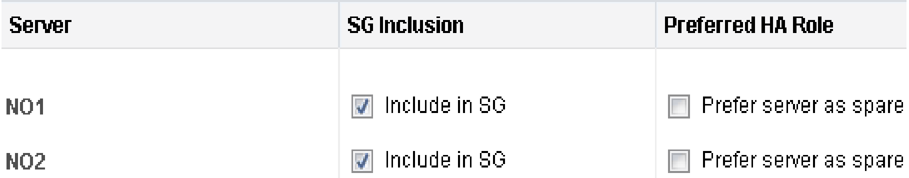
1. From the GUI session on the first NOAM server, navigate to **Configuration > Server Groups**.



2. Select the NOAM server group and click **Edit**.

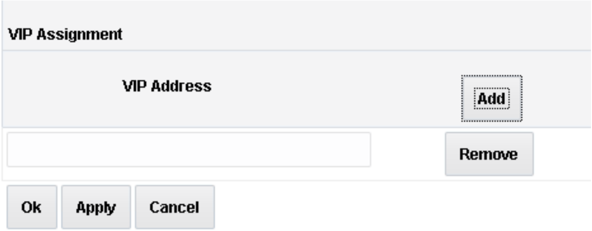


3. Add the second NOAM server to the server group by marking the **Include in SG** checkbox for the second NOAM server. Click **Apply**.

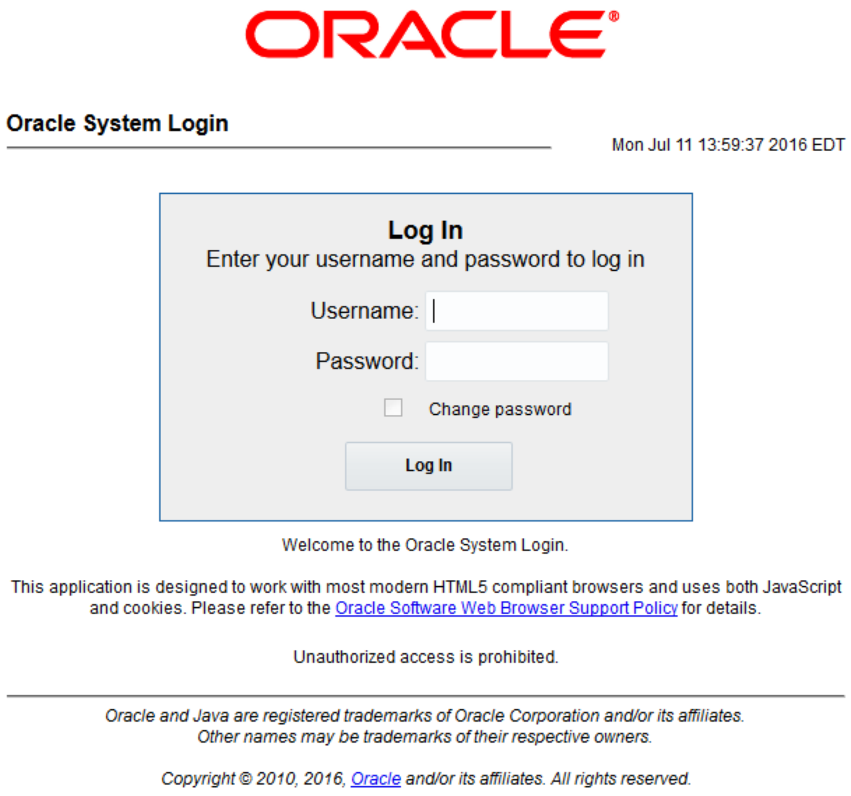


Server	SG Inclusion	Preferred HA Role
NO1	☑ Include in SG	□ Prefer server as spare
NO2	☑ Include in SG	□ Prefer server as spare

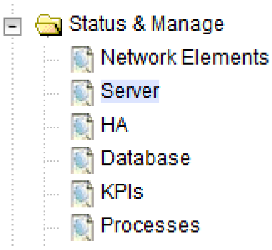
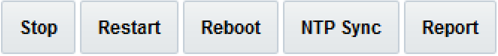
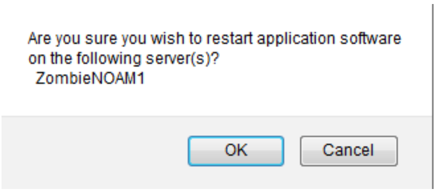
4. Click **Add** to add a NOAM VIP. Type the VIP Address and click **OK**.



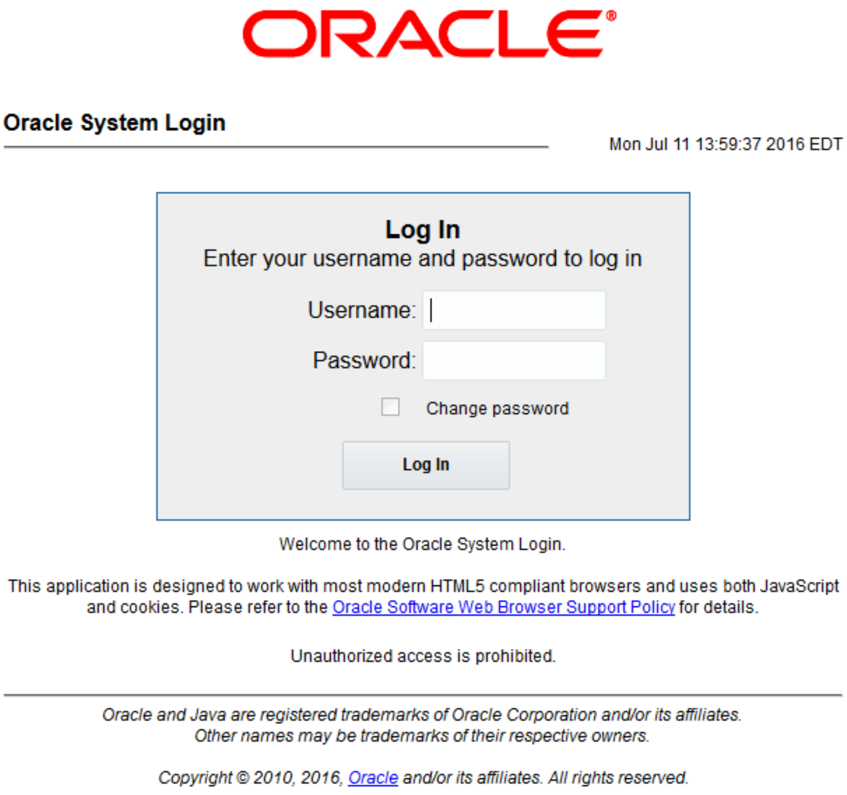
Procedure 16. Complete Configuring the NOAM Server Group

2. □	Establish GUI session on the NOAM VIP	Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.  ORACLE **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: | Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
3. □	Wait for remote database alarm to clear	Wait for the alarm ID 10200 **Remote Database re-initialization in progress** to be cleared before proceeding (**Alarms & Events > View Active**).

Procedure 16. Complete Configuring the NOAM Server Group

4. □	**NOAM GUI**: Restart 2nd NOAM VM	1. Navigate to **Status & Manage > Server** and select the second NOAM server.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Click **Restart**.  3. Click **OK** on the confirmation screen.  Are you sure you wish to restart application software on the following server(s)? ZombieNOAM1 Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the **Appl State** as **Enabled**.
5. □	SDS can now be installed (Optional)	If this deployment contains SDS, SDS can now be installed. Refer to document referenced in [6] SDS SW Installation and Configuration Guide.

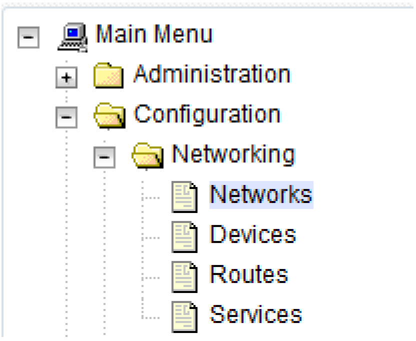
Procedure 17. Configure the DR NOAM NE and Server (Optional)

S T E P #	This procedure configures the first DR NOAM VM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Login	Establish a GUI session on the primary NOAM server by using the XMI VIP IP address.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

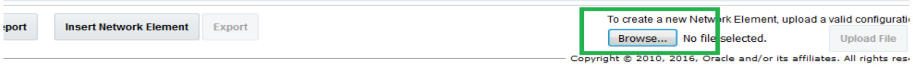
Procedure 17. Configure the DR NOAM NE and Server (Optional)

2. □ **Primary NOAM VIP GUI**: Create the DR NOAM network element using the XML file

1. Navigate to **Configuration > Networking > Networks**.

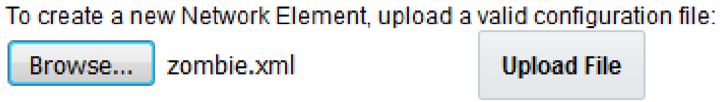


2. Click **Browse** and type the pathname to the NOAM network XML file.



To create a new Network Element, upload a valid configurati
No file selected.
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights res

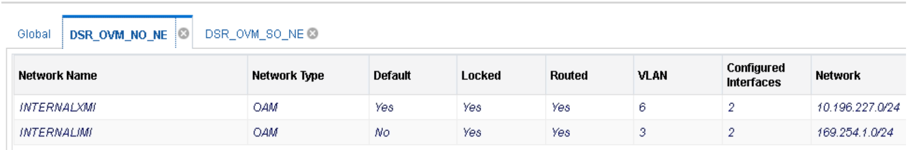
3. Click **Upload File** to upload the XML file.



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

See the examples in Appendix A Sample Network Element and Hardware Profiles and configure the NOAM network element.

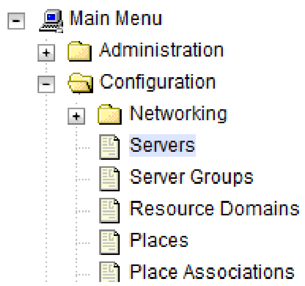
4. Once the data has been uploaded, you should see a tabs appear with the name of your network element. Click on this tab, which describes the individual networks that are now configured:



Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
INTERNALXMI	OAM	Yes	Yes	Yes	6	2	10.196.227.0/24
INTERNALIMI	OAM	No	Yes	Yes	3	2	169.254.1.0/24

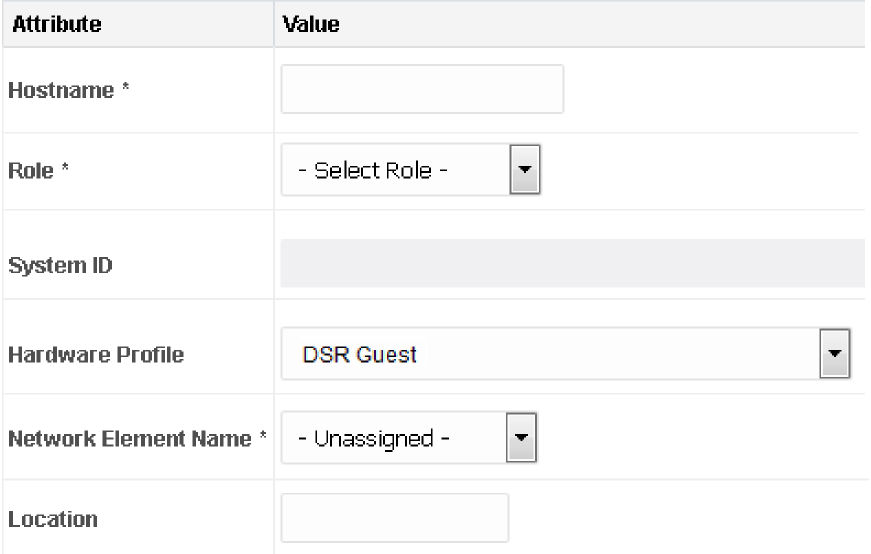
3. □ **Primary NOAM VIP GUI**: Insert the 1st DR NOAM VM

1. Navigate to **Configuration > Servers**.



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

Procedure 17. Configure the DR NOAM NE and Server (Optional)



Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

3. Fill in the fields as follows:

   Hostname: <Hostname>

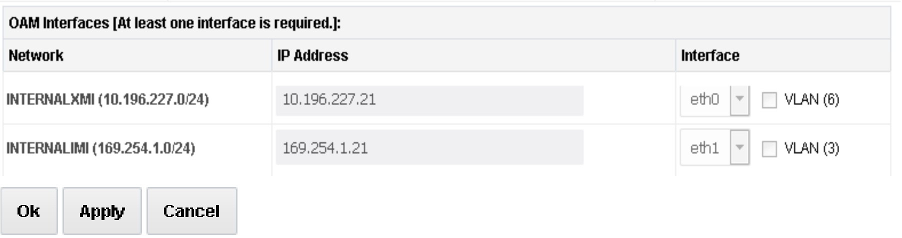
   Role: `NETWORK OAM&P`

   System ID: <Site System ID>

   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



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 □ VLAN (3)

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

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

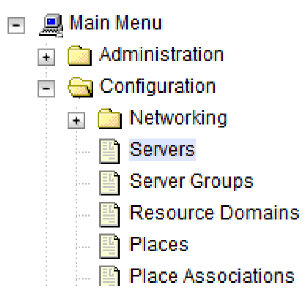
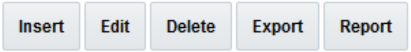
6. Add the following NTP servers:

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

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

Note: Properly configure the NTP on the controller node to reference lower stratum NTP servers.

Procedure 17. Configure the DR NOAM NE and Server (Optional)

4. □	**Primary NOAM VIP GUI**: Export the initial configuration	1. Navigate **to Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. 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. 
5. □	**Primary NOAM Server**: Copy configuration file to 1st NOAM server	1. Obtain a terminal window to the Primary NOAM server, logging in as the **admusr** user. 2. Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the 1st NOAM to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example: `$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh`
6. □	**First DR NOAM Server**: 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.
7. □	**First DR NOAM Server**: Reboot the server	Obtain a terminal window to the 1st DR NOAM server, logging in as the admusr user. `$ sudo init 6` Wait for server to reboot.

Procedure 17. Configure the DR NOAM NE and Server (Optional)

8.
□
	First DR NOAM Server: Verify server health	1. Obtain a terminal window to the 1st DR NOAM server, logging in as the **admusr** user.
		2. Execute the following command as admusr 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`

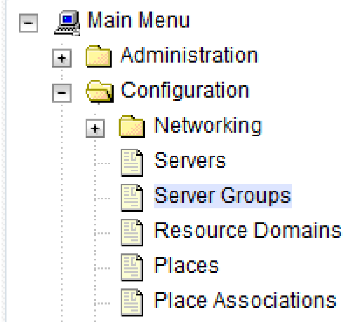
Procedure 18. Configure the DR NOAM Server Group (Optional)

S T E P #	This procedure configures the DR 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. □	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the primary 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. 2. Login as the **guiadmin** user. If prompted by a security warming, click **Continue to this Website** to proceed.

Procedure 18. Configure the DR NOAM Server Group (Optional)

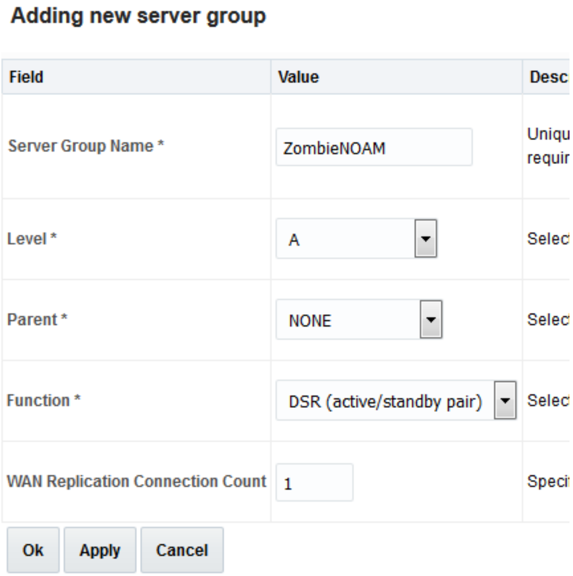
2. □ **Primary NOAM VIP GUI**: Enter DR NOAM server group data

1. Using the GUI session on the primary NOAM server, navigate to **Configuration > Server Groups**.



2. Click **Insert** and fill in 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



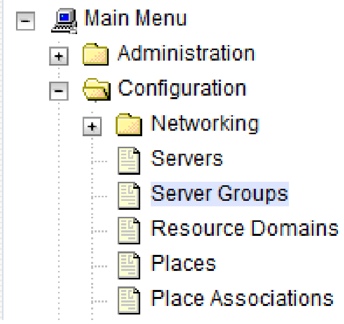
Adding new server group

Field	Value	Desc
Server Group Name *	ZombieNOAM	Uniqu requir
Level *	A	Selec
Parent *	NONE	Selec
Function *	DSR (active/standby pair)	Selec
WAN Replication Connection Count	1	Speci

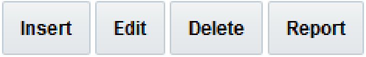
3. Click **OK** when all fields are filled in.

Procedure 18. Configure the DR NOAM Server Group (Optional)

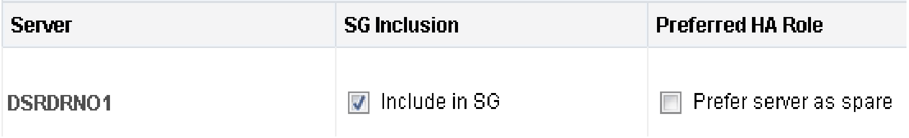
<table>
<tr>
<td>3.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Edit the DR NOAM server group</td>
<td>
1. Navigate to <b>Configuration > Server Groups</b>.



2. Select the new server group and click <b>Edit</b>.



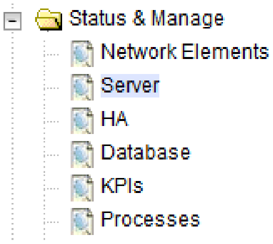
3. Select the network element that represents the DR NOAM.


<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>DSRDRNO1</td><td>☑ Include in SG</td><td>□ Prefer server as spare</td></tr>
</table>

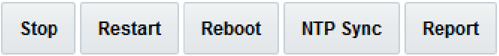
4. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the <b>Include in SG</b> checkbox.

5. Leave other boxes unchecked.

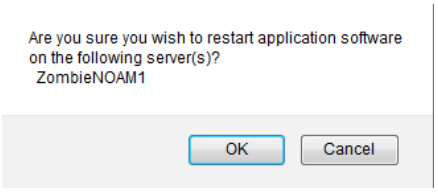
6. Click <b>OK</b>.
</td>
</tr>
<tr>
<td>4.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Restart 1st DR NOAM VM</td>
<td>
1. From the NOAM GUI, navigate to <b>Status & Manage > Server</b>.



2. Select the first NOAM server. Click <b>Restart</b>.



3. Click <b>OK</b> on the confirmation screen and wait for restart to complete.

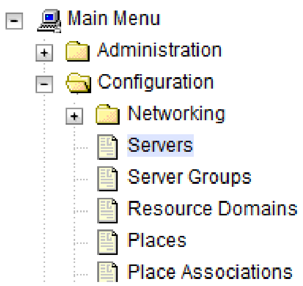

Are you sure you wish to restart application software on the following server(s)?
ZombieNOAM1

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

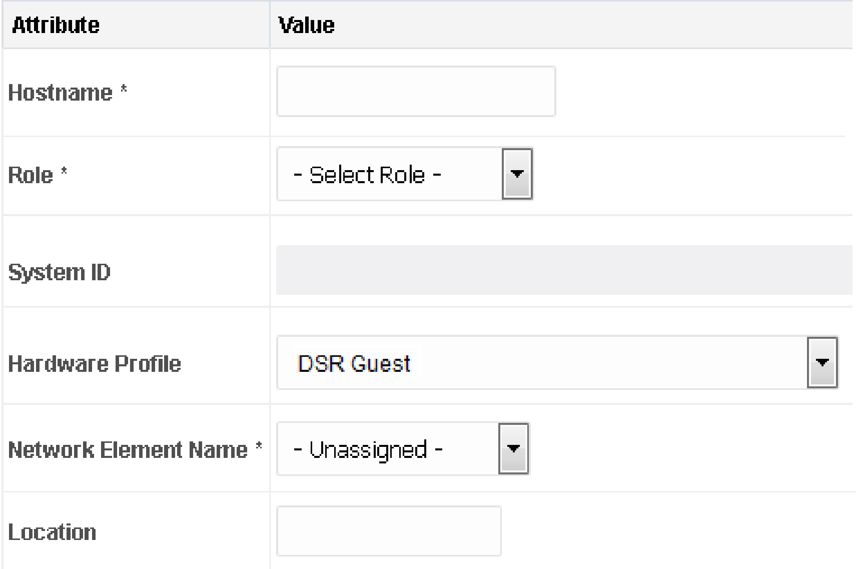
Procedure 18. Configure the DR NOAM Server Group (Optional)

5.
□
	NOAM Server: Set sysmetric threshold for VMs.
	Note: These commands disable the message rate threshold alarms
		From console window of the first NOAM VM, execute the **iset** commands as **admusr**.
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RoutingMsgRate' and function='DIAM'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxRbarMsgRate' and function='RBAR'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxFabrMsgRate' and function='FABR'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxCpaMsgRate' and function='CPA'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxDmiwfMsgRate' and function='DM-IWF'"`
		`$ sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxMdIwfIngressMsgRate' and function='MD-IWF'"`

Procedure 19. Configure the Second DR NOAM Server (Optional)

S **T** **E** **P** **#**	This procedure configures the second DR NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Login	1. 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://<NOAM1_XMI_IP_Address>** as the URL. 2. Login as the **guiadmin** user.
2. □	**Primary NOAM VIP GUI**: Insert the 2nd DR NOAM VM	1. Navigate to **Main Menu > Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert** to insert the new NOAM server into servers table (the first or second server).

Procedure 19. Configure the Second DR NOAM Server (Optional)

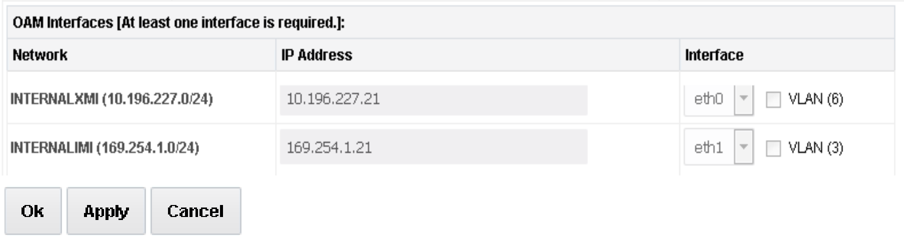


Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

3. Fill in the fields as follows:

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

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



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 □ VLAN (3)

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

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

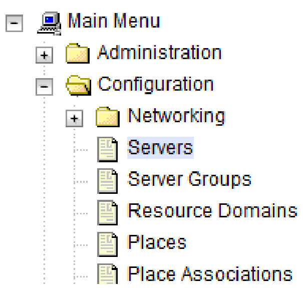
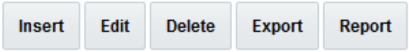
6. Add the following NTP servers:

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

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

Note: Properly configure the NTP on the controller node to reference lower

Procedure 19. Configure the Second DR NOAM Server (Optional)

		stratum NTP servers.
3. □	**Primary NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the server just configured and click **Export** to generate the initial configuration data for that server.  3. Go to the Info tab to confirm the file has been created.

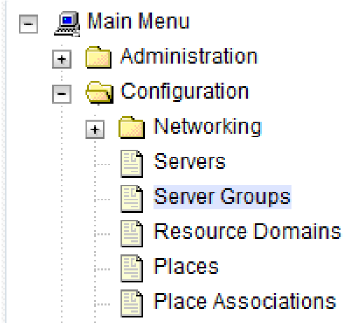
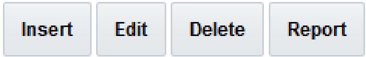
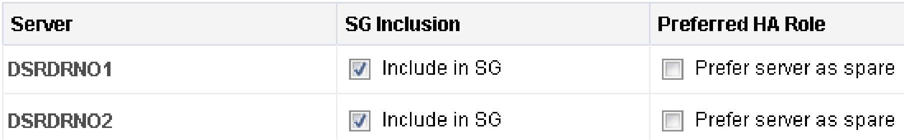
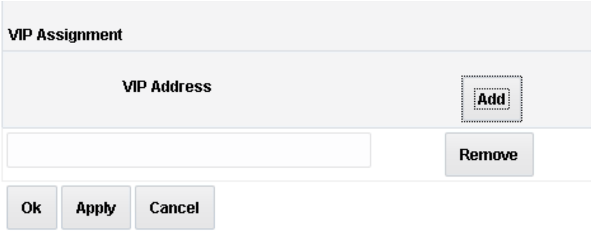
4.
□
	Primary NOAM: Copy configuration file to 2nd DR NOAM server	1. Obtain a terminal session to the primary NOAM as the **admusr** user.
		2. Login as the **admusr** user to the NOAM1 shell and issue the following commands:
		`$ sudo scp`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh`
		`admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh`
		Note: ipaddr is the IP address of DR NOAM assigned to its ethx interface associated with the XMI network.

5. □	**Second DR NOAM Server**: Wait for configuration to complete	1. Obtain a terminal session to the 2nd DR 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. 2. 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. 3. 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. □	**Second DR NOAM Server**: Reboot the server	Obtain a terminal session to the 2nd DR NOAM as the **admusr** user. `$ sudo init 6` Wait for server to reboot.

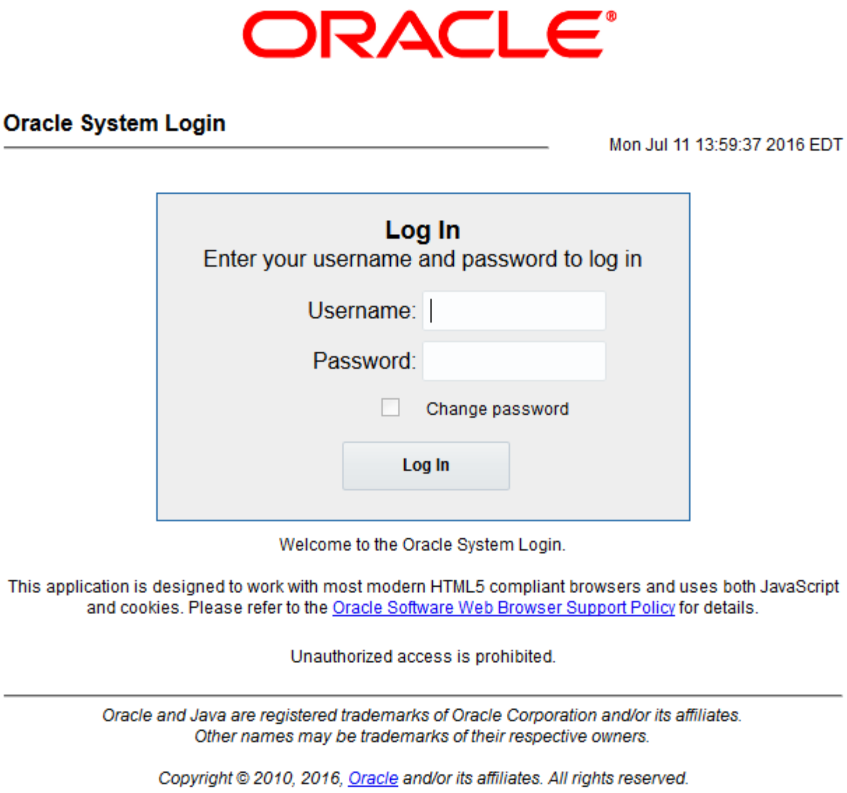
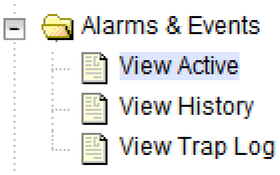
Procedure 19. Configure the Second DR NOAM Server (Optional)

7.
□
	Second DR NO Server: Verify server health	1. Obtain a terminal session to the **2nd** DR NOAM as the **admusr** user.
		2. Execute the following command as super-user 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`

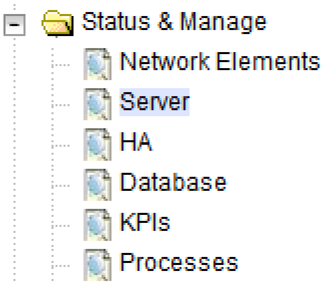
Procedure 20. Complete Configuring the DR NOAM Server Group (Optional)

STEP #	This procedure finishes configuring the DR 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. □	**PRIMARY NOAM VIP GUI**: Edit the DR NOAM server group data	1. From the GUI session on the primary NOAM server, navigate to **Configuration > Server Groups.**  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Select the NOAM server group and click **Edit**.  3. Add the second NOAM server to the server group by marking the **Include in SG** checkbox for the second NOAM server. Click **Apply**.  Server — SG Inclusion — Preferred HA Role DSRDRNO1 — ☑ Include in SG — □ Prefer server as spare DSRDRNO2 — ☑ Include in SG — □ Prefer server as spare 4. Click **Add** to add an NOAM VIP. Type the **VIP Address** and click **OK**.  VIP Assignment VIP Address

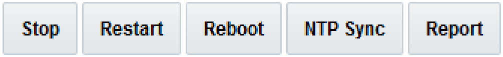
Procedure 20. Complete Configuring the DR NOAM Server Group (Optional)

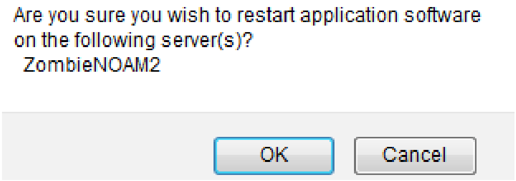
2. □	**Primary NOAM VIP GUI**: Establish GUI Session on the NOAM VIP	Establish a GUI session on the primary NOAM by using the NOAM VIP address. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
3. □	**Primary NOAM VIP GUI**: Wait for Remote Database Alarm to Clear	Wait for the alarm ID 10200 **Remote Database re-initialization in progress** to be cleared before proceeding (**Alarms & Events > View Active**).  Alarms & Events View Active View History View Trap Log

Procedure 20. Complete Configuring the DR NOAM Server Group (Optional)

<table>
<tr>
<td>4.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Restart 2nd DR NOAM VM</td>
<td>1. Navigate to <b>Status & Manage > Server</b> and select the second DR NOAM server.


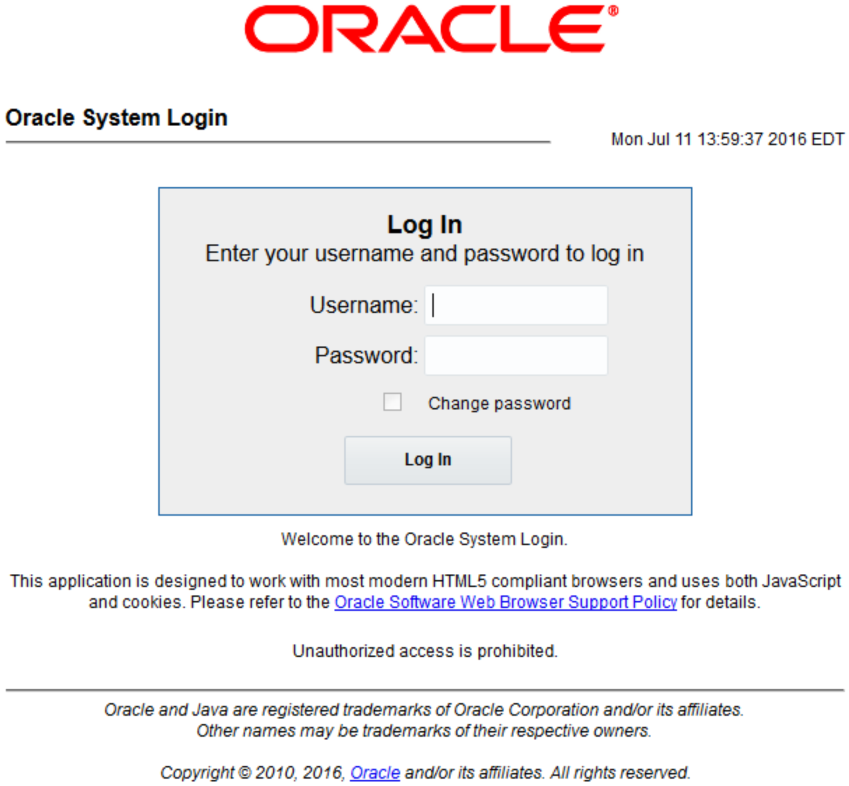
Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. Click <b>Restart</b>.


3. Answer <b>OK</b> on the confirmation screen.

Are you sure you wish to restart application software on the following server(s)?
ZombieNOAM2

Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the <b>Appl State</b> as <b>Enabled</b>.</td>
</tr>
<tr>
<td>5.
□</td>
<td><b>Primary NOAM</b>: Modify DSR OAM process</td>
<td>Establish an SSH session to the primary NOAM, login as the <b>admusr</b> user. Execute the following commands:
1. Retrieve the cluster ID of the DR-NOAM:
$ sudo iqt -NodeID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"
Server_ID   NodeID   ClusterID
1   Oahu-DSR-DR-NOAM-2   A1055
2. Execute the following command to start the DSR OAM process on the DR-NOAM.
$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</td>
</tr>
</table>

Procedure 21. 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) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Establish GUI session on the NOAM VIP	If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.  ORACLE Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 21. Configure the SOAM NE

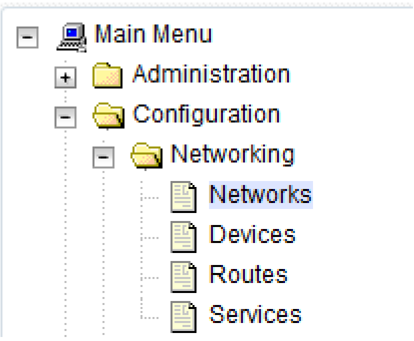
2. □

Primary NOAM VIP GUI: Create the SOAM network element using an XML file

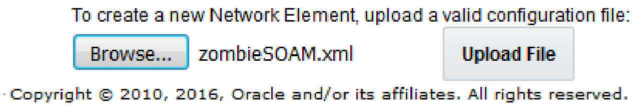
Make sure to have an SOAM network element XML file available on the PC running the web browser. The SOAM network element XML file is similar to what was created and used in Procedure 13, but defines the SOAM network element.

Refer to Appendix A Sample Network Element and Hardware Profiles for a sample network element xml file

1. Navigate to **Configuration > Networking > Networks**.

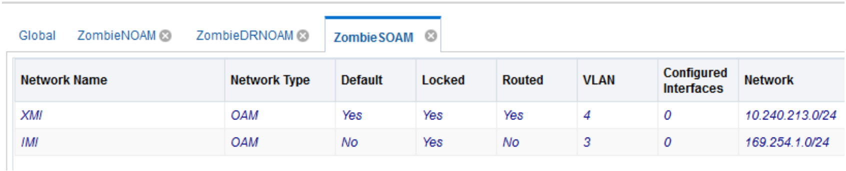


2. Click **Browse** and type the path and name of the SOAM network XML file.



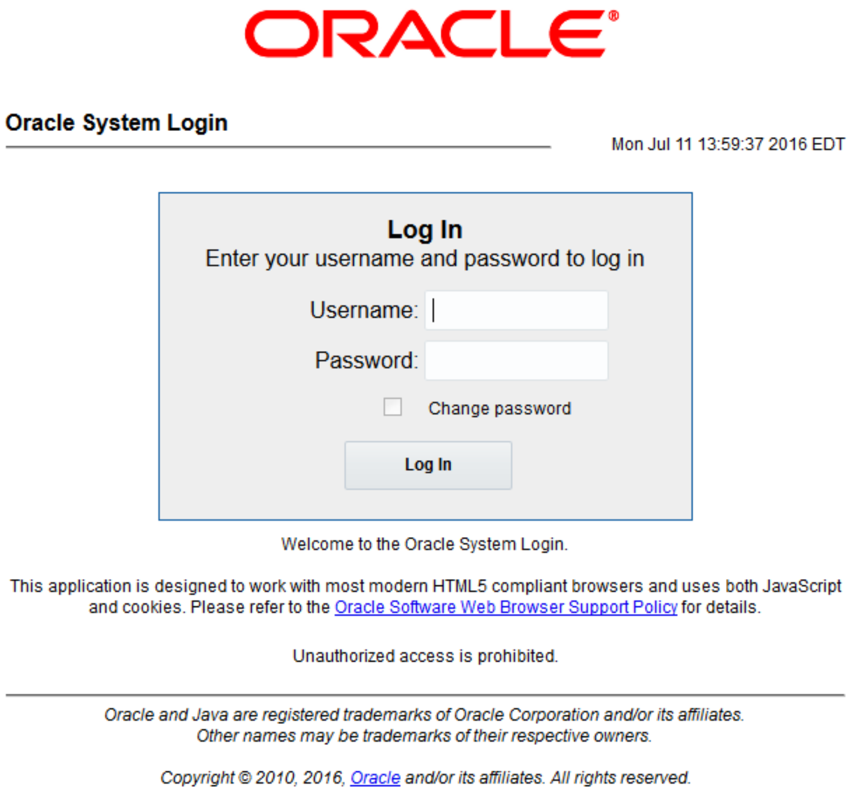
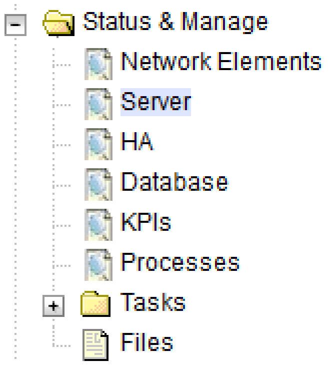
To create a new Network Element, upload a valid configuration file:

3. Click **Upload** to upload the XML file and configure the SOAM network element.

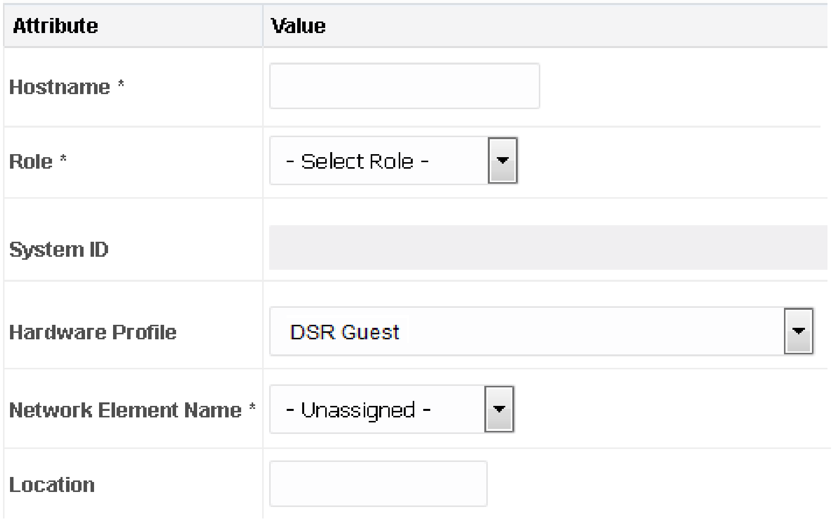


Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24
IMI	OAM	No	Yes	No	3	0	169.254.1.0/24

Procedure 22. Configure the SOAM Servers

STEP #	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. □	**Primary NOAM VIP GUI**: Establish GUI session on the NOAM VIP	If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.  ORACLE Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.* *Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
2. □	**Primary NOAM VIP GUI**: Insert the 1st SOAM server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click **Insert** to insert the new SOAM server into servers table.

Procedure 22. Configure the SOAM Servers

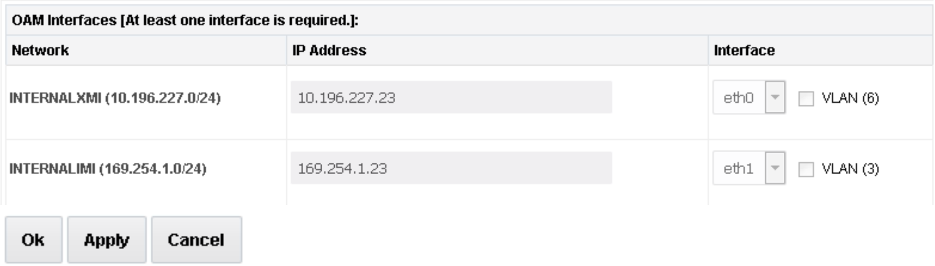


Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

3. Fill in the fields as follows:

Hostname:	<SO1-Hostname>
Role:	SYSTEM OAM
System ID:	<Site System ID>
Hardware Profile:	`DSR Guest`
Network Element Name:	[Choose **NE** from list]

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



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.23	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.23	eth1 □ VLAN (3)

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

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

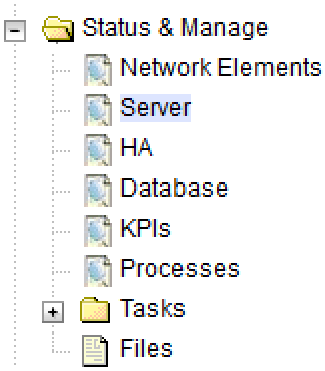
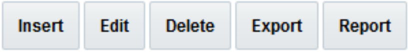
6. Add the following NTP servers:

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

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

Note Properly configure the NTP on the controller node to reference lower stratum NTP servers.

Procedure 22. Configure the SOAM Servers

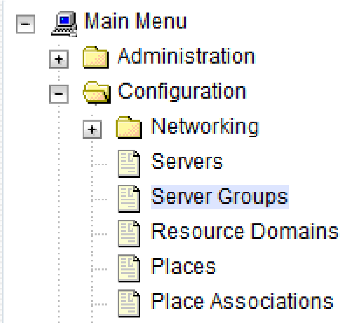
3. □	**Primary NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. From the GUI screen, select the desired server and click **Export** to generate the initial configuration data for that server.  3. Go to the Info tab to confirm the file has been created.
4. □	**Primary NOAM**: Copy configuration file to the 1st SOAM server	Login as the **admusr** user to the NOAM1 shell and issue the commands: `$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh`
5. □	**First SOAM Server**: Wait for configuration to complete	1. 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. 2. 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. 3. 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. □	**First SOAM Server**: Reboot the server	Obtain a terminal session to the 1st SOAM as the **admusr** user. `$ sudo init 6` Wait for server to reboot.

Procedure 22. Configure the SOAM Servers

7.
□
	First SOAM Server: Verify Server Health	1. After the system reboots, login again as the **admusr** user.
		2. 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`

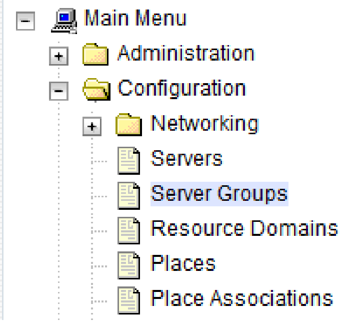
8. □	Insert and Configure the 2nd SOAM server, repeat steps 1 through 7 for 2nd SOAM	1. Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so: Enter the network data for the 2**nd** SOAM server, transfer the **TKLCConfigData** file to the 2**nd** SOAM server, and reboot the 2**nd** SOAM server when asked at a terminal window. 2. Wait approximately 5 minutes for the 2nd SOAM server to reboot. ***Note***: For DSR mated sites, repeat this step for additional/spare SOAM server for mated site.

Procedure 23. Configure the SOAM Server Group

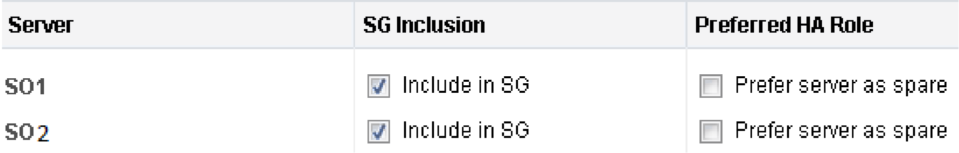
STEP #	This procedure configures the SOAM server group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Enter SOAM server group data	1. From the GUI session on the NOAM VIP address, navigate to **Configuration > Server Groups**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert** and add the SOAM server group name along with the values for the following fields: Name: [Enter Server Group Name] Level: `B` Parent: [Select the NOAM Server Group] Function: `DSR (Active/Standby Pair)` WAN Replication Connection Count: Use Default Value 3. Click **OK** when all fields are filled. ***Note***: For DSR mated sites, repeat this step for additional SOAM server groups where the preferred SOAM spares may be entered before the active/standby SOAMs.

Procedure 23. Configure the SOAM Server Group

<table>
<tr>
<td>2.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Edit the SOAM server group and add VIP</td>
<td>
1. Navigate to <b>Configuration > Server Groups</b>.

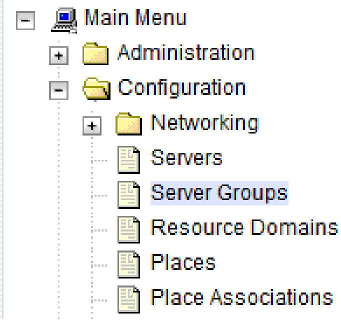


2. Select the new <b>SOAM</b> server group and click <b>Edit</b>.


<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>SO1</td><td>☑ Include in SG</td><td>□ Prefer server as spare</td></tr>
<tr><td>SO2</td><td>☑ Include in SG</td><td>□ Prefer server as spare</td></tr>
</table>

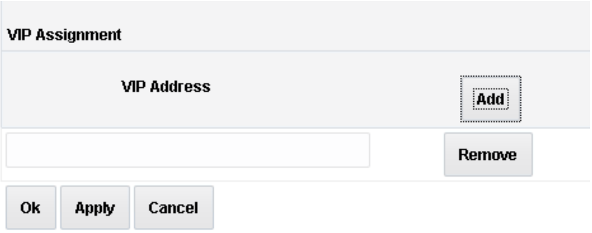
3. Add both SOAM servers to the server group primary site by marking the <b>Include in SG</b> checkbox.

4. Click <b>Apply</b>.
</td>
</tr>
<tr>
<td>3.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Add the SOAM VIP</td>
<td>
1. Navigate to <b>Configuration > Server Groups</b>.



2. Select the new <b>SOAM</b> server group and click <b>Edit</b>.

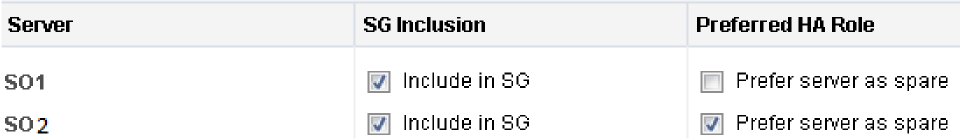
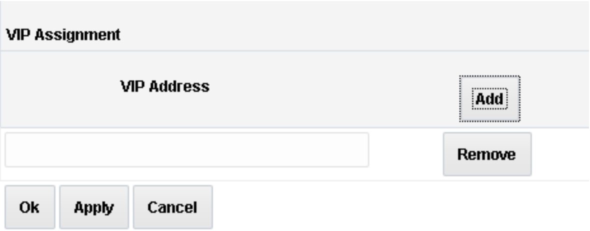
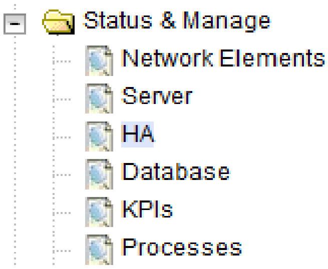
3. Click <b>Add</b> to add a SOAM VIP. Type the <b>VIP Address</b> and click <b>OK</b>.


VIP Assignment

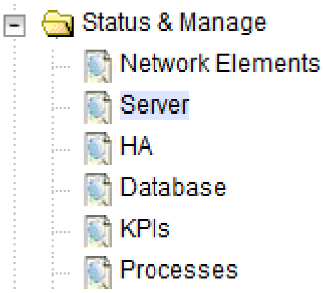
VIP Address

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

Procedure 23. Configure the SOAM Server Group

4. ☐	**Primary NOAM VIP GUI**: Edit the SOAM server group and add preferred spares for site redundancy (Optional)	If the two-site redundancy feature is wanted for the SOAM server group, add an SOAM server located in its server group secondary site by marking the **Include in SG** and **Preferred Spare** checkboxes.  Server | SG Inclusion | Preferred HA Role SO1 | ☑ Include in SG | ☐ Prefer server as spare SO2 | ☑ Include in SG | ☑ Prefer server as spare For more information about server group secondary site or site redundancy, see the Terminology section.
5. ☐	**Primary NOAM VIP GUI**: Edit the SOAM server group and add additional SOAM VIPs (Optional)	1. Click **Add** to add SOAM VIPs. 2. Type the **VIP Address** and click **OK**. **Note**: Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.  VIP Assignment VIP Address
6. ☐	**Primary NOAM VIP GUI**: Wait for replication	After replication, the server status should be active (**Status & Manage > HA**).  Status & Manage Network Elements Server HA Database KPIs Processes ***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 (**Alarms > View Active**).

Procedure 23. Configure the SOAM Server Group

7. □	**Primary NOAM VIP GUI**: Restart 1st SOAM server	1. From the NOAM GUI, navigate to **Status & Manage > Server** and select the **1st SOAM** server.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Click **Restart**. 3. Click **OK** on the confirmation screen. Wait for restart to complete. Wait for the Appl State to change to Enabled, and all other columns to Norm.
8. □	**Primary NOAM VIP GUI**: Restart 2nd SOAM server	Repeat step 7 for the second SOAM.
9. □	**Primary NOAM VIP GUI**: Restart all preferred spare SOAM servers (Optional)	1. If additional preferred spare servers are configured for secondary sites, navigate to **Status & Manage > Server** and select all **Preferred Spare** SOAM servers. 2. 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**.

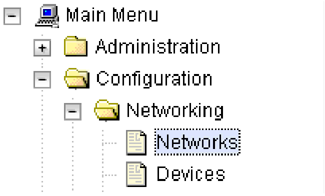
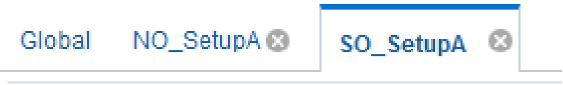
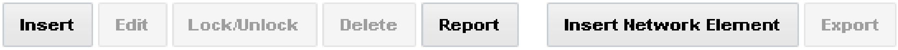
Procedure 24. Activate PCA/DCA (PCA/DCA Only)

STEP #	This procedure activates PCA/DCA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	(PCA Only) activate PCA feature	If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) of the DSR PCA Activation Guide [2] to activate PCA. ***Note***: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online. ***Note***: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

Procedure 24. Activate PCA/DCA (PCA/DCA Only)

2. □	(DCA Only) activate DCA feature	If you are installing PCA, execute [24] DCA Framework and Application Activation and Deactivation Guide to activate the DCA framework and feature. ***Note***: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online. ***Note***: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

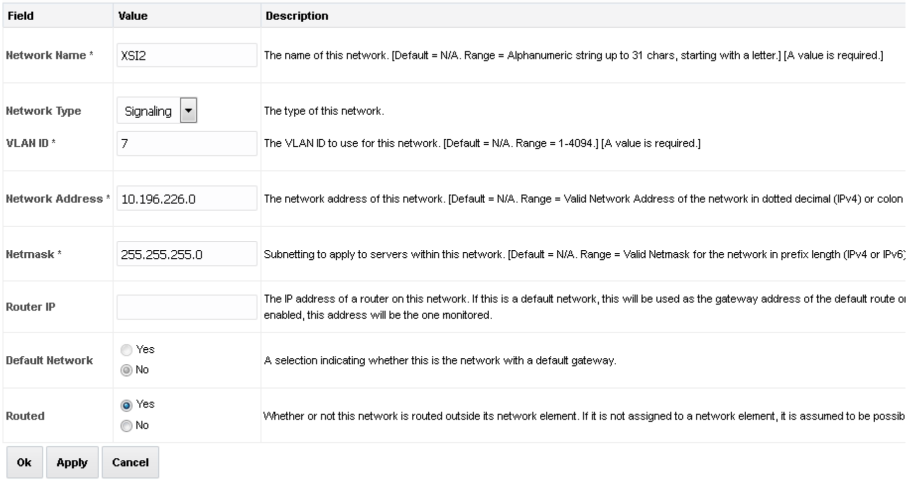
Procedure 25. Configure the MP Virtual Machines

STEP #	This procedure configures MP VMs (IPFE, SBR, SS7-MP, DA-MP, and vSTP). ***Note***: If you are adding MPs to expand an existing DSR, which was upgraded from 7.x to 8.x, skip this procedure and execute Procedure 26. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Establish GUI Session on the NOAM VIP	1. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. 2. Login as the **guiadmin** user.
2. □	**Primary NOAM VIP GUI**: Navigate to the signaling network configuration screen	1. Navigate to **Configuration > Networking > Networks**.  Main Menu Administration Configuration Networking Networks Devices 2. Navigate to the **SO Network Element** tab under which the MPs are to be configured.  3. Click **Insert** in the lower left corner.  Insert Edit Lock/Unlock Delete Report Insert Network Element Export

Procedure 25. Configure the MP Virtual Machines

<table>
<tr>
<td>3.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Add signaling networks</td>
<td>

The following screen displays:



<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Network Name *</td><td>XSI2</td><td>The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.] [A value is required.]</td></tr>
<tr><td>Network Type</td><td>Signaling</td><td>The type of this network.</td></tr>
<tr><td>VLAN ID *</td><td>7</td><td>The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]</td></tr>
<tr><td>Network Address *</td><td>10.196.226.0</td><td>The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon</td></tr>
<tr><td>Netmask *</td><td>255.255.255.0</td><td>Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6)</td></tr>
<tr><td>Router IP</td><td></td><td>The IP address of a router on this network. If this is a default network, this will be used as the gateway address of the default route or enabled, this address will be the one monitored.</td></tr>
<tr><td>Default Network</td><td>○ Yes
● No</td><td>A selection indicating whether this is the network with a default gateway.</td></tr>
<tr><td>Routed</td><td>● Yes
○ No</td><td>Whether or not this network is routed outside its network element. If it is not assigned to a network element, it is assumed to be possib</td></tr>
</table>

1. Type the **Network Name**, **Network Type**, **VLAN ID**, **Network Address**, **Netmask**, and **Router IP** that matches the signaling network.

   Note: Even if the network does not use VLAN tagging, you should type the correct VLAN ID here as indicated by the NAPD.

   a. Select **Signaling** for Network Type.

   b. Select **No** for Default Network.

   c. Select **Yes** for Routable.

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

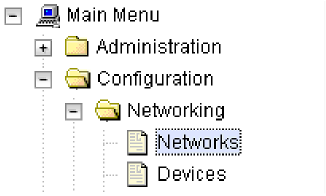
   -OR-

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

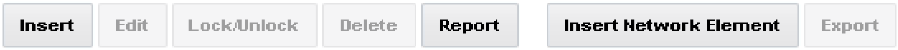
</td>
</tr>
<tr>
<td>4.
□</td>
<td><b>Primary NOAM VIP GUI</b>: (PCA/DCA only) Navigate to signaling network configuration screen</td>
<td>

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

1. Navigate to **Configuration > Networking > Networks**.



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

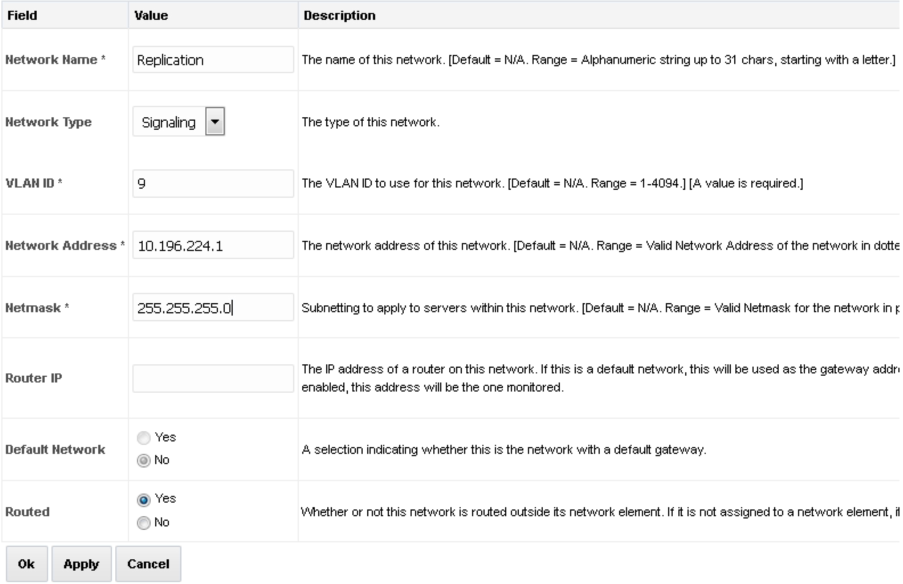


</td>
</tr>
</table>

Procedure 25. Configure the MP Virtual Machines

5. □ **Primary 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.



Field	Value	Description
Network Name *	Replication	The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.]
Network Type	Signaling	The type of this network.
VLAN ID *	9	The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]
Network Address *	10.196.224.1	The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotte
Netmask *	255.255.255.0	Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in
Router IP		The IP address of a router on this network. If this is a default network, this will be used as the gateway addr enabled, this address will be the one monitored.
Default Network	○ Yes ● No	A selection indicating whether this is the network with a default gateway.
Routed	● Yes ○ No	Whether or not this network is routed outside its network element. If it is not assigned to a network element, i

1. Type the **Network Name**, **Network Type**, **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.

   a. Select **No** for Default Network.

   b. Select **Yes** for Routable.

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

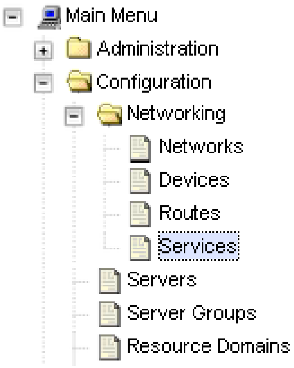
   -OR-

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

6. □ **Primary 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.

1. Navigate to **Configuration > Networking > Services**.



2. Click **Edit**.

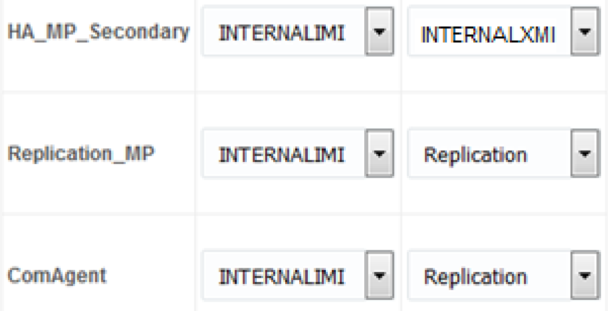
Procedure 25. Configure the MP Virtual Machines

3. Set the services using one of the following scenarios:

- **If the dual-path HA configuration is required**:

  For HA_MP_Secondary, Oracle recommends the inter-NE network is set as the XMI network and intra-NE network is set as the IMI network. If the primary interface (Replication_MP) SBR DB Replication Network interface goes down, use the secondary network for sharing HA status to reduce the likelihood of a split brain. This leads to DSR mate isolation from the active SBR and results in traffic loss until SBR DB Replication Network is down.

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



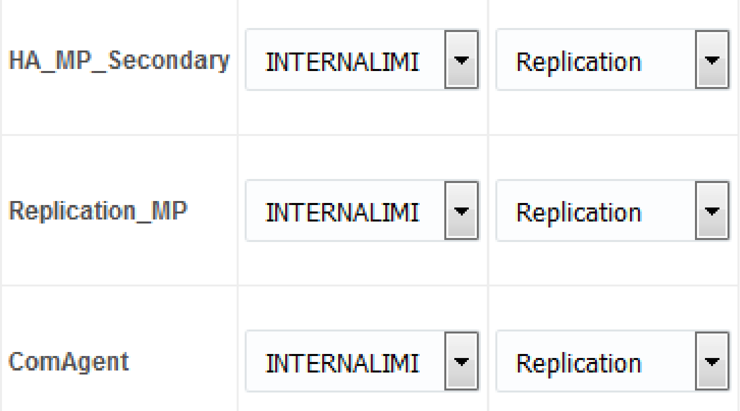
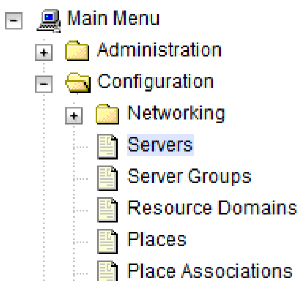
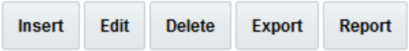
HA_MP_Secondary	INTERNALIMI	INTERNALXMI
Replication_MP	INTERNALIMI	Replication
ComAgent	INTERNALIMI	Replication

- **If the dual-path HA configuration is NOT required**:

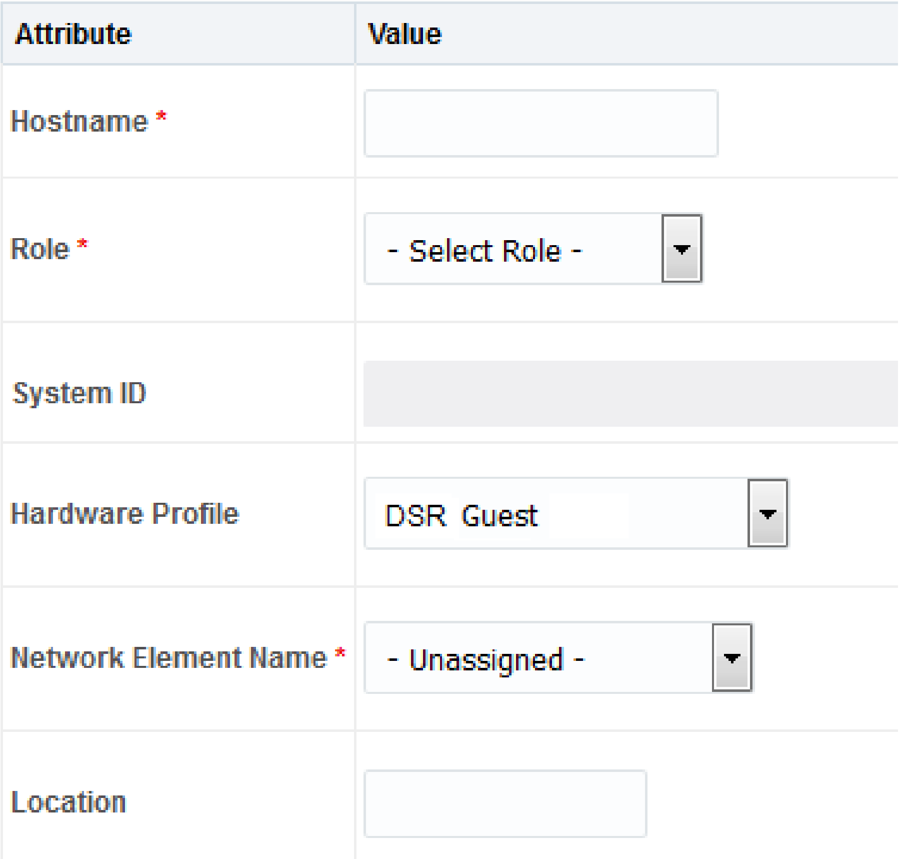
  The intra-NE network is set as the IMI network and inter-NE network is set as the PCA replication network (configured in step 5. This may lead to a split database scenario in case the SBR DB Replication Network interface goes down. Due to this, an active SBR server in each site is in effect.

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

Procedure 25. Configure the MP Virtual Machines

		 HA_MP_Secondary INTERNALIMI Replication Replication_MP INTERNALIMI Replication ComAgent INTERNALIMI Replication 4. Click **OK** to apply the Service-to-Network selections.
7. □	**Primary NOAM VIP GUI**: Insert the MP or IPFE server – Part 1	1. Navigate to **Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert** to add the new MP or IPFE server into servers table.  3. Fill in the following values:

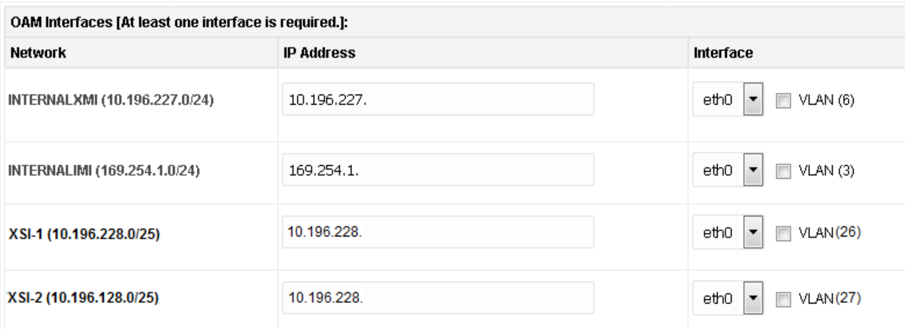
Procedure 25. Configure the MP Virtual Machines



Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

4. 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]



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.	eth0 □ VLAN (3)
XSI-1 (10.196.228.0/25)	10.196.228.	eth0 □ VLAN(26)
XSI-2 (10.196.128.0/25)	10.196.228.	eth0 □ VLAN(27)

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

6. Leave the **VLAN** checkbox unmarked.

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

Procedure 25. Configure the MP Virtual Machines

interface.

a. Leave the **VLAN** checkbox unmarked.

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

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

   a. Leave the **VLAN** checkbox unmarked.

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

   a. 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.

10. Add the following NTP servers:

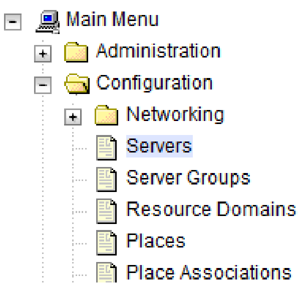
NTP Server	Preferred?
Valid NTP server	Yes
Valid NTP server	No
Valid NTP server	No

11. Click **OK** when all fields are filled in to finish MP server insertion.

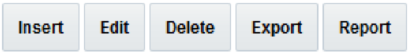
Note: Properly configure the NTP on the controller node to reference lower stratum NTP servers.

8. □ **Primary NOAM VIP GUI**: Export the initial configuration

1. Navigate to **Configuration > Networking > Servers**.



2. From the GUI screen, select the server that was just configured and click **Export** to generate the initial configuration data for that server.



3. Go to the Info tab to confirm the file has been created.

9. □ **MP Server**: Log into the MP

Obtain a terminal window connection on the MP or IPFE server.

Procedure 25. Configure the MP Virtual Machines

10. □	**Primary NOAM VIP GUI**: Copy configuration file to MP or IPFE server	From the active NOAM console, login as the **admusr** user. `$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh` ***Note***: ipaddr is the XMI IP address of the MP or IPFE.
11. □	**MP Server**: Wait for configuration to complete	1. Obtain a terminal session on the **MP or IPFE** 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. 2. 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. 3. 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.
12. □	**MP Server**: Reboot the server	Obtain a terminal session on the **MP** or **IPFE** as the **admusr** user. `$ sudo init 6` Wait for server to reboot.

13.
□
	MP Server: Verify server health	1. After the reboot, login as the **admusr** user.
		2. Execute the following command as super-user on the server and make sure that no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

14. □	**MP Server**: Delete Auto-Configured Default Route on MP and Replace it with a Network Route using the	***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.

Procedure 25. Configure the MP Virtual Machines

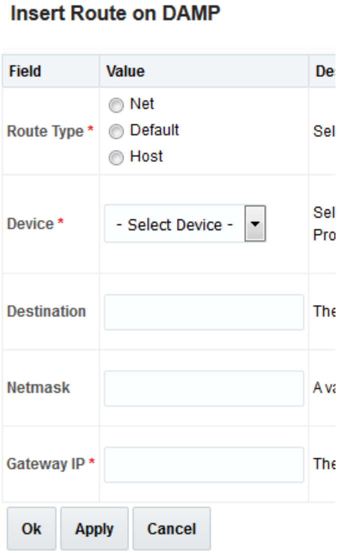
XMI Network (Optional)

1. Log into the MP as the **admusr** user. (Alternatively, you can log into the VM's console.)
2. Determine <XMI_Gateway_IP> from your SO site network element information.
3. 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 **Configuration > Networking > Networks** menu.

4. Create network routes to the NO's XMI (OAM) network:
   a. Navigate to NOAM VIP GUI **Configuration** > **Networking** > **Routes**.
   b. Select the Specific MP.
   c. Click **Insert**.
   d. Enter details.
   e. Click **OK**.



Insert Route on DAMP

Field	Value	De
Route Type *	○ Net ○ Default ○ Host	Sel
Device *	- Select Device - ▾	Sel Pro
Destination		The
Netmask		A va
Gateway IP *		The

5. (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>
```

6. Route to <MP_XMI_Interface> added.
7. Repeat for any existing customer NMS stations.

Procedure 25. Configure the MP Virtual Machines

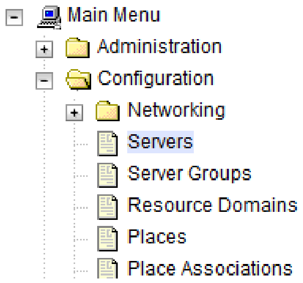
		8. Delete the existing default route:
		`$  sudo /usr/TKLC/plat/bin/netAdm delete --route=default --gateway=<MP_XMI_Gateway_IP>  --device=<MP_XMI_Interface>`
		Route to <MP_XMI_Interface> removed.
		9. [MP Console] Ping active NO XMI IP address to verify connectivity:
		`$ ping <ACTIVE_NO_XMI_IP_Address>`
		`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`
		10. (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`
		11. 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.

15. □	Repeat for remaining MPs and IPFEs	Repeat steps 7 through 14 for all remaining MP (SBR, SS7-MP, DA-MP, IPFE and vSTP) servers.

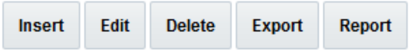
Procedure 26. Configure the MP Virtual Machines (Optional)

STEP #	This procedure configures MP VMs (IPFE, SBR, SS7-MP, DA-MP, and vSTP). ***Note***: This procedure is ONLY required if additional MPs are required to be added to expand an existing DSR, which was upgraded from 7.x to 8.x. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**Primary NOAM VIP GUI**: Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.
2. □	**Primary NOAM VIP GUI**: Insert the MP or IPFE server – Part 1	1. Navigate to **Configuration > Servers**.

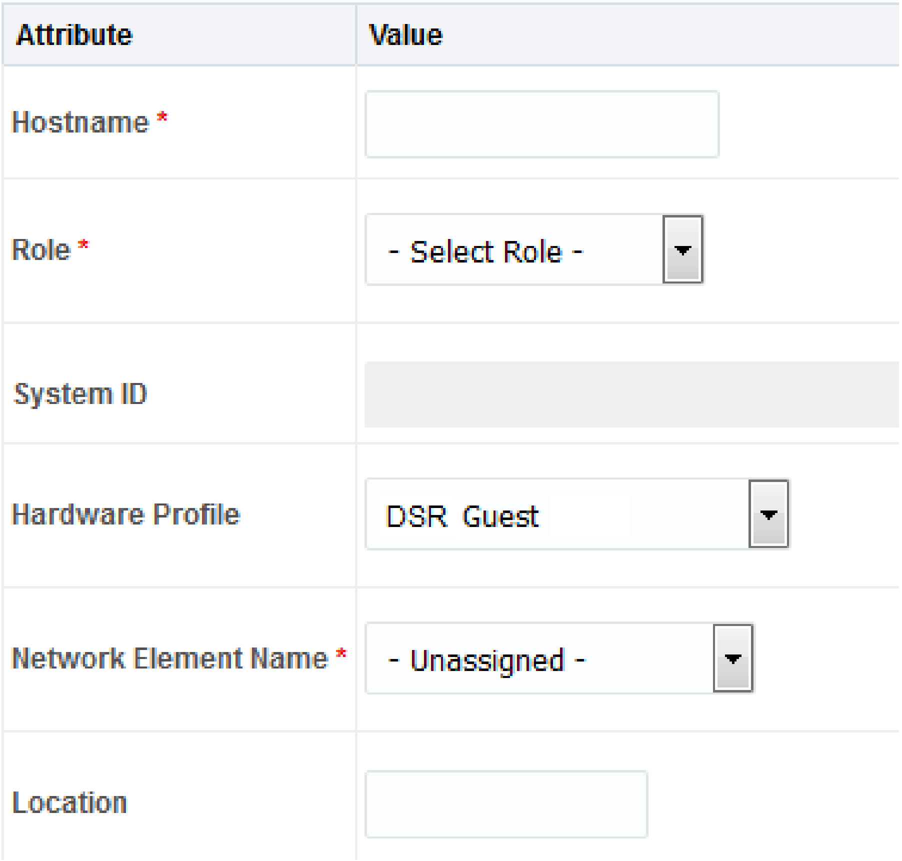
Procedure 26. Configure the MP Virtual Machines (Optional)



2. Click **Insert** to add the new MP or IPFE server into servers table.



3. Fill in the following values:

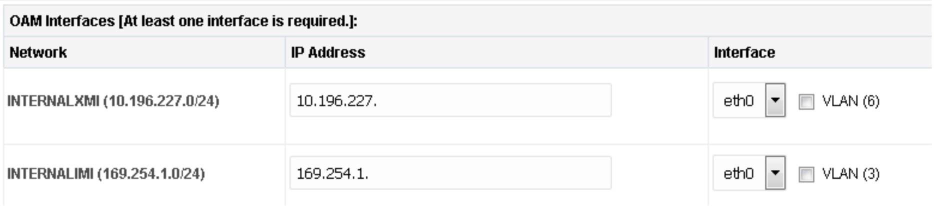


Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

4. 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]

Procedure 26. Configure the MP Virtual Machines (Optional)

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


OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.	eth0 ▾ □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.	eth0 ▾ □ VLAN (3)

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

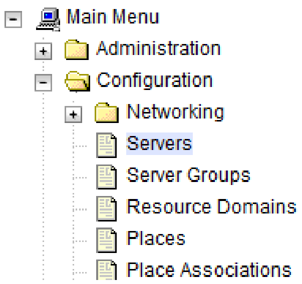
   Leave the **VLAN** checkbox unmarked.
6. For the IMI network, type the MP's IMI IP address. Select the correct interface.

   Leave the **VLAN** checkbox unmarked.
7. Add the following NTP servers:

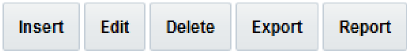
NTP Server	Preferred?
Valid NTP server	Yes
Valid NTP server	No
Valid NTP server	No

8. Click **OK** when all fields are filled in to finish MP server insertion.

Note: Properly configure the NTP on the controller node to reference lower stratum NTP servers.
</td>
</tr>
<tr>
<td>3.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Export the initial configuration</td>
<td>
1. Navigate to **Configuration > Networking > Servers**.



2. From the GUI screen, select the server that was just configured and click **Export** to generate the initial configuration data for that server.



3. Go to the Info tab to confirm the file has been created.
</td>
</tr>
<tr>
<td>4.
□</td>
<td><b>MP Server</b>: Log into the MP</td>
<td>Obtain a terminal window connection on the MP or IPFE server.</td>
</tr>
</table>

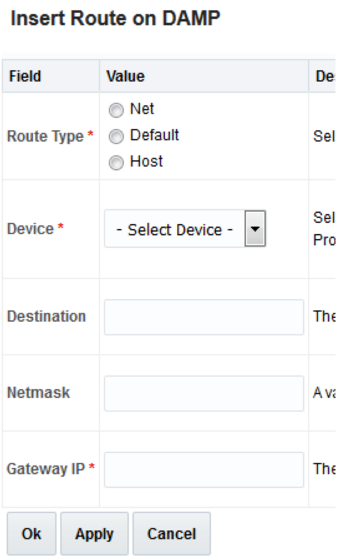
Procedure 26. Configure the MP Virtual Machines (Optional)

5. □	**Primary NOAM VIP Server**: Copy configuration file to MP or IPFE server	From the active NOAM console, login as the **admusr** user. `$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh` ***Note***: ipaddr is the XMI IP address of the MP or IPFE.
6. □	**MP Server**: Wait for configuration to complete	1. Obtain a terminal session on the **MP or IPFE** 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. 2. 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. 3. 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.
7. □	**MP Server**: Reboot the server	Obtain a terminal session on the **MP** or **IPFE** as the **admusr** user. `$ sudo init 6` Wait for server to reboot.

8.
□
	MP Server: Verify server health	1. After the reboot, login as the **admusr** user.
		2. Execute the following command as super-user on the server and make sure that no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

9. □	**MP Server**: Delete Auto-Configured Default Route on MP and Replace it with a Network Route using the	***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.

Procedure 26. Configure the MP Virtual Machines (Optional)

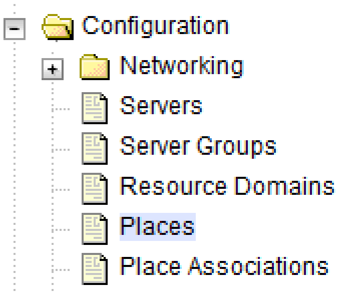
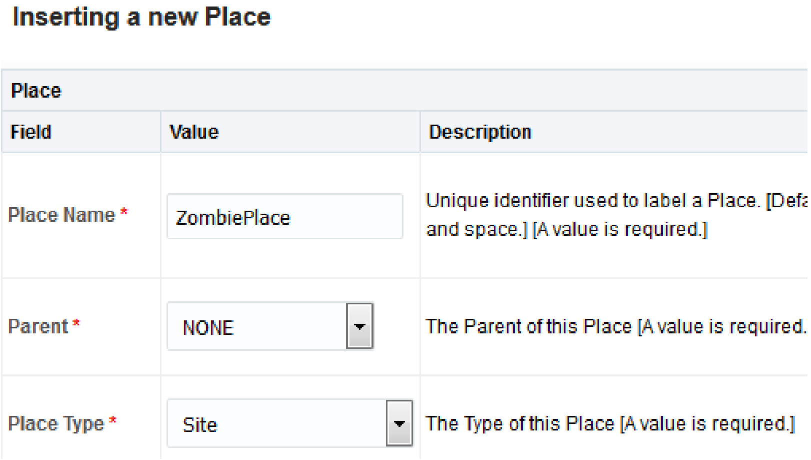
	XMI Network (Optional)	1. Log into the MP as the **admusr** user. (Alternatively, you can log into the VM's console.)
		2. Determine <XMI_Gateway_IP> from your SO site network element information.
		3. Gather the following items:
		<NO_XMI_Network_Address>
		<NO_XMI_Network_Netmask>
		Note: You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the **Configuration > Networking > Networks** menu.
		4. Create network routes to the NO's XMI (OAM) network:
		a. Navigate to NOAM VIP GUI **Configuration** > **Networking** > **Routes**.
		b. Select the Specific MP.
		c. Click **Insert**.
		d. Enter details.
		e. Click **OK**.
		
		Insert Route on DAMP
		Field / Value / De
		Route Type * ○ Net ○ Default ○ Host Sel
		Device * - Select Device - Sel Pro
		Destination The
		Netmask A va
		Gateway IP * The
		Ok Apply Cancel
		5. (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>`
		6. Route to <MP_XMI_Interface> added.
		7. Repeat for any existing customer NMS stations.

Procedure 26. Configure the MP Virtual Machines (Optional)

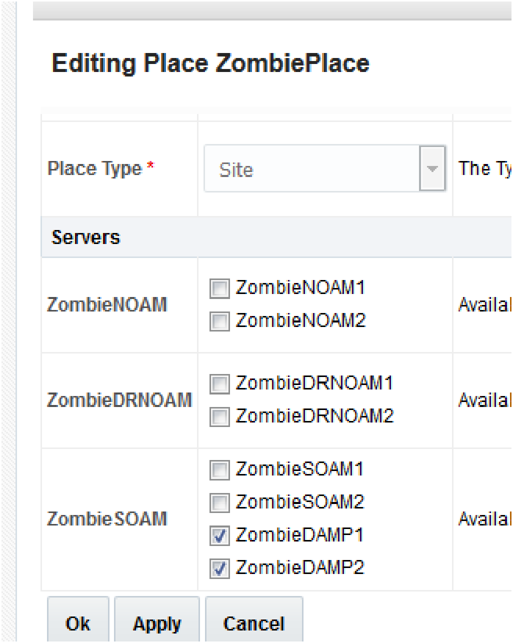
		8. Delete the existing default route:
		`$  sudo /usr/TKLC/plat/bin/netAdm delete --route=default --gateway=<MP_XMI_Gateway_IP>  --device=<MP_XMI_Interface>`
		Route to <MP_XMI_Interface> removed.
		9. [MP Console] Ping active NO XMI IP address to verify connectivity:
		`$ ping <ACTIVE_NO_XMI_IP_Address>`
		`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`
		10. (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`
		11. 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.

10. □	Repeat for remaining MPs and IPFEs	Repeat steps 2 through 9 for all remaining newly created MPs.

Procedure 27. Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)

STEP #	This procedure adds places in the MAP-IWF, PCA, and DCA 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. □	(PCA Only) **Primary NOAM VIP GUI**: Configure Places	1. Establish a GUI session on the NOAM by using the XMI VIP address. Login as the **guiadmin** user. 2. Navigate to **Configuration > Networking > Places**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 3. Click **Insert**. 4. Fill in the fields as follows:  Inserting a new Place Place Field Value Description Place Name * ZombiePlace Unique identifier used to label a Place. [Defa and space.] [A value is required.] Parent * NONE The Parent of this Place [A value is required. Place Type * Site The Type of this Place [A value is required.] **Place Name**: <Site Name> **Parent**: `NONE` **Place Type**: `Site` 5. Repeat this step for each of the PCA/DCA Places (Sites) in the network. See the Terminology section for more information on Sites & Places.

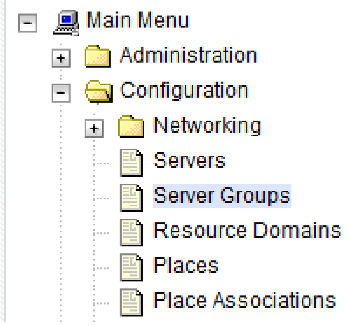
Procedure 27. Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)

2. □	**NOAM VIP GUI**: Assign MP server to places	1. Select the place configured in step 1 and click **Edit**.  Editing Place ZombiePlace Place Type * Site The Ty Servers ZombieNOAM ☐ ZombieNOAM1 ☐ ZombieNOAM2 Availal ZombieDRNOAM ☐ ZombieDRNOAM1 ☐ ZombieDRNOAM2 Availal ZombieSOAM ☐ ZombieSOAM1 ☐ ZombieSOAM2 ☑ ZombieDAMP1 ☑ ZombieDAMP2 Availal Ok Apply Cancel 2. Mark all the checkboxes for SS7-MPs and PCA/DCA DA-MP and SBR servers that are assigned to this place. 3. Repeat this step for all other DA-MP or SBR servers you wish to assign to places. ***Note***: All **DA-MPs** and **SBR** servers must be added to the **Site Place** that corresponds to the physical location of the server. See the Terminology section for more information on Sites & Places.

Procedure 28. 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.	
1. □	**Primary NOAM VIP GUI**: Enter MP Server Group Data Applicable to all C level servers (DAMP, IPFE, SS7, VSTP, SBRs)	1. From the GUI session on the NOAM VIP address, navigate to **Configuration > Server Groups**.

Procedure 28. Configure the MP Server Group(s) and Profiles



2. 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
IP Front End	IPFE application	1 Active MP Per SG
SBR	Policy and Charging Session/or Policy Binding Function/Universal SBR	1 Active MP, 1 Standby MP, 2 Optional Spare Per SG
SS7-IWF	MAP IWF Application	1 Active MP per SG
STP	vSTP	Multiple vSTP MP per SG

For vSTP:

If configuring only vSTP application, ignore all other IPFE configuration. Currently, there is no specific MP profile for vSTP MP.

Notes:

- IPFE interaction with vSTP MP is **NOT** supported. There is no support of TSA/Auto selection for vSTP MPs.
- vSTP MP can co-exist with DA-MP under a SOAM but different server group.

For PCA application:

- Online Charging function(only)

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

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

Procedure 28. Configure the MP Server Group(s) and Profiles

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

- Policy DRA function

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

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

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))

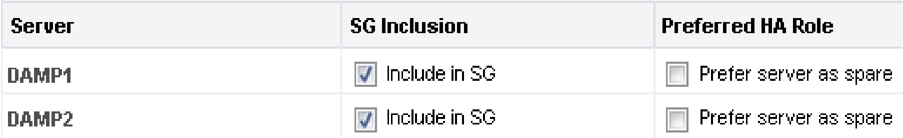
SBR (Function: SBR)

IPFE (Function: IP Front End)

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

</td>
</tr>
<tr>
<td>2.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Repeat for additional 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><b>Primary NOAM VIP GUI</b>: Edit the MP server groups to include MPs</td>
<td>

1. Navigate to **Configuration > Server Groups**, select a server group that you just created, and click **Edit**.
2. Select the network element representing the MP server group you wish to edit.
3. Mark the **Include in SG** checkbox for every MP server you wish to include in this server group. Leave other checkboxes blank.



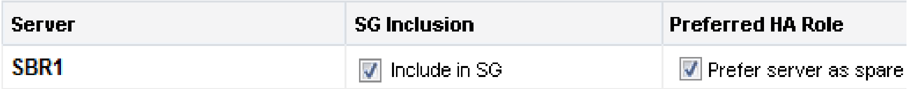
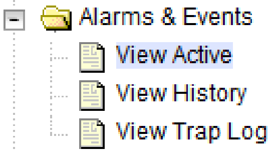
<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>DAMP1</td><td>☑ Include in SG</td><td>□ Prefer server as spare</td></tr>
<tr><td>DAMP2</td><td>☑ Include in SG</td><td>□ Prefer server as spare</td></tr>
</table>

Note: Each **IPFE, SS7-MP and vSTP-MP** server should be in its own server group.

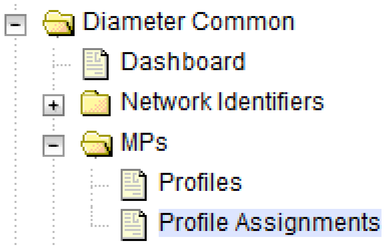
4. Click **OK**.

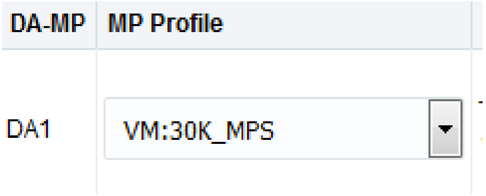
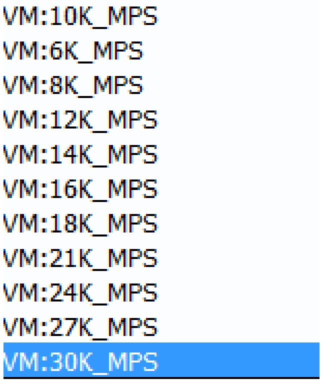
</td>
</tr>
</table>

Procedure 28. Configure the MP Server Group(s) and Profiles

4. □	(PCA only) **Primary NOAM VIP GUI**: Edit the MP server group and add preferred spares for site redundancy (Optional)	If two-site redundancy for the Policy and Charging SBR Server Group is wanted, add a MP server that is physically located in a separate site(location) to the server group by marking the **Include in SG** checkbox and also mark the **Preferred Spare** checkbox.  Server | SG Inclusion | Preferred HA Role SBR1 | ☑ Include in SG | ☑ Prefer server as spare If three-site redundancy for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the **Include in SG** and **Preferred Spare** checkboxes for both servers. ***Note***: The preferred spare servers should be different sites from the original server. There should be servers from three separate sites (locations). ***Note***: There must first be non-preferred spare present in the server group before adding the preferred spare. For more information about site redundancy for Policy and Charging SBR Server Groups, see the **Terminology** section. Click **OK** to save.
5. □	**Primary NOAM VIP GUI**: Repeat For additional server groups	Repeat steps 1 through 4 for any remaining MP and IPFE server groups you need to create.
6. □	**Primary NOAM VIP GUI**: Wait for replication to complete on all MPs	Wait for the alarm 10200: **Remote Database re-initialization in progress** to be cleared (**Alarms & Events > Active Alarms**).  Alarms & Events View Active View History View Trap Log This should happen shortly after you have verified the **Norm** DB status in the previous step.

Procedure 28. Configure the MP Server Group(s) and Profiles

<table>
<tr>
<td>7.
□</td>
<td><b>SOAM VIP GUI</b>: Assign profiles to DA-MPs from SOAM GUI</td>
<td>
1. Log into the GUI of the active SOAM server as the <b>guiadmin</b> user.
2. From the SO GUI, navigate to <b>Diameter Common > MPs > Profiles Assignments</b>.


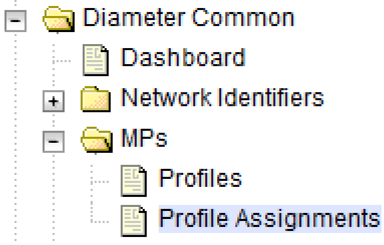
Refer to the <b>DA-MP</b> section. If the site has both DSR and MAP-IWF server groups, you see both DA-MP and SS7-MP sections.

<table>
<tr><th>DA-MP</th><th>MP Profile</th></tr>
<tr><td>DA1</td><td>VM:30K_MPS</td></tr>
</table>
3. For each MP, select the proper profile assignment based on the MP’s type and the function it serves:


<b><i>Note</i></b>: 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.
4. When finished, click <b>Assign</b>.
</td>
</tr>
</table>

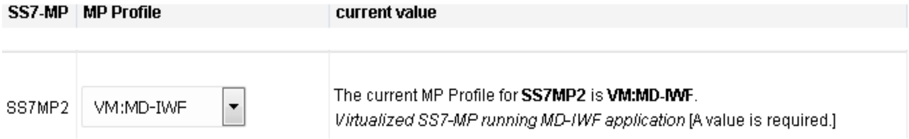
Procedure 28. Configure the MP Server Group(s) and Profiles

<table>
<tr>
<td>8.
□</td>
<td><b>SOAM VIP GUI</b>: Assign Profiles to SS7-MPs from SOAM GUI</td>
<td>

1. Log into the GUI of the active SOAM server as the **guiadmin** user.
2. From the SO GUI, navigate to **Diameter > Configuration > 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.



SS7-MP	MP Profile	current value
SS7MP2	VM:MD-IWF	The current MP Profile for **SS7MP2** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is required.]

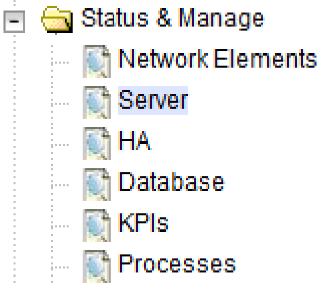
3. For each SS7 MP, select the proper profile assignment based on the SS7 MP's type and the function it serves:

<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>

4. When finished, click **Assign**.

</td>
</tr>
<tr>
<td>9.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Restart MP VM</td>
<td>

1. From the NOAM GUI, navigate to **Status & Manage > Server**.



2. For each MP server:
   a. Select the MP server.
   b. Click **Restart**.
   c. Click **OK** on the confirmation screen. Wait for the message that tells you that the restart was successful.

Policy and Charging DRA/DCA Installations: You may continue to see alarms related to ComAgent until you complete PCA/DCA installation.

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

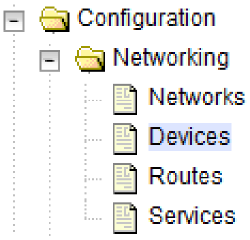
5.1 Configure Signaling Devices (Optional)

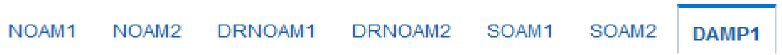
Procedure 29. Configure the Signaling Devices (Optional)

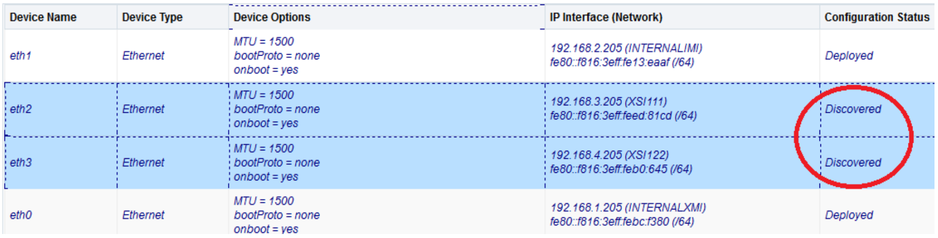
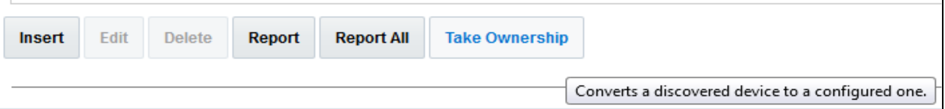
STEP #	This procedure configures signaling network interfaces to the newly added MP servers. ***Note***: This procedure is ONLY required if additional MPs need to be added to expand an existing DSR, which was upgraded from 7.x to 8.x. **Prerequisite**: Execute Procedure 26. Check off (√) each step as 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.
□
	Newly created MP Server console: Manually configure signaling interface	1. SSH into the newly added MP
		`$ ssh admusr@<XMI_Interface_Of_Newly_Created_MP>`
		2. Configure the signaling network interfaces, conforming the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		`$ sudo netAdm add --onboot=yes --bootproto=none --device=eth2 --address=<xsi1 ip> --netmask=<xsi1 netmask>`
		`$ sudo netAdm add --onboot=yes --bootproto=none --device=eth3 --address=<xsi2 ip> --netmask=<xsi2 netmask>`
		Repeat the above netAdm commands to configure the required number of the Signaling network interfaces.
		3. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`

Procedure 29. Configure the Signaling Devices (Optional)

<table>
<tr>
<td>2.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Take ownership of the Signaling interfaces and make it Deployed</td>
<td>
1. Navigate to <b>Configuration > Networking > Devices</b>.


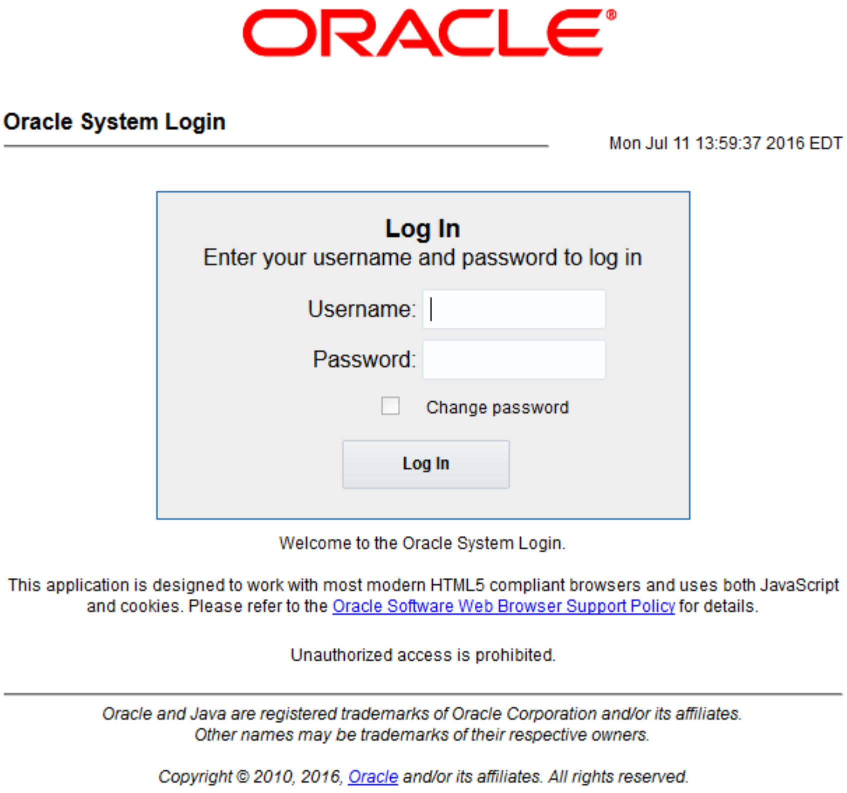
2. You should see several tabs each representing a server in the system. Click on the tab representing the newly created MP.


3. Select all newly configured Signaling Ethernet devices that have <b>Discovered</b> as their Configuration Status.

<table>
<tr><th>Device Name</th><th>Device Type</th><th>Device Options</th><th>IP Interface (Network)</th><th>Configuration Status</th></tr>
<tr><td>eth1</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td>192.168.2.205 (INTERNALIMI)
fe80::f816:3eff:fe13:eaaf (/64)</td><td>Deployed</td></tr>
<tr><td>eth2</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td>192.168.3.205 (XSI111)
fe80::f816:3eff:feed:81cd (/64)</td><td>Discovered</td></tr>
<tr><td>eth3</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td>192.168.4.205 (XSI122)
fe80::f816:3eff:feb0:645 (/64)</td><td>Discovered</td></tr>
<tr><td>eth0</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td>192.168.1.205 (INTERNALXMI)
fe80::f816:3eff:febc:f380 (/64)</td><td>Deployed</td></tr>
</table>
Click <b>Take Ownership</b>.


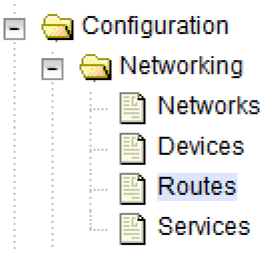
After a brief moment, the selected devices display a Configuration Status of <b>Deployed</b>.
</td>
</tr>
<tr>
<td>3.
□</td>
<td>Repeat for remaining MPs and IPFEs</td>
<td>Repeat steps 1 and 2 for all remaining newly created MPs.</td>
</tr>
</table>

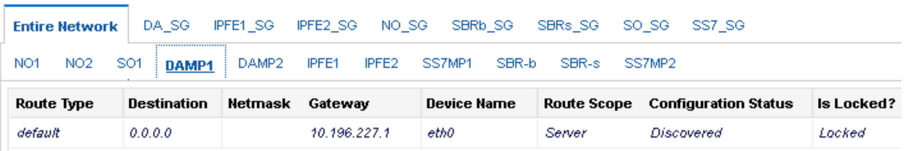
5.2 Configure Signaling Network Routes

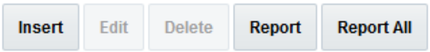
Procedure 30. Configure the Signaling Network Routes

STEP #	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 the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 30. Configure the Signaling Network Routes

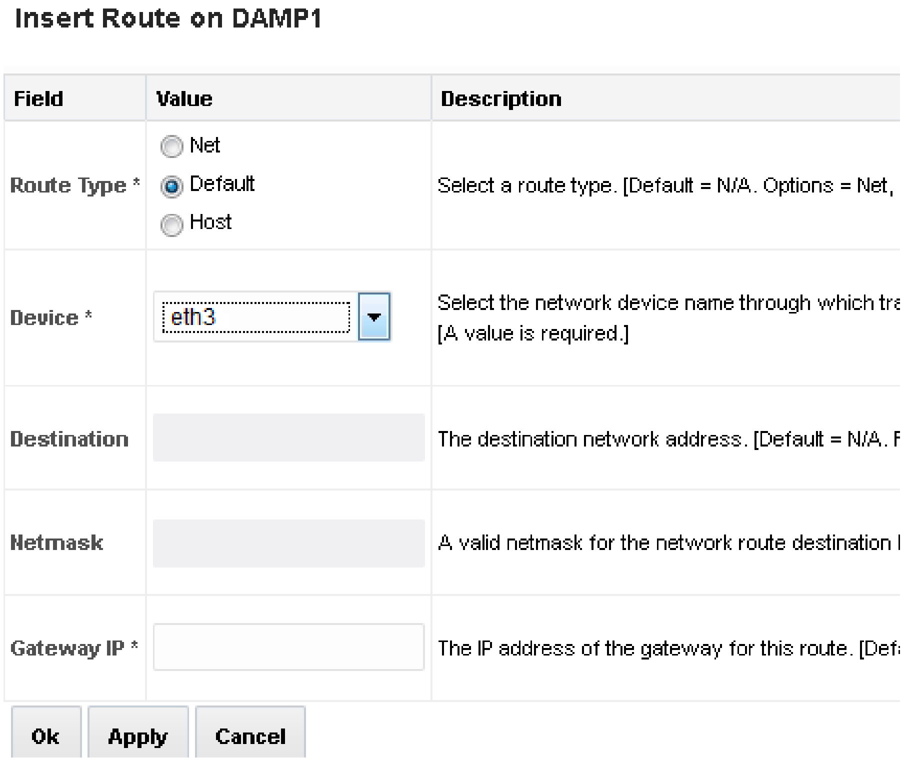
<table>
<tr>
<td>2.
□</td>
<td><b>NOAM VIP</b>: Navigate to routes configuration screen</td>
<td>1. Navigate to <b>Configuration > Networking > Network > Routes</b>.


2. Select the first MP Server you see listed on the first row of tabs as shown, and click the <b>Entire Server Group</b> link. Initially, no routes should display.


<table>
<tr><th>Route Type</th><th>Destination</th><th>Netmask</th><th>Gateway</th><th>Device Name</th><th>Route Scope</th><th>Configuration Status</th><th>Is Locked?</th></tr>
<tr><td><i>default</i></td><td><i>0.0.0.0</i></td><td></td><td><i>10.196.227.1</i></td><td><i>eth0</i></td><td><i>Server</i></td><td><i>Discovered</i></td><td><i>Locked</i></td></tr>
</table>
</td>
</tr>
<tr>
<td>3.
□</td>
<td><b>NOAM VIP</b>: Add route</td>
<td>Click <b>Insert</b> at the bottom of the screen to add additional routes.


</td>
</tr>
<tr>
<td>4.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Add default route for MPs going through signaling network gateway (Optional)</td>
<td><b>***OPTIONAL</b> — Only execute this step if you performed Procedure 25, step 14. , that you have deleted default XMI route and plan to replace it with default XSI routes.
<b>To delete the existing default route</b>:
1. Log into the PRIMARY NOAM VIP GUI.
2. Navigate to <b>Configuration > Networking > Networks</b>.
3. Select the specific SO tab.
4. Select the XMI network and click <b>Unlock</b>. Click <b>OK</b>.
5. Navigate to <b>Configuration > Networking > Routes</b>.
6. Select the Specific MP XMI route and click <b>Delete</b>.
7. Click <b>OK</b>.
8. Repeat the above steps for all required MPs to delete the XMI routes.
9. Navigate to <b>Configuration > Networking > Networks</b>.
10. Select the respective SOAM tab.
11. Select the XMI network and click <b>Lock</b>.
12. Click <b>OK</b>.
If your MP servers no longer have a default route, then you can insert a default route here, which uses one of the signaling network gateways.</td>
</tr>
</table>

Procedure 30. Configure the Signaling Network Routes



Insert Route on DAMP1

Field	Value	Description
Route Type *	○ Net ● Default ○ Host	Select a route type. [Default = N/A. Options = Net,
Device *	eth3	Select the network device name through which tra [A value is required.]
Destination		The destination network address. [Default = N/A. F
Netmask		A valid netmask for the network route destination I
Gateway IP *		The IP address of the gateway for this route. [Def

Route Type: `Default`

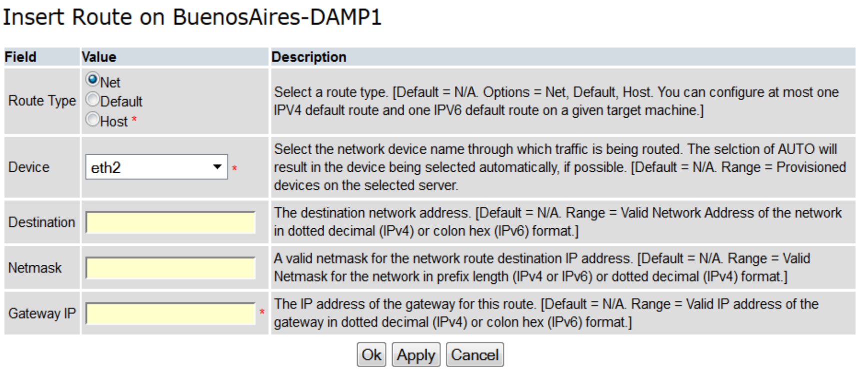
Device: Select the signaling device directly attached to the network where the XSI default gateway resides.

Gateway IP: The XSI gateway you wish to use for default signaling network access.

13. Click **OK**.

Procedure 30. Configure the Signaling Network Routes

<table>
<tr>
<td>5.
□</td>
<td><b>Primary NOAM VIP GUI</b>: Add network routes for Diameter peers</td>
<td>
1. Use this step to add IP4 and/or IPv6 routes to <b>Diameter</b> peer destination networks. The goal for this step is to ensure 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>

<b>Route Type</b>: Net

<b>Device</b>: Select the appropriate signaling interface that is used to connect to that network

<b>Destination</b>: Type the <b>Network ID</b> of network to which the peer node is connected to

<b>Netmask</b>: Type the corresponding Netmask

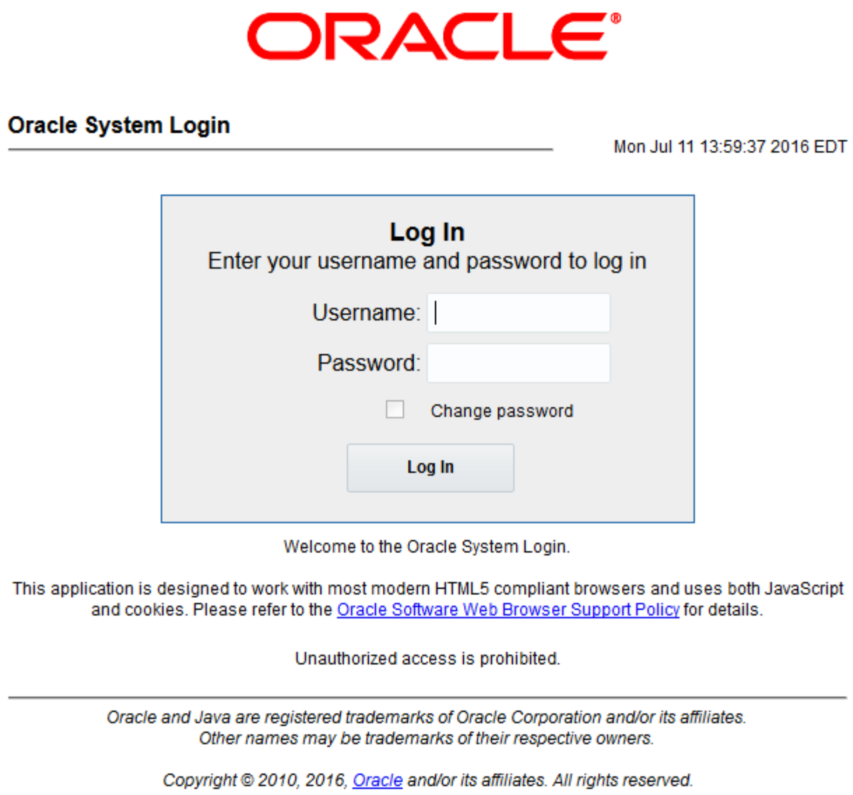
<b>Gateway IP</b>: Type the <b>IP</b> of the customer gateway.

2. If you have more routes to enter, click <b>Apply</b> to save the current route entry. Repeat this step to enter more routes.

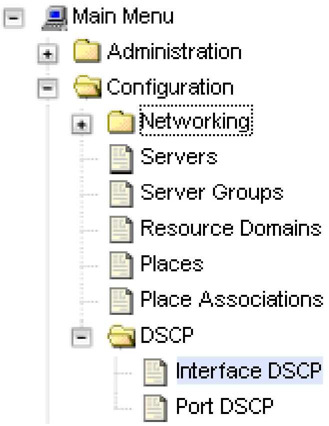
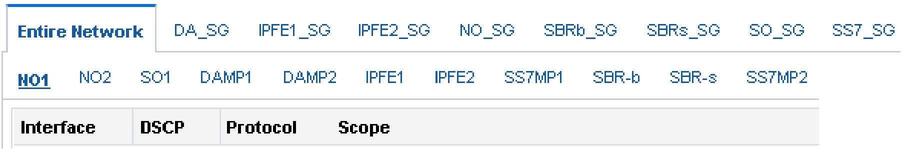
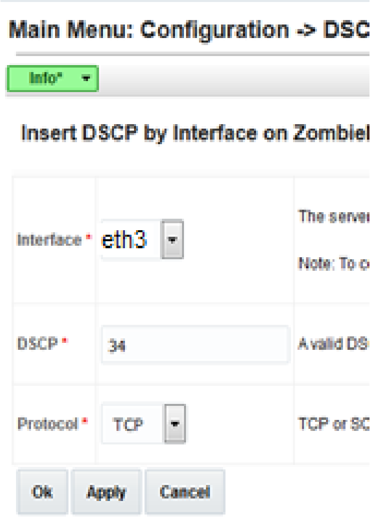
3. If you have finished entering routes, click <b>OK</b> to save the latest route and leave this screen.
</td>
</tr>
<tr>
<td>6.
□</td>
<td>Repeat steps 2-5 for all other MP server groups</td>
<td>The routes entered in this procedure should now be configured on <b>all</b> MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from step 2 but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups.</td>
</tr>
</table>

5.3 Configure DSCP (Optional)

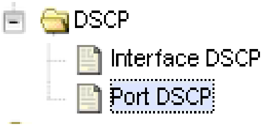
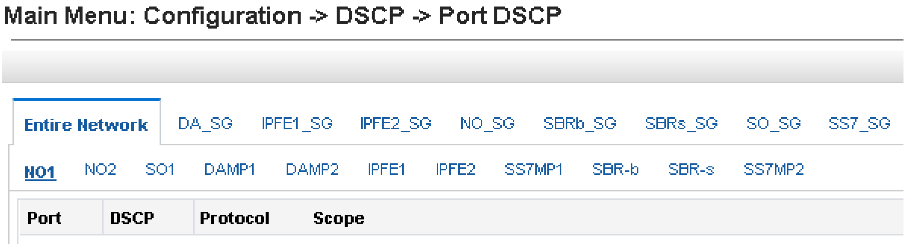
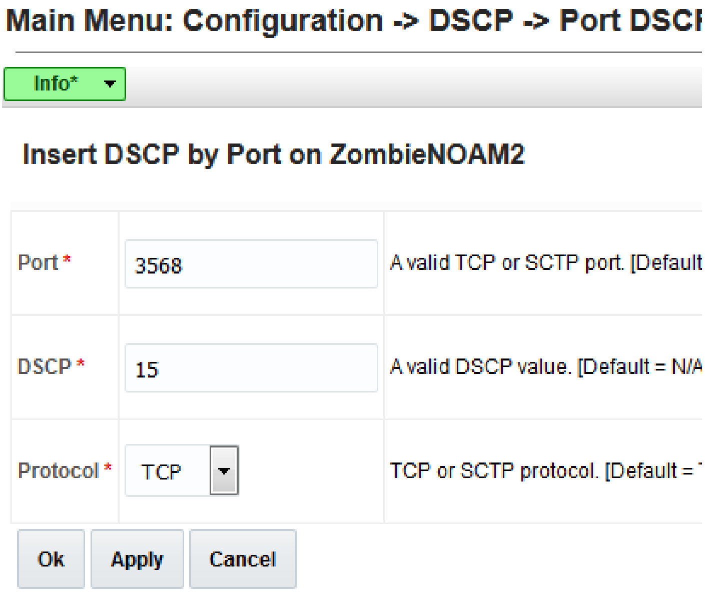
Procedure 31. Configure DSCP Values for Outgoing Traffic (Optional)

STEP #	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.	
1. □	**Primary NOAM VIP GUI**: Establish GUI session on the NOAM VIP	Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.  ORACLE **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 31. Configure DSCP Values for Outgoing Traffic (Optional)

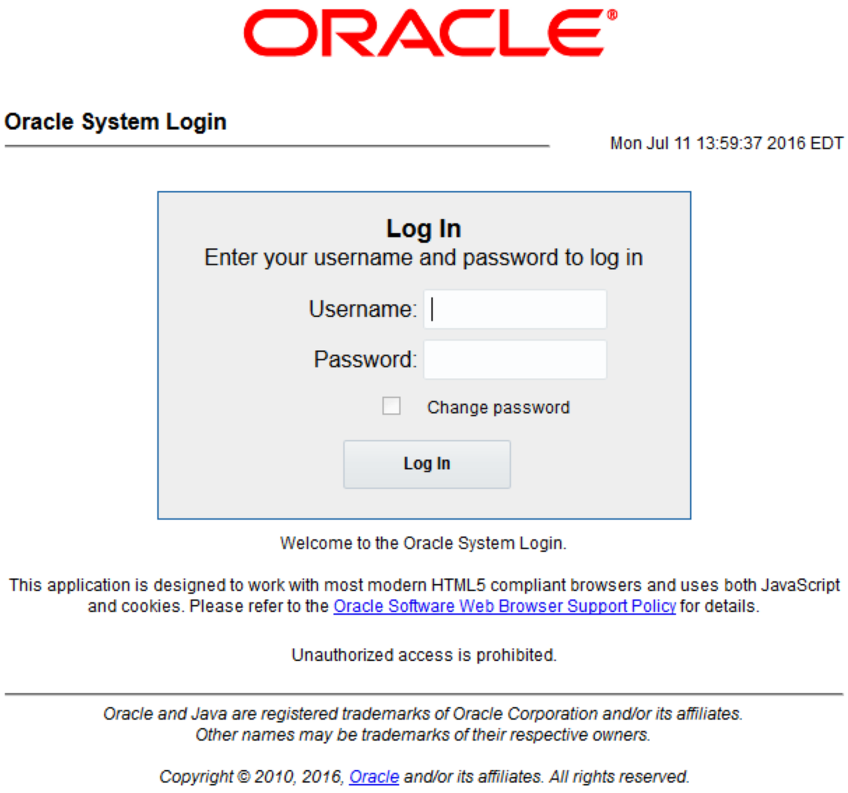
2. □	**Primary NOAM VIP GUI**: Option 1: Configure interface DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. 1. Navigate to **Configuration > Networking>DSCP > Interface DSCP**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations DSCP Interface DSCP Port DSCP 2. Select the server 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 the server group name's tab. 3. Click **Insert**.  Entire Network DA_SG IPFE1_SG IPFE2_SG NO_SG SBRb_SG SBRs_SG SO_SG SS7_SG NO1 NO2 SO1 DAMP1 DAMP2 IPFE1 IPFE2 SS7MP1 SBR-b SBR-s SS7MP2 Interface DSCP Protocol Scope 4. Select the network **Interface** from the list, and type the **DSCP** value to apply to packets leaving this interface. Main Menu: Configuration -> DSC Insert DSCP by Interface on Zombiel Interface * eth3 The serve Note: To c DSCP * 34 A valid DS Protocol * TCP TCP or SC 5. Click **OK** if there are no more interfaces on this server to configure, or **Apply** to finish this interface and continue with more interfaces by selecting them from the list and typing their **DSCP** values.

Procedure 31. Configure DSCP Values for Outgoing Traffic (Optional)

3. □	**Primary NOAM VIP GUI**: Option 2: Configure port DSCP	***Note***: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. 1. Navigate to **Configuration > Networking > DSCP > Port DSCP**.  2. Select the server 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 the server group name's tab. 3. Click **Insert**.  Main Menu: Configuration -> DSCP -> Port DSCP Entire Network DA_SG IPFE1_SG IPFE2_SG NO_SG SBRb_SG SBRs_SG SO_SG SS7_SG NO1 NO2 SO1 DAMP1 DAMP2 IPFE1 IPFE2 SS7MP1 SBR-b SBR-s SS7MP2 Port DSCP Protocol Scope 4. Type the source **Port** and **DSCP** value, and select the transport **Protocol**.  Main Menu: Configuration -> DSCP -> Port DSCI Insert DSCP by Port on ZombieNOAM2 Port * 3568 A valid TCP or SCTP port. [Default DSCP * 15 A valid DSCP value. [Default = N/A Protocol * TCP TCP or SCTP protocol. [Default = 5. Click **OK** if there are no more port DSCPs on this server to configure, or **Apply** to finish this port entry and continue entering more port **DSCP mappings**.
4. □	Repeat for additional servers	Repeat steps 2-3 for all remaining servers.

5.4 Configure IP Front End (Optional)

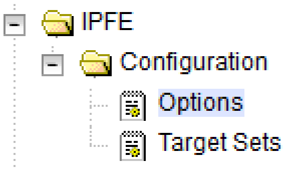
Procedure 32. IP Front End (IPFE) Configuration

STEP #	This procedure configures IP Front End (IPFE) and optimizes performance. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**SOAM VIP**: Login	Log into the **SOAM VIP** GUI as the **guiadmin** user.  ORACLE® **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

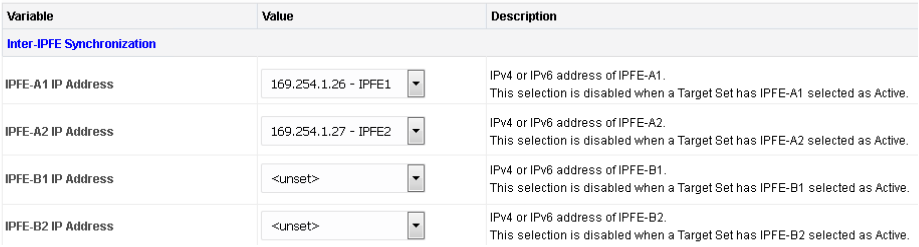
Procedure 32. IP Front End (IPFE) Configuration

2. □ **SOAM VIP**: Configuration of replication IPFE association data

1. Navigate to **IPFE > Configuration > Options**.



2. 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.
3. If applicable, type the address of the **3rd** and **4th** IPFE servers in **IPFE-B1 IP Address** and **IPFE-B2 IP Address** fields.

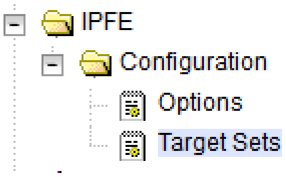
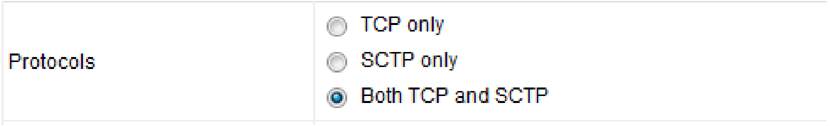
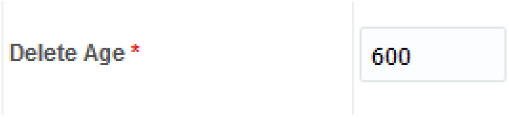
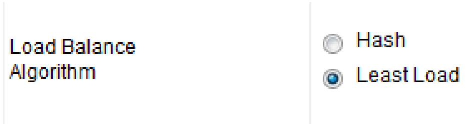
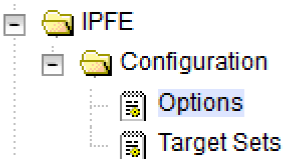


Variable	Value	Description
Inter-IPFE Synchronization		
IPFE-A1 IP Address	169.254.1.26 - IPFE1	IPv4 or IPv6 address of IPFE-A1. This selection is disabled when a Target Set has IPFE-A1 selected as Active.
IPFE-A2 IP Address	169.254.1.27 - IPFE2	IPv4 or IPv6 address of IPFE-A2. This selection is disabled when a Target Set has IPFE-A2 selected as Active.
IPFE-B1 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B1. This selection is disabled when a Target Set has IPFE-B1 selected as Active.
IPFE-B2 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B2. This selection is disabled when a Target Set has IPFE-B2 selected as Active.

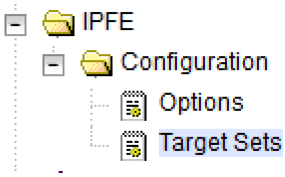
Note: It is recommended the address reside on the **IMI (Internal Management Interface)** network.

Note: **IPFE-A1** and **IPFE-A2** must have connectivity between each other using these addresses. The same applies with **IPFE-B1** and **IPFE-B2**.

Procedure 32. IP Front End (IPFE) Configuration

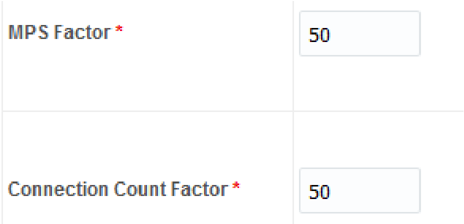
3. □	**SOAM VIP**: Configuration of IPFE target sets (Part 1)	1. Log into the **SOAM VIP** GUI as the **guiadmin** user. 2. Navigate to **IPFE > Configuration > Target Sets**.  3. Click either **Insert IPv4** or **Insert IPv6** depending on the IP version of the target set you plan to use. This screen displays the following configurable settings: **Protocols**: Protocols the target set supports.  Protocols ○ TCP only ○ SCTP only ● Both TCP and SCTP **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.  Delete Age * 600 **Load Balance Algorithm**: Hash or Least Load options.  Load Balance Algorithm ○ Hash ● Least Load ***Note***: For the IPFE to provide Least Load distribution, navigate to **IPFE > Configuration > Options**, Monitoring Protocol must be set to Heartbeat so the application servers can provide the load information the IPFE uses to select the least-loaded server for connections.  ***Note***: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.
4. □	**SOAM VIP**: Configuration of IPFE target sets (Part 2)	1. Navigate to **IPFE > Configuration > Target Sets**.

Procedure 32. IP Front End (IPFE) Configuration



(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 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.



MPS Factor * 50

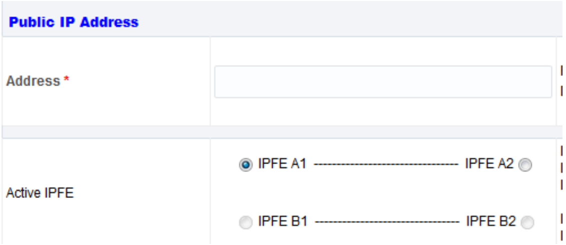
Connection Count Factor * 50

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 Deusingtion: Percentage within which two application server's load calculation results are considered to be equal. If very short, intense connection bursts are expected to occur, increase the value to smooth out the distribution.

Allowed Deviation * 5

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



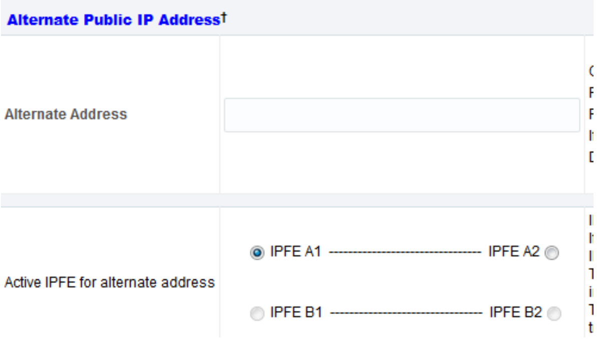
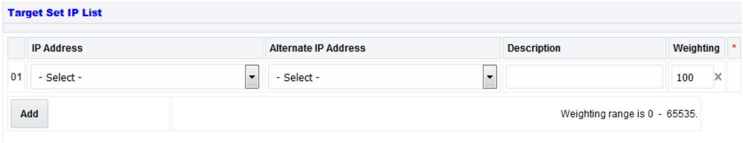
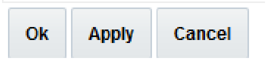
Public IP Address

Address *

Active IPFE ● IPFE A1 ---------- IPFE A2 ○ ○ IPFE B1 ---------- IPFE B2 ○

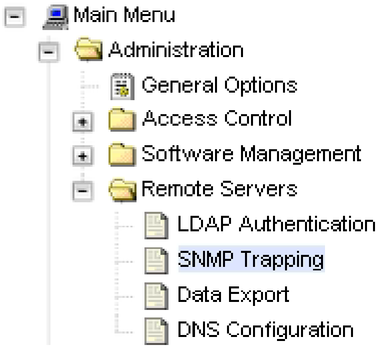
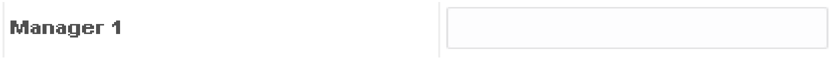
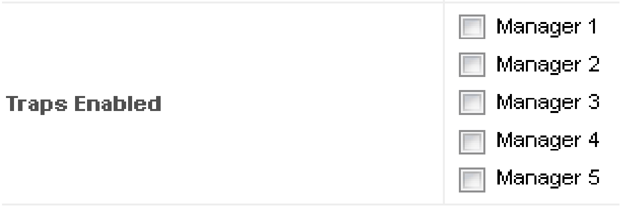
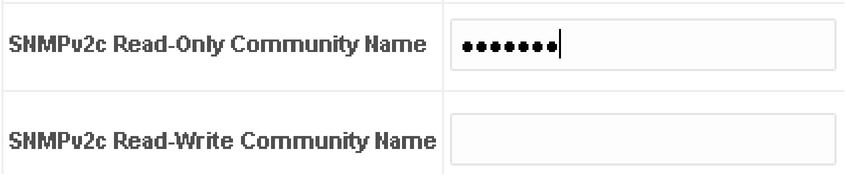
Note: This address must reside on the XSI (External Signaling Interface) network because it is used by the application clients to reach the application servers. This address MUST NOT be a real interface

Procedure 32. IP Front End (IPFE) Configuration

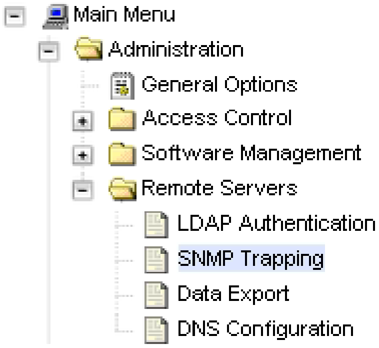
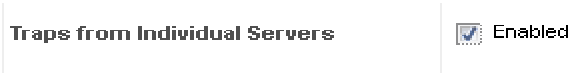
		address (that is, must not be associated with a network interface card). **Active IPFE**: IPFE to handle the traffic for the target set address. **Secondary Public IP Address**: If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.  Alternate Public IP Address† Alternate Address Active IPFE for alternate address ● IPFE A1 ---------------------------- IPFE A2 ○ ○ IPFE B1 ---------------------------- IPFE B2 ○ ***Note***: A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections are not multi-homed. ***Note***: If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure SCTP failover functions as designed. **Target Set IP List**: Select an IP address, a secondary IP address if supporting **SCTP multi-homing**, a description, and a weight for the application server.  Target Set IP List IP Address | Alternate IP Address | Description | Weighting | * 01 | - Select - | - Select - | | 100 × Add Weighting range is 0 - 65535. ***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 (for example, 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. 2. Click **Add** to add more application servers (up to 16). 3. Click **Apply**. 
5. □	**SOAM VIP**: Repeat for additional configuration of IPFE target sets	Repeat for steps 3 and 4 for each target set (up to 16). At least one target set must be configured.

5.5 SNMP Configuration (Optional)

Procedure 33. 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.	
1. □	**NOAM VIP**: Configure system-wide SNMP trap receiver(s)	1. Using a web browser, log into the NOAM VIP as the **guiadmin** user. Navigate to **Administration** > **SNMP**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Click **Insert**. 3. Type the **IP address** or **Hostname** of the Network Management Station (NMS) to forward traps to. This IP should be reachable from the NOAM's **XMI** network. 4. Continue to add secondary manager IPs in the corresponding fields, if needed. Manager 1 **Traps Enabled** checkboxes can be marked on a per manager basis. Traps Enabled ☐ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5 Type the **SNMP Community Name**. SNMPv2c Read-Only Community Name: ••••••• SNMPv2c Read-Write Community Name: 5. Leave all other fields with their default values. 6. Click **OK**.

Procedure 33. Configure SNMP Trap Receiver(s) (Optional)

2. □	**NOAM VIP**: Enable traps from individual servers (Optional)	***Note***: By default, SNMP traps from MPs are aggregated and displayed at the active NOAM. If instead, you want every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable. 1. Using a web browser, log into the NOAM VIP as the **guiadmin** user. Navigate to **Administration** > **SNMP**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Make sure the **Enabled** checkbox is marked, if not, mark it as shown below:  Traps from Individual Servers ☑ Enabled 3. Click **Apply** and verify the data is committed.

5.6 Create iDIH Virtual Machines - VMware (Optional)

Procedure 34. (VMware 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.	
1. □	Add the iDIH Oracle OVA to VMware	1. Launch the VMware client of your choice. 2. Add the **iDIH Oracle OVA** image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.
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 data store.

Procedure 34. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

3. □	Configure resources for the iDIH Oracle VM	1. Configure the **iDIH Oracle VM** per the resource profiles defined in [27] DSR Cloud Benchmarking Guide using the vSphere client or the vSphere web client. 2. Record the Ethernet addresses associated with each interface and the virtual network with which it is associated. ***Note***: Make sure the order of the interface creation is XMI, INT, and then IMI, if there is any. Only the Mediation VM requires the IMI interface.
4. □	iDIH Oracle VM Only: Create a raw storage block device (external device)	***Note***: This step is **ONLY** required for iDIH Oracle VM. Create an extra disk for the Oracle VM. Add the second disk using the vSphere client or the vSphere web client.
5. □	Power on the iDIH Oracle VM	Use the **vSphere client** or **vSphere web client** to power on the **iDIH Oracle VM**.

6.
□
	iDIH Oracle VM Only: Verify the extra/second disk exists	***Note***: This step is **ONLY** required for iDIH Oracle VM.
		Check if the raw storage block device (external disk) added in step 3 exits by executing any of these commands:
		`$ ls /dev/[sv]db`
		`$ fdisk -l`
		`$ df -h`
		Note: Please DO NOT mount or format the added raw block device. Oracle ASM (Automatic Storage Management) automatically manages it. If you see it has been mounted, unmount it and make sure to completely remove the entry in the /etc/fstab.

7. □	Repeat	Repeat steps 1 through 6 for the following VMs. Use unique labels for the VM names: iDIH Application iDIH Mediation

5.7 Create iDIH Virtual Machines - KVM/OpenStack (Optional)

Procedure 35. (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.

1. □ Add the iDIH Oracle OVA to KVM/OpenStack

1. Copy the OVA file to the OpenStack control node.

   ```
   $ scp oracle-8.2.x.x.x.ova admusr@node:~
   ```

2. Log into the OpenStack control node.

   ```
   $ ssh admusr@node
   ```

3. In an empty directory, unpack the OVA file using **tar**.

   ```
   $ tar xvf oracle-8.2.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-8.2.x.x.x-disk1.vmdk

   Note: The OVA format only supports files with a max size of 8GB, so a vmdk file larger than that is split. You should be able to concatenate the files together to merge them back into one file:

   ```
   $ cat ORA-80_x_x.vmdk.000000000 ORA-
   80_x_x.vmdk.000000001 > ORA-80_x_x.vmdk
   ```

5. Source the OpenStack **admin** user credentials.

   ```
   $ .  keystonerc_admin
   ```

6. Select an informative name for the new image.

   ORA-8.2_x_x

7. Import the image using the **glance** utility from the command line.

   ```
   $ glance image-create --name oracle-8.2.x.x.x-original
   --visibility public --protected false  --progress --
   container-format bare --disk-format vmdk --file oracle-
   8.2.x.x.x-disk1.vmdk
   ```

This process takes about 5 minutes depending on the underlying infrastructure.

8. (Optional – Steps 8 and 9 are not needed if VMDK is used.) Convert VMDK to QCOW2 format.

   Use the qemu-img tool to create a qcow2 image file using this command.

   ```
   qemu-img convert -f vmdk -O qcow2 <VMDK filename>
   <QCOW2 filename>
   ```

   For example:

   ```
   qemu-img convert -f vmdk -O qcow2 DSR-82_12_0.vmdk DSR-
   82_12_0.qcow2
   ```

   Install the qemu-img tool (if not already installed) using this yum command.

Procedure 35. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

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

```
sudo yum install qemu-img
```

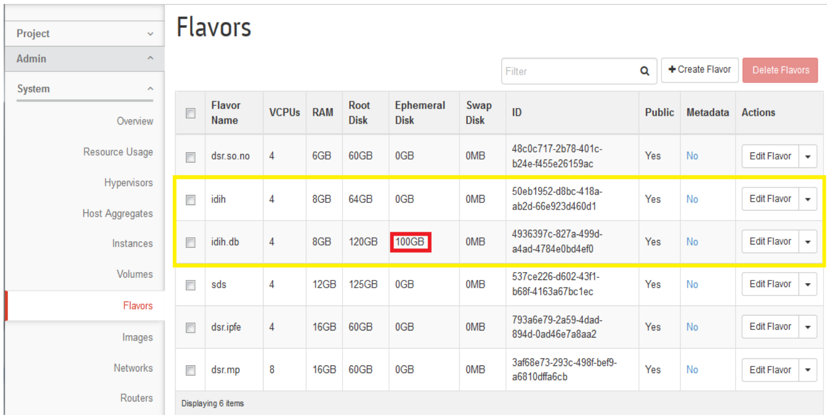
9. Import the coverted qcow2 image using the **glance** utility from the command line.

```
$ glance image-create --name dsr-x.x.x-original --is-
public True --is-protected False --progress  --
container-format bare --disk-format qcow2 --file DSR-
x.x.x-disk1.qcow2
```

This process take about 5 minutes depending on the underlying infrastructure.

</td>
</tr>
<tr>
<td>2.
□</td>
<td>Create flavors for iDIH</td>
<td>

Examine the storage recommendations in the resource profiles defined in [27] DSR Cloud Benchmarking Guide. A block storage must be created and attached for the Oracle VM. For example, create an idih.db for the Oracle database with an 100GB ephemeral disk.



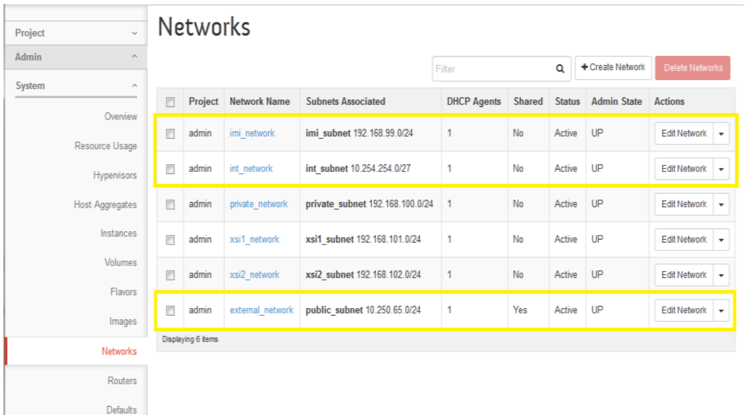
Flavors

<table>
<tr><th>□</th><th>Flavor Name</th><th>VCPUs</th><th>RAM</th><th>Root Disk</th><th>Ephemeral Disk</th><th>Swap Disk</th><th>ID</th><th>Public</th><th>Metadata</th><th>Actions</th></tr>
<tr><td>□</td><td>dsr.so.no</td><td>4</td><td>6GB</td><td>60GB</td><td>0GB</td><td>0MB</td><td>48c0c717-2b78-401c-b24e-f455e26159ac</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
<tr><td>□</td><td>idih</td><td>4</td><td>8GB</td><td>64GB</td><td>0GB</td><td>0MB</td><td>50eb1952-d8bc-418a-ab2d-66e923d460d1</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
<tr><td>□</td><td>idih.db</td><td>4</td><td>8GB</td><td>120GB</td><td>100GB</td><td>0MB</td><td>4936397c-827a-499d-a4ad-4784e0bd4ef0</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
<tr><td>□</td><td>sds</td><td>4</td><td>12GB</td><td>125GB</td><td>0GB</td><td>0MB</td><td>537ce226-d602-43f1-b68f-4163a67bc1ec</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
<tr><td>□</td><td>dsr.ipfe</td><td>4</td><td>16GB</td><td>60GB</td><td>0GB</td><td>0MB</td><td>793a6e79-2a59-4dad-894d-0ad46e7a8aa2</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
<tr><td>□</td><td>dsr.mp</td><td>8</td><td>16GB</td><td>60GB</td><td>0GB</td><td>0MB</td><td>3af68e73-293c-498f-bef9-a6810dffa6cb</td><td>Yes</td><td>No</td><td>Edit Flavor</td></tr>
</table>

Displaying 6 items

</td>
</tr>
<tr>
<td>3.
□</td>
<td>Create network interfaces</td>
<td>

Examine the network interface recommendations defined in [27] DSR Cloud Benchmarking Guide. Network ports must be created for each recommended interface. For example:



Networks

<table>
<tr><th>□</th><th>Project</th><th>Network Name</th><th>Subnets Associated</th><th>DHCP Agents</th><th>Shared</th><th>Status</th><th>Admin State</th><th>Actions</th></tr>
<tr><td>□</td><td>admin</td><td>imi_network</td><td>imi_subnet 192.168.99.0/24</td><td>1</td><td>No</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
<tr><td>□</td><td>admin</td><td>int_network</td><td>int_subnet 10.254.254.0/27</td><td>1</td><td>No</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
<tr><td>□</td><td>admin</td><td>private_network</td><td>private_subnet 192.168.100.0/24</td><td>1</td><td>No</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
<tr><td>□</td><td>admin</td><td>xsi1_network</td><td>xsi1_subnet 192.168.101.0/24</td><td>1</td><td>No</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
<tr><td>□</td><td>admin</td><td>xsi2_network</td><td>xsi2_subnet 192.168.102.0/24</td><td>1</td><td>No</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
<tr><td>□</td><td>admin</td><td>external_network</td><td>public_subnet 10.250.65.0/24</td><td>1</td><td>Yes</td><td>Active</td><td>UP</td><td>Edit Network</td></tr>
</table>

Displaying 6 items

</td>
</tr>
<tr>
<td>4.
□</td>
<td>Create and boot the iDIH VM instance from the glance image</td>
<td>

1. Get the following configuration values.

The image ID.

```
$ glance image-list
```

The flavor ID.

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

Procedure 35. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

```
$ 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. Use one **--nic** argument for each IP/interface. Number of IP/interfaces for each VM type must conform with the interface-to-network mappings defined in [27] DSR Cloud Benchmarking Guide.

   Note: IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.

For Oracle VM Only

Create the ephermeral storage for only the Oracle VM.

```
$ nova boot --image <image ID> --flavor <flavor id or
name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip
address> --nic net-id=<int network id>,v4-fixed-ip=<int
ip address> --ephemeral size=100 --config-drive true
<instance name>
```

For example:

```
$ nova boot --image 7e881048-190c-4b66-b26e-
dc5b9dc3c07f --flavor idih.db --nic net-id=e96cb10a-
9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.161 -
-nic net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-
fixed-ip=10.254.254.2 --ephemeral size=100 –config-
drive true iDIH-Oracle
```

For Application VM Only

```
$ nova boot --image <image ID> --flavor <flavor id or
name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip
address> --nic net-id=<int network id>,v4-fixed-ip=<int
ip address> --config-drive true <instance name>
```

For example:

```
$ nova boot --image 7e881048-190c-4b66-b26e-
dc5b9dc3c07f --flavor idih.db --nic net-id=e96cb10a-
9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.161 -
-nic net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-
fixed-ip=10.254.254.2 –config-drive true iDIH-App
```

For Mediation VM Only

For Mediation, add the IMI interface as the IMI interface.

```
$ nova boot --image <image ID> --flavor <flavor id or
name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip
```

Procedure 35. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

		`address> --nic net-id=<int network id>,v4-fixed-ip=<int ip address> --nic net-id=<imi network id>,v4-fixed-ip=<imi ip address> -config-drive true <instance name>`
		For example:
		`$ nova boot --image f548c2cd-1ddd-4c56-b619-b49a69af8801 --flavor idih --nic net-id=e96cb10a-9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.162 --nic net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-fixed-ip=10.254.254.3 --nic net-id=3d9b9da8-96ad-4f29-9f82-98b00ea30446,v4-fixed-ip=192.168.99.3 -config-drive true iDIH-Mediation`
		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.

5. □	Verify configured interface	If DHCP is enabled on the Neutron subnet, VM configures the VNIC with the IP address provided in step 4. To verify, ping the XMI IP address provided with the **nova boot**… command from step 4: `$ ping <XMI-IP-Provided-During-Nova-Boot>` If successfully pinging, ignore the step 6 to manually configuring the interface.

Procedure 35. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

6.
□
	Manually configure interface, if not already done (Optional)	***Note***: If the instance is already configured with an interface and has successfully pinged (step 5), then **ignore** this step to configure the interface manually.
		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** user.
		6. Configure the network interfaces, conforming with the interface-to-network mappings defined in [27] DSR Cloud Benchmarking Guide.
		`$ 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.
		7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible using both network and Horizon consoles.

7. □	Repeat	Repeat steps 1 through 4 for the following VMs. Use unique labels for the VM names: iDIH-Application iDIH-Mediation

5.8 Create iDIH Virtual Machines - OVM-S/OVM-M (Optional)

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

STEP #

This procedure imports the IDIH image and creates/configures a VM. Repeat this procedure three times for:

- IDIH-Oracle (db)
- IDIH-Application (app)
- IDIH-Mediation (med)

Replace XXX in variable names with the different suffix – when repeating.

This procedure requires values for these variables:

- <OVM-M IP> = IP address to access a sh prompt on the OVM server
- <URL to IDIH-XXX OVA>= link(s) to a source for each IDIH product image (.ova)
- <MyRepository name> = name of the repository in the OVM to hold the product images (.ova)
- <ServerPool name>
- <VM name>
- <OVM network ID for XMI>
- <OVM network ID for IDIH Internal>
- <OVM network ID for IMI>

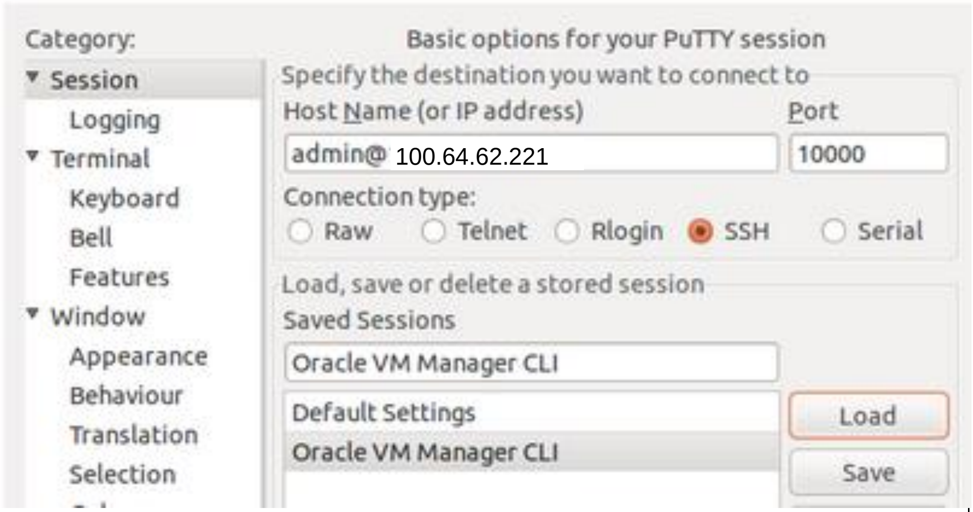
Execution of this procedure will discover and use the values of these variables:

- <Virtual Appliance IDIH-XXX OVA ID>
- <IDIH-XXX-OVA VM name_vm_vm>
- <VM id>
- <vCPUs Production>
- <Vnic 1 id>
- <size in GB>
- <VirtualDiskId>
- <VirtualDiskName>
- <Slot#>

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 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

1. □	**Preparation**: Access command line of OVM	Refer to Common OVM Manager Tasks (CLI) for setting up the platform. 1. Use the respective value for <OVM-M IP> into the command. `ssh -l admin <OVM-M IP> -p 10000` Example: `ssh -l admin 100.64.62.221 -p 10000` Alternate: use a terminal emulation tool like putty.  Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Basic options for your PuTTY session Specify the destination you want to connect to Load, save or delete a stored session Default Settings Load Save Host Name (or IP address): admin@ 100.64.62.221 Port: 10000 Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial Saved Sessions: Oracle VM Manager CLI Oracle VM Manager CLI

2.
□
	OVM-M CLI: Import the VirtualAppliance/ OVA for IDIH-XXX	1. Use the respective values for <MyRepository name> and <URL to IDIH-XXX OVA> into the command.
		`OVM>importVirtualAppliance Repository name=’<MyRepository name>’ url=<URL to IDIH-XXX OVA>`
		Example:
		`OVM> importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/IDIH/8.2/ova/oracle-8.2.0.0.0_82.4.0.ova`
		2. Execute the command and validate success.
		3. Examine the screen results to find site-specific text for variables in these locations:
		`Command: importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`Status: Success`
		`Time: 2017-04-18 15:23:31,044 EDT`
		`JobId: 1492543363365`
		`Data:`
		`  ID: 1128a1c6ce name: DSR-8.2.0.0.0_82.4.0.ova`
		4. Use the respective values for values for these variables (overwrite example).
		<Virtual Appliance IDIH-XXX OVA ID> = `1128a1c6ce`

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

3.
□
	OVM-M CLI:
	Get the virtual appliance name. It is used in <IDIH-XXX OVA VM name> in later steps
		1. Use the respective values for <Virtual Appliance IDIH-XXX OVA ID> in the command.
		`OVM> show VirtualAppliance id=<Virtual Appliance IDIH-XXX OVA id>`
		Example:
		`OVM> show VirtualAppliance id=1128a1c6ce`
		2. Execute the command and validate success.
		3. Examine the screen results to find site-specific text for variables in these locations:
		Command: `show VirtualAppliance id=1128a1c6ce`
		`Status: Success`
		`Time: 2017-04-18 15:23:53,534 EDT`
		`Data:`
		`  Origin = http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`  Repository = 0004fb0000030000da5738315337bfc7  [XLab Utility Repo01]`
		`  Virtual Appliance Vm 1 = 11145510c0_vm_vm  [vm]`
		`  Virtual Appliance VirtualDisk 1 = 11145510c0_disk_disk1  [disk1]`
		`  Id = 11145510c0  [DSR-8.2.0.0.0_82.4.0.ova]`
		`  Name = DSR-8.2.0.0.0_82.4.0.ova`
		`  Description = Import URL: http://10.240.155.70/iso/DSR/8.2/ova/DSR-8.2.0.0.0_82.4.0.ova`
		`  Locked = false`
		4. Use the respective values for these variables (overwrite example).
		<IDIH-XXX-OVA VM name_vm_vm> = `11145510c0_vm_vm`

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

4.
□
	OVM-M CLI:
	Create a VM for IDIH-XXX OVA VM
		Create a virtual machine from the virtual machine in the OVA virtual appliance.
		1. Use the respective value for <IDIH-db-OVA VM name_vm_vm> into the command.
		`OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=<IDIH-XXX-OVA VM name_vm_vm>`
		Example:
		`OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm`
		2. Execute the command and validate success.
		3. Examine the screen results to find site-specific text for variables in these locations:
		Command: `createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm`
		`Status: Success`
		`Time: 2017-04-18 16:02:09,141 EDT`
		`JobId: 1492545641976`
		`Data:`
		`  id: 0004fb00000600004a0e02bdf9fc1bcd name: oracle-8.2.0.0.0_82.4.0.ova`
		4. Use the respective values for these variables (overwrite example).
		<VM id> = `0004fb00000600004a0e02bdf9fc1bcd`

5.
□
	OVM-M CLI:
	Add the VM to the server pool
		1. Use the respective values for <VM ID> and <ServerPool name> into the command.
		`OVM> add Vm id=<VM id> to ServerPool name=”<ServerPool name>”`
		Example:
		`OVM> add Vm id=0004fb00000600004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"`
		2. Execute the command and validate success.
		Note: Refer Server Pool section in Appendix D.2 for further information on Server Pool.

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

<table>
<tr>
<td>6.
□</td>
<td><b>OVM-M CLI</b>:
Edit VM to apply required profile/ resources</td>
<td>
1. Refer to [27] DSR Cloud Benchmarking Guide for recommended resource.
<table>
<tr><th>VM Name</th><th>vCPUs Lab</th><th>RAM (GB) Lab</th><th>vCPUs Production</th><th>RAM (GB) Production</th><th>Storage (GB) Lab and Production</th></tr>
<tr><td>Type of guest host</td><td>#</td><td>#</td><td>#</td><td>#</td><td>#</td></tr>
</table>
2. Use the respective values for <VM ID>, <VM name>, and <vCPUs Production> into the command.
<pre>
OVM> edit Vm id=<VM id> name=<VM name> memory=6144
memoryLimit=6144 cpuCountLimit=<vCPUs Production>
cpuCount=<vCPUs Production> domainType=XEN_HVM
description="<VM name>"
</pre>
Example:
<pre>
OVM> edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=
na_idih-db memory=6144 memoryLimit=6144 cpuCountLimit=4
cpuCount=4 domainType=XEN_HVM description="na_idih-db"
</pre>
3. Execute the command and validate success.
Now, the VM has a name and resources.
</td>
</tr>
<tr>
<td>7.
□</td>
<td><b>OVM-M CLI:</b>
Detemine VNIC ID</td>
<td>
1. Use the respective value for <VM name> in the command.
<pre>
OVM> show Vm name=<VM name>
</pre>
Example:
<pre>
OVM> show Vm name= na_idih-db
</pre>
2. Execute the command and validate success.
3. Examine the screen results to find site-specific text for variables in these locations:
<pre>
Vnic 1 = 0004fb0000070000091e1ab5ae291d8a
</pre>
4. Use the respective values for these variables (overwrite example).
<Vnic 1 ID> = 0004fb0000070000091e1ab5ae291d8a
</td>
</tr>
<tr>
<td>8.
□</td>
<td>Determine network interfaces for the type of guest host</td>
<td>
Refer to [27] DSR Cloud Benchmarking Guide to learn which network interfaces need to be configured for each guest type. The table looks like this:
<table>
<tr><th></th><th>OAM (XMI)</th><th>Local (IMI)</th><th>Sig A (XSI1)</th><th>Sig B (XSI2)</th><th>Sig C (XSI3-16)</th><th>Rep (SBR)</th><th>DIH Internal</th></tr>
<tr><td>Type of guest host</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td></tr>
</table>
<b><i>Note</i></b>: The VNICs need to be created in the correct order so the interfaces are associated with the correct network.
</td>
</tr>
</table>

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

9.
□
	OVM-M CLI: Add (attach) XMI VNIC ID of the XMI network to VM (if required by guest host type)	1. Use the respective values for <Vnic 1 ID> and <OVM network ID for XMI> into the command
		`OVM> add Vnic ID=<Vnic 1 ID> to Network name=<OVM network ID for XMI>`
		Example:
		`OVM> add Vnic ID=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9`
		2. Execute the command and validate success.

10.
□
	OVM-M CLI: Create and attach IDIH Internal VNIC to VM (if required by guest host type)	1. Use the respective values for <OVM network ID for IDIH Internal> and <VM name> into the command
		`OVM> create Vnic network=<OVM network id for IDIH Internal> name=<VM name>-int on Vm name=<VM name>`
		Example:
		`OVM> create Vnic network=DIH Internal name=na_idih-db-int on Vm name=na_idih-db`
		2. Execute the command and validate success

11.
□
	OVM-M CLI: Create and attach IMI VNIC ID to VM (if required by guest host type)	1. Use the respective values for <OVM network ID for IMI> and <VM name> into the command.
		`OVM> create Vnic network=<OVM network ID for IMI> name=<VM name>-IMI on VM name=<VM name>`
		Example:
		`OVM> create Vnic network=102e89a481 name= na_idih-db-IMI on Vm name= na_idih-db`
		2. Execute the command and validate success.

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

12.
□
	[iDIH Oracle VM Only] OVM-M CLI: Create a raw storage block device (external device)	**Create an extra virtual disk (only required on IDIH-Oracle (db) if the system is using OVM).**
		1. Decide on a name for the virtual disk: <VirtualDiskName>
		2. Refer the resource profiles defined in [27] DSR Cloud Benchmarking Guide to learn the required GB of Storage for the IDIH type: <size in GB>
		3. Use the respective value for <MyRepository Name> into the command.
		`OVM> create VirtualDisk name=’<VirtualDiskName>’ size=<size in GB> sparse=<Yes/No> shareable=<Yes/No> on Repository name=’<MyRepository Name>’`
		Example:
		`OVM> create VirtualDisk name=idih-db_disk1 size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'`
		4. Examine the screen results to find site-specific text for variables in these locations:
		`Command: create VirtualDisk name=idih-db_disk size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'`
		`Status: Success`
		`Time: 2017-04-24 15:29:12,502 EDT`
		`JobId: 1493061481113`
		`Data:`
		`  id:0004fb00001200001bae7adbe6b20e19.img  name:idih-db_disk`
		5. Use the respective values for these variables (overwrite example).
		<VirtualDiskId> = `0004fb00001200001bae7adbe6b20e19.img`
		<VirtualDiskName> = `idih-db_disk`

Procedure 36. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each

13.
□
	[iDIH Oracle VM Only] OVM-M CLI: Map the created virtual disk to a slot on the VM	1. Decide on a slot for the virtual disk: <Slot#>
		2. Use the respective values for <Slot#> & <VirtualDiskId> & <VirtualDiskName> & <VM name> into the command.
		`OVM> create VmDiskMapping slot=<Slot#> virtualDisk=<VirtualDiskId> name="<VirtualDiskName>" on Vm name=<VM name>`
		Example:
		`OVM> create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db`
		3. Execute the command and validate success.
		`Command: create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db`
		`Status: Success`
		`Time: 2017-04-24 15:32:50,875 EDT`
		`JobId: 1493062370724`
		`Data:`
		`  id:0004fb000013000057ab9b00e6d47add  name:idih-db_disk`

14.
□
	OVM-M CLI: Start VM	1. Use the respective value for <VM name> into the command
		`OVM> start Vm name=<VM name>`
		Example:
		`OVM> start Vm name= na_idih-db`
		2. Execute the command and validate success

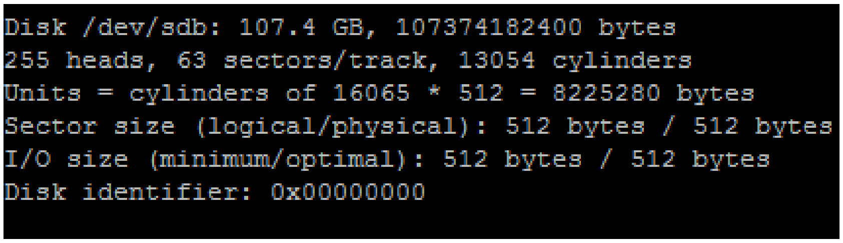
15. □	Repeat	Repeat steps 2 through 14 for the following VMs. Use Unique labels for the VM names: iDIH-Application iDIH-Mediation

5.9 Configure iDIH Virtual Machines (Optional)

Procedure 37. Configure iDIH VM Networks (Optional)

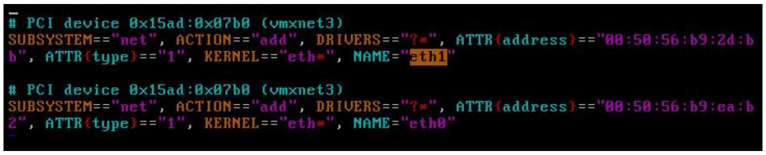
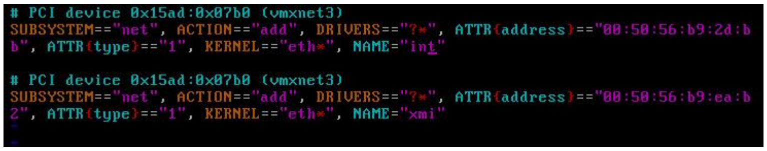
S T E P #	This procedure configures the iDIH guest VM external management networks. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	Log into the Oracle VM console	1. Access the iDIH Oracle VM console. 2. Login as the **admusr** user.

Procedure 37. Configure iDIH VM Networks (Optional)

2.
□
	(Oracle VM only) Verify the extra/second disk exists	***Note***: This step is required **ONLY** for the Oracle VM.
		Check if the raw storage block device (external disk) exists by executing any of below commands (similar to the screenshot):
		`$ ls /dev/[sv]db`
		`$ sudo fdisk -l`
		`$ df -h`
		
		`Disk /dev/sdb: 107.4 GB, 107374182400 bytes`
		`255 heads, 63 sectors/track, 13054 cylinders`
		`Units = cylinders of 16065 * 512 = 8225280 bytes`
		`Sector size (logical/physical): 512 bytes / 512 bytes`
		`I/O size (minimum/optimal): 512 bytes / 512 bytes`
		`Disk identifier: 0x00000000`
		If the extra disk does not exist, revisit the procedures for respective hypervisors. (Procedure 34 for VMware, Procedure 35 for KVM, and Procedure 36 for OVM-M).
		Note: Please DO NOT mount or format the added raw block device. Oracle ASM (Automatic Storage Management) automatically manages it. To verify it, execute the following command:
		`$ df`
		Note: If you see it has been mounted, unmount it and completely remove the entry in the /etc/fstab.
		For example:
		1. If any external drive (such as, /dev/vdb) is mounted, then unmount the external drive by executing the following command on oracle server: `umount /dev/vdb`
		2. Edit the /etc/fstab file on the Oracle server, and if any entry for /dev/vdb is present in the file, then remove the entry and save the file.

3. □	Delete the eth0 interface	`$ sudo netAdm delete --device=eth0`
4. □	Trigger net rules file creation	Run the udevadm command to recreate net rules file. `$ sudo udevadm trigger --subsystem-match=net` ***Note***: If this command does not create the net rules file, create it manually. Refer to Sample Net Rules File.

Procedure 37. Configure iDIH VM Networks (Optional)

5.
□
	Modify the ethernet interface names in the net rules file	1. Update the net rules file to replace the default interfaces names ethX with XMI and INT interfaces names. Replace **eth0** with **XMI**; and **eth1** with **INT** interface. Also, respective MAC addresses should be updated for each interface in lower case. MAC addresses can be determined using `ifconfig -a` command from the console.
		Note: The Mediation VM requires the user to rename a third interface: **eth2** as **IMI** interface.
		2. Refer to Sample Net Rules File for a sample net rules file.
		`$ 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:b9:2d: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:b9:2d: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"`
		3. Reboot the VM.
		`$ sudo init 6`

6.
□
	As admusr on the Oracle VM configure the networks with netAdm	1. Log into the **iDIH Oracle VM** console as the **admusr** user.
		2. The XMI network should already exist, but it can be created with the following command.
		`$ sudo netAdm add --device=xmi --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes`
		3. Configure the int network IP address and netmask.
		`$ sudo netAdm add --device=int --address=10.254.254.2 --netmask=255.255.255.224`
		Note: Oracle VM internal IP = 10.254.254.2; the Mediation VM 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.
		4. **Mediation Only**. If this is a Mediation VM, configure the Mediation internal management network.
		`$ sudo netAdm add --device=imi --address=<IP Address in Internal Management Network> --netmask=<Netmask>`
		5. Configure the default gateway.
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External Management Network> --device=xmi`
		The VM network configuration has been completed. You should be able to **ssh** into the server through XMI interface.

Procedure 37. Configure iDIH VM Networks (Optional)

7. □	As admusr on the Oracle VM configure NTP and the Oracle VM hostname	1. On the Oracle VM console, launch the platform configuration menu. `$ sudo su - platcfg` 2. From the platform configuration menu configure ntpserver1 with the IP address supplied for NTP. Navigate to **Network Configuration > NTP > Edit > ntpserver1**. Click **Yes** when asked to restart NTP. ***Note***: Properly configure the NTP on the controller node to reference lower stratum NTP servers. 3. Exit the network configuration menu. 4. Configure the Oracle VM hostname. Navigate to **Server Configuration > Hostname > Edit**. ***Notes***: • Typically, we select hostname and identify the host as iDIH application, iDIH Mediation, and iDIH Oracle. • Remove any occurrence of "**.**" and the "**.<availability zone>**" name, such as "**.novalocal**" from the hostname that might have been appended. 5. Exit the platform configuration menu.
8. □	Repeat	Repeat Steps 1 through 7 for the following VMs. Use unique labels for the VM names: iDIH Mediation iDIH Application

5.10 Post iDIH Installation Configuration (Optional)

Procedure 38. Run Post Installation Scripts on iDIH VMs (Optional)

S T E P #	This procedure runs post installation scripts on the iDIH VMs. **Prerequisite**: Procedure 3 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.	
1. □	Log into the iDIH Oracle VM Console	1. Access the iDIH Oracle VM console. 2. Login as the **admusr** user.

Procedure 38. Run Post Installation Scripts on iDIH VMs (Optional)

2. □	Run the iDIH Oracle post installation script	1. Wait for the software upgrades to complete on all iDIH VMs. 2. 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 5 to 15 minutes depending on the Oracle version and patch level. Wait for it to complete before the next step is executed. Once the script execution is over, it will come out without any message. ***Note***: To verify the install status, check the /var/TKLC/xIH/log/oracle/post_image_install.log file for any errors. The error stating: **Cannot use backup/restore functions while using dispatcher** can safely be ignored.
3. □	Log into the iDIH Mediation VM Console as admusr	1. Access the **iDIH Mediation VM** console. 2. Login as the **admusr** user.

4.
□
	Run the iDIH Mediation VM post installation script	The Oracle post installation script must come to completion before the Mediation post installation script is run.
		1. As the **admusr** user on the **iDIH Mediation VM** console, run the Mediation post installation script.
		`$ sudo /opt/xIH/mediation/install.sh`
		Note: The Mediation post installation script runs for 2 to 10 minutes. Wait for it to complete before the next step is executed. To verify the install status, check the /var/TKLC/xIH/log/mediation/post_image_install.log file for any errors.
		Note: It is assumed network configuration and functionality is correct before 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:
		a. Log into the Mediation server as **admusr**.
		b. Execute the command **sudo su - tekelec**.
		c. Execute the command **sqlplus /@NSP**.
		2. 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 ``

5. □	Log into the iDIH application VM console as admusr	1. Access the iDIH Application VM console. 2. Login as the **admusr** user.

Procedure 38. Run Post Installation Scripts on iDIH VMs (Optional)

6. □	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 the **admusr** user 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 2 to 10 minutes. Wait for it to complete before executing the next step.
7. □	Run the iDIH health check script on each of the iDIH VMs	Once all of the iDIH VMs have restarted. Run the health check scripts on each iDIH VM. 1. As the **admusr** user on the **iDIH Oracle VM** console, run the **health check 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` 2. As **admusr** on the **iDIH Application VM** console, run the **health check 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` 3. As **admusr** on the **iDIH Mediation VM** console, run the **health check script** and verify results. Ignore 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 39. Configure DSR Reference Data Synchronization for iDIH (Optional)

STEP #	This procedure configures DSR reference data synchronization for iDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**iDIH Application Server**: Login	1. Establish an SSH session to the iDIH Application Server. 2. Login as the **admusr** user. 3. Issue the following command to login as a **tekelec** user. `$ sudo su - tekelec`

2.
□
	iDIH Application Server: Execute configuration script	1. Execute the following script:
		`Apps/trda-config.sh`
		Example output:
		`corsair-app:/usr/TKLC/xIH apps/trda-config.sh`
		`dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-ad`

Procedure 39. Configure DSR Reference Data Synchronization for iDIH (Optional)

```
Please enter DSR oam server IP address: 10.240.39.175

SQL*Plus: Release 12.1.0.2.0 Production on Thu Oct 1
15:04:40 2015

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

Last Successful login time: Thu Oct 01 2015 13:27:57 -
04:00

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.2.0
- 64bit Production

With the Partitioning, Automatic Storage Management, OLAP,
Advanced Analytics and Real Application Testing options

SQL> SQL>   2    3    4    5

1 row merged.

SQL>

Commit complete.

SQL> Disconnected from Oracle Database 12c Enterprise
Edition Release 12.1.0.2.0 - 64bit Produ

With the Partitioning, Automatic Storage Management, OLAP,
Advanced Analytics and Real Application Testing options

Buildfile: /usr/TKLC/xIH/apps/trace-refdata-
adapter/build.xml

app.disable:

common.weblogic.stop:

     [echo]

     [echo]

     [echo]
==========================================================

     [echo] application: xihtra

     [echo] date:    2015-10-01 15:04:41

     [echo]
==========================================================

     [echo] === stop application EAR

     [echo] date:    2015-10-01 15:04:41

     [java] weblogic.Deployer invoked with options:  -
adminurl t3://appserver:7001 -
userconfigprojects/domains/tekelec/keyfile.secure -name
xIH Trace Reference Data Adapter -stop

     [java] <Oct 1, 2015 3:05:08 PM EDT> <Info> <J2EE
Deployment SPI> <BEA-260121> <Initiating

     [java] Task 24 initiated: [Deployer:149026]stop
```

Procedure 39. Configure DSR Reference Data Synchronization for iDIH (Optional)

```
application xIH Trace Reference Data Adap
     [java] Task 24 completed: [Deployer:149026]stop
application xIH Trace Reference Data Adap
     [java] Target state: stop completed on Server nsp
     [java]
BUILD SUCCESSFUL
Total time: 29 seconds
Buildfile: /usr/TKLC/xIH/apps/trace-refdata-
adapter/build.xml
app.enable:
common.weblogic.start:
     [echo]
     [echo]
     [echo]
==========================================================
     [echo] application: xihtra
     [echo] date:    2015-10-01 15:05:10
     [echo]
==========================================================
     [echo] === start application EAR
     [echo] date:    2015-10-01 15:05:10
     [java] weblogic.Deployer invoked with options:  -
adminurl t3://appserver:7001 -
userconfigprojects/domains/tekelec/keyfile.secure -name
xIH Trace Reference Data Adapter -start
     [java] <Oct 1, 2015 3:05:56 PM EDT> <Info> <J2EE
Deployment SPI> <BEA-260121> <Initiating
     [java] Task 25 initiated: [Deployer:149026]start
application xIH Trace Reference Data Ada
     [java] Task 25 completed: [Deployer:149026]start
application xIH Trace Reference Data Ada
     [java] Target state: start completed on Server nsp
     [java]
BUILD SUCCESSFUL
Total time: 1 minute 17 seconds
```

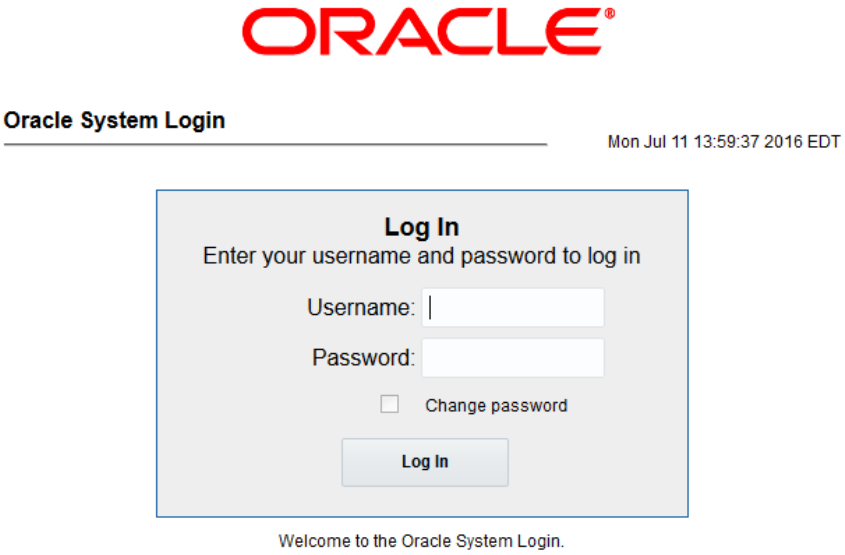
2. When asked to **Please enter DSR OAM server IP address**, type the **VIP** of the DSR SOAM (or active DSR SOAM if VIP is not available) and click **Enter**.

Note: If the address typed is unreachable, the script exits with error **Unable to connect to <ip-address>!**

Procedure 39. Configure DSR Reference Data Synchronization for iDIH (Optional)

3. □	**iDIH Application Server**: Monitor completion	1. Monitor the log file located at: `/var/TKLC/xIH/log/apps/weblogic/apps/application.log` 2. Examine the log file for entries containing text **Trace Reference Data Adapter**.
4. □	**iDIH Application Server** (Optional): Switch iDIH from one DSR to another DSR in a different network	***Note***: This is an optional step which is needed to switch an IDIH from one DSR to another DSR in a different network 1. Establish an SSH session to the iDIH Application Server. 2. Login as the **tekelec** user 3. Execute these commands: a. cd /usr/TKLC/xIH/apps/trace-refdata-adapter b. ant clean.data c. cd /usr/TKLC/xIH/apps/xihoam d. ant imp.init (flush comagent connection data) e. cd /usr/TKLC/xIH/apps/trace-refdata-adapter f. ant app.enable (Sync MOs from SOAM) g. cd /usr/TKLC/xIH/apps h. ./trda-config.sh <DSR SOAM VIP in different network>

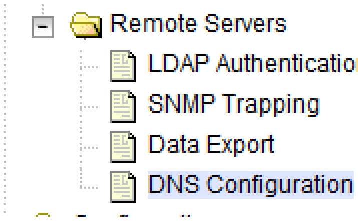
Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

S T E P #	This procedure configures the SSO domain for iDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type **https://<Primary_NOAM_VIP_IP_Address>** as the URL. 2. Login as the **admusr** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login.

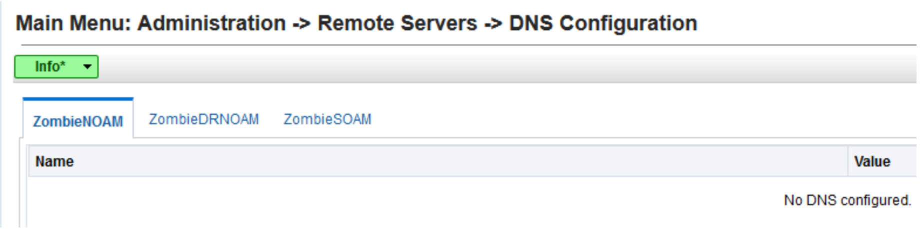
Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

2. □ **NOAM VIP GUI**: Configure DNS

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



2. Select the NOAM tab.

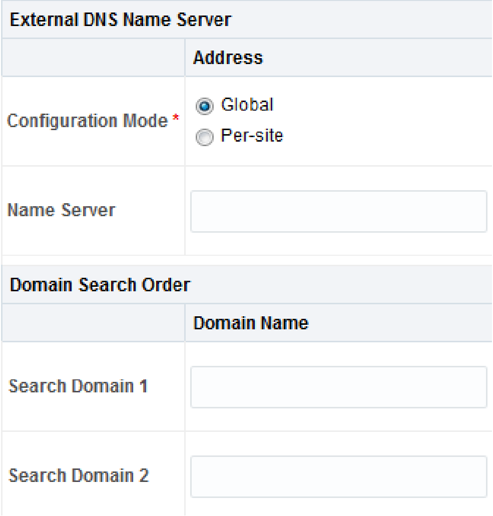


Main Menu: Administration -> Remote Servers -> DNS Configuration

Name	Value
	No DNS configured.

3. Configure values for the following fields:

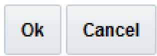
Domain Name
Name Server
Search Domain 1



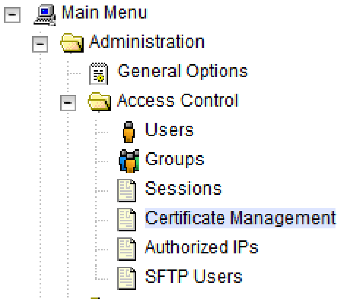
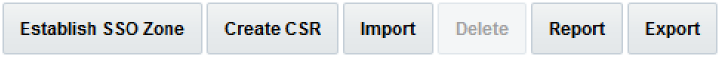
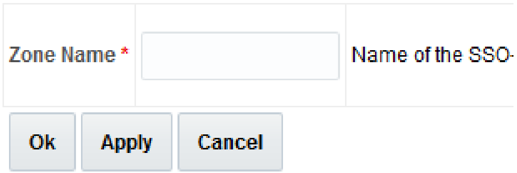
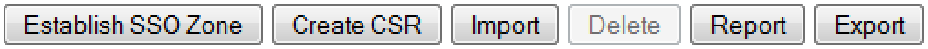
External DNS Name Server	
	Address
Configuration Mode *	● Global ○ Per-site
Name Server	

Domain Search Order	
	Domain Name
Search Domain 1	
Search Domain 2	

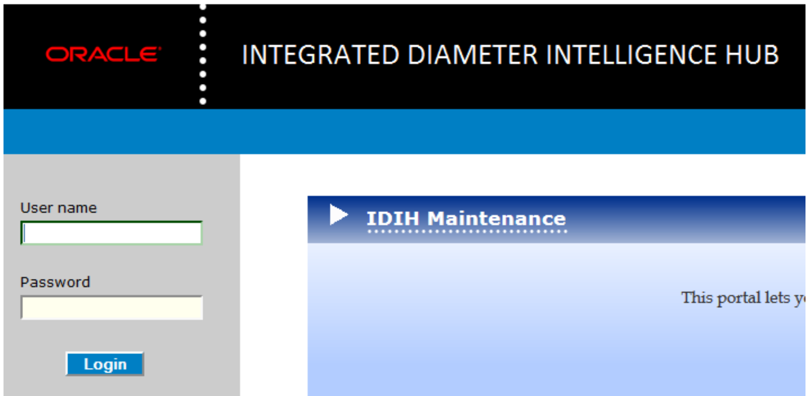
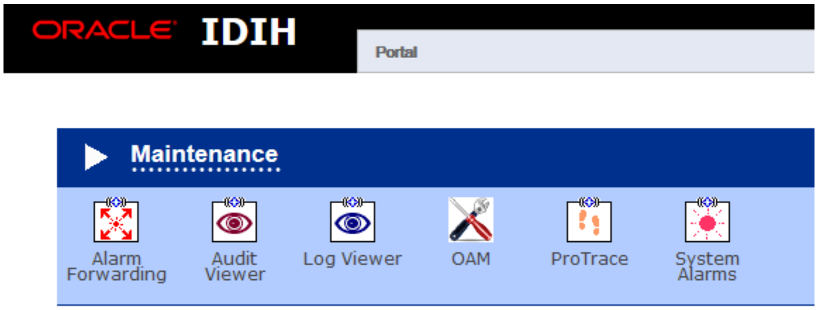
4. If values have already been configured, click **Cancel**; otherwise configure the values and click **OK**.



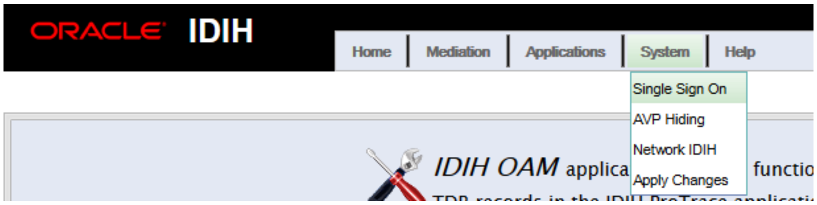
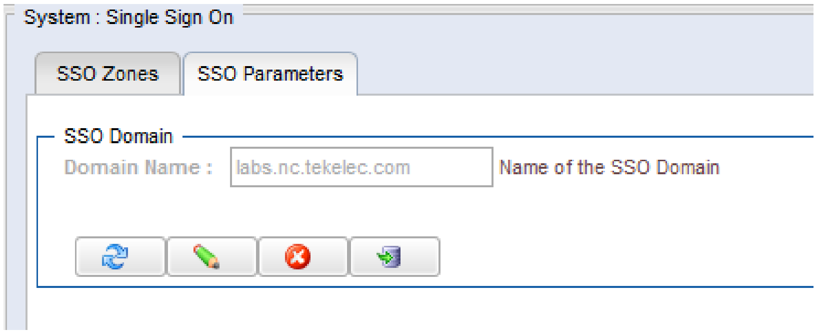
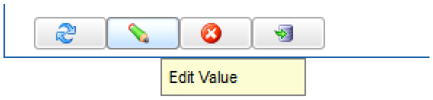
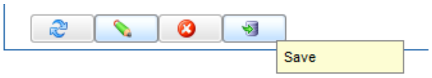
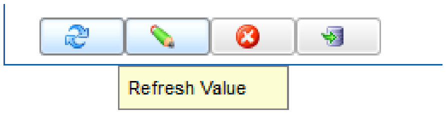
Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

3. □	**NOAM VIP GUI**: Establish SSO local zone	1. Navigate to **Access Control > Certification Management**.  Main Menu Administration General Options Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users 2. Click **Establish SSO Zone**.  Establish SSO Zone Create CSR Import Delete Report Export 3. Type a value for **Zone Name**.  4. Click **OK**. Information for the new certificate type of SSO local displays. 5. Click **Report**.  Establish SSO Zone Create CSR Import Delete Report Export 6. The Certificate Report displays. Select and copy the encoded certificate text to the clipboard for future access. Example of Certificate Report: -----BEGIN CERTIFICATE----- MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV BAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwG T3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqGSIb3 DQEJARYEdGVzdDAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ BgNVBAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UE CgwGT3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqG SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZ/MpkhlvMP/iJ s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAf BgNVHSMEGDAWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAMBgNVHRMEBTADAQH/MA0G CSqGSIb3DQEBCwUAA0EAOwIqBMEQyvfvt38r/yfgIx3w5dN8SBwHjHC5TpJrHV6U zFlg5dfzoLz7ditjGOhWJ9l9VRw39LQ8lKFp7SMXwA== -----END CERTIFICATE-----

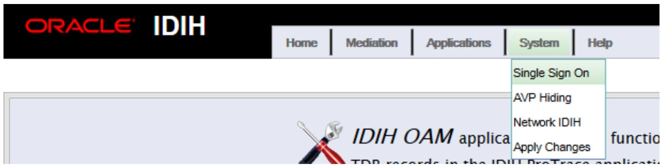
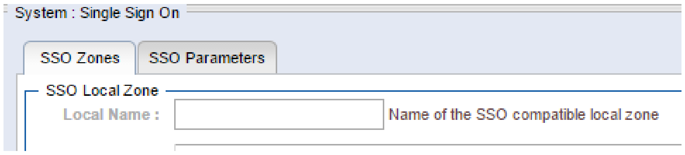
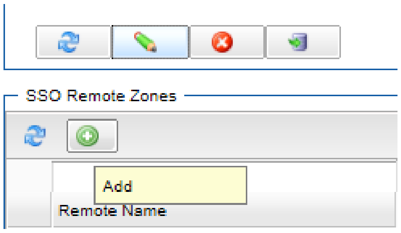
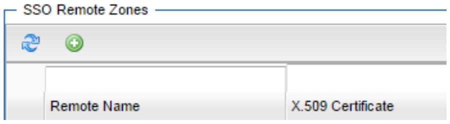
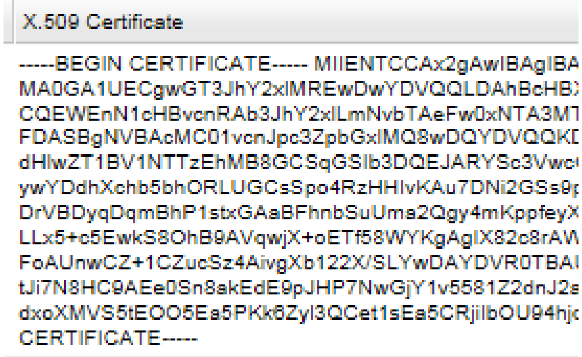
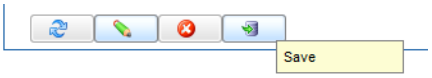
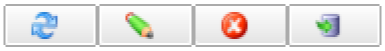
Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

4. □	**iDIH Application Server GUI**: Login	1. Establish a GUI session on the iDIH application server. `https://<app server IP>` 2. Login as the idihadmin user.  ORACLE INTEGRATED DIAMETER INTELLIGENCE HUB User name Password Login IDIH Maintenance This portal lets y
5. □	**iDIH Application Server GUI**: Launch the OAM portal	Navigate to the OAM portal icon to start the OAM web application.  ORACLE IDIH Portal Maintenance Alarm Forwarding Audit Viewer Log Viewer OAM ProTrace System Alarms

Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

6. □	**iDIH Application Server GUI**: Configure the SSO domain	1. Navigate to **System > Single Sign On**.  ORACLE IDIH Home Mediation Applications System Help Single Sign On AVP Hiding Network IDIH Apply Changes IDIH OAM applica functio Select the **SSO Parameters** tab.  System : Single Sign On SSO Zones SSO Parameters SSO Domain Domain Name : labs.nc.tekelec.com Name of the SSO Domain 2. Click the **Edit Value** icon.  3. Type a value for the **Domain Name**. ***Note***: This should be the same domain name assigned in the DSR NOAM DNS Configuration (step 2). 4. Click the **Save** icon.  5. Click the **Refresh** icon to display data saved for the remote zone. 

Procedure 40. iDIH Configuration: Configuring the SSO Domain (Optional)

7. □	**iDIH Application Server GUI**: Configure the SSO Remote Zone	1. Navigate to **System > Single Sign On**.  ORACLE IDIH Home Mediation Applications System Help Single Sign On AVP Hiding Network IDIH Apply Changes IDIH OAM applica functio 2. Select the **SSO Zones** tab.  System : Single Sign On SSO Zones SSO Parameters SSO Local Zone Local Name : Name of the SSO compatible local zone 3. Click the **Add** icon.  4. Type a value for field **Remote Name**.  5. For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.  X.509 Certificate -----BEGIN CERTIFICATE----- MIIENTCCAx2gAwIBAgIBA MA0GA1UECgwGT3JhY2xlMREwDwYDVQQLDAhBcHB CQEWEnN1cHBvcnRAb3JhY2xlLmNvbTAeFw0xNTA3M FDASBgNVBAcMC01vcnJpc3ZpbGxlMQ8wDQYDVQQK dHlwZT1BV1NTTzEhMB8GCSqGSIb3DQEJARYSc3Vwc ywYDdhXchb5bhORLUGCsSpo4RzHHIvKAu7DNi2GSs9 DrVBDyqDqmBhP1stxGAaBFhnbSuUma2Qgy4mKppfeyX LLx5+c5EwkS8OhB9AVqwjX+oETf58WYKgAgIX82c8rAW FoAUnwCZ+1CZucSz4AivgXb122X/SLYwDAYDVR0TBA tJi7N8HC9AEe0Sn8akEdE9pJHP7NwGjY1v5581Z2dnJ2 dxoXMVS5tEOO5Ea5PKk6ZyI3QCet1sEa5CRjiIbOU94hj CERTIFICATE----- 6. Click the **Save** icon.  7. Click the **Refresh** icon to display the data saved for remote zone. 

Procedure 41. Integrate iDIH into DSR (Optional)

STEP #

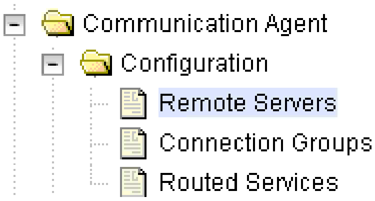
This procedure configures the iDIH connections to DSR.

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.

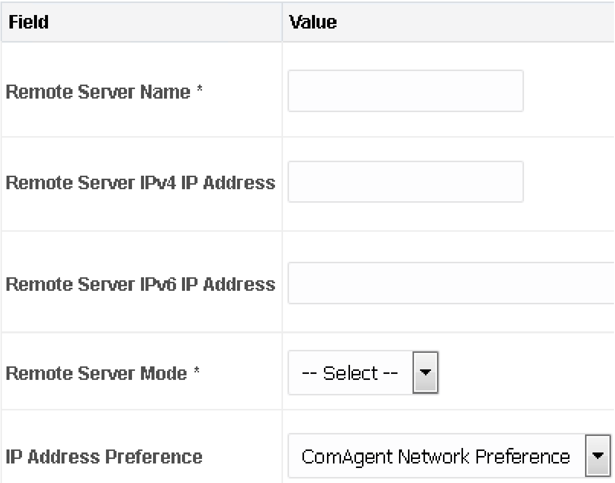
1. □ Configure the iDIH ComAgent connection on the NOAM

1. Navigate to **Communication Agent > Configuration > Remote Servers**.



2. Click **Insert**.

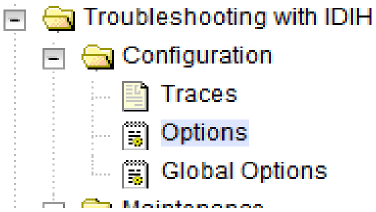
3. Add the iDIH Mediation server.
4. For the **Remote Server IP Address** field, type the **IMI IP address** of the iDIH Mediation server.
5. For the **IP Address Preference** field, select the **IP protocol preference** (if IPv6 and IPv4 are configured).

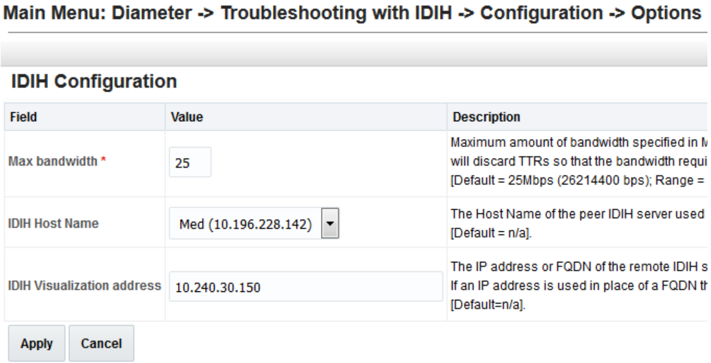


Field	Value
Remote Server Name *	
Remote Server IPv4 IP Address	
Remote Server IPv6 IP Address	
Remote Server Mode *	-- Select --
IP Address Preference	ComAgent Network Preference

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

Procedure 41. Integrate iDIH into DSR (Optional)

<table>
<tr>
<td>2.
□</td>
<td>Configure the Troubleshooting with iDIH on the SOAM</td>
<td>
1. Navigate to <b>Diameter > Troubleshooting with iDIH > Configuration > Options</b>.


2. Type the fully qualified iDIH host name (or IP address) in the iDIH <b>Visualization Address</b> field:

Main Menu: Diameter -> Troubleshooting with IDIH -&gt; Configuration -> Options
IDIH Configuration
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Max bandwidth *</td><td>25</td><td>Maximum amount of bandwidth specified in M
will discard TTRs so that the bandwidth requi
[Default = 25Mbps (26214400 bps); Range =</td></tr>
<tr><td>IDIH Host Name</td><td>Med (10.196.228.142)</td><td>The Host Name of the peer IDIH server used
[Default = n/a].</td></tr>
<tr><td>IDIH Visualization address</td><td>10.240.30.150</td><td>The IP address or FQDN of the remote IDIH s
If an IP address is used in place of a FQDN th
[Default=n/a].</td></tr>
</table>

3. Click <b>Apply</b>.
</td>
</tr>
</table>

Procedure 42. iDIH Configuration: Configure the Mail Server (Optional)

<table>
<tr>
<td><b>S
T
E
P
#</b></td>
<td colspan="2">This procedure configures the SMTP mail server.
<b><i>Note</i></b>: This procedure is optional; however, this option is required for security (password initialization set to AUTOMATIC) and forwarding (forwarding by mail filter defined), and is available only on the Application server.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.
□</td>
<td><b>iDIH Application Server</b>: Login</td>
<td>1. Establish an SSH session to the iDIH Application server.
2. Login as the <b>admusr</b> user.</td>
</tr>
</table>

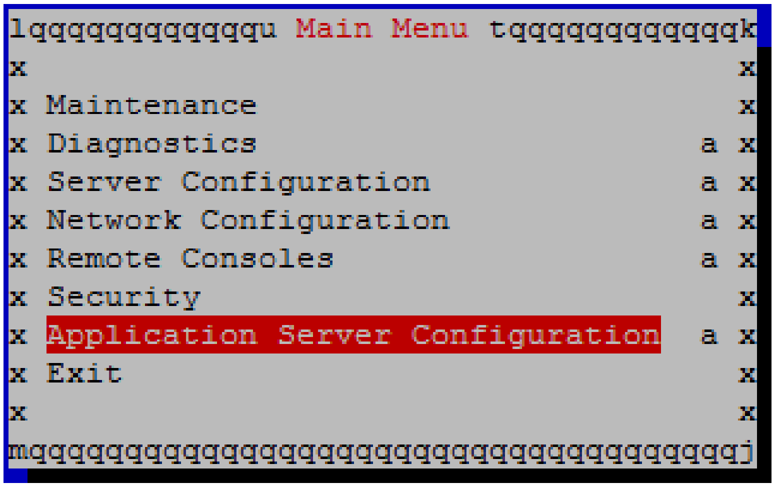
Procedure 42. iDIH Configuration: Configure the Mail Server (Optional)

2. □ **iDIH Application Server**: Configure the authenticated mail server

1. From the platcfg menu, type the following command:

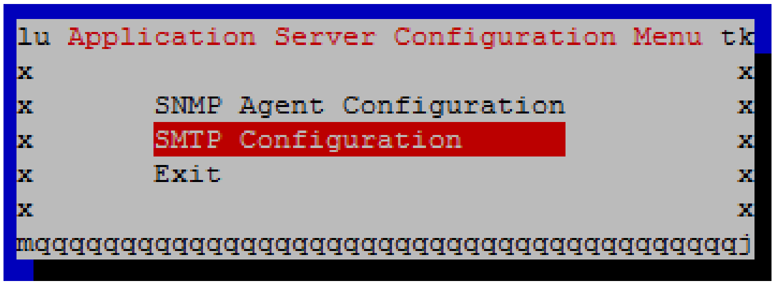
```
$ sudo su - platcfg
```

2. Select **Application Server Configuration**.



```
lqqqqqqqqqqqqqu Main Menu tqqqqqqqqqqqqqk
x                                       x
x Maintenance                           x
x Diagnostics                         a x
x Server Configuration                a x
x Network Configuration               a x
x Remote Consoles                     a x
x Security                              x
x Application Server Configuration    a x
x Exit                                  x
x                                       x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

3. Select **SMTP Configuration**.

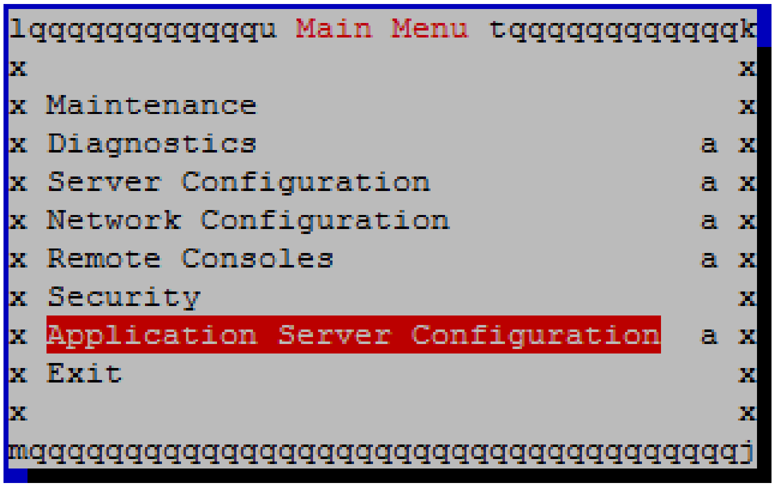
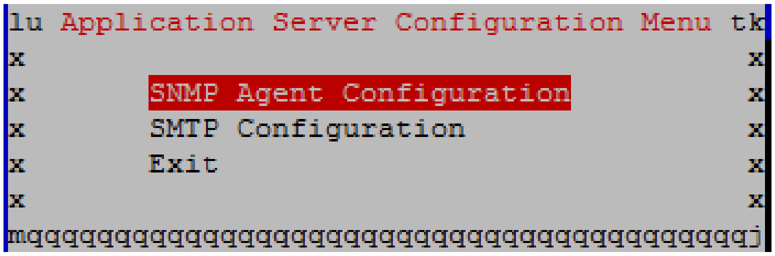


```
lu Application Server Configuration Menu tk
x                                         x
x       SNMP Agent Configuration          x
x       SMTP Configuration                x
x       Exit                              x
x                                         x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

4. Select **Edit**.
5. Enter the following parameters:
   - Mail Server IP Address
   - User
   - Password
   - Email Address (From)
   - Mail smtp timeout
   - Mail smtp connectiontimeout
   - SNMP over SSL used?
6. Select **OK**.
7. Select **Exit** to exit the platcfg menu.

Procedure 43. iDIH Configuration: Configure SNMP Management Server (Optional)

S T E P #	This procedure configures the SNMP management server. ***Note***: This procedure is optional; however, this option is required for forwarding (forwarding by SNMP filter defined), and is available only on the Application server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**iDIH Application Server**: Login	1. Establish an SSH session to the iDIH Application server. 2. Login as the **admusr** user.

2.
□
	iDIH Application Server: Configure the authenticated mail server	1. From the platcfg menu, type the following command:
		`$ sudo su - platcfg`
		2. Select **Application Server Configuration**.
		`lqqqqqqqqqqqqu Main Menu tqqqqqqqqqqqqk`
		`x                                     x`
		`x Maintenance                         x`
		`x Diagnostics                       a x`
		`x Server Configuration              a x`
		`x Network Configuration             a x`
		`x Remote Consoles                   a x`
		`x Security                            x`
		`x Application Server Configuration  a x`
		`x Exit                                x`
		`x                                     x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`
		3. Select **SNMP Agent Configuration**.
		`lu Application Server Configuration Menu tk`
		`x                                        x`
		`x       SNMP Agent Configuration         x`
		`x       SMTP Configuration               x`
		`x       Exit                             x`
		`x                                        x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`
		4. Select **Edit**.
		5. Enter the IP Address of the SNMP management server.
		Note: The SNMP agent configuration is updated and the SNMP management server automatically restarts.
		6. Select **OK**.
		7. Select **Exit** to exit the platcfg menu.

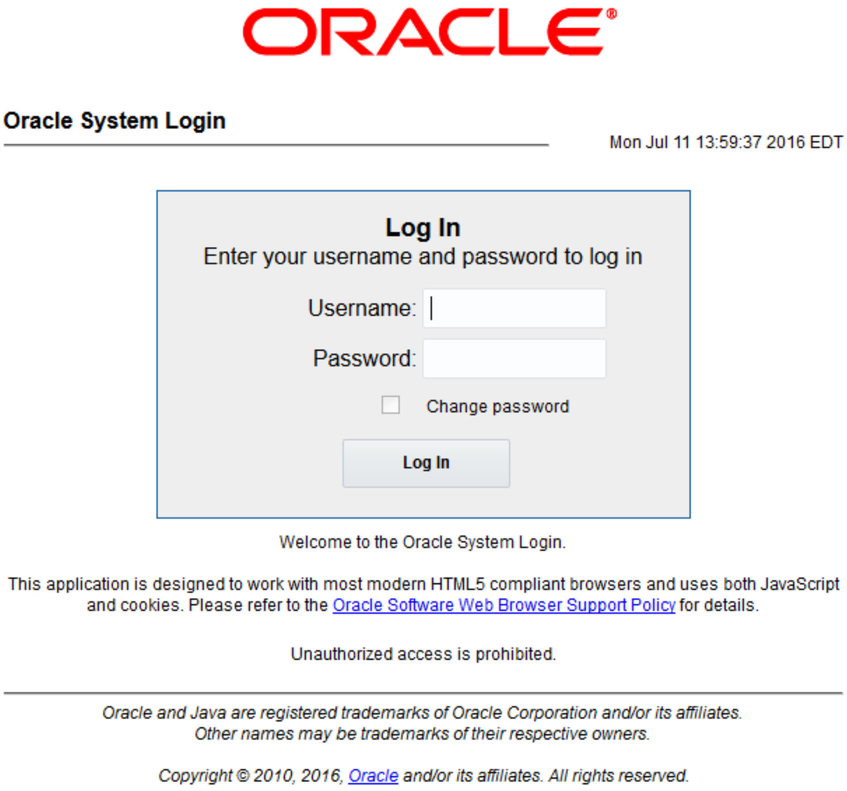
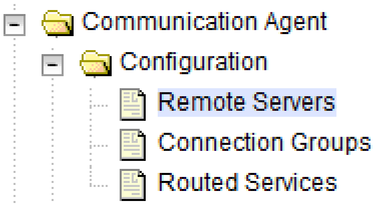
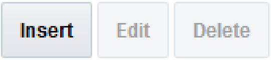
Procedure 44. iDIH Configuration: Change Network Interface (Optional)

S T E P #	This procedure changes the default network interface. ***Note***: Initially, the default network interface used to transport TTRs from DSR to DIH uses the internal IMI network; however, this can be changed, if required. It should be noted that changing this interface could degrade performance of TTR transmission. ***Note***: A script is provided to manage the settings so the operator does not need to know the details required to apply the settings. There are two settings **interface.name** and **interface.enabled**. When **interface.enabled=True**, then communications over the interface.name =value, where value is the name of the network interface as defined on the platform, is the only specified interface used for communications. When **interface.enabled=False** then communications over the named interface is not enforced, that is, all interfaces configured on the platform are allowed to be used for communications. For example, if it is required to use the XMI interface for communication instead of the default internal IMI interface, then the operator would supply **XMI** when asked for the interface name and **True** when asked if interface filtering should be applied. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	**iDIH Mediation Server**: Login	1. Establish an SSH session to the iDIH Mediation server. 2. Login as the **admusr** user. 3. Type the following command to login in as the **Tekelec** user. `$ sudo su - tekelec`

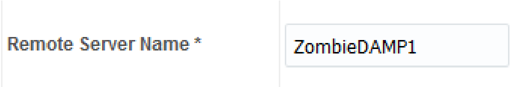
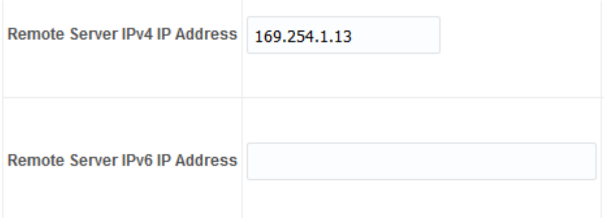
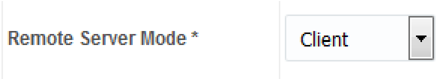
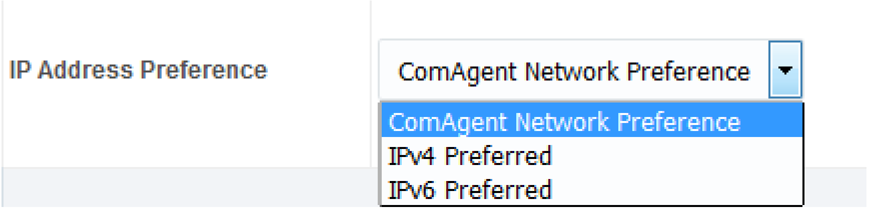
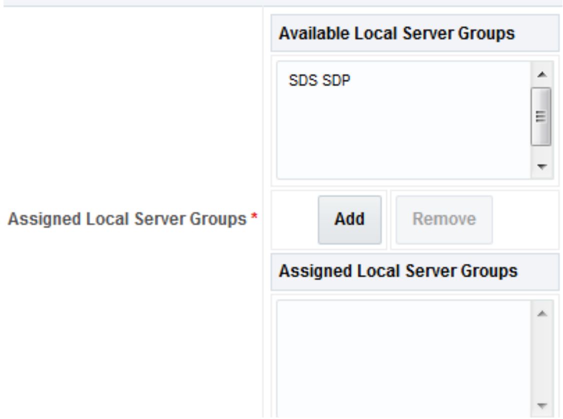
2.
□
	iDIH Mediation Server: Execute the change interface script	1. To execute the change interface script, type the following command:
		`$ chgIntf.sh`
		2. Answer the questions during the script as follows.
		`This script is used to change the interface name (default = imi) used for mediation communications and whether to enable network interface filtering or not.  Please answer the following questions or enter CTLR-C to exit out of the script.`
		`Current setting are: interface.name=imi interface.enabled=True`
		`Enter new network interface name, return to keep current [imi]: xmi`
		`Do you want to enable network interface filtering [True|False], return to keep current [True]:`
		`Updating configuration properties file with 'interface.name=xmi' and 'interface.enable=True', and restarting mediation configuration bundle...`

6. Post-Install Activities

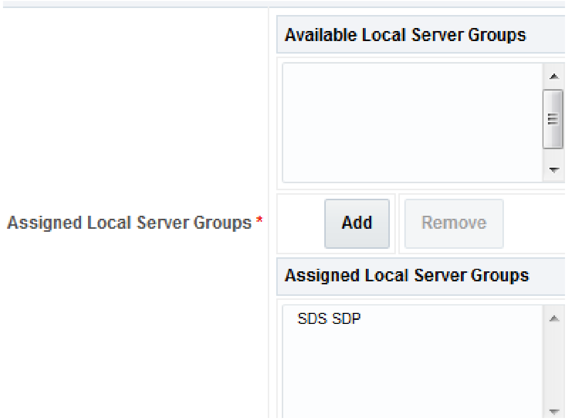
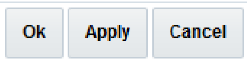
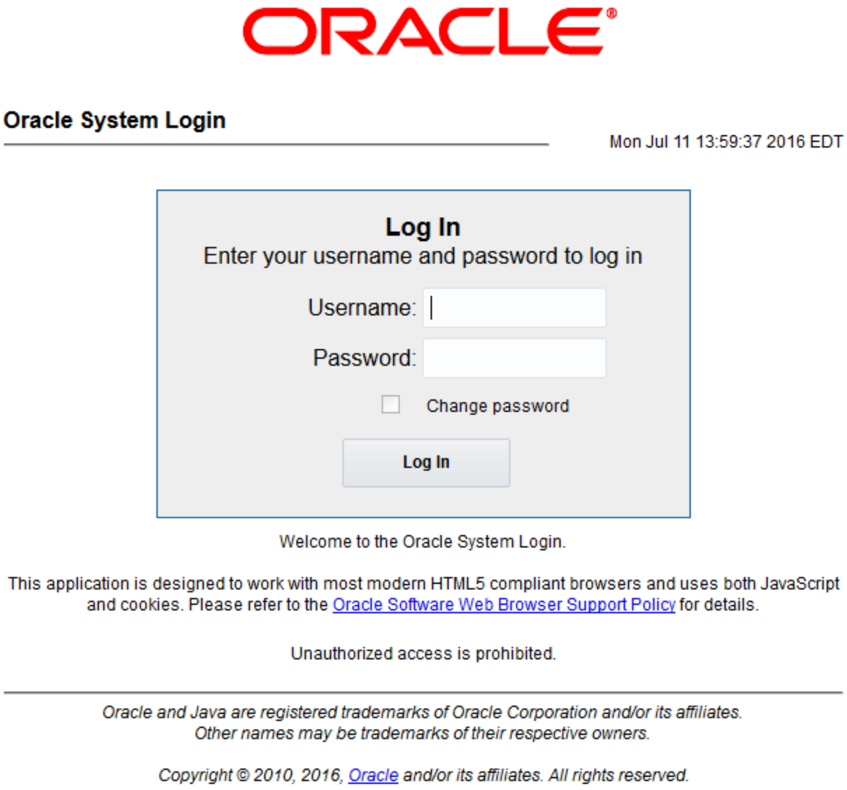
Procedure 45. Configure ComAgent Connections

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. □	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type **https://<Primary_SDS_NOAM_VIP_IP_Address>** as the URL. 2. Login as the **admusr** user.  ORACLE® **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
2. □	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  Communication Agent Configuration Remote Servers Connection Groups Routed Services 2. Click **Insert**. 

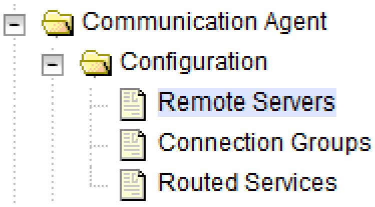
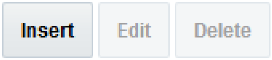
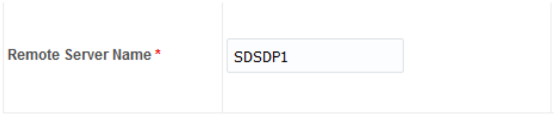
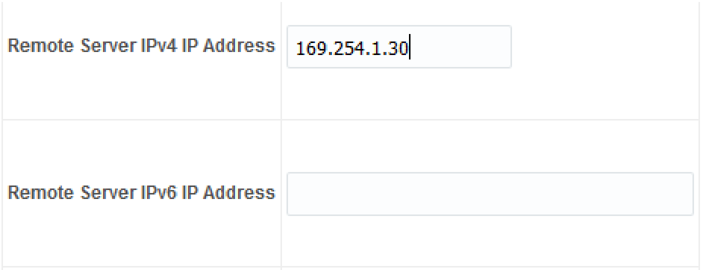
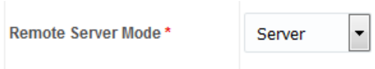
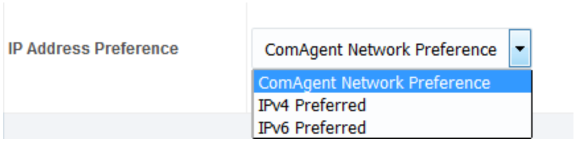
Procedure 45. Configure ComAgent Connections

3. □	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Type **Remote Server Name** for the DSR MP server. Remote Server Name * ZombieDAMP1 2. Type the **Remote Server** IMI IP address. Remote Server IPv4 IP Address 169.254.1.13 Remote Server IPv6 IP Address ***Note***: This should be the IMI IP address of the DAMP server. 3. Select **Client** for the Remote Server Mode from the list. Remote Server Mode * Client 4. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6) from the list. IP Address Preference ComAgent Network Preference ComAgent Network Preference IPv4 Preferred IPv6 Preferred 5. Select the **Local Server Group** from the available SDS DP server groups and click **'Add'** to assign. Available Local Server Groups SDS SDP Assigned Local Server Groups * Assigned Local Server Groups

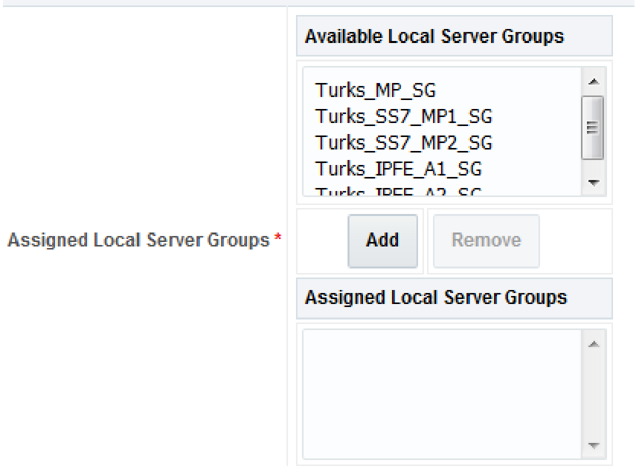
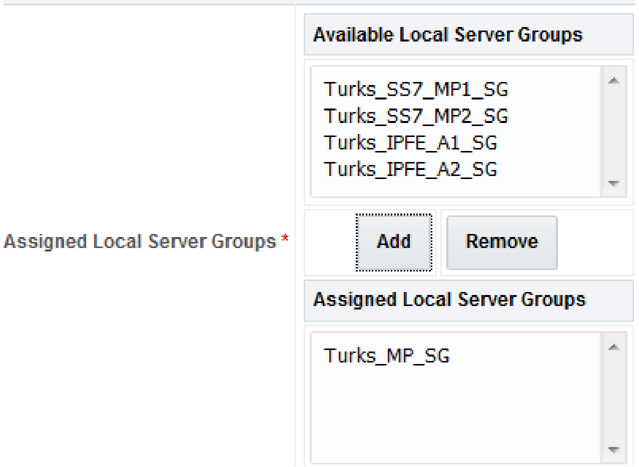
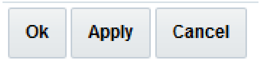
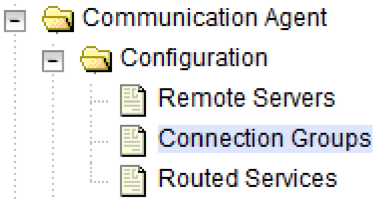
Procedure 45. Configure ComAgent Connections

		 Available Local Server Groups Assigned Local Server Groups * Add Remove Assigned Local Server Groups SDS SDP 6. Click **Apply**. 
4. □	**SDS NOAM VIP GUI**: Repeat	Repeat steps 2-3 for each remote MP in the same SOAM NE.
5. □	**DSR NOAM VIP GUI**: Login	1. Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type **https://<Primary_DSR_NOAM_VIP_IP_Address>** as the URL 2. Login as the **guiadmin** user.  ORACLE® Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: □ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 45. Configure ComAgent Connections

6. □	**DSR NOAM VIP GUI**: Configure remote server IP address	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  Communication Agent Configuration Remote Servers Connection Groups Routed Services 2. Click **Insert**. 
7. □	**DSR NOAM VIP GUI**: Configure remote server IP address	1. Type **Remote Server Name** for the DSR MP server.  Remote Server Name * SDSDP1 2. Type the **Remote Server** IMI IP address.  Remote Server IPv4 IP Address 169.254.1.30 Remote Server IPv6 IP Address ***Note***: This should be the IMI IP address of the DP server. 3. Select **Server** for the Remote Server Mode from the list.  Remote Server Mode * Server 4. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6) from the list.  IP Address Preference ComAgent Network Preference ComAgent Network Preference IPv4 Preferred IPv6 Preferred 5. Select the **Local Server Group** from the available DSR MP server groups and click **'Add'** to assign.

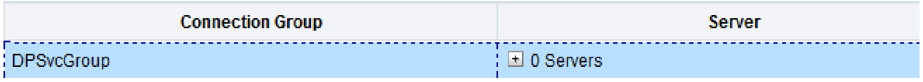
Procedure 45. Configure ComAgent Connections

		 Assigned Local Server Groups * Available Local Server Groups Turks_MP_SG Turks_SS7_MP1_SG Turks_SS7_MP2_SG Turks_IPFE_A1_SG Turks_IPFE_A2_SG Add Remove Assigned Local Server Groups  Assigned Local Server Groups * Available Local Server Groups Turks_SS7_MP1_SG Turks_SS7_MP2_SG Turks_IPFE_A1_SG Turks_IPFE_A2_SG Add Remove Assigned Local Server Groups Turks_MP_SG 6. Click **Apply**.  Ok Apply Cancel
8. □	**DSR NOAM VIP GUI**: Repeat	Repeat steps 6-7 for each remote DP in the same SOAM NE.
9. □	**DSR NOAM VIP GUI**: Configure connection groups	Navigate to **Communication Agent > Configuration > Connection Groups**.  Communication Agent Configuration Remote Servers Connection Groups Routed Services

Procedure 45. Configure ComAgent Connections

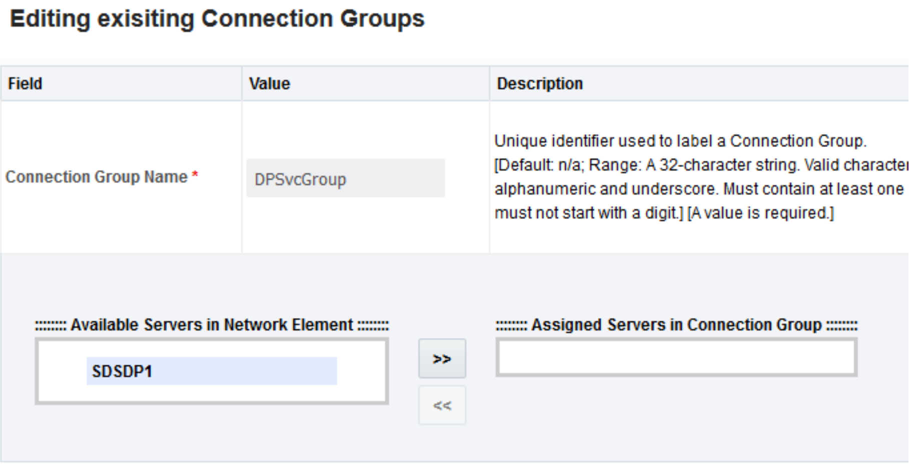
10. □ **DSR NOAM VIP GUI**: Edit connection groups

1. Select the **DPSvcGroup** connection group.



Connection Group	Server
DPSvcGroup	⊞ 0 Servers

2. Click **Edit**.
3. Select the **DP Servers** from the Available Servers in Network Element list and click **>>** to assign.

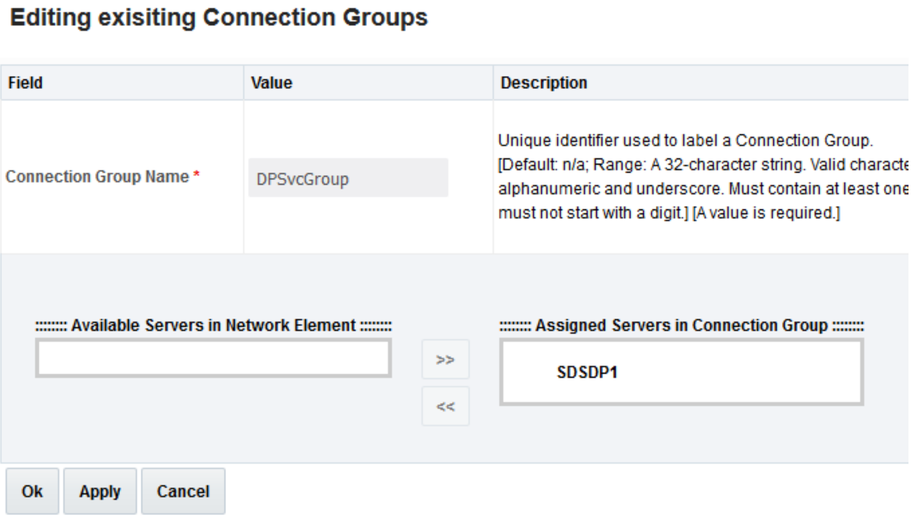


Editing exisiting Connection Groups

Field	Value	Description
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid characte alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]

:::::::: Available Servers in Network Element :::::::: SDSDP1

:::::::: Assigned Servers in Connection Group ::::::::



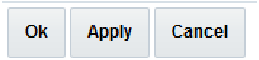
Editing exisiting Connection Groups

Field	Value	Description
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid characte alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]

:::::::: Available Servers in Network Element ::::::::

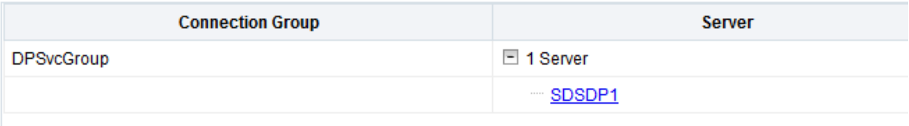
:::::::: Assigned Servers in Connection Group :::::::: SDSDP1

4. Click **OK**.



11. □ **DSR NOAM VIP GUI**: Verify servers in group

Verify the correct number of servers are in the connection group.



Connection Group	Server
DPSvcGroup	⊟ 1 Server
	SDSDP1

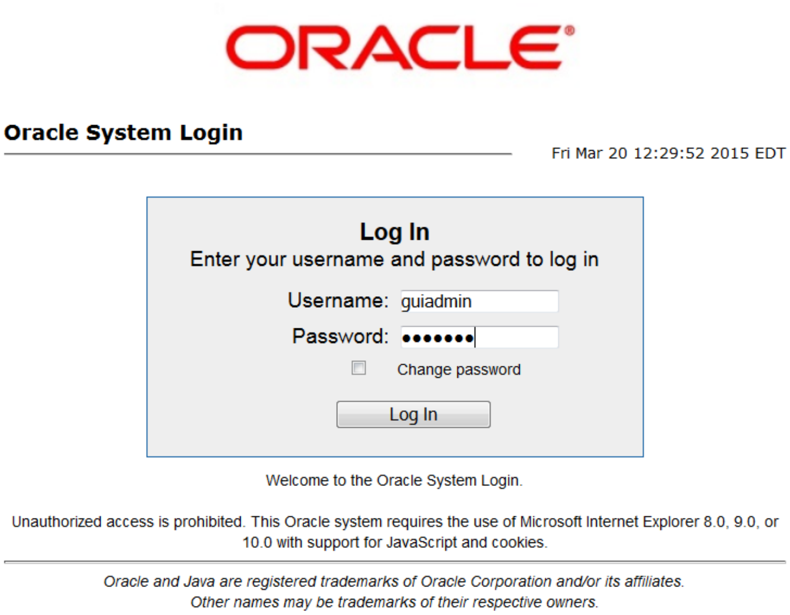
Procedure 46. Complete PCA Configuration (Optional)

S T E P #	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] DSR PCA Activation Guide for the steps required to complete PCA configuration.

Procedure 47. Backups and Disaster Prevention

S T E P #	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.	
1. □	**Backup from VIM**	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. ***Note***: To be on the safer side, follow the below steps also to back up the NOAM and SOAM database
2. □	**Identify Backup Server**	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • Cloud Infrastructure Manager Server/Controller • DSR NOAM • DSR SOAM

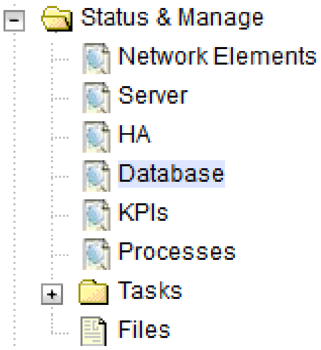
Procedure 47. Backups and Disaster Prevention

3. □	**NOAM/SOAM VIP**: Login	1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

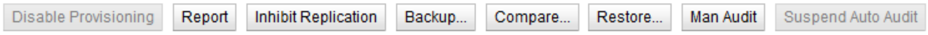
Procedure 47. Backups and Disaster Prevention

4. □ **NOAM/SOAM VIP**: Backup configuration data for the system

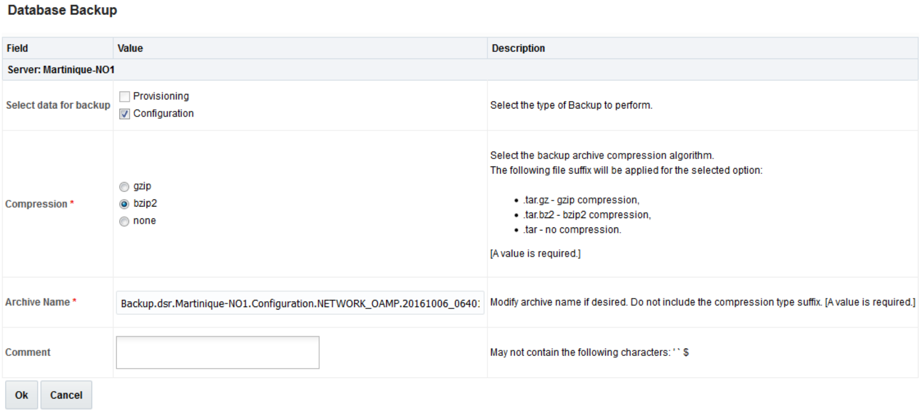
1. Navigate to **Main Menu > Status & Manage > Database**.



2. Select the active NOAM server and click **Backup**.



3. Make sure the **Configuration** checkbox is marked.



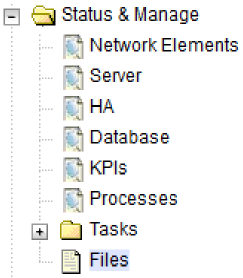
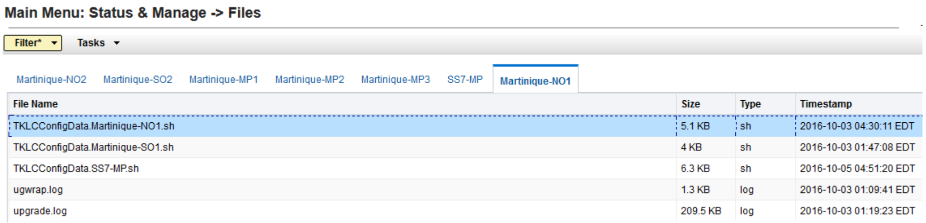
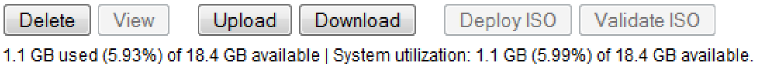
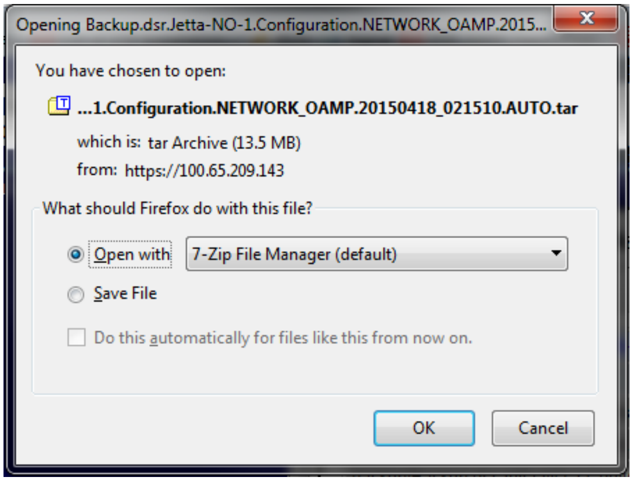
Database Backup

Field	Value	Description
Server: Martinique-NO1		
Select data for backup	□ Provisioning ☑ Configuration	Select the type of Backup to perform.
Compression *	○ gzip ● bzip2 ○ none	Select the backup archive compression algorithm. The following file suffix will be applied for the selected option: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression. [A value is required.]
Archive Name *	Backup.dsr.Martinique-NO1.Configuration.NETWORK_OAMP.20161006_0640:	Modify archive name if desired. Do not include the compression type suffix. [A value is required.]
Comment		May not contain the following characters: ' ` $

Ok Cancel

4. Enter a filename for the backup and click **OK**.

Procedure 47. Backups and Disaster Prevention

5. □	**NOAM/SOAM VIP**: Verify the backup file existence.	1. Navigate to **Main Menu > Status & Manage > Files**.  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files  Main Menu: Status & Manage -> Files Filter* Tasks Martinique-NO2 Martinique-SO2 Martinique-MP1 Martinique-MP2 Martinique-MP3 SS7-MP Martinique-NO1 File Name | Size | Type | Timestamp TKLCConfigData.Martinique-NO1.sh | 5.1 KB | sh | 2016-10-03 04:30:11 EDT TKLCConfigData.Martinique-SO1.sh | 4 KB | sh | 2016-10-03 01:47:08 EDT TKLCConfigData.SS7-MP.sh | 6.3 KB | sh | 2016-10-05 04:51:20 EDT ugwrap.log | 1.3 KB | log | 2016-10-03 01:09:41 EDT upgrade.log | 209.5 KB | log | 2016-10-03 01:19:23 EDT 2. Select the active NOAM or SOAM tab. 3. The files on this server display. Verify the existence of the backup file.
6. □	**NOAM/SOAM VIP**: Download the file to a local machine.	1. From the previous step, select the backup file. 2. Click **Download**.  Delete View Upload Download Deploy ISO Validate ISO 1.1 GB used (5.93%) of 18.4 GB available | System utilization: 1.1 GB (5.99%) of 18.4 GB available. 3. Click **OK**.  Opening Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.2015... You have chosen to open: ...1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar which is: tar Archive (13.5 MB) from: https://100.65.209.143 What should Firefox do with this file? ● Open with 7-Zip File Manager (default) ○ Save File □ Do this automatically for files like this from now on.
7. □	Upload the image to secure location	Transfer the backed up image to a secure location identified in step 2 where the server backup files are fetched in case of system disaster recovery.
8. □	Backup active SOAM	Repeat **Steps 4 through 8** to back up the active SOAM.

Procedure 48. (KVM/OpenStack Only) Configure Port Security

STEP #	This procedure configures port security on TSA. **Prerequisite**: Perform **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 Disable Port Security in Appendix G.6 where this is discussed. 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 allowable address pair security on IPFE XSI network and DAMP XSI interfaces on IPFE and MP instances	If stacks are deployed using HEAT template, follow this step.
		1. Determine the TSA IP address used in Procedure 32,step 2.
		2. Determine the corresponding XSI interface IP address assigned to that TSA used in Procedure 32,step 2.
		3. Determine the XSI IP address of IPFE used in Procedure 32,step 2.
		4. Log into the OpenStack control node as the **admusr** user.
		5. Source the tenant user credentials.
		6. Determine the port ID of the XSI interface IP address.
		`$ neutron port-list -F id -F fixed_ips | grep <XSI network>`
		Note: <port ID> is the value in first column of the output to this command.
		7. Remove allowed_address_pairs:
		`$ neutron port-update <Port ID> --no-allowed-address-pairs`
		Note: Execute neutron port-show command to verify allowed_address_pairs attribute is empty.

2.
□
	IPFE with TSA only. Remove port security on TSA XSI network interfaces on IPFE and MP instances	If using IPFE with Target Set Addresses (TSA).
		1. Determine the TSA IP address as used in section 5.4, Procedure 32.
		2. Determine the corresponding XSI interface IP address as used in section 5.4, Procedure 32.
		3. Log into the OpenStack control node as the **admusr** user.
		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.

Procedure 48. (KVM/OpenStack Only) Configure Port Security

Alternatively, use the following syntax:

```
$ 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.

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.

11. 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>
```

12. 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.

Procedure 49. Enable/Disable DTLS (SCTP Diameter Connections Only)

S T E P #	This procedure prepares clients before configuring SCTP Diameter connections. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	Enable/Disable DTLS (SCTP Diameter connections only)	Oracle's SCTP Datagram Transport Layer Security (DTLS) has SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers 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 WILL NOT establish after the DSR is installed. • https://access.redhat.com/security/cve/CVE-2015-1421 • https://access.redhat.com/security/cve/CVE-2014-5077 Execute procedures in [22] DSR DTLS Feature Activation Procedure to disable/enable the DTLS feature.

Procedure 50. Shared Secret Encryption Key Revocation (RADIUS Only)

S T E P #	This procedure changes the shared secret encryption key on DSR RADIUS setup. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	Revoke RADIUS shared secret encryption key	Refer to RADIUS Shared Secret Key revocation MOP to change the encryption key on the DSR installed setup. Refer to [23] DSR RADIUS Shared Secret Encryption Key Revocation MOP MO008572. ***Note***: It is highly recommended to change the key after installation due to security reasons.

Procedure 51. DSR Performance Tuning

S T E P #	This procedure changes tuning parameters for the system to achieve better performance. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. □	Performance tuning (Optional)	Refer Appendix I Performance Tuning Recommended for performance tuning on DSR.

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 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 3. Example Network Element XML File

Note: NetworkElement Name shall be unique while creating multiple Network Element.

Appendix B. List of Frequently Used Time Zones

This table lists several valid time zone 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 time zone.

Table 6. List of Selected Time Zone Values

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

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

Appendix C. Common KVM/OpenStack Tasks

Appendix C.1 Create a Network Port

Procedure 52. 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`

Appendix C.2 Create and Boot OpenStack Instance

Procedure 53. Create and Boot OpenStack Instance

1.
□
	Create a VM instance from a 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.
		NO1
		SO2
		MP5
		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 OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
		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.

Appendix C.3 Configure Networking for OpenStack Instance

Procedure 54. Configure Networking for OpenStack Instance

1.
□
	Verify/Configure the network interface	1. Check if the interface is configured automatically.
		2. If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address. To verify, ping the XMI IP address provided with the **nova boot** command:
		`$ping <XMI-IP-Provided-During-Nova-Boot>`
		If the ping is successful, ignore the next part to configure the interface manually.
		Manually configure the interface, if not already done (optional).
		a. Log into the **Horizon** GUI as the DSR tenant user.
		b. Go to the Compute/Instances section.
		c. Click on the **Name** field of the newly created instance.
		d. Select the Console tab.
		e. Login as the **admusr** user.
		f. Configure the network interfaces, conforming with the interface-to-network mappings defined in [27] DSR Cloud Benchmarking Guide.
		`$ 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.
		3. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible using both network and Horizon console.

Appendix D. Common OVM Manager Tasks (CLI)

Appendix D.1 Set Up the Server

Note: This section sets up the server using the command line interface of OVM Manager. All configurations/setup **can also be done** from the GUI/dashboard of OVM Manager.

Procedure 55. Set Up the Server

1.
□
	Log into the OVM-M command line interface	`ssh -l admin <OVM-M IP> -p 1000`
		Example:
		`[root@manager01 ~]# ssh -l admin 10.240.16.138 -p 10000`
		`admin@10.240.16.138's password:`

Procedure 55. Set Up the Server

<table>
<tr><td>2.
□</td><td><b>OVM-M CLI</b>:
Discover Oracle VM server</td><td>discoverServer ipAddress=value password=value takeOwnership= { Yes | No }
Example:
OVM>discoverServer ipAddress=10.240.16.139 password=password takeOwnership=Yes</td></tr>
<tr><td>3.
□</td><td><b>OVM-M CLI</b>:
Create an ethernet-based network with the VM role</td><td>create Network [roles= { MANAGEMENT | LIVE_MIGRATE | CLUSTER_HEARTBEAT | VIRTUAL_MACHINE | STORAGE }] name=value [description=value] [on Server instance]
Example:
OVM>create Network name=XMI roles=VIRTUAL_MACHINE</td></tr>
<tr><td>4.
□</td><td><b>OVM-M CLI</b>:
Add a port from each Oracle VM server to the network</td><td><b><i>Note</i></b>: Skip this step and proceed to step 5 for bonded interfaces.
1. Find the ID of an Ethernet port.
OVM> show Server name=MyServer1
...
Ethernet Port 1 = 0004fb00002000007711332ff75857ee
[eth0 on MyServer3.virtlab.info]
Ethernet Port 2 = 0004fb0000200000d2e7d2d352a6654e
[eth1 on MyServer3.virtlab.info]
Ethernet Port 3 = 0004fb0000200000c12192a08f2236e4
[eth2 on MyServer3.virtlab.info]
2. Add a port from each Oracle VM Server to the network.
OVM>add Port instance to { BondPort | Network } instance
Example:
OVM>add Port id=0004fb0000200000d2e7d2d352a6654e to Network name=MyVMNetwork</td></tr>
</table>

Procedure 55. Set Up the Server

5.
□
	OVM-M CLI:
	Create Bondport (For Bonded Interfaces)
		1. Find the ID of an Ethernet port.
		`OVM>list Port`
		`Status: Success`
		`Time: 2016-08-22 04:43:02,565 EDT`
		`Data:`
		`id:0004fb0000200000045b4e8dc0b3acc6  name:usb0 on vms01.test.com`
		`id:0004fb00002000005fde208ce6392c0a  name:eth4 on vms01.test.com`
		`id:0004fb0000200000b1dceeb39006d839  name:eth5 on vms01.test.com`
		`id:0004fb000020000027e3a02bc28dd153  name:eth2 on vms01.test.com`
		`id:0004fb0000200000fce443e0d30cd3d5  name:eth3 on vms01.test.com`
		`id:0004fb0000200000a908e402fc542312  name:eth0 on vms01.test.com`
		`id:0004fb0000200000247b03c2a4a090ec  name:eth1 on vms01.test.com`
		2. Create Bondport on required interfaces.
		`OVM>create BondPort ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com`
		Command: `create BondPort ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com`
		`Status: Success`

6.
□
	OVM-M CLI:
	Add VLAN Interface to network (for VLAN tagged networks)
		1. Find the ID of an Ethernet port.
		`OVM>list BondPort`
		`Command: list BondPort`
		`Status: Success`
		`Time: 2016-08-22 04:38:22,327 EDT`
		`Data:`
		`id:0004fb00002000005a45a0761813d512  name:bond1`
		`id:0004fb0000200000645cfc865736cea8  name:bond0 on compute01.test.com`
		2. Create VLAN interface.
		`OVM>create VlanInterface vlanId=43 name=bond1.43 on BondPort id=0004fb00002000005a45a0761813d512`

Procedure 55. Set Up the Server

```
Command: create VlanInterface vlanId=43 name=bond1.43
on BondPort id=0004fb00002000005a45a0761813d512

Status: Success
```

3. Add remaining VLAN interfaces to the same bond accordingly, like:

```
OVM>create VlanInterface vlanId=44 name=bond1.44 on
BondPort id=0004fb00002000005a45a0761813d512

OVM>create VlanInterface vlanId=30 name=bond1.30 on
BondPort id=0004fb00002000005a45a0761813d512

OVM>create VlanInterface vlanId=31 name=bond1.31 on
BondPort id=0004fb00002000005a45a0761813d512
```

4. Add VLAN interfaces to network.

```
OVM>add VlanInterface name=bond1.43 to Network name=XMI

Command: add VlanInterface name=bond1.43 to Network
name=XMI

Status: Success

Time: 2016-08-22 05:14:29,321 EDT

JobId: 1471857258238

OVM>add VlanInterface name=bond1.44 to Network name=IMI

Command: add VlanInterface name=bond1.44 to Network
name=IMI

Status: Success

Time: 2016-08-22 05:15:24,216 EDT

JobId: 1471857321329

OVM>add VlanInterface name=bond1.30 to Network
name=XSI1

Command: add VlanInterface name=bond1.30 to Network
name=XSI1

Status: Success

Time: 2016-08-22 05:15:39,190 EDT

JobId: 1471857337005

OVM>add VlanInterface name=bond1.31 to Network
name=XSI2

Command: add VlanInterface name=bond1.31 to Network
name=XSI2

Status: Success

Time: 2016-08-22 05:15:52,576 EDT

JobId: 1471857349684
```

Procedure 55. Set Up the Server

7. □	**OVM-M CLI**: Create unclustered server pool	***Note***: To create clustered server pool, ignore this step and proceed to next. `OVM>create ServerPool clusterEnable=No name=MyServerPool description='Unclustered server pool'`

8.
□
	OVM-M CLI:
	Create clustered server pool (Optional)
		Note: Skip this step if an unclustered server pool is already created. This step is only if required to create a clustered server pool.
		1. To create a clustered server pool you must provide a file system or physical disk to use for the server pool file system. To find a file system or physical disk, use the list command:
		`OVM>list FileSystem`
		`id:66a61958-e61a-44fe-b0e0-9dd64abef7e3  name:nfs on 10.172.76.125:/mnt/vol1/poolfs03`
		`id:0004fb0000050000b85745f78b0c4b61  name:fs on 350014ee2568cc0cf`
		`id:4ebb1575-e611-4662-87b9-a84b40ce3db7  name:nfs on 10.172.76.125:/mnt/vol1/poolfs04`
		`id:858d98c5-3d8b-460e-9160-3415cbdda738  name:nfs on 10.172.76.125:/mnt/vol1/poolfs01`
		`id:0dea4818-20e6-4d3a-958b-b12cf91588b5  name:nfs on 10.172.76.125:/mnt/vol1/poolfs02`
		`id:35b4f1c6-182b-4ea5-9746-51393f3b515c  name:nfs on 10.172.76.125:/mnt/vol2/repo03`
		`id:aeb6143d-0a96-4845-9690-740bbf1e225e  name:nfs on 10.172.76.125:/mnt/vol1/repo01`
		`id:05e8536f-8d9c-4d7c-bbb2-29b3ffafe011  name:nfs on 10.172.76.125:/mnt/vol2/repo02`
		`id:0004fb00000500006a46a8dbd2461939 name:MyServerPool_cluster_heartbeat`
		`id:0004fb00000500000809e28f4fab56b1  name:fs on 350014ee20137ee44`
		`OVM>list PhysicalDisk`
		`id:0004fb000018000019b86ccf3f473a9e  name:FreeBSD (9)`
		`id:0004fb0000180000c4609a67d55b5803  name:FreeBSD (3)`
		`id:0004fb00001800002179de6afe5f0cf3 name:SATA_WDC_WD5001ABYS-_WD-WCAS86288968`
		`id:0004fb0000180000a0b43f9684fc78ac  name:FreeBSD (2)`
		`id:0004fb0000180000732be086afb26911  name:FreeBSD (7)`
		`id:0004fb000018000067ce80973e18374e  name:FreeBSD (8)`
		`id:0004fb000018000035ce16ee4d58dc4d  name:FreeBSD (1)`
		`id:0004fb00001800006855117242d9a537  name:FreeBSD (6)`
		`id:0004fb0000180000a9c7a87ba52ce5ec  name:FreeBSD (5)`
		`id:0004fb0000180000ebabef9838188d78 name:SATA_WDC_WD5001ABYS-_WD-WCAS86571931`

Procedure 55. Set Up the Server

<table>
<tr>
<td></td>
<td></td>
<td>
<pre>
id:0004fb00001800008f6ea92426f2cfb8
name:SATA_WDC_WD5001ABYS-_WD-WCAS86257005

id:0004fb00001800008ccb1925cdbbd181
name:SATA_WDC_WD5001ABYS-_WD-WCAS86578538

id:0004fb0000180000e034b4662665161c name:FreeBSD (4)
</pre>
2. Before you create a clustered server pool you must refresh the file system or physical disk to be used for the server pool file system. To refresh a file system:
<pre>
OVM>refresh { AccessGroup | Assembly | FileServer |
FileSystem | PhysicalDisk | Repository | Server |
StorageArray | VirtualAppliance } instance
</pre>
For example, to refresh a physical disk:
<pre>
OVM>refresh PhysicalDisk
id=0004fb000018000035ce16ee4d58dc4d
</pre>
3. Refresh a file system:
<pre>
OVM>refresh FileSystem name="nfs on
10.172.76.125://mnt//vol1//repo01"

OVM>create ServerPool clusterEnable=Yes filesystem="nfs
on 10.172.76.125://mnt//vol1//poolfs01"
name=MyServerPool description='Clustered server pool'
</pre>
</td>
</tr>
<tr>
<td>9.
□</td>
<td><b>OVM-M CLI</b>:
Add Oracle VM servers to the server pool</td>
<td>
<pre>
OVM>add Server name=MyServer to ServerPool
name=MyServerPool
</pre>
</td>
</tr>
<tr>
<td>10.
□</td>
<td><b>OVM-M CLI</b>:
Create storage repository</td>
<td>
1. Find the physical disk (LUN) to use for creating the storage repository.
<pre>
OVM>list FileServer

Command: list FileServer

Status: Success

Time: 2016-08-19 02:11:39,779 EDT

Data:

id:0004fb00000900000445dac29e88bc38 name:Local FS
vms03.test.com

id:0004fb000009000045715cad6f165ecf name:Local FS
vms01.test.com

id:0004fb0000090000df4cd9c3170092e4 name:Local FS
vms02.test.com

id:0004fb000009000064b96ed88a9a0185 name:Local FS
vms04.test.com
</pre>
2. Find a local file system on an Oracle VM server that has access to the LUN.
<pre>
OVM>list FileServer

Command: list FileServer

Status: Success
</pre>
</td>
</tr>
</table>

Procedure 55. Set Up the Server

```
Time: 2016-08-19 02:11:39,779 EDT

Data:

id:0004fb00000900000445dac29e88bc38  name:Local FS
vms03.test.com

id:0004fb000009000045715cad6f165ecf  name:Local FS
vms01.test.com

id:0004fb0000090000df4cd9c3170092e4  name:Local FS
vms02.test.com

id:0004fb000009000064b96ed88a9a0185  name:Local FS
vms04.test.com
```

3. Create file system.

```
OVM>create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e
490ac3f392" on FileServer name="Local FS
vms01.test.com"

Command: create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e
490ac3f392" on FileServer name="Local FS
vms01.test.com"

Status: Success

Time: 2016-08-19 02:22:46,581 EDT

JobId: 1471587738752

Data:

id:0004fb00000500006779d42da60c0be6  name:VmsFs01
```

4. Create repository.

```
OVM>create Repository name=Vms01Repo on FileSystem
name=VmsFs01

Command: create Repository name=Vms01Repo on FileSystem
name=VmsFs01

Status: Success

Time: 2016-08-19 02:24:04,092 EDT

JobId: 1471587843432

Data:

id:0004fb00000300003c8f771791114d53  name:Vms01Repo
```

5. Add server pool to repository.

```
OVM> add ServerPool name=TestPool001 to Repository
name=Vms01Repo

Refresh the storage repository using the syntax:

OVM> refresh Repository name=MyRepository
```

Appendix D.2 Server Pool

A server pool is a required entity in Oracle VM, even if it contains a single Oracle VM Server. In practice, several Oracle VM servers form a server pool, and an Oracle VM environment may contain one or several server pools. Server pools are typically clustered, although an unclustered server pool is also possible. Server pools have shared access to storage repositories and exchange and store vital cluster information in the server pool file system. Refer [25] Oracle VM Concepts Guide for more information.

Appendix E. Scale a Signaling Node

Execute this procedure only if an additional signaling node(s) needs to be deployed to an existing DSR deployment.

Procedure 56. Scale a Signaling Node

STEP #	***Note***: This procedure is ONLY required if additional Signaling Node(s) needs to be deployed to an existing DSR deployment. **Prerequisite**: DSR topology is already deployed and configured as per section 4 Software Installation Using HEAT Templates (OpenStack). 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 new signaling stack	1. Prepare OpenStack templates and environment files for signaling stacksby following instructions in Procedure 9 for signaling stacks. 2. Create OpenStack parameter file for signaling stacks by following instructions in Procedure 11. ***Note***: Change the number of signaling node(s) as per the requirement. 3. Deploy the stacks by following instructions in Procedure 12. ***Note***: New stack is created as part of this procedure.
2. □	Configure new site in the existing topology	1. Create a new network element by following Procedure 21 to define the network for new site being configured. 2. Configure the SOAM servers by following Procedure 22 to create the SOAM servers. 3. Configure the SOAM server group by following Procedure 23 to create SOAM server group. 4. Configure the MP virtual machines by following Procedure 25. 5. Configure the MP server group(s) and profiles by following Procedure 28. 6. Configure the signaling network routes by following Procedure 30. 7. If deployed stack contains IPFE servers, then configure the IPFE by following Procedure 32.
3. □	Repeat	Repeat this procedure if more signaling nodes are required.

Appendix F. Firewall Ports

Flow Description	Purpose	Protocol/Port	IP Protocol Version
NTP flow for time sync	XMI network	UDP:123	IPv4 , IPv6
hostname resolution (dns)	XMI, IMI Network	UDP/TCP: 53	IPv4, IPv6
LightWeight Directory Access Protocol (LDAP)	XMI Network	UDP/TCP: 389	IPv4, IPv6
SSH	XMI Network	TCP: 22	IPv4, IPv6
GUI	XMI Network	TCP: 80, TCP:443	IPv4, IPv6

Appendix G. Application VIP Failover Options (OpenStack)

Appendix G.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 Figure 4:

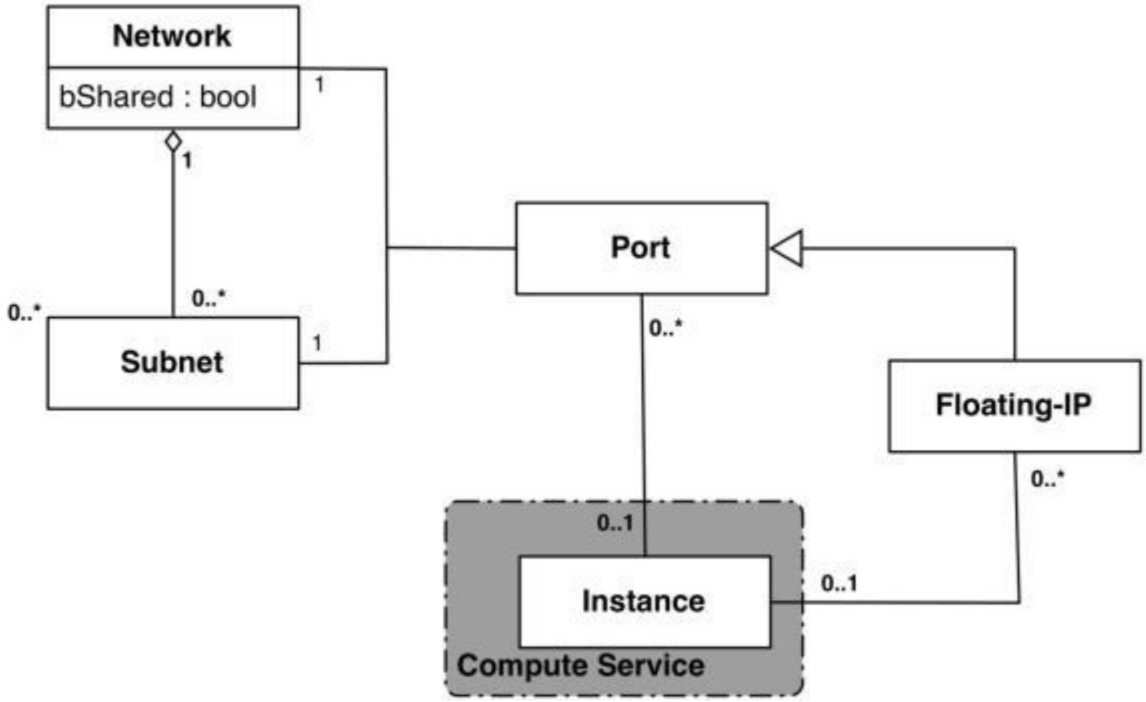


Figure 4. Neutron High-Level Data Model

Note how a port in the Neutron data model maps to at most one VM instance where internal to the VM instance, the port is 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 using 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.

Appendix G.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 use this option after a VM instance has already booted, and how to utilize this option before a VM instance has booted.

Appendix G.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.

Appendix G.4 After a VM Instance has been Booted: Allowed Address Pairs

If a VM instance has already been booted, that is, 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, for example, 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
```

Appendix G.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.

Appendix G.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, to disable 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 use 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 the 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 meantime, 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.

Appendix G.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.

Appendix G.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.

Appendix G.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 H. Sample Net Rules File

Udev uses rules files that determine how it identifies devices and creates device names. The udev daemon (udevd) reads the rules files at system startup and stores the rules in memory. If the kernel discovers a new device or an existing device goes offline, the kernel sends an event action (uevent) notification to udevd, which matches the in-memory rules against the device attributes in /sys to identify the device. As part of device event handling, rules can specify additional programs that should run to configure a device. Rules file, which have the file extension .rules, is located in the following directory: /etc/udev/rules.d/*.rules

Sample File:

```
# eth0 interface with MAC address "fa:16:3e:cc:12:d6" will be assigned "xmi"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="fa:16:3e:cc:12:d6", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="xmi"

# eth1 interface with MAC address "fa:16:3e:1a:8d:8a" will be assigned "int"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="fa:16:3e:1a:8d:8a", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="int"
```

Note: If you need a 3rd interface add respective entry also. The iDIH Mediation VM needs an imi interface too.

```
# eth1 interface with MAC address "fa:16:3e:1a:8d:8a" will be assigned "int"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="
fa:16:3e:8a:1a:12", ATTR{dev_id}=="0x0", ATTR{type}=="1", KERNEL=="eth*",
NAME="imi":
```

Notes:

1. MAC address of each interfaces can be determined using the following command issued from the console: `ifconfig -a`
2. Update MAC address for each interface. The MAC addresses must be entered in all lower case.
3. Update the interface names as in the above example

Appendix I. Performance Tuning Recommended

Appendix I.1 KVM/OpenStack

For the DSR system to achieve 50K MPS or more through IPFE, a few tuning parameters need to be changed.

txqueuelen

Tuned on the compute hosts.

Purpose: default value of 500 is too small. Our recommendation is to set to 30000. Increases the network throughput of a VM.

How/What to change:

On each compute host, do the following as root.

```
# cat > /etc/udev/rules.d/60-tap.rules << EOF
KERNEL=="tap*", RUN+="/sbin/ip link set %k txqueuelen 30000"
EOF
```

Reload and apply to the running system

```
# udevadm control --reload-rules
# udevadm trigger --attr-match=subsystem=net
```

Ring buffer increase on the physical ethernet interfaces

Tuned on the compute hosts.

Purpose: Improves the overall network throughput of the host.

How/What to change: This varies depending on the Host OS. The following steps are applicable to centos/fedora/rhel.

Add the following line into the network script of the interface you want to change. For example: To change the ring buffer on the eth2 interface. Edit /etc/sysconfig/network-scripts/ifcfg-eth2 to add the `ETHTOOL_OPTS=` line as shown.

```
DEVICE=eth2
TYPE=Ethernet
ETHTOOL_OPTS="--set-ring eth2 rx 4096 tx 4096"
```

Restart the network using "service network restart" as root. Check the setting using `ethtool -g eth2`.

Multiqueue [on IPFE]

To be enabled on the openstack flavor and glance image for IPFE instance.

Purpose: Improves the network throughput of a VM.

How/What to change:

You need to update the flavor and the image to enable multiqueue. All guests using that image will be created with multiqueue.

```
# openstack flavor set m1.large --property hw:vif_multiqueue_enabled=true
# glance image-update b5592ed4-8f41-48a9-9f0c-e0e46cb3dd6c --property
hw_vif_multiqueue_enabled=true
```

On the Guest set the number of queues to number of vcpus.

```
ethtool -L <eth interface> combined <number of vcpus>
```

Appendix I.2 VMware

txqueuelen

Tuned on the ESXi hosts.

Purpose: Default value of 500 is too small. The recommendation is to set to 10000 which increases the network throughput of a VM.ESXi defaults the value to 500 and permits a max value of 10000

How/What to change:

Log into the cli console of the ESX host and execute the below esxcli command:

```
#esxcli system settings advanced set -i=10000 -o=/Net/MaxNetifTxQueueLen
```

Ring buffer increase on the physical Ethernet interfaces

Tuned on the ESXi hosts.

Purpose: Improves the overall network throughput of the host.On an ESXi host Rx buffer defaults to 512 and Tx buffer defaults to 1024 and the max value for both is 4096

How/What to change:

Log into the cli console of the ESX host and execute the below esxcli commands:

```
#esxcfg-nics -l    (lists all the physical NICs attached to the host)

#ethtool -g <interface name>  (shows the current ring buffer size)

#ethtool -G <interface name> rx 4096  (increases the rx buffer size to
4096)

#ethtool -G <interface name> tx 4096  (increases the tx buffer size to
4096)
```

Multiqueue

Already enabled on ESXi for vmxnet3 adapters.

Purpose: Improves the network throughput of a VM.

Advanced NUMA settings

Tuned on ESXi hosts.

Purpose: Prevents the ESXi scheduler to move VMs around from one NUMA node to another.

How/What to change:

Log into the cli console of the ESX host and execute the below esxcli commands:

```
#esxcli system settings advanced set -i=0 -o=/Numa/SwapLoadEnable

#esxcli system settings advanced set -i=0 -o=/Numa/SwapLocalityEnable
```

Appendix J. Example Files

Appendix J.1 Example Template File

Basic guidelines to follow while working with YAML files:

- The file must be ended with .yaml extension.
- YAML must be case-sensitive and indentation-sensitive.
- YAML does not support the use of tabs. Instead of tabs, it uses spaces.

YAML is a human-friendly data serialization standard for all programming languages.

The values of the **key:value** can be broadly classified into the following types:

Type	Description	Examples
string	A literal string.	“String param”
number	An integer or float.	“2”; “0.2”
comma_delimited_list	An array of literal strings that are separated by commas. The total number of strings should be one more than the total number of commas.	[“one”, “two”]; “one, two”; ***Note***: “one, two” returns [“one”, ” two”]
json	A JSON-formatted map or list.	{“key”: “value”}
boolean	Boolean type value, which can be equal “t”, “true”, “on”, “y”, “yes”, or “1” for true value and “f”, “false”, “off”, “n”, “no”, or “0” for false value.	“on”; “n”

Appendix J.2 Example Parameter File

The parameter file defines the topology details. This includes all VM details such as the number of VMs, flavors, network names, etc. It is a list of key/value pairs. By referring to the **parameters** definition section in the template file, the initialization of the parameters has to be done in this section.

File Naming Convention

It is not mandatory to have a specific name for the file; but just to provide a self-explanatory name for the file, it is recommended to follow this convention:

<DSR Name>_<Site Name>_<NetworkOam/SignallingNode>_Params.yaml

For example:

- dsrCloudInit_Site00_NetworkOam_Params.yaml
- dsrCloudInit_Site00_SignalingNode_Params.yaml

Sample File

Network OAM params file

```
parameters:
  numPrimaryNoams: 1
  numNoams: 1
  noamImage: DSR-60147
  noamFlavor: dsr.noam
  primaryNoamVmNames: ["DsrSite00NOAM00"]
  noamVmNames: ["DsrSite00NOAM01"]
  noamAZ: nova
  xmiPublicNetwork: ext-net
  imiPrivateNetwork: imi
  imiPrivateSubnet: imi-sub
  imiPrivateSubnetCidr: 192.168.221.0/24
  ntpServer: 10.250.32.10
  noamSG: Site00_NOAM_SG
```

Signaling params file

```
parameters:
  numSoams: 2
  numDas: 1
  numIpfes: 1
  numSs7s: 0
  numStps: 0
  soamImage: DSR-60147
  soamFlavor: dsr.soam
  soamVmNames: ["DsrSite00SOAM00", "DsrSite00SOAM01"]
```

```
daImage: DSR-60147
daFlavor: dsr.da
daVmNames: ["DsrSite00DAMP00", "DsrSite00DAMP01"]
daProfileName: "VM_30K_Mps"
ipfeImage: DSR-60147
ipfeFlavor: dsr.ipfe
ipfeVmNames: ["DsrSite00IPFE00", "DsrSite00IPFE01"]
ss7Image: none
ss7Flavor: none
ss7VmNames: none
stpImage: none
stpFlavor: none
stpVmNames: none
xmiPublicNetwork: ext-net
imiPrivateNetwork: imi
imiPrivateSubnet: imi-sub
imiPrivateSubnetCidr: 192.167.2.0/24
xsiPublicNetwork: ext-net
ntpServer: 10.250.32.10
soamAZ: nova
daAZ: nova
ipfeAZ: nova
ss7AZ: nova
stpAZ: nova
soamSG: Site00_SOAM_SG
daSG: Site00_DAMP_SG
ipfeSGs: ["Site00_IPFE_SG0", "Site00_IPFE_SG1"]
ss7SG: Site00_SS7_SG
stpSG: Site00_STP_SG
primaryNoamVmName: DsrSite00NOAM00
noamXmiIps: ["10.75.191.170"]
diameterTcpPorts: [3868]
diameterSctpPorts: []
stpSctpPorts:[]
```

Network OAM params file (Fixed IP)

```
parameters:
  numPrimaryNoams: 1
  numNoams: 1
  noamImage: DSR-8.2.0.0.0_82.5.1.vmdk
  noamFlavor: dsr.noam
  primaryNoamVmNames: ["DsrSite00NOAM00"]
  noamVmNames: ["DsrSite00NOAM01"]
  noamAZ: nova
  primaryNoamXmiIps: ["10.196.12.83"]
  noamXmiIps: ["10.196.12.84"]
  noamVip: 10.196.12.85
  xmiPublicNetwork: ext-net3
  imiPrivateNetwork: imi
  imiPrivateSubnet: imi-sub
  imiPrivateSubnetCidr: 192.168.221.0/24
  ntpServer: 10.75.185.194
  noamSG: Site00_NOAM_SG
```

Signaling params file (Fixed IP)

```
parameters:
  numSoams: 2
  numDas: 2
  numIpfes: 1
  numSs7s: 0
  numStps: 0
  soamImage: DSR-8.2.0.0.0_82.5.1.vmdk
  soamFlavor: dsr.soam
  soamVmNames: ["DsrSite00SOAM00", "DsrSite00SOAM01"]
  soamXmiIps: ["10.196.12.83", "10.196.12.84"]
  soamVip: 10.196.12.86
  daProfileName: "VM_30K_Mps"
  daImage: DSR-8.2.0.0.0_82.5.1.vmdk
  daFlavor: dsr.da
  daVmNames: ["DsrSite00DAMP00", "DsrSite00DAMP01"]
  daMpXmiIps: ["10.196.12.25", "10.196.12.26"]
  daMpXsiIps: ["10.196.52.73", "10.196.52.74"]
```

```
ipfeImage: DSR-8.2.0.0.0_82.5.1.vmdk
ipfeFlavor: dsr.ipfe
ipfeVmNames: ["DsrSite00IPFE00", "DsrSite00IPFE01"]
ipfeXmiIps: ["10.196.12.85"]
ipfeXsiIps: ["10.196.52.75"]
ipfeXsiPublicIp: 10.196.52.80
ss7Image: DSR-8.2.0.0.0_82.5.1.vmdk
ss7Flavor: dsr.ss7
ss7VmNames: ["DsrSite00SS700", "DsrSite00SS701"]
ss7XmiIps: ["10.196.12.27", "10.196.12.28"]
ss7XsiIps: ["10.196.52.72", "10.196.52.76"]
stpImage: DSR-8.2.0.0.0_82.5.1.vmdk
stpFlavor: dsr.vstp
stpVmNames: ["DsrSite00STP00", "DsrSite00STP01"]
stpXmiIps: ["10.196.12.29", "10.196.12.30"]
stpXsiIps: ["10.196.52.77", "10.196.52.78"]
xmiPublicNetwork: ext-net3
imiPrivateNetwork: imi
imiPrivateSubnet: imi-sub
imiPrivateSubnetCidr: 192.167.2.0/24
xsiPublicNetwork: ext-net2
ntpServer: 10.250.32.10
soamAZ: nova
daAZ: nova
ipfeAZ: nova
ss7AZ: nova
stpAZ: nova
soamSG: Site00_SOAM_SG
daSG: Site00_DAMP_SG
ipfeSGs: ["Site00_IPFE_SG0", "Site00_IPFE_SG1"]
ss7SG: Site00_SS7_SG
stpSG: Site00_STP_SG
diameterTcpPorts: [3868]
diameterSctpPorts: []
stpSctpPorts:[]
```

Appendix K. My Oracle Support (MOS)

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

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

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:

   For technical issues such as creating a new Service Request (SR), select 1.

   For non-technical issues such as registration or assistance with MOS, select 2.

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center

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

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click Industries.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings N**etwork Session Delivery and Control Infrastructure** or **Platforms**.

4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.