Oracle® Communications

Diameter Signaling Router

SDS 8.0 Cloud Installation

E76333-02

June 2017

ORACLE

Oracle Communications SDS Cloud Installation Procedure, Release 8.0

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

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

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

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

See more information on MOS in the Appendix G, My Oracle Support (MOS).

Table of Contents

List of Tables

List of Procedures

1. Introduction

1.1 Purpose and Scope

This document describes how to install the Oracle® Communications Diameter Signal Router Full Address Resolution product also known as Eagle XG Subscriber Data Server (SDS) within a customer network. It makes use of the AppWorks 7.2 network installation and covers the initial network configuration steps for an SDS/Query Server NE for production use as part of the DSR solution.

This document only describes the SDS product SW installation on a virtualized solution into virtual machines (VMs) hosted by the following hypervisors: VMWare, KVM, and OVM-S. It does not cover hardware installation, site survey, customer network configuration, IP assignments, customer router configurations, or the configuration of any device outside of the SDS VMs.

1.2 References

[1] Oracle Acronym Guide, MS005077, Latest Revision

[2] Diameter Signaling Router Cloud Installation Guide, E76331, cgbu_019911, Latest Revision

[3] Network Architecture Planning Document, cgbu_010618, Latest Revision

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
CSV	Comma Separated Values
DR	Disaster Recovery
FABR	Full Address Based Resolution
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAM	Network Operation Administration and Maintenance
OS	Operating System (e.g. TPD)
OVA	Open Virtualization Archive
OVM-M	Oracle VM Manager
OVM-S	Oracle VM Server
SDS	Subscriber Data Server
SNMP	Simple Network Management Protocol
SOAM	Software Operation Administration and Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
VIP	Virtual IP
VM	Virtual Machine
XMI	External Management Interface

1.4 Assumptions

This document assumes the following:

- The user has reviewed the latest customer-specific Network Architecture Planning document [3] Network Architecture Planning Document, cgbu_010618, Latest Revision and has received assigned values for all requested information related to SDS, DR SDS NO, Query Server, DP-SOAM, and DP installation.
- The user has taken assigned values from the latest customer-specific Network Architecture Planning document [3] Network Architecture Planning Document, cgbu_010618, Latest Revision and used them to compile XML files (See Error! Reference source not found.) for each SDS and DP-SOAM site's NE before attempting to execute this procedure.
- The user conceptually understands DSR topology and SDS network configuration as described in the latest customer-specific Network Architecture Planning document [3] Network Architecture Planning Document, cgbu_010618, Latest Revision.
- The user has at least an intermediate skill set with command prompt activities on an Open systems computing environment such as Linux or TPD.

1.5 XML Files

The XML files compiled for installation of the each of the SDS and DP-SOAM site's NE must be maintained and accessible for use in disaster recovery procedures. The Oracle Professional Services Engineer (PSE) provides a copy of the XML files used for installation to the designated customer operations POC. The customer is ultimately responsible for maintaining and providing the XML files to Oracle's Customer Service (US: 1-888-367-8552, Intl: +1-919-460-2150) if needed for use in disaster recovery operations.

1.6 How to Use This Document

Although this document is primarily used as an initial installation guide, its secondary purpose is as a reference for disaster recovery procedures. When executing this document for either purpose, there are a few points that help ensure the user understands the author's intent. These points are as follows;

- Before beginning a procedure, completely read the instructional text (it appears immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before execution of a STEP within a procedure, completely read the left and right columns including any step-specific WARNINGS or NOTES.

If a procedural step fails to execute successfully, STOP and contact Oracle's Help Center (US: 1-888-367-8552, Intl: +1-919-460-2150) for assistance before attempting to continue. See Appendix G My Oracle Support (MOS) for information on contacting Oracle customer support.

2. Pre-Installation Setup

The following items/settings are required to install SDS.

- A laptop or desktop computer equipped with the following:
  - Administrative privileges for the OS
  - An approved web browser
- TPD **admusr** password

2.1 Activity Logging

All activity while connected to the system should be logged using a convention that notates the **Customer Name**, **Site/Node** location, **Server hostname**, and **Date**. All logs should be provided to Oracle Communications for archiving post installation.

3. Software Installation Procedure

Installing SDS requires multiple installations of varying types. This document only covers the necessary configuration required to for a complete production installation. Refer to the online help or contact Oracle Help Center for assistance with post-installation configuration options.

3.1 Create SDS Guests

Procedure 1. Create SDS Guests from OVA (VMware)

Step	Procedure	Result
1 ☐	**Cloud Client**: Add SDS OVA image	1. Launch the cloud client of your choice. 2. Add the DDS OVA image to the cloud catalog or repository. Follow the instructions provided by the cloud solutions manufacturer.
2 ☐	**Cloud Client**: Create the SDS VM from the OVA image	1. Browse the library or repository that you placed the **OVA** image. 2. Deploy the OVA Image using **Cloud Client** or **Cloud Web Client**. 3. Name the **SDS NOAM VM** and select the data store.
3 ☐	**Cloud Client**: Configure resources for the SDS NOAM-A VM	Configure the SDS NOAM VM per the Appendix C Resource Profile for the **SDS NOAM** using the **Cloud Client** or **Cloud Web Client**.
4 ☐	**Cloud Client**: Power on the SDS NOAM-A VM	Use the **Cloud Web Client** to power on the **SDS NOAM-A VM**.

Procedure 1. Create SDS Guests from OVA (VMware)

Step	Procedure	Result

5 ☐	**Cloud Client**: Configure SDS NOAM-A	1. Access the **SDS NOAM-A VM** console via the **Cloud Client** or **Cloud 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>`
		Note: When reconfiguring virtual NICs under VMware, the proper procedure is to remove the UDEV rules file (/etc/udev/rules.d/70-persistent-net.rules), shut down the guest, and remove the interfaces. Power on the VM, and add the interfaces one by one in the desired order of enumeration. Clicking **OK** each time to have VMware instantiate the device.

6 ☐	Verify network connectivity	Ping the default gateway. `$ ping -c3 <Gateway of External Management Network>`
7 ☐	Repeat	Repeat steps 1 through 6 for the server before continuing to the next procedure (e.g., NOAM-A, NOAM-B, DR SDS servers, Query server, DP).

Procedure 2. Create SDS Guest from OVA (KVM/OpenStack)

Step	Procedure	Result
1 ☐	Preparation	1. Create instance flavors. Use the Appendix C Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the Admin section, or with the `nova flavor-create` command line tool. Make the flavor names as informative as possible. Since 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) represent the RAM allocation in GB, and the final three figures (060) represent the disk space in GB. 2. If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, note the default LRO (Large Receive Offload) option must be disabled on the host command line. See the Intel release notes for more details. This action can be performed with the following command. `$ sudo ethtool -K <ETH_DEV> lro off`

Procedure 2. Create SDS Guest from OVA (KVM/OpenStack)

Step	Procedure	Result

2
☐
	Add SDS OVA image	1. Copy the OVA file to the OpenStack control node.
		`$ scp SDS-x.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 SDS-x.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.
		SDS-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.
		sds-x.x.x-original
		7. Import the image using the **glance** utility from the command line.
		`$ glance image-create --name sds-x.x.x-original --visibility public --protected false progress --container-format bare --disk-format vmdk --file SDS-x.x.x-disk1.vmdk`
		This process takes about 5 minutes, depending on the underlying infrastructure.

3 ☐	Name the new VM instance	1. Create an informative name for the new instance: **SDS-NOAM-A**. 2. Examine the network interface recommendations at the bottom of the Resource Profile in Appendix C.

Procedure 2. Create SDS Guest from OVA (KVM/OpenStack)

Step	Procedure	Result

4
☐
	OpenStack Control Node: Create and boot the VM instance from the glance image	1. Get the following configuration values.
		The image ID.
		`$ glance image-list`
		The flavor ID.
		`$ nova flavor-list`
		The network ID(s)
		`$ neutron net-list`
		An informative name for the instance.
		SDS-NOAM-A
		SDS-NOAM-B
		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.
		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> --config-drive true <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.

5
☐
	OpenStack Control Node: Configure VIP (Optional)	***Note***: Refer to Allowed Address Pairs in Appendix F for more information on VIP.
		If an NOAM VIP is needed, execute the following commands:
		1. Find the port ID associated with the instance's network interface.
		`$ neutron port-list`
		2. Add the VIP IP address to the address pairs list of the instance network interface port.
		`$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>`

6 ☐	Check if interface is configured	If DHCP is enabled on the Neutron subnet, VM configures the VNIC with the IP address provided in step 4. To verify, ping the network IP address provided with **nova boot…** command from step 4: `$ ping <XMI-IP-Provided-During-Nova-Boot>` If the ping is successful, ignore step 7 to configure the interface manually.

Procedure 2. Create SDS Guest from OVA (KVM/OpenStack)

Step	Procedure	Result

7
☐
	OpenStack Dashboard (Horizon): Manually configure interface, if not already done (Optional)	***Note***: If the instance is already configured with an interface and has successfully pinged (step 6), then **ignore** this step to configure the interface manually.
		1. Log into the **Horizon** GUI as the 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. Select an informative hostname for the new VM instance.
		SDS-NOAM-A
		SDS-SO2
		7. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C.
		`$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi port 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 more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions:
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly.
		Re-run the `netAdm command`. It creates and configures the interface in one action.
		8. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
		`$ sudo init 6`
		The new VM should now be accessible via both network and Horizon consoles.

8 ☐	Verify network connectivity	Ping the default gateway. `$ ping -c3 <Gateway of External Management Network>`
9 ☐	Repeat	Repeat steps 1 through 8 for each server before continuing to the next procedure (e.g., NOAM-A, NOAM-B, DR SDS servers, Query server, DP).

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result
1 ☐	Preparation	Refer to Appendix E Common OVM-Manager Tasks (CLI) for setting up the platform. Log into the OVM-M CLI for executing all the OVM commands. Refer to step 1 of Appendix E Common OVM-Manager Tasks (CLI).

2 ☐	**OVM-M CLI**: Import the OVA	Import the Virtual Appliance/OVA.
		`OVM>importVirtualAppliance Repository name=MyRepository url="http:////example.com//myvirtualappliance.ova"`
		Example:
		`OVM>importVirtualAppliance Repository name=Vms01Repo url=http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Command: importVirtualAppliance Repository name=Vms01Repo url=http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Status: Success`
		`Time: 2016-09-09 07:33:11,777 EDT`
		`JobId: 1473420749759`
		`Data:`
		`id:11cdf999eb name:SDS-8.0.0.0.0_80.11.0.ova`
		Note: Use the highlighted ID for referring the newly created virtual appliance in any further commands.

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result

3 ☐	**OVM-M CLI**: Create VM	1. Show the virtual appliance to get the virtual appliance VM name.
		Note: The ID referred to in the command below is the virtual appliance ID from the above step.
		`OVM>show VirtualAppliance id=11cdf999eb`
		`Command: show VirtualAppliance id=11cdf999eb`
		`Status: Success`
		`Time: 2016-09-09 07:39:12,491 EDT`
		`Data:`
		`Origin = http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Repository = 0004fb000003000072973b7457792d93 [Vms01Repo]`
		`Virtual Appliance Vm 1 = 11cdf999eb_vm_vm [vm]`
		`Virtual Appliance VirtualDisk 1 = 11cdf999eb_disk_disk1 [disk1]`
		`Id = 11cdf999eb [SDS-8.0.0.0.0_80.11.0.ova]`
		`Name = SDS-8.0.0.0.0_80.11.0.ova`
		`Description = Import URL: http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Locked = false`
		2. Create a VM from a virtual machine in a virtual appliance.
		Note: The virtual appliance VM name referred to in the command below is the name from the above step.
		`OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name= 11cdf999eb_vm_vm`
		`Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11cdf999eb_vm_vm`
		`Status: Success`
		`Time: 2016-09-09 07:53:05,702 EDT`
		`JobId: 1473421832449`
		`Data:`
		`id:0004fb000006000009a08ec97ad5496b name:SDS-8.0.0.0.0_80.11.0.ova_vm`

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result

4 ☐	**OVM-M CLI**: Add VM to server pool	Add VM to server pool.
		Note: Use the VM ID/Name from step 3 for any related commands.
		`OVM>add Vm instance to { AntiAffinityGroup | Server | ServerPool } instance`
		Example:
		`OVM>add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001`
		`Command: add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001`
		`Status: Success`
		`Time: 2016-08-30 02:15:00,859 EDT`
		`JobId: 1472537700721`
		Note: Refer E-3 Server Pool section for further information on server pool.

5 ☐	**OVM-M CLI**: Edit NOAM VM with required profile/resource	Edit NOAM VM with required resources. Refer Appendix C Resource Profile for recommended resource profile. Create an informative name for the new instance: SDS-NOAM-A
		Note: Use the VM ID/Name in any related commands.
		`OVM>edit Vm id=0004fb000006000009a08ec97ad5496b name=SDS-NOAM-A memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="SDS-NOAM-A"`
		`Command: edit Vm id=0004fb000006000009a08ec97ad5496b name=SDS-NOAM-A memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="SDS-NOAM-A"`
		`Status: Success`
		`Time: 2016-08-22 02:04:09,329 EDT`
		`JobId: 1471845849193`

6 ☐	**OVM-M CLI**: Attach VNIC	1. If VNIC is already created, attach it. First, get the VNIC ID:
		`OVM>show Vm name=SDS-NOAM-A`
		`Command: show Vm name=SDS-NOAM-A`
		`Status: Success`
		`Time: 2016-08-24 06:42:00,115 EDT`
		`Data:`
		`Status = Running`
		`Memory (MB) = 6584`
		`Max. Memory (MB) = 6584`
		`Processors = 6`
		`Max. Processors = 6`

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result
		Priority = 50 Processor Cap = 100 High Availability = No Operating System = Oracle Linux 6 Mouse Type = PS2 Mouse Domain Type = Xen HVM PV Drivers Keymap = en-us Start Policy = Use Pool Policy Origin = http://10.240.191.134/SDS-8.0.0.0.0_80.8.0.ova Disk Limit = 107 Huge Pages Enabled = No Config File Absolute Path = /dev/mapper/OVM_SYS_REPO_PART_3600605b00a15b2601cb8a56a1410036a/VirtualMachines/0004fb0000060000e07023e7051a923c/vm.cfg Config File Mounted Path = /OVS/Repositories/0004fb000003000072973b7457792d93/VirtualMachines/0004fb0000060000e07023e7051a923c/vm.cfg Server = 08:00:20:ff:ff:ff:ff:ff:ff:ff:00:10:e0:71:91:34 [compute01.test.com] Server Pool = 0004fb0000020000ff238819a2310353 [TestPool001] Repository = 0004fb000003000072973b7457792d93 [Vms01Repo] Vnic 1 = 0004fb000007000078f3fdb5bea01697 [00:21:f6:6f:b6:b1] VmDiskMapping 1 = 0004fb0000130000ac3e9f3d21e90188 [Mapping for disk Id (0004fb0000120000c95393297e1028e9.img)] VmDiskMapping 2 = 0004fb00001300002852a93587c1893a [Mapping for disk Id (EMPTY_CDROM)] Restart Action On Crash = Restart Id = 0004fb0000060000e07023e7051a923c [SDS-NOAM-A] Name = SDS NOAM-A Description = SDS NOAM-A Locked = false DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)] 2. Add VNIC to network.

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result

		Note: The VNIC ID referred to in the following command is the ID from the above step.
		`OVM>add Vnic id=0004fb000007000078f3fdb5bea01697 to Network name=XMI`
		3. List the networks.
		`OVM>list Network`
		`Command: list Network`
		`Status: Success`
		`Time: 2016-09-26 05:34:25,088 EDT`
		`Data:`
		`id:109560cfdc name:XSI1`
		`id:10e361d8ee name:XSI2`
		`id:107561a2ba name:XMI`
		`id:10333df5b6 name:IMI`
		`id:0af01080 name:10.240.16.128`

7
☐
	OVM-M CLI: Create and attach remaining VNICs for the VM	Create VNIC on the network and attach to it.
		Note: The network referred to in the following command is the network name from the above step.
		`OVM>create Vnic network=IMI name=SDS-NOAM-A-IMI on Vm name=SDS-NOAM-A`
		`Command: create Vnic network=IMI name=SDS-NOAM-A-IMI on Vm name=SDS-NOAM-AStatus: Success`
		`Time: 2016-08-22 05:38:34,252 EDT`
		`JobId: 1471858714114`
		`Data:`
		`id:0004fb0000070000b51a093ec88ed87d name: SDS-NOAM-A-IMI`
		Note: Repeat this step for all required interfaces (XSI1, XS2, etc.).

Procedure 3. Create SDS Guests from OVA (OVM-S/OVM-M)

Step	Procedure	Result

8 ☐	**OVM-M CLI**: Configure instance networking	1. Log into the **OVM-Manager** console.
		`https://<OVM-M-IP:port>/ovm/console/faces/login.jspx`
		2. Go to the servers and VMs tab.
		3. Select the host from the server pools.
		4. Select the VM and click **Launch Console**.
		5. Login as the **admusr** user.
		6. Configure the required network interfaces, conforming to the interface-to-network mappings described at the bottom of Appendix C Resource Profile.
		`$ sudo netAdm set --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 Gateway>`
		Under some circumstances, it may be necessary to configure more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions:
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly.
		Re-run the `netAdm command`. It creates and configures the interface in one action.
		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 via both network and console.

9 ☐	**OVM-M CLI**: Start VM	Start the VM.
		`OVM>start Vm name=SOAM-A`
		`Command: start Vm name=SOAM-A`
		`Status: Success`
		`Time: 2016-08-22 06:32:37,853 EDT`
		`JobId: 1471861954163`

10 ☐	Repeat	Repeat steps 2 through 9 for each server before continuing to the next procedure (e.g., NOAM-A, NOAM-B, DR SDS servers, Query server, DP).

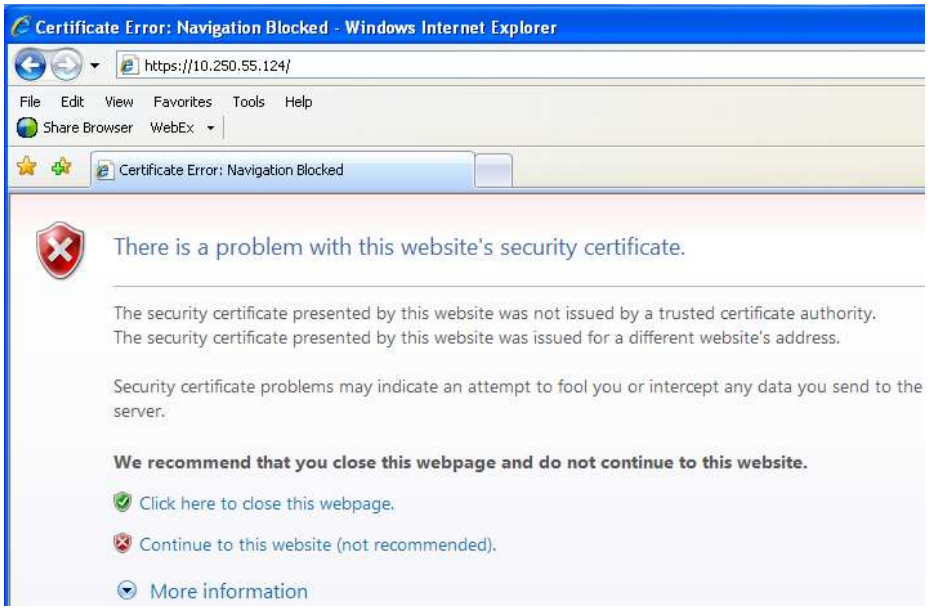
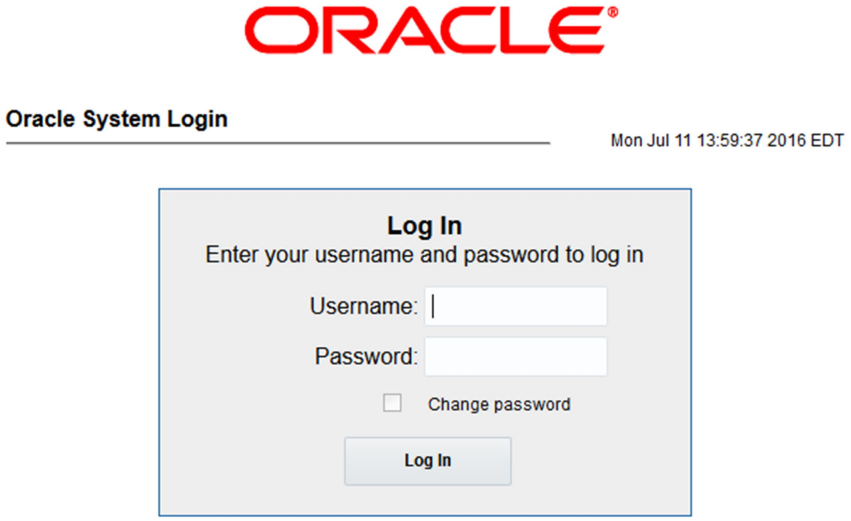
3.2 Configure SDS NOAM Servers (First Site Only)

Assumptions:

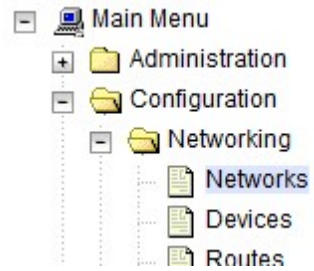
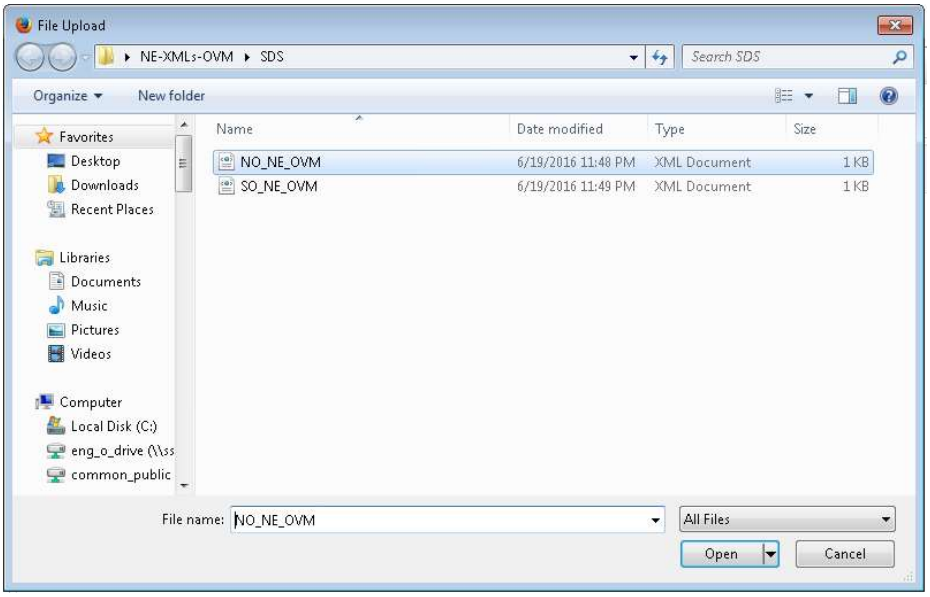
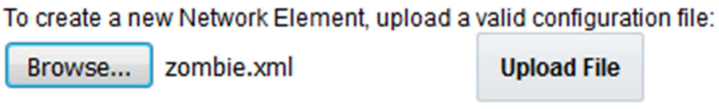
- This procedure assumes the SDS Network Element XML file for the Primary Provisioning SDS site has previously been created as described in the Appendix A Create an XML File for Installing SDS Network Elements.
- This procedure assumes that the Network Element XML files are on the laptop's hard drive.

This procedure requires a connection to the SDS GUI before configuring the first SDS server.

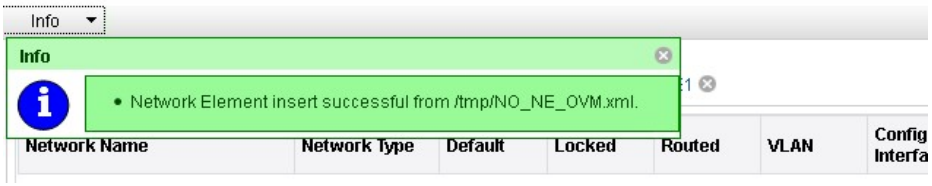
Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

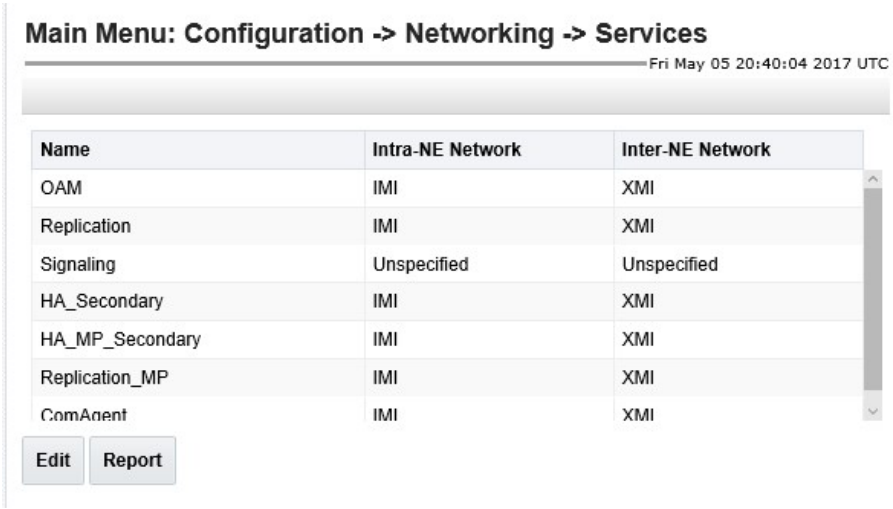
Step	Procedure	Result
1 ☐	**SDS NOAM-A**: Launch an approved web browser and connect to the SDS NOAM-A XMI IP address.	If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**SDS NOAM-A**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server by using the XMI IP address. 

Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

Step	Procedure	Result
3 ☐	**SDS NOAM-A**: Create the SDS NOAM-A network element using the XML file	Navigate to **Main Menu->Configuration->Networking->Networks**.  Click **Browse** and type the pathname of the NOAM network XML file.  ***Note***: This step assumes the **XML** files were previously prepared as described in Appendix A Create an XML File for Installing SDS Network Elements. Select the location of the **XML** file and click **Open**.  Click **Upload File** to upload the XML file.  If the values in the **XML** file pass, an information banner displays.

Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

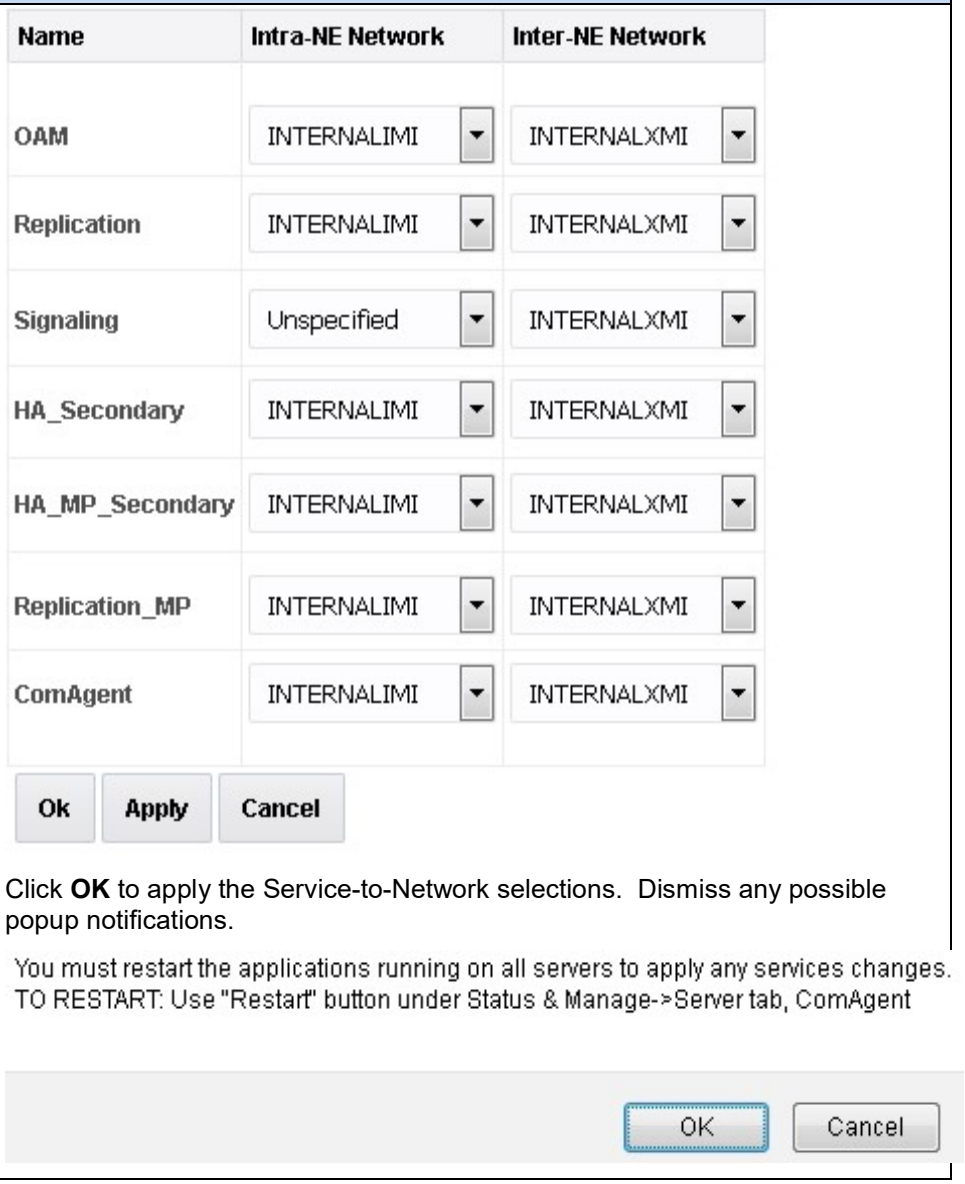
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>Main Menu: Configuration -> Networking -> Networks
 

Note: You may need to left-click on the Info banner to display the banner.</td></tr>
<tr><td>4
☐</td><td>SDS NOAM-A: Map services to networks</td><td>Navigate to Main Menu->Configuration->Networking->Services.
Click Edit.
 

Set the services as shown in the table below:
<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>OAM</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>Replication</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>Signaling</td><td>Unspecified</td><td><XMI Network></td></tr>
<tr><td>HA_Secondary</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>HA_MP_Secondary</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>Replication_MP</td><td><IMI Network></td><td><XMI Network></td></tr>
<tr><td>ComAgent</td><td><IMI Network></td><td><XMI Network></td></tr>
</table>
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:</td></tr>
</table>

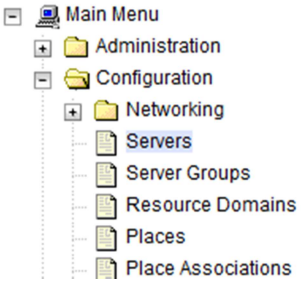
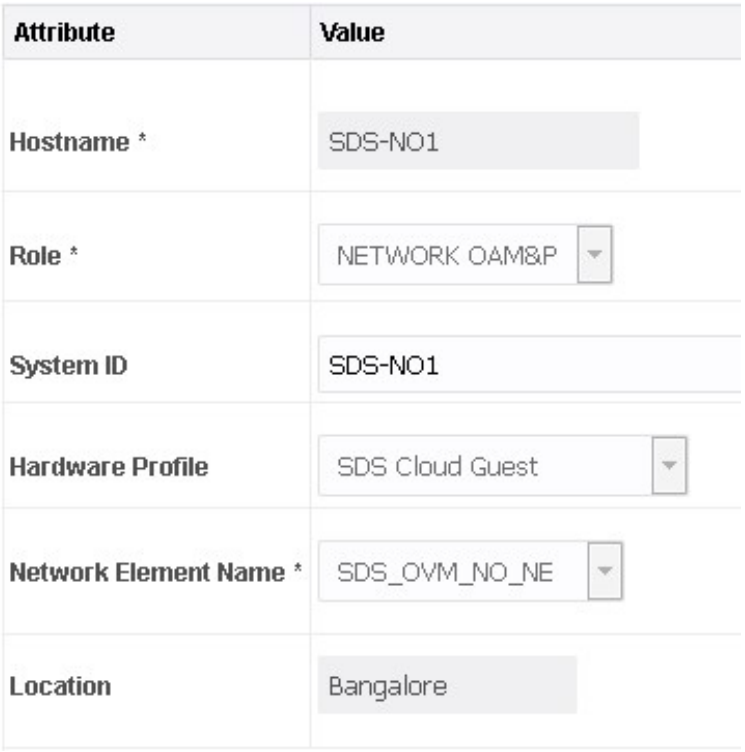
Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

Step	Procedure	Result



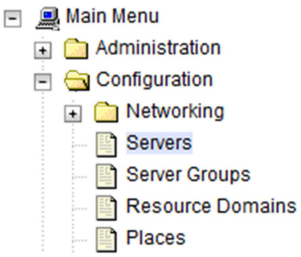
Click **OK** to apply the Service-to-Network selections. Dismiss any possible popup notifications.

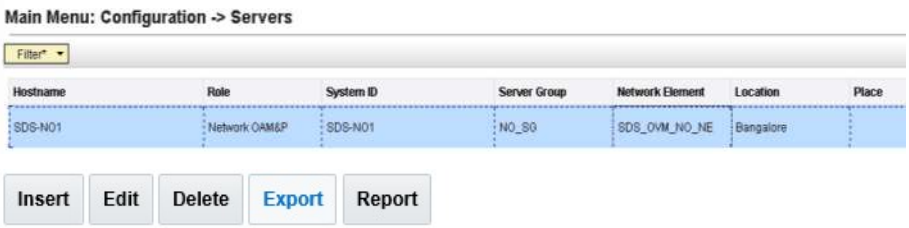
Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

Step	Procedure	Result
5 ☐	**SDS NOAM-A**: Insert the 1st VM	Navigate to **Main Menu->Configuration->Servers**.  Click **Insert** to insert the new NOAM server into servers table (the first or server). Fill in the fields as follows: Hostname: Assigned Hostname Role: NETWORK OAM&P System ID: Assigned Hostname Hardware Profile: SDS Cloud Guest Network Element Name: [Select **NE** from list] Location: Optional 

Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>6
☐</td><td>SDS NOAM-A:
Insert the 1st VM</td><td>The network interface fields are now available with selection choices based on the chosen hardware profile and network element.
 

Type the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
Type the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
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 (Optional)</td><td>No</td></tr><tr><td>Valid NTP Server (Optional)</td><td>No</td></tr></table>
Click OK when you have completed entering all the server data.</td></tr>
<tr><td>7
☐</td><td>SDS NOAM-A:
Export the initial configuration</td><td>Navigate to Main Menu->Configuration->Servers.
 

From the GUI screen, select the SDS 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.
 
</td></tr>
</table>

Procedure 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

Step	Procedure	Result

8
☐
	SDS NOAM-A: Copy server configuration file to /var/tmp directory	Obtain a terminal window to the SDS NOAM-A server, logging in as the **admusr** user.
		Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the SDS NOAM-A to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		`$ cp /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM-A_hostname>.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the configuration file and automatically executes it.
		For the NOAM-B server, the command is:
		`$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<NOAM-B_hostname>.sh \`
		`<NOAM-B_ipaddr>:/var/tmp/TKLCConfigData.sh`
		Note: The IPADDR is the IP address of NOAM-B associated with the XMI network.

9 ☐	**SDS NOAM-A**: 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. A broadcast message is sent to the terminal. This can take anywhere from 3-20 minutes to complete. 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
☐
	SDS NOAM-A: 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 4. Configure SDS Servers A and B (First SDS NOAM Site Only)

Step	Procedure	Result

9 ☐	**SDS NOAM-A**: Verify server health	Login into the NOAM1 as the **admusr** user.
		Execute the following command 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`

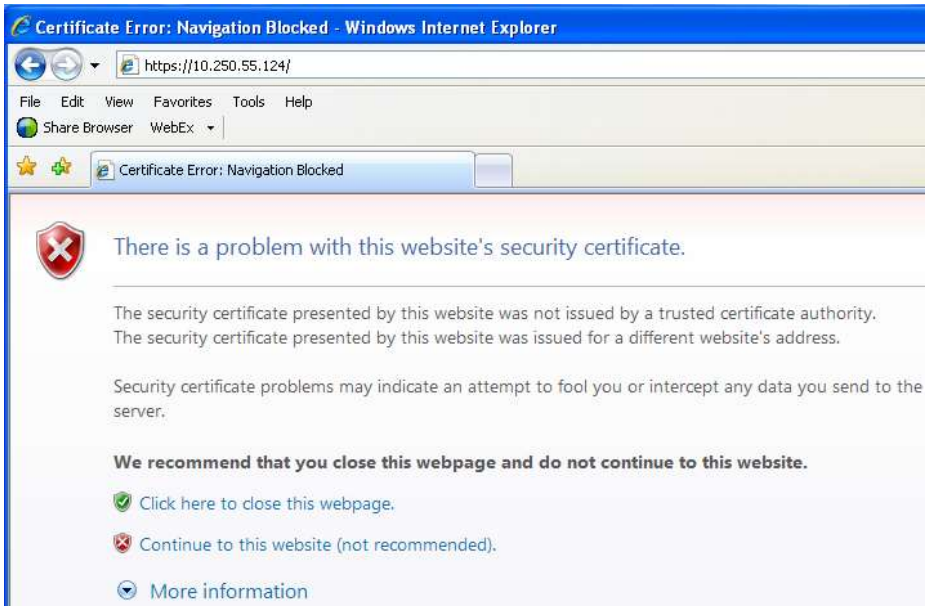
10 ☐	**SDS NOAM-A**: Verify server health	Exit from the command line to return to the server console.
		`$ exit`
		`sds-mrsvnc-a login:`

11 ☐	**SDS NOAM-B**: Repeat	Configure DR SDS NOAM-B by repeating steps 5 through 10 of this procedure.

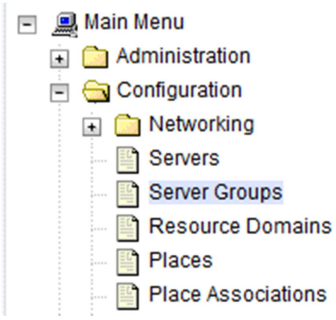
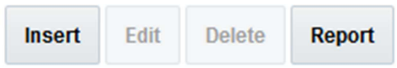
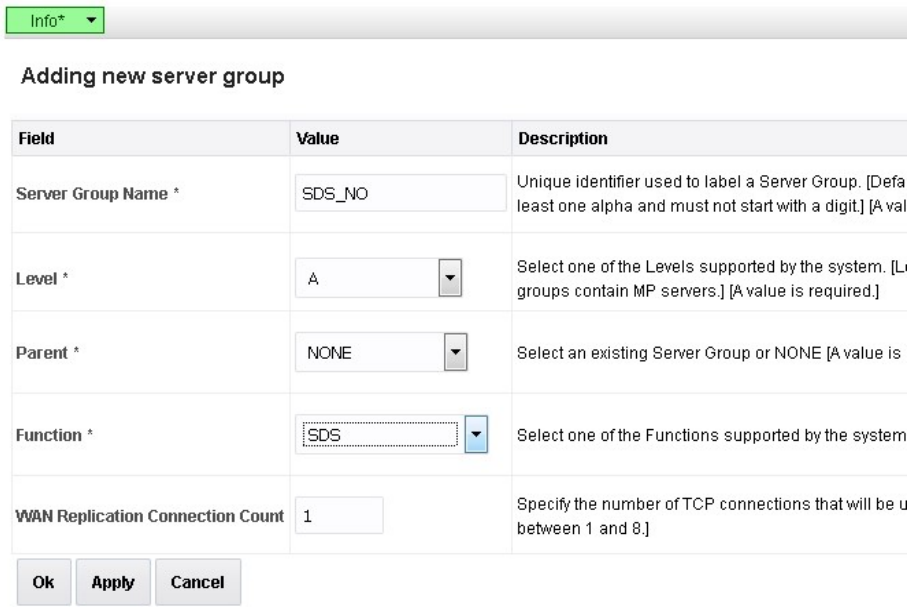
3.3 OAM Pairing (First SDS NOAM Site Only)

During the OAM pairing procedure, various errors may display at different stages of the procedure. During the execution of a step, ignore errors related to values other than the ones referenced by that step.

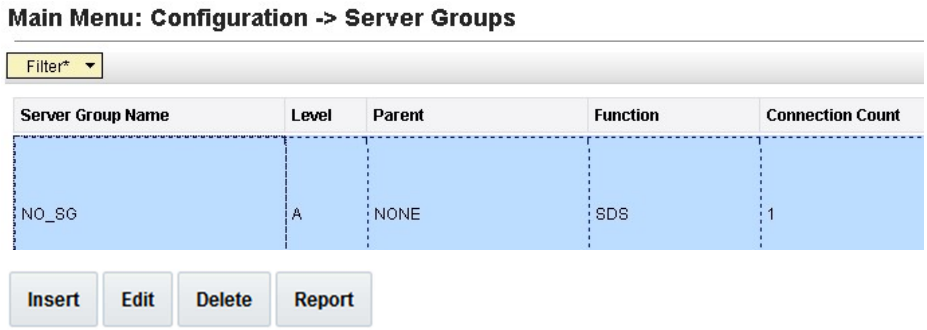
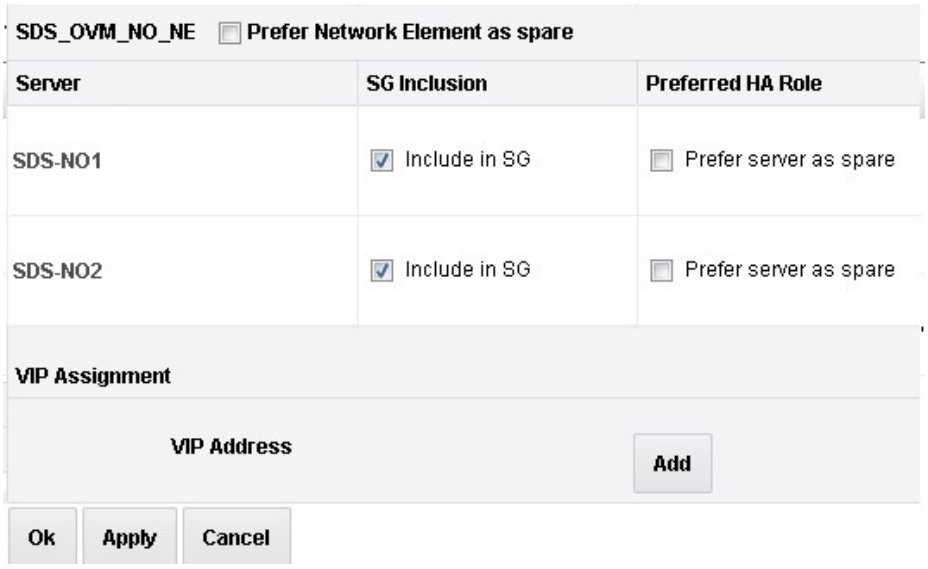
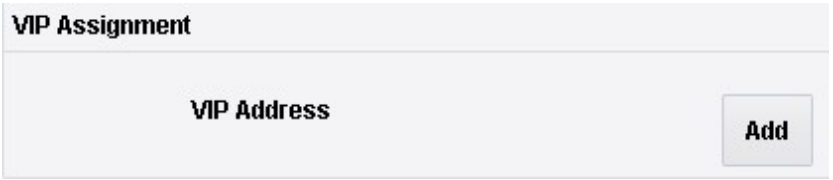
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
1 ☐	**SDS NOAM-A**: Launch an approved web browser and connect to the SDS NOAM-A using an https:// address.	If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**SDS NOAM-A**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server. 

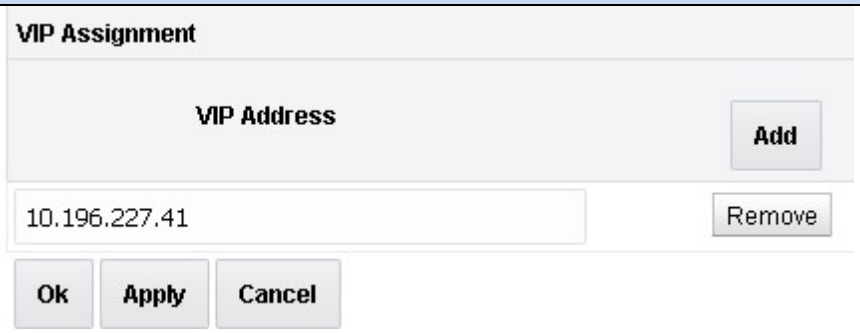
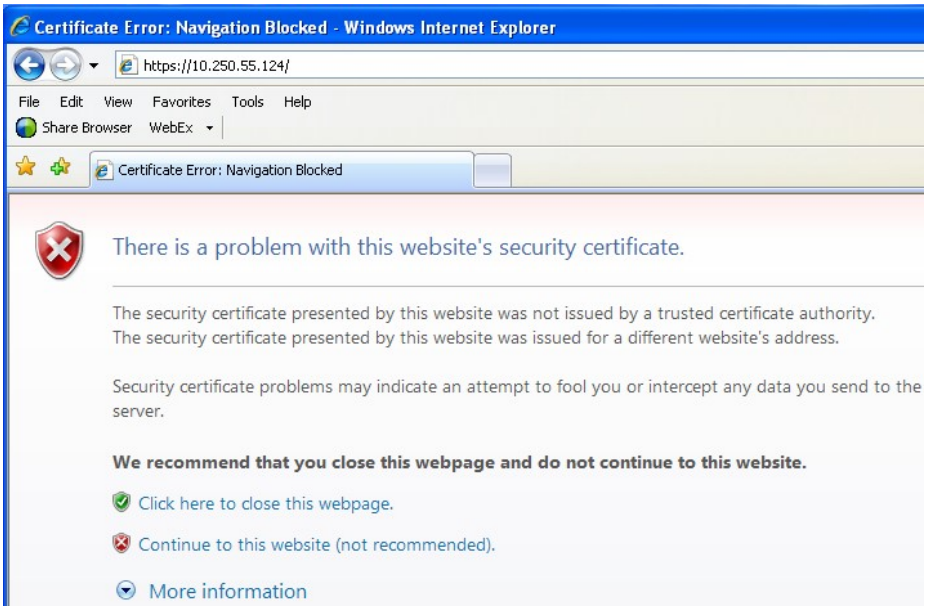
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
3 ☐	**SDS NOAM-A**: Enter group data	Navigate to **Main Menu->Configuration->Server Groups**.  Click **Insert**.  Fill in the following fields: Server Group Name: [Type Server Group Name] Level: A Parent: None Function: SDS WAN Replication Connection Count: Use Default Value **Main Menu: Configuration -> Server Groups [Insert]**  Click **OK** when all fields are filled in.

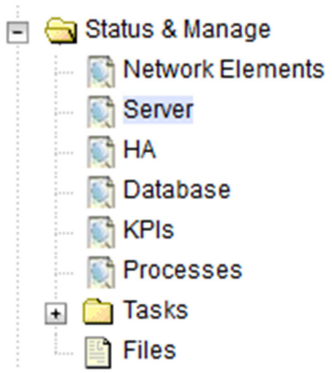
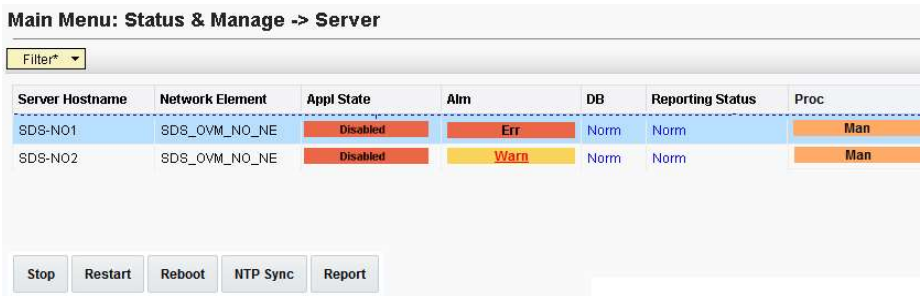
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
4 ☐	**SDS NOAM-A**: Add server to OAM Server Group	Select the new server group and click **Edit**.  In the portion of the screen that lists the servers for the server group, find the SDS-NOAM servers being configured. Mark the **Include in SG** checkbox.  Leave other boxes unchecked. Click **Apply**.
5 ☐	**SDS NOAM-A**: Add VIP address	Click **Add**.  Type the **VIP Address** and click **Apply**.

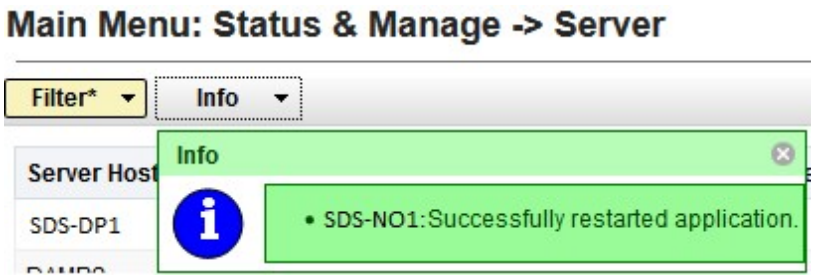
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
		 This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).
6 ☐	**SDS VIP**: Launch an approved web browser and connect to the XMI virtual IP address assigned in step 5 to the SDS server group using https://.	If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 

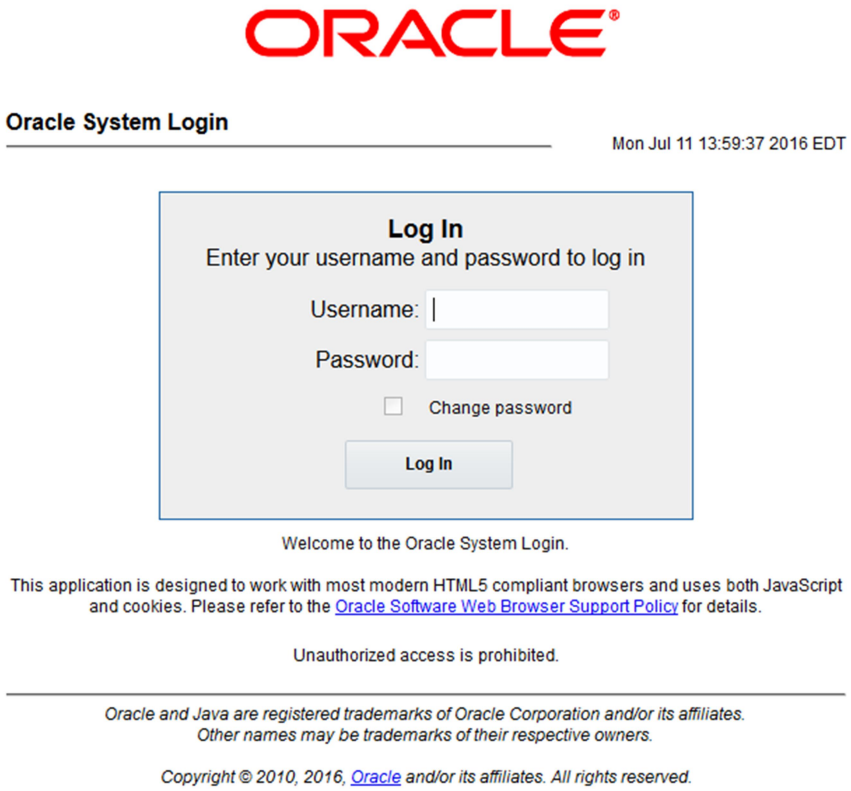
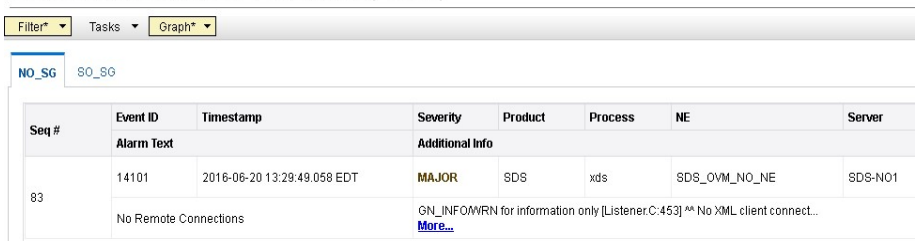
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
7 ☐	**SDS VIP**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server by using the XMI IP address. 
8 ☐	**SDS VIP**: Verify and restart the servers	Navigate to **Main Menu->Status & Manage->Server**.  Verify the DB status is **Norm** and the Proc status is **Man**.  Select the SDS NOAM-A server and click **Restart**.

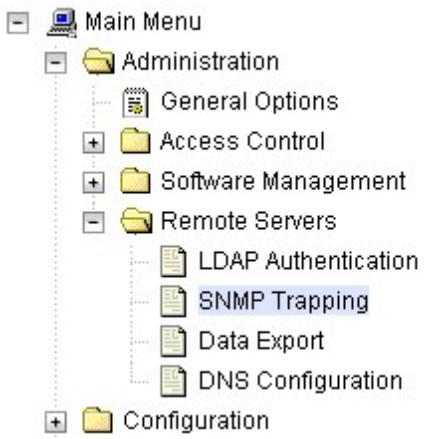
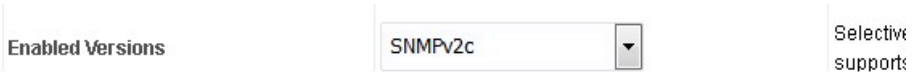
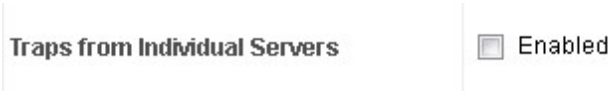
Procedure 5. Configure the SDS Server Group

Step	Procedure	Result
		Click **OK** on the confirmation screen. A confirmation banner displays  Verify the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.  ***Note***: To refresh the server status screen before the 15-30 second default, navigate to the **Main Menu->Status & Manage->Server** screen again.
9 ☐	**SDS NOAM-B**: Repeat	Configure SDS NOAM-B by repeating step 8 of this procedure. This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).

Procedure 6. Verify SDS Server Alarm Status

Step	Procedure	Result
1 ☐	**SDS VIP**: 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 ☐	**SDS VIP**: Wait for remote database alarm to clear	Navigate to **Main Menu->Alarms & Events->View Active**. Verify Event ID **14101** (No Remote Connections) is the only alarm present on the system at this time. 

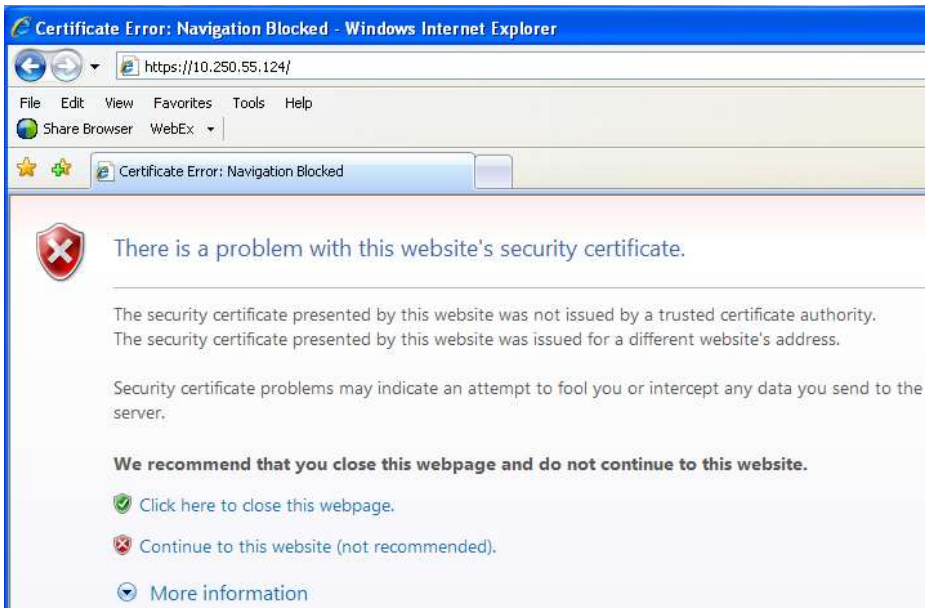
Procedure 7. Configure SNMP for Traps from Individual Servers

Step	Procedure	Result
1 ☐	**SDS VIP**: 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.
2 ☐	**SDS VIP**: Navigate to SNMP Trapping screen	Navigate to **Main Menu->Administration->Remote Servers->SNMP Trapping**.  Click **Insert**. Change the Enabled Versions to **SNMPv2c**.  Mark the Traps from Individual Servers checkbox as **Enabled**.  Click **OK**.

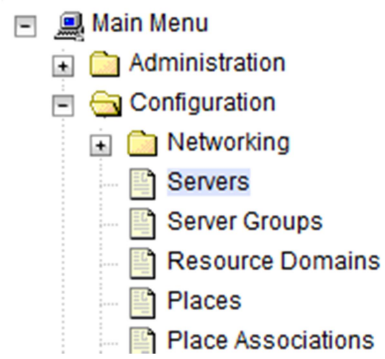
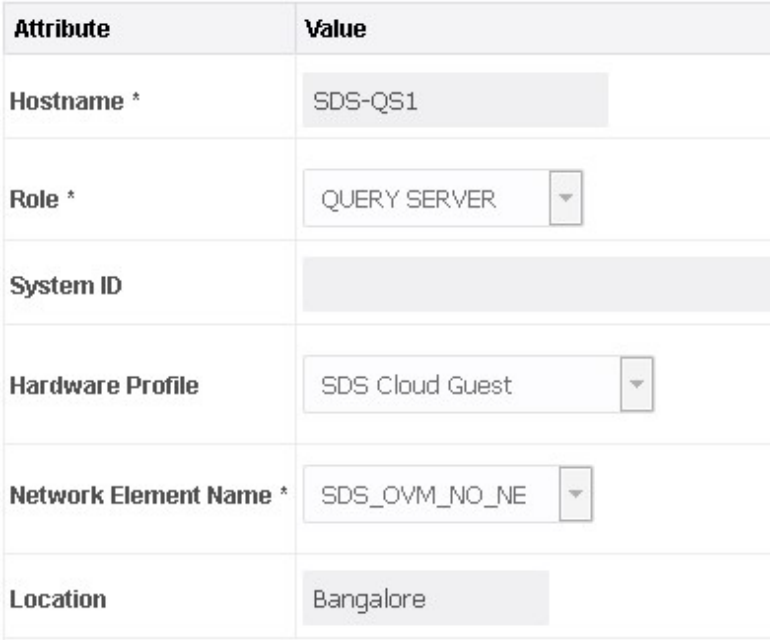
3.4 Query Server Installation (All SDS NOAM Sites)

During the Query Server installation procedure, various errors may display at different stages of the procedure. During the execution of a step, ignore errors related to values other than the ones referenced by that step

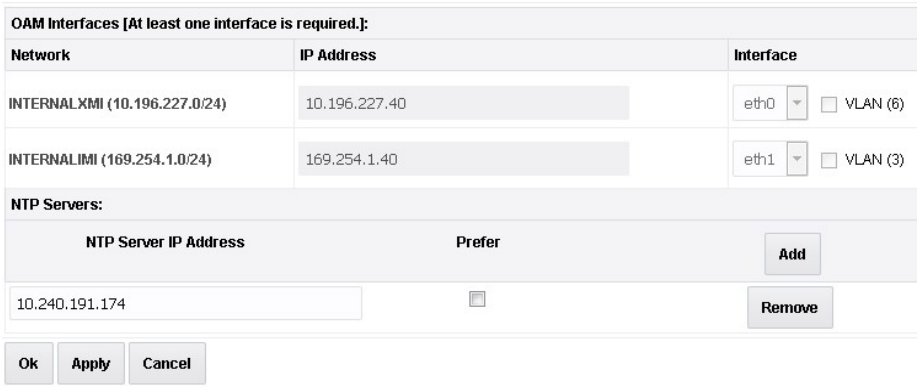
Procedure 8. Configure Query Server (All SDS NOAM Sites)

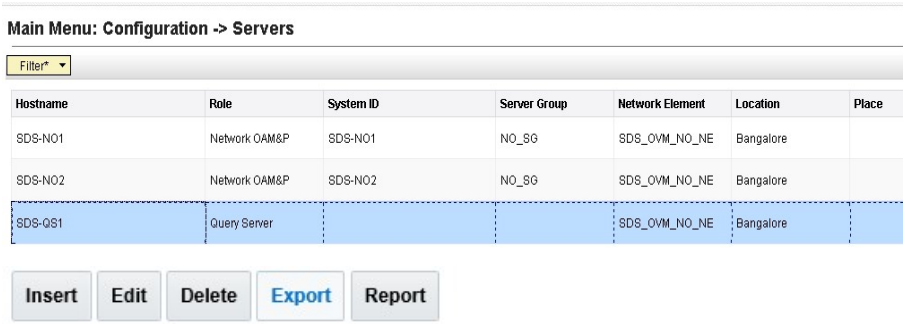
Step	Procedure	Result
1 ☐	**Active SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**Active SDS VIP**: Login	Establish a GUI session as the **default** user. 

Procedure 8. Configure Query Server (All SDS NOAM Sites)

Step	Procedure	Result
3 ☐	**Active SDS VIP**: Configure Query server	Navigate to **Main Menu->Configuration->Servers**.  Click **Insert** to insert the new NOAM server into servers table (the first or server). Fill in the fields as follows: Hostname: Assigned Hostname Role: `Query Server` System ID: Leave Blank Hardware Profile: `SDS Cloud Guest` Network Element Name: [Select **NE** from list where Query server is physically located] Location: Optional 

Procedure 8. Configure Query Server (All SDS NOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>4
☐</td><td>Active SDS VIP: Insert the Query server</td><td>The network interface fields are now available with selection choices based on the chosen hardware profile and network element.
 

Type the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
Type the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
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 (Optional)</td><td>No</td></tr><tr><td>Valid NTP Server (Optional)</td><td>No</td></tr></table>
Click OK when you have completed entering all the server data.</td></tr>
<tr><td>5
☐</td><td>Active SDS VIP: Export the initial configuration</td><td>From the GUI screen, select the SDS 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.
 
</td></tr>
</table>

Procedure 8. Configure Query Server (All SDS NOAM Sites)

Step	Procedure	Result

6 ☐	**Active SDS VIP**: Copy server configuration file to /var/tmp directory	Obtain a terminal window to the Active SDS VIP server, logging in as the **admusr** user.
		
		Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the Active SDS VIP to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		
		`$ cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh`
		
		Note: The server polls the /var/tmp directory for the configuration file and automatically executes it.
		
		For the NOAM-B server, the command is:
		
		`$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh \`
		`<ipaddr>:/var/tmp/TKLCConfigData.sh`
		
		Note: The IPADDR is the IP address of the Query server associated with the XMI network.

7 ☐	**Active SDS VIP**: 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. A broadcast message is sent to the terminal. This can take anywhere from 3-20 minutes to complete. 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. `$ 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.

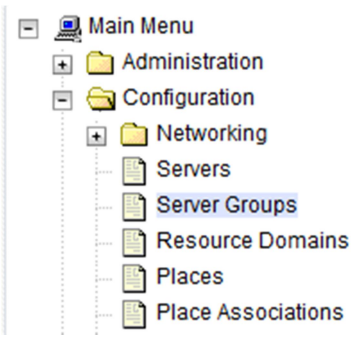
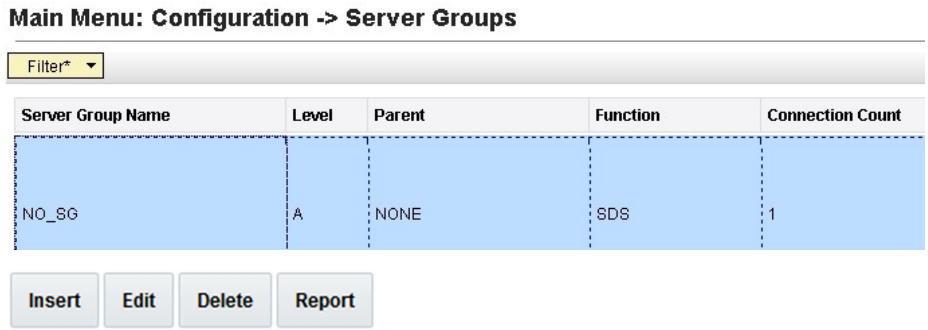
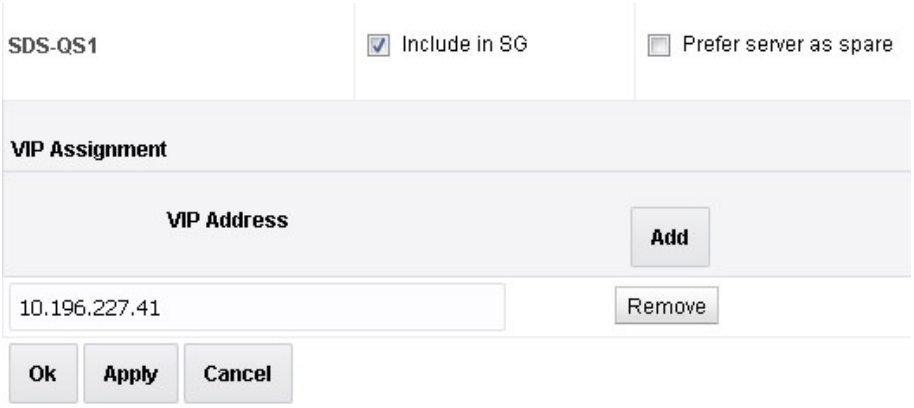
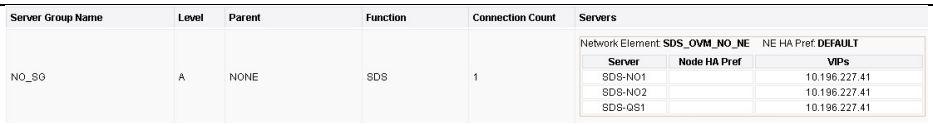
Procedure 8. Configure Query Server (All SDS NOAM Sites)

Step	Procedure	Result

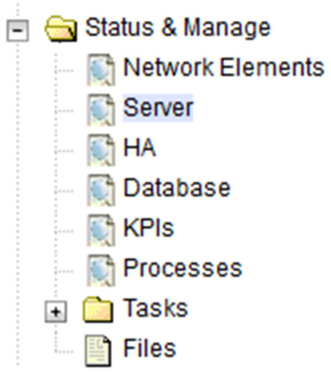
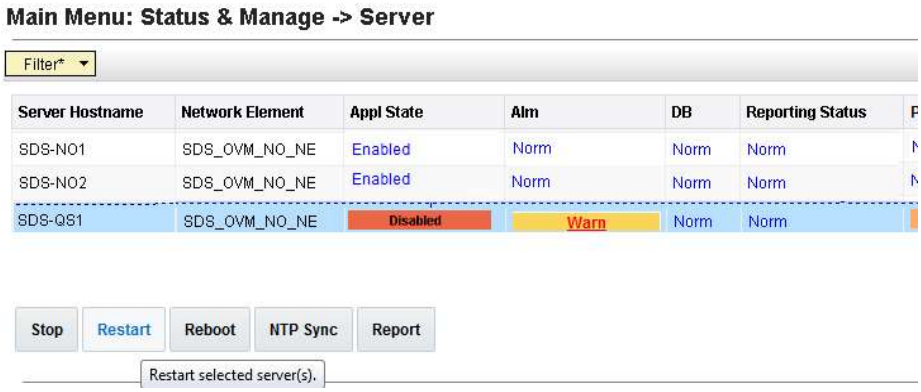
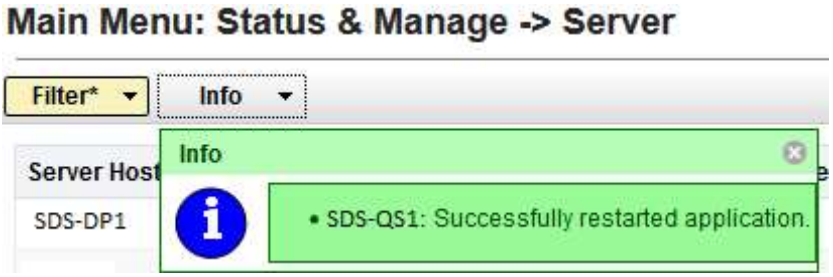
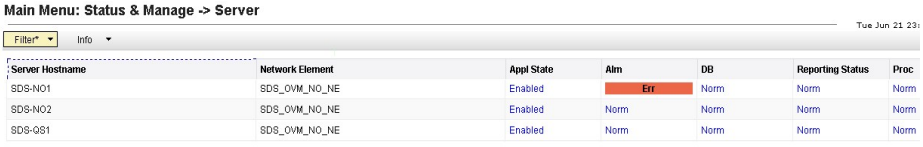
8 ☐	**Active SDS VIP**: Set the time zone (Optional) and reboot the server	To change the system time zone, from the command line prompt, execute **set_ini_tz.pl**. The following command example uses the America/New_York time zone.
		Replace, as appropriate, with the time zone you have selected for this 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.

9 ☐	**Active SDS VIP**: Verify server health	Login into the Query server as the **admusr** user.
		Execute the following command on the Query 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 9. Add Query Server to the SDS Server Group

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Add server to OAM Server Group	Navigate to **Main Menu->Configuration->Server Groups**.  Select the new server group and click **Edit**.  In the portion of the screen that lists the servers for the server group, find the Query server being configured. Mark the **Include in SG** checkbox.  Leave other boxes unchecked. Click **OK**.
2 ☐	**Active SDS VIP**: Wait for process to complete	 This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server establishes DB replication with the active SDS server.

Procedure 9. Add Query Server to the SDS Server Group

Step	Procedure	Result
3 ☐	**Active SDS VIP**: Verify and restart the servers	Navigate to **Main Menu->Status & Manage->Server**.  Verify the DB status is **Norm** and the Proc status is **Man**.  Select the Query server and click **Restart**. Click **OK** on the confirmation screen. A confirmation banner displays  Verify the Appl state is **Enabled** and the Alm, DB, Reporting Status, and Proc is **Norm**.  ***Note***: To refresh the server status screen before the 15-30 second default, navigate to the **Main Menu->Status & Manage->Server** screen again.

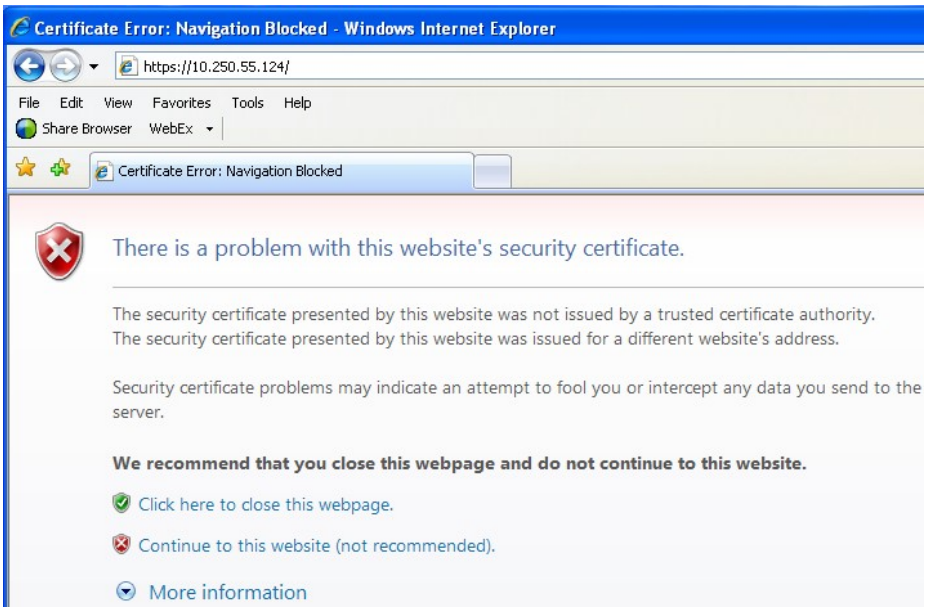
3.5 OAM Installation for DR SDS NOAM Site (Optional)

Assumptions:

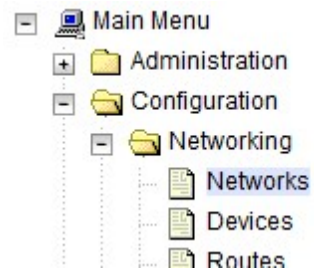
- This procedure assumes the SDS Network Element XML file for Disaster Recovery Provisioning SDS site has previously been created as described in the Appendix A Create an XML File for Installing SDS Network Elements.
- This procedure assumes that the Network Element XML files are on the laptop's hard drive.

This procedure requires a connection to the SDS GUI before configuring the first SDS server.

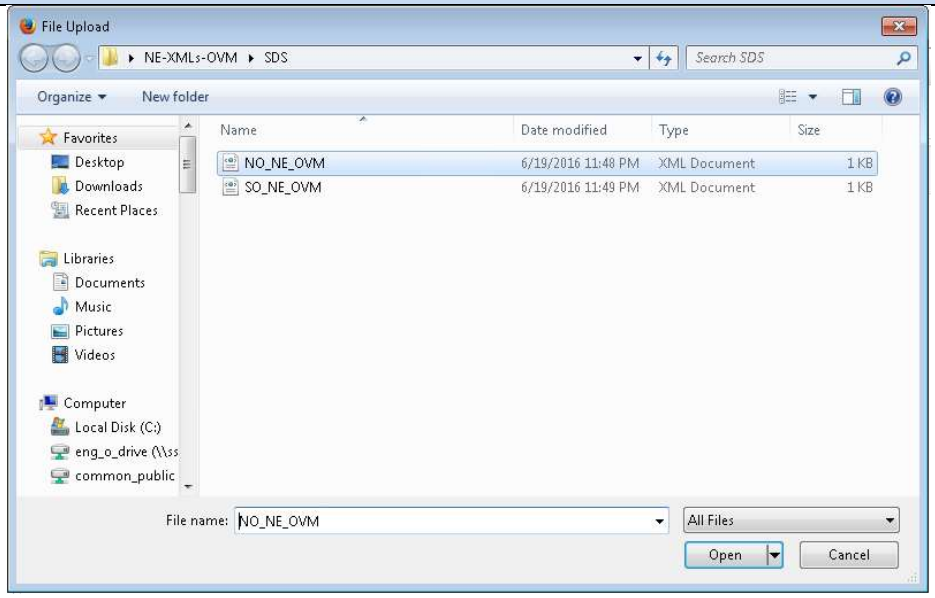
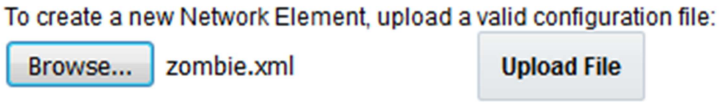
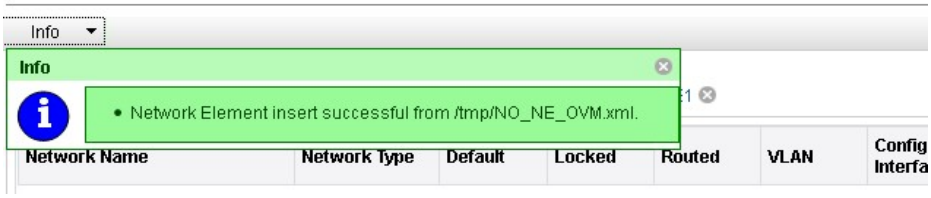
Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
1 ☐	**DR SDS NOAM-A**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 

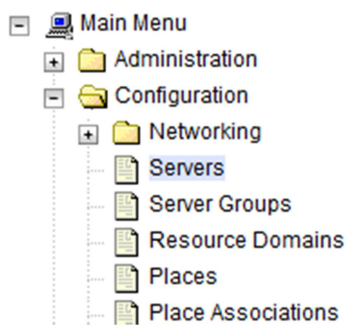
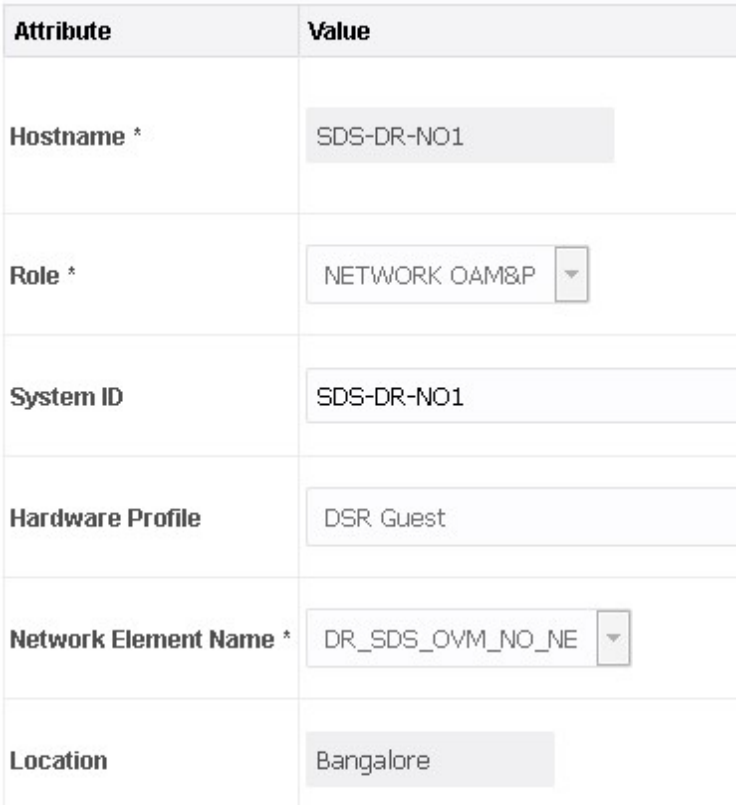
Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
2 ☐	**DR SDS NOAM-A**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server. 
3 ☐	**DR SDS NOAM-A**: Create the SDS VIP network element using the XML file	Navigate to **Main Menu->Configuration->Networking->Networks**.  Click **Browse** and type the pathname of the NOAM network XML file.  ***Note***: This step assumes the **XML** files were previously prepared as described in Appendix A Create an XML File for Installing SDS Network Elements. Select the location of the **XML** file and click **Open**.

Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
		 Click **Upload File** to upload the XML file.  If the values in the **XML** file pass, an information banner displays. **Main Menu: Configuration -> Networking -> Networks**  ***Note***: You may need to left-click on the Info banner to display the banner.

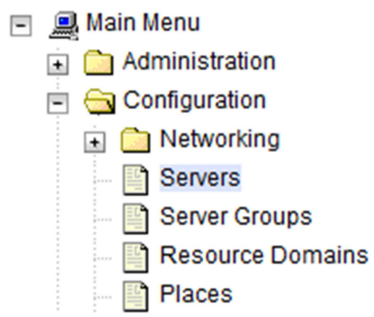
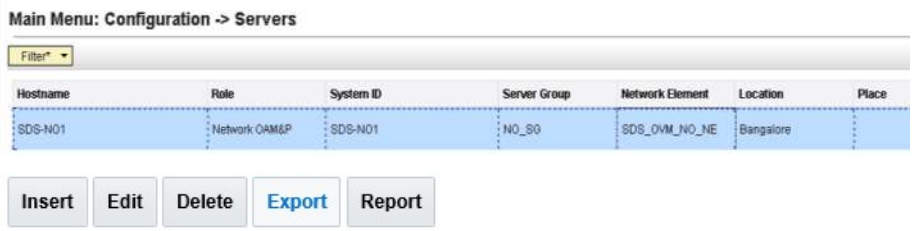
Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
4 ☐	**DR SDS NOAM-A**: Insert the DR NOAM-A and DR NOAM-B servers	Navigate to **Main Menu->Configuration->Servers**.  Click **Insert** to insert the new NOAM server into servers table (the first or server). Fill in the fields as follows: Hostname: Assigned Hostname Role: NETWORK OAM&P System ID: Assigned Hostname Hardware Profile: SDS Cloud Guest Network Element Name: [Select **NE** from list] Location: Optional 

Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
5 ☐	**DR SDS NOAM-A**: Insert the 1st VM	The network interface fields are now available with selection choices based on the chosen hardware profile and network element.  Type the server IP addresses for the XMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unchecked. Type the server IP addresses for the IMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unchecked. ***Note***: For OpenStack, these IP addresses must be the addresses used during instance booting and networking. Click **Add** in the NTP servers box. Add the following NTP servers: **NTP Server** / **Preferred?** Valid NTP Server / Yes Valid NTP Server (Optional) / No Valid NTP Server (Optional) / No Click **OK** when you have completed entering all the server data.

Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
6 ☐	**DR SDS NOAM-A**: Export the initial configuration	Navigate to **Main Menu->Configuration->Servers**.  From the GUI screen, select the SDS 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. 

7 ☐	**DR SDS NOAM-A**: Copy server configuration file to /var/tmp directory	Obtain a terminal window to the SDS NOAM-A server, logging in as the **admusr** user.
		Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the SDS NOAM-A to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		`$ cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the configuration file and automatically executes it.
		For the NOAM-B server, the command is:
		`$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh \`
		`<ipaddr>:/var/tmp/TKLCConfigData.sh`
		Note: The IPADDR is the IP address of NOAM-B associated with the XMI network.

Procedure 10. Configure DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
8 ☐	**DR SDS NOAM-A**: 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. A broadcast message is sent to the terminal. This can take anywhere from 3-20 minutes to complete. 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.

9 ☐	**DR SDS NOAM-A**: Verify server health	Login into the NOAM1 as the **admusr** user.
		Execute the following command 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`

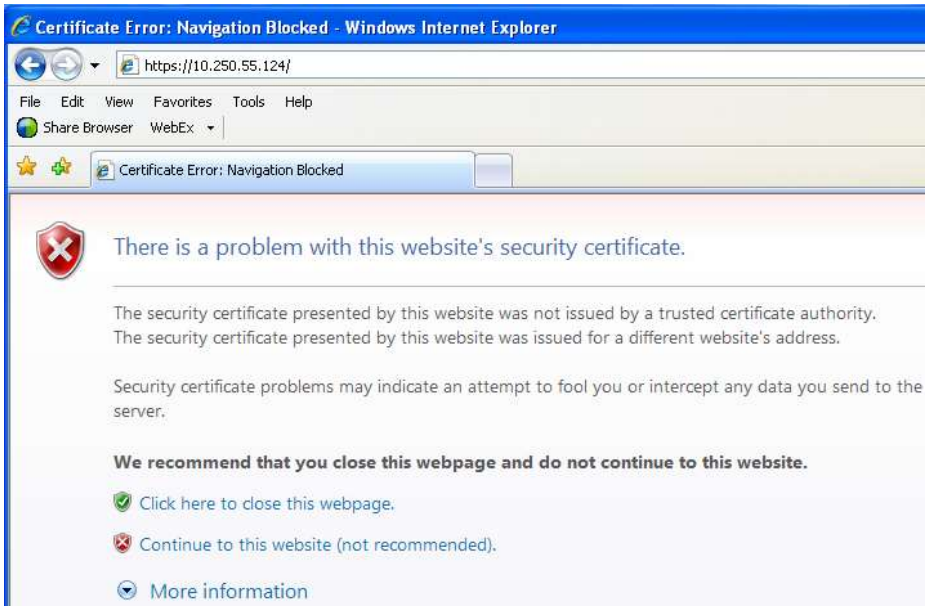
10 ☐	**DR SDS NOAM-A**: Verify server health	Exit from the command line to return to the server console.
		`$ exit`
		`sds-mrsvnc-a login:`

11 ☐	**DR SDS NOAM-B**: Repeat	Configure SDS NOAM-B by repeating steps 5 through 10 of this procedure.

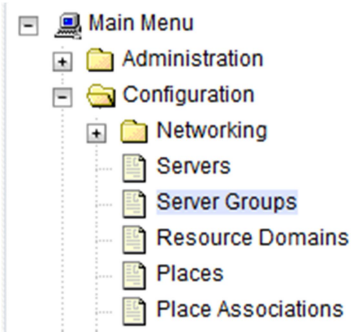
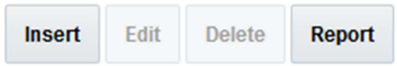
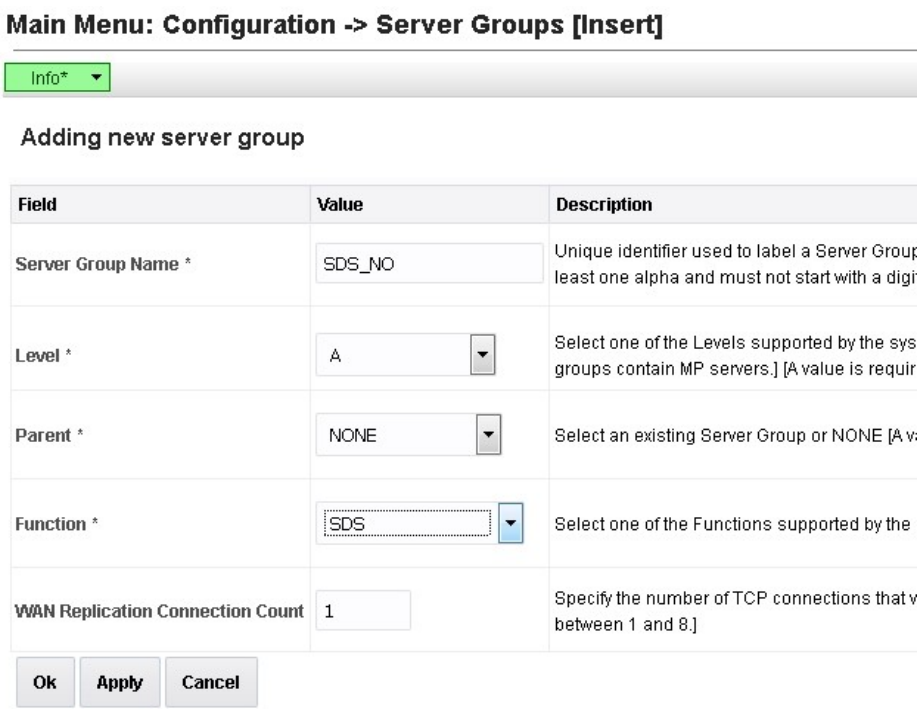
3.6 OAM Pairing for DR SDS NOAM Site (Optional)

During the OAM pairing procedure, various errors may display at different stages of the procedure. During the execution of a step, ignore errors related to values other than the ones referenced by that step

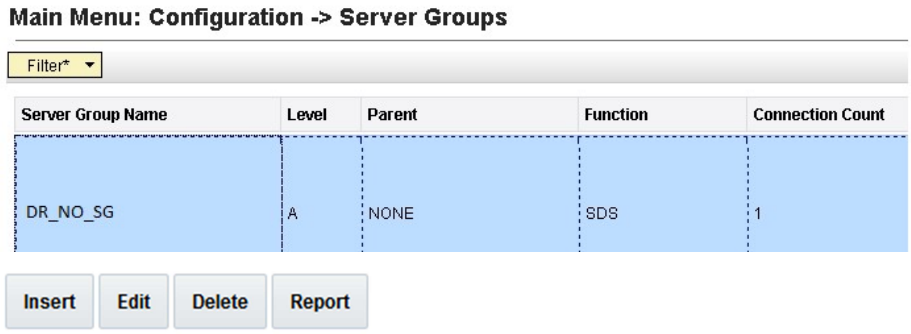
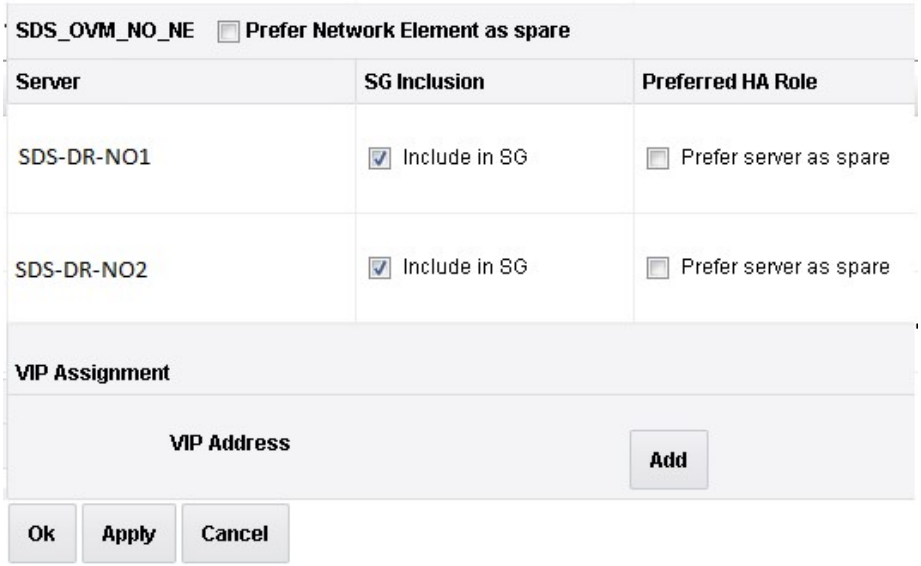
Procedure 11. Pair the DR OAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
1 ☐	**Primary SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Primary SDS NOAM-A site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**Primary SDS VIP**: Login	Establish a GUI session as the **default** user. 

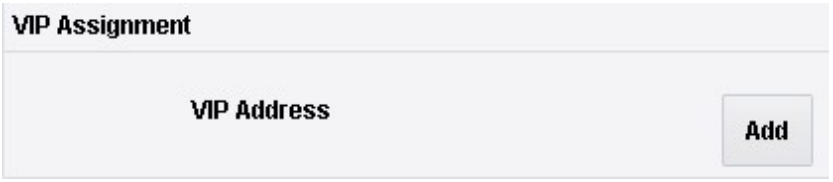
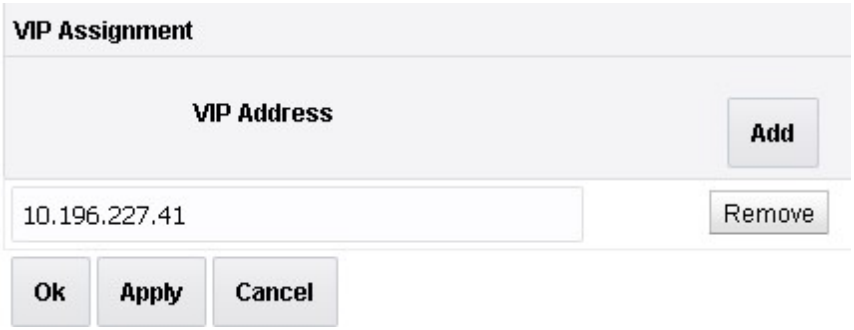
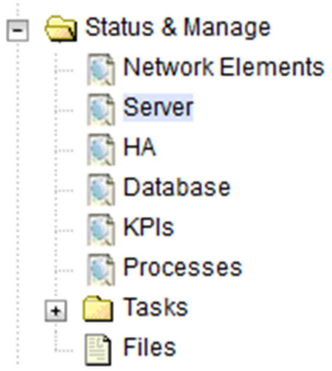
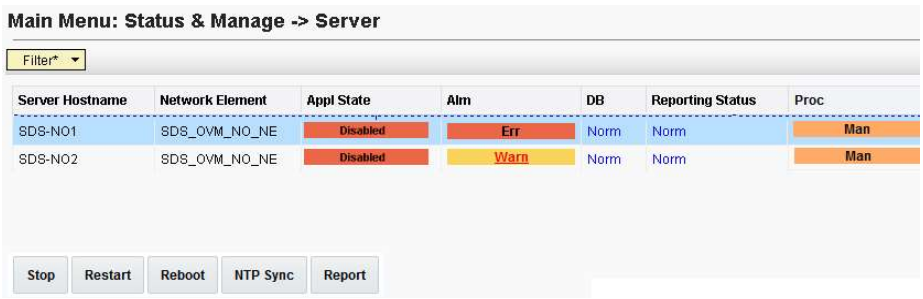
Procedure 11. Pair the DR OAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
3 ☐	**DR SDS NOAM-A**: Enter group data	Navigate to **Main Menu->Configuration->Server Groups**.  Click **Insert**.  Fill in the following fields: Server Group Name: [Type DR Server Group Name] Level: A Parent: None Function: SDS WAN Replication Connection Count: Use Default Value  Click **OK** when all fields are filled in.

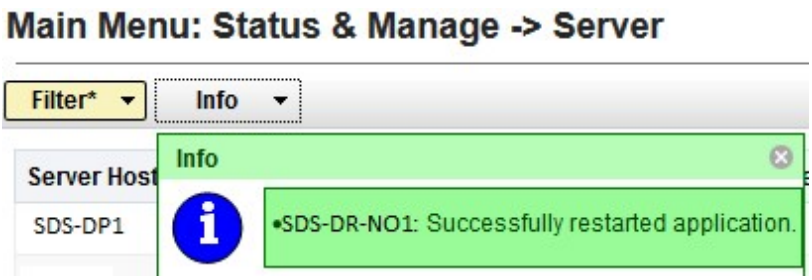
Procedure 11. Pair the DR OAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
4 ☐	**DR SDS NOAM-A**: Add server to OAM Server Group	Select the new server group and click **Edit**.  In the portion of the screen that lists the servers for the server group, find the SDS-NOAM servers being configured. Mark the **Include in SG** checkbox.  Leave other boxes unchecked. Click **Apply**.

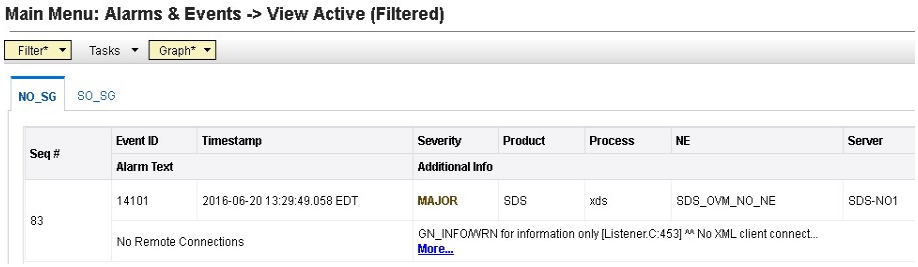
Procedure 11. Pair the DR OAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
5 ☐	**DR SDS NOAM-A**: Add VIP address	Click **Add**.  Type the **VIP Address** and click **Apply**.  This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).
6 ☐	**DR SDS VIP**: Verify and restart the servers	Navigate to **Main Menu->Status & Manage->Server**.  Verify the DB status is **Norm** and the Proc status is **Man**.  Select the SDS NOAM-A server and click **Restart**. Click **OK** on the confirmation screen.

Procedure 11. Pair the DR OAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
		A confirmation banner displays  Verify the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.  ***Note***: To refresh the server status screen before the 15-30 second default, navigate to the **Main Menu->Status & Manage->Server** screen again.
7 ☐	**DR SDS NOAM-B**: Repeat	Configure SDS NOAM-B by repeating step 6 of this procedure. This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).

Procedure 12. Verify SDS Server Alarm Status

Step	Procedure	Result
1 ☐	**SDS VIP**: 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 ☐	**SDS VIP**: Wait for remote database alarm to clear	Navigate to **Main Menu->Alarms & Events->View Active**. Verify Event ID **14101** (No Remote Connections) is the only alarm present on the system at this time. 
3 ☐	**SDS VIP**: Add Query server for the DR SDS server	Repeat all steps in Section 3.4 except use the DR SDS NOAM NE and server group instead of the primary SDS NOAM NE and server group.

3.7 OAM Installation for DP-SOAM Sites (All DP-SOAM Sites)

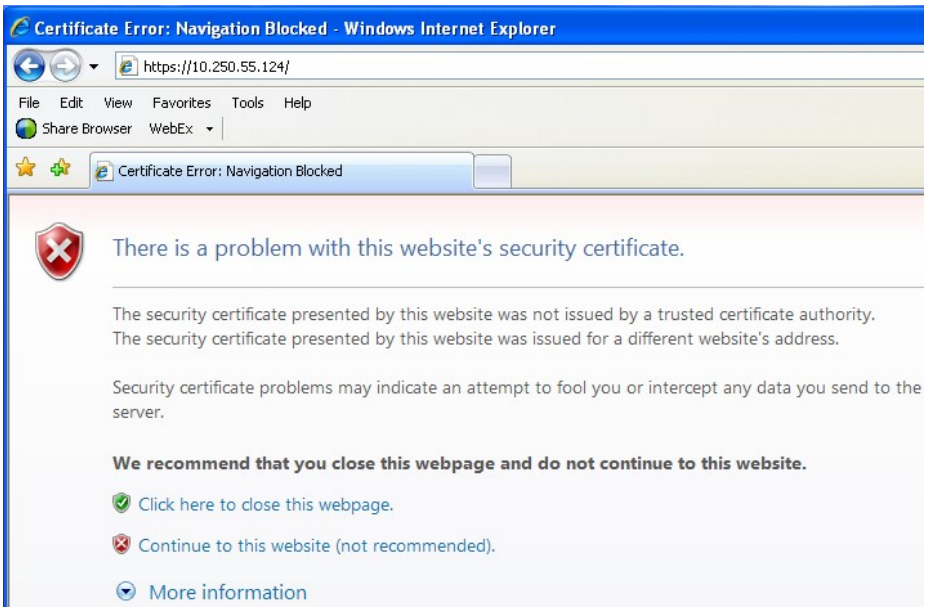
Assumptions:

- This procedure assumes the DP-SOAM Network Element XML file for the DP-SOMA site has previously been created as described in the Appendix A Create an XML File for Installing SDS Network Elements.
- This procedure assumes that the Network Element XML files are on the laptop's hard drive.

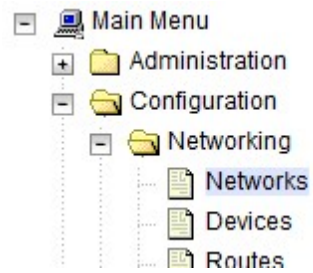
This procedure is for installing the DP-SOAM software on the OAM server located at each DSR Signaling Site. The DP-SOAM and DSR OAM servers run on two virtual machines.

This procedure assumes the DSR x.x.x OAM has already been installed in a virtual environment as described in [2] Diameter Signaling Router Cloud Installation Guide, E76331, cgbu_019911, Latest Revision.

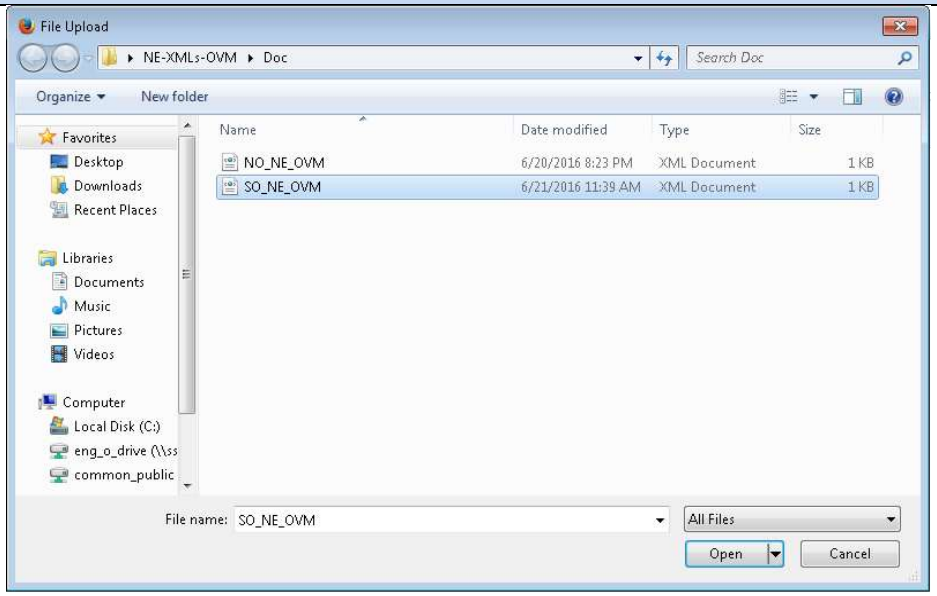
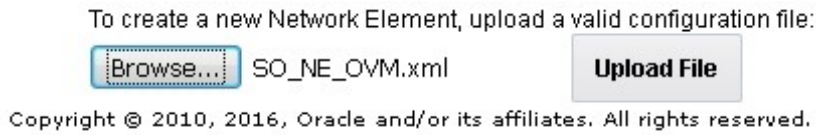
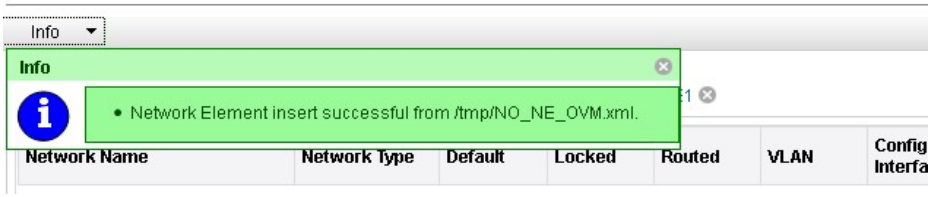
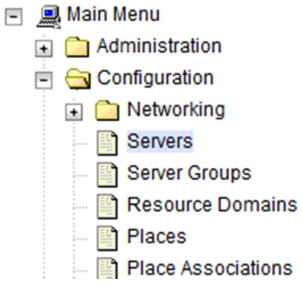
Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 

Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
2 ☐	**Active SDS VIP**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server. 
3 ☐	**Active SDS VIP**: Configure the DP SOAM network element	Navigate to **Main Menu->Configuration->Networking->Networks**.  Click **Browse** and type the pathname of the NOAM network XML file.  ***Note***: This step assumes the **XML** files were previously prepared as described in Appendix A Create an XML File for Installing SDS Network Elements. Select the location of the **XML** file and click **Open**.

Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
		 Click **Upload File** to upload the XML file.  If the values in the **XML** file pass, an information banner displays. **Main Menu: Configuration -> Networking -> Networks**  ***Note***: You may need to left-click on the Info banner to display the banner.
4 ☐	**Active SDS VIP**: Configure the SOAM server	Navigate to **Main Menu->Configuration->Servers**.  Click **Insert** to insert the new SOAM server into servers table.

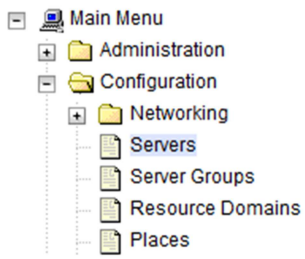
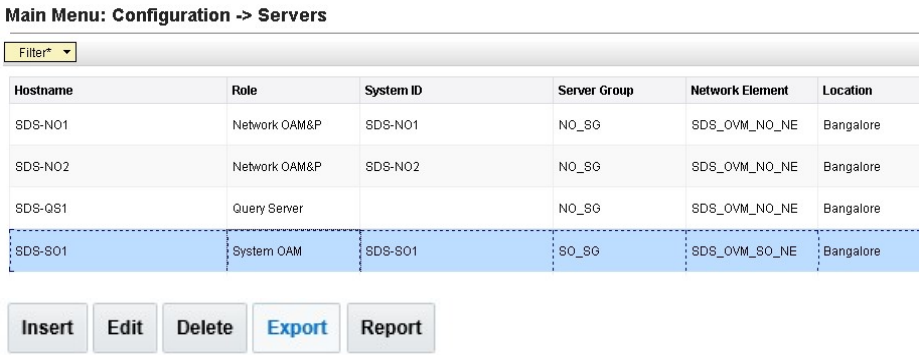
Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
		Main Menu: Configuration -> Servers Filter* Hostname / Role / System ID / Server Group / Network Element SDS-NO1 / Network OAM&P / SDS-NO1 / NO_SG / SDS_OVM_NO_NE SDS-NO2 / Network OAM&P / SDS-NO2 / NO_SG / SDS_OVM_NO_NE SDS-QS1 / Query Server / / NO_SG / SDS_OVM_NO_NE Insert Edit Delete Export Report Fill in the fields as follows: Hostname: Assigned Hostname Role: `SYSTEM OAM` System ID: Assigned Hostname Hardware Profile: `SDS Cloud Guest` Network Element Name: [Select **NE** from list] Location: Optional **Main Menu: Configuration -> Servers [Insert]** Adding a new server Attribute / Value Hostname * SDS-SO1 Role * SYSTEM OAM System ID SDS-SO1 Hardware Profile SDS Cloud Guest Network Element Name * SDS_OVM_SO_NE Location Bangalore

Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
5 ☐	**Active SDS VIP**: Insert the network element	The network interface fields are now available with selection choices based on the chosen hardware profile and network element.  Type the server IP addresses for the XMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unchecked. Type the server IP addresses for the IMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unchecked. Add the following NTP servers: **NTP Server** / **Preferred?** Valid NTP Server — Yes Valid NTP Server (Optional) — No Valid NTP Server (Optional) — No Click **OK** when you have completed entering all the server data.

Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
6 ☐	**Active SDS VIP**: Export the initial configuration	Navigate to **Main Menu->Configuration->Servers**.  From the GUI screen, select the SDS 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. 

7 ☐	**Active SDS VIP**: Copy server configuration file to /var/tmp directory	Obtain a terminal window to the SDS NOAM-A server, logging in as the **admusr** user.
		Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the SDS NOAM-A to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		`$ cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the configuration file and automatically executes it.
		For the NOAM-B server, the command is:
		`$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh \`
		`<ipaddr>:/var/tmp/TKLCConfigData.sh`
		Note: The IPADDR is the IP address of SOAM associated with the XMI network.

Procedure 13. OAM Installation for DP-SOAM Servers

Step	Procedure	Result
8 ☐	**SDS 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. A broadcast message is sent to the terminal. This can take anywhere from 3-20 minutes to complete. 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. `$ 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.

9 ☐	**SDS 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.

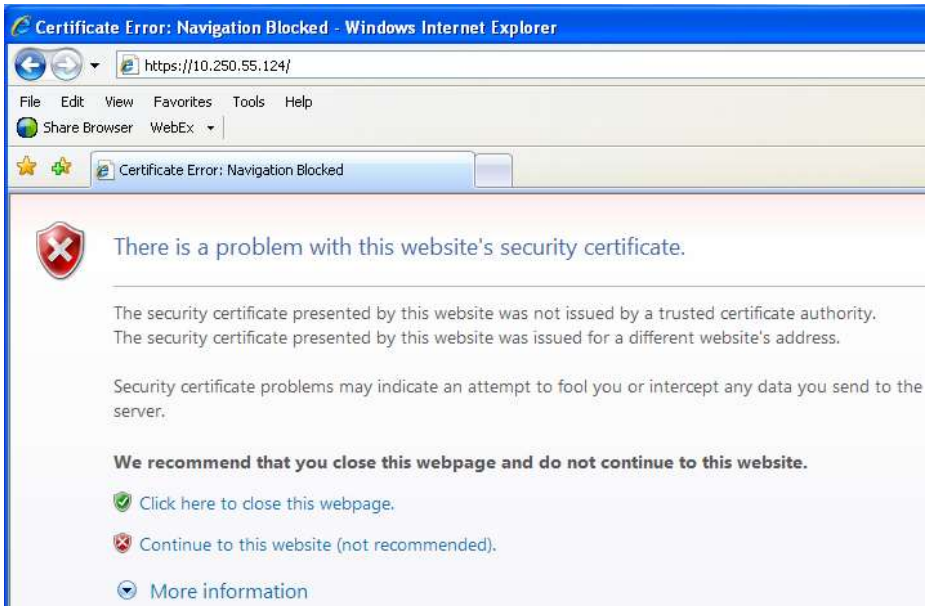
10 ☐	**SDS NOAM-A**: Verify server health	Login into the NOAM1 as the **admusr** user.
		Execute the following command on the 1st NOAM server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware... OK`
		`Running modules in class disk... OK`
		`Running modules in class net... OK`
		`Running modules in class system... OK`
		`Running modules in class proc... OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

11 ☐	**SDS NOAM-B**: Repeat	Configure DR SDS NOAM-B by repeating steps 4 through 10 of this procedure.

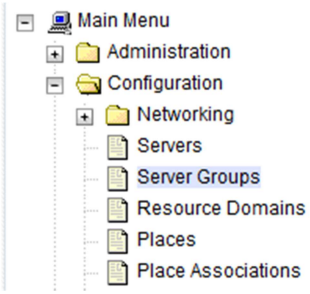
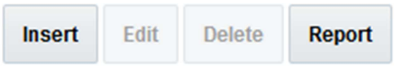
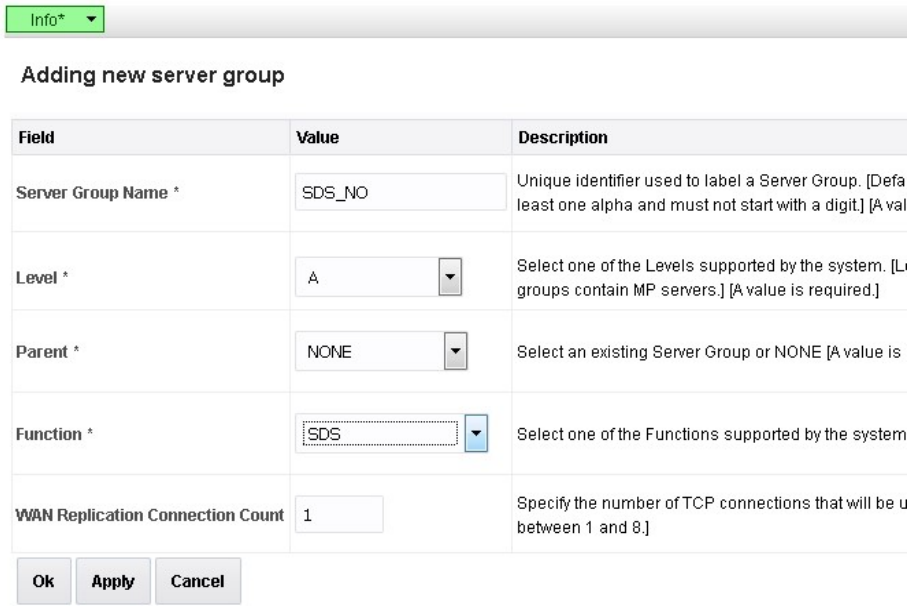
3.8 OAM Pairing for DP-SOAM Sites (All DP-SOAM Sites)

During the OAM pairing procedure, various errors may display at different stages of the procedure. During the execution of a step, ignore errors related to values other than the ones referenced by that step

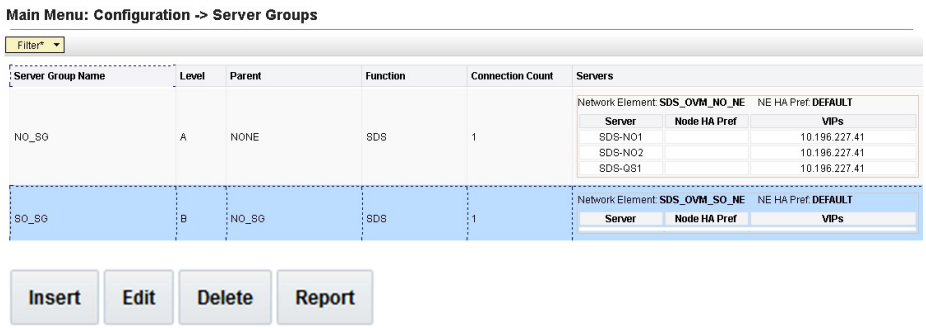
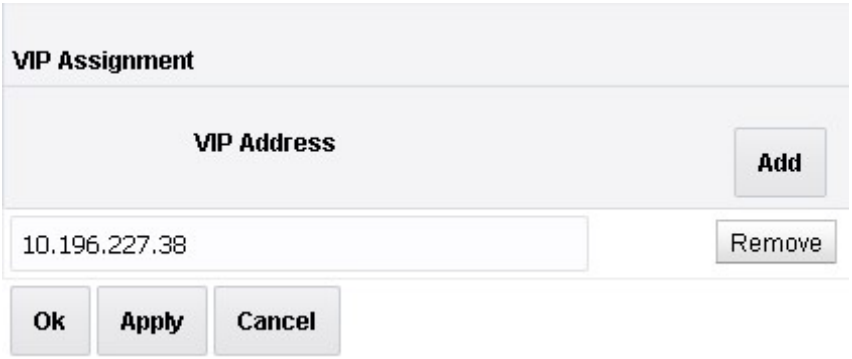
Procedure 14. Pair the OAM Servers for DP-SOAM Sites

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**Active SDS VIP**: Login	Establish a GUI session as the **default** user. 

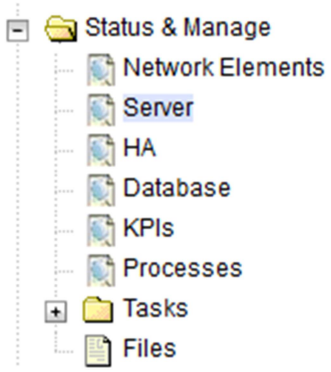
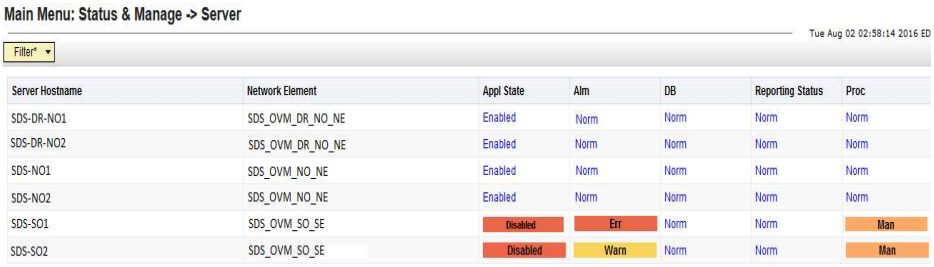
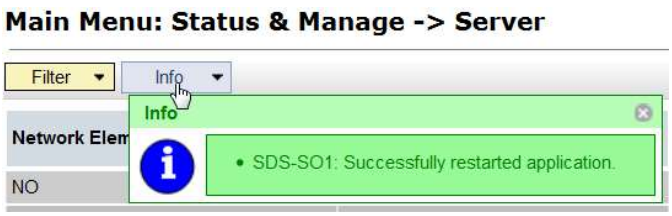
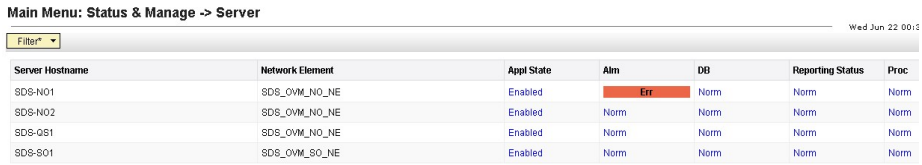
Procedure 14. Pair the OAM Servers for DP-SOAM Sites

Step	Procedure	Result
3 ☐	**Active SDS VIP**: Enter group data	Navigate to **Main Menu->Configuration->Server Groups**.  Click **Insert**.  Fill in the following fields: Server Group Name: [Type Server Group Name] Level: B Parent: [Select SDS Server Group Name from Procedure 3. Step 5] Function: SDS WAN Replication Connection Count: Use Default Value **Main Menu: Configuration -> Server Groups [Insert]**  Click **OK** when all fields are filled in.

Procedure 14. Pair the OAM Servers for DP-SOAM Sites

Step	Procedure	Result
4 ☐	**SDS SOAM-A**: Add server to OAM Server Group	Select the new server group and click **Edit**.  In the portion of the screen that lists the servers for the server group, find the SDS-NOAM servers being configured. Mark the **Include in SG** checkbox.  Leave other boxes unchecked. Click **Apply**.
5 ☐	**SDS SOAM-A**: Add VIP address	Click **Add**. Type the **VIP Address** and click **OK**.  This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).

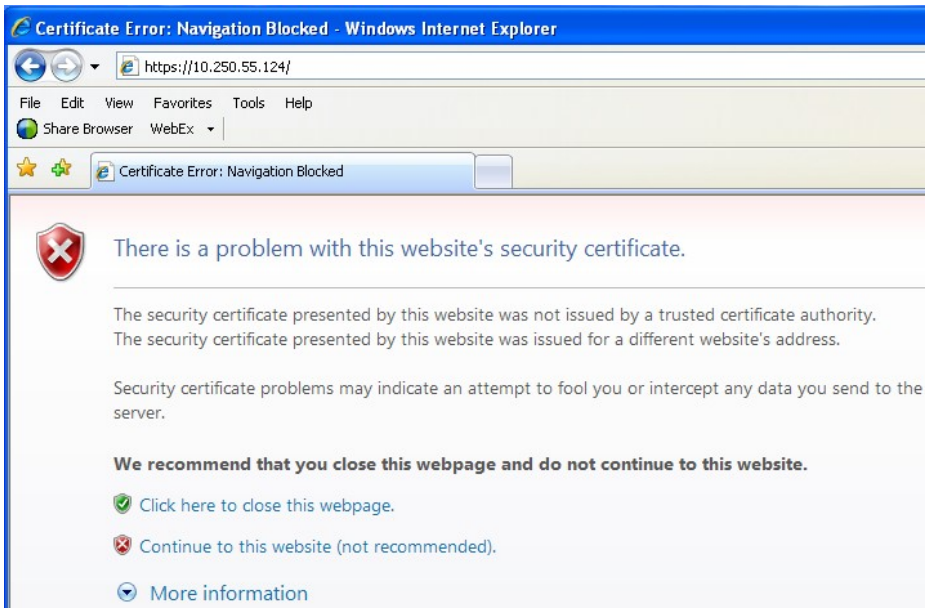
Procedure 14. Pair the OAM Servers for DP-SOAM Sites

Step	Procedure	Result
6 ☐	**Active SDS VIP**: Verify and restart the servers	Navigate to **Main Menu->Status & Manage->Server**.  Verify the DB status is **Norm** and the Proc status is **Man**.  Select the DP SOAM-A server and click **Restart**. Click **OK** on the confirmation screen. A confirmation banner displays  Verify the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.  ***Note***: To refresh the server status screen before the 15-30 second default, navigate to the **Main Menu->Status & Manage->Server** screen again.
7 ☐	**SDS SOAM-B**: Repeat	Configure SDS SOAM-B by repeating step 7 of this procedure. This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/slave relationship for High Availability (HA).

3.9 DP Installation (All DP-SOAM Sites)

During the Data Processor (DP) installation procedure, various errors may display at different stages of the procedure. During the execution of a step, ignore errors related to values other than the ones referenced by that step

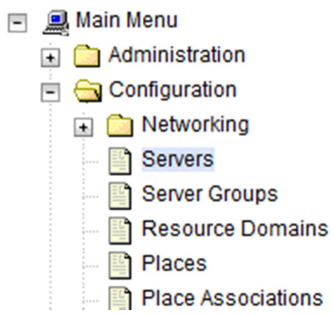
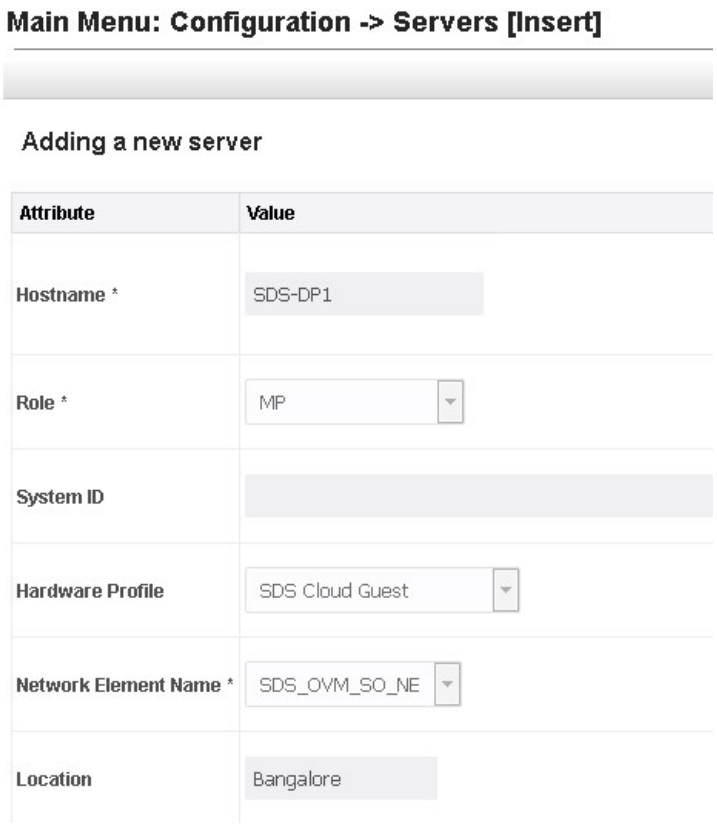
Procedure 15. Configure the Database Processor (DP) Server

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 

Procedure 15. Configure the Database Processor (DP) Server

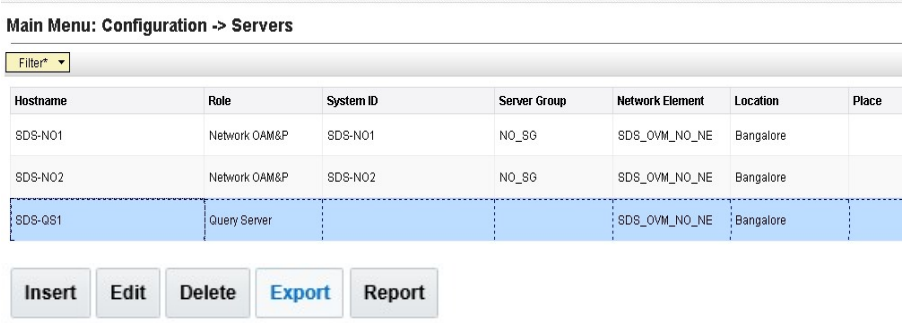
Step	Procedure	Result
2 ☐	**Active SDS VIP**: Login	Establish a GUI session as the **guiadmin** user on the NOAM-A server. 

Procedure 15. Configure the Database Processor (DP) Server

Step	Procedure	Result
3 ☐	**Active SDS VIP**: Configure DP server	Navigate to **Main Menu->Configuration->Servers**.  Click **Insert** to insert the new NOAM server into servers table (the first or server). Fill in the fields as follows: Hostname: Assigned Hostname Role: MP System ID: Leave Blank Hardware Profile: SDS Cloud Guest Network Element Name: [Select **NE** from list where Query server is physically located] Location: Optional 

Procedure 15. Configure the Database Processor (DP) Server

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>4
☐</td><td>Active SDS VIP: Insert the DP server</td><td>The network interface fields are now available with selection choices based on the chosen hardware profile and network element.
 

Type the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
Type the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.
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 (Optional)</td><td>No</td></tr><tr><td>Valid NTP Server (Optional)</td><td>No</td></tr></table>
Click OK when you have completed entering all the server data.</td></tr>
<tr><td>5
☐</td><td>Active SDS VIP: Export the initial configuration</td><td>From the GUI screen, select the SDS 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.
 
</td></tr>
<tr><td>6
☐</td><td>Active SDS VIP: Login and change directory</td><td>Obtain a terminal window to the Active SDS VIP server, logging in as the admusr user.
Change directory to filemgmt:
<pre>$ cd /var/TKLC/db/filemgmt</pre></td></tr>
</table>

Procedure 15. Configure the Database Processor (DP) Server

Step	Procedure	Result

7 ☐	**Active SDS VIP**: Copy server configuration file to /var/tmp directory	Copy the configuration file created in the previous step from the **/var/TKLC/db/filemgmt** directory on the Active SDS VIP to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example:
		`$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh \`
		`<ipaddr>:/var/tmp/TKLCConfigData.sh`
		Note: The IPADDR is the IP address of the DP server associated with the XMI network.

8 ☐	**DP 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. A broadcast message is sent to the terminal. This can take anywhere from 3-20 minutes to complete. 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. `$ 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.

9 ☐	**DP 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.

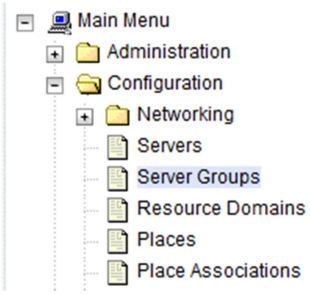
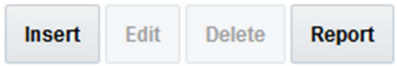
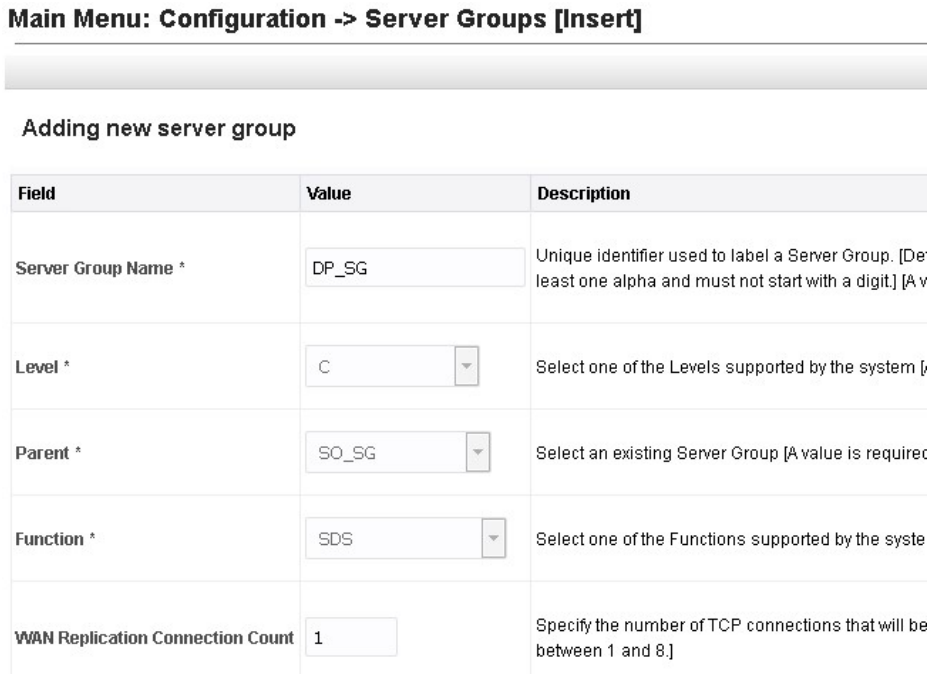
Procedure 15. Configure the Database Processor (DP) Server

Step	Procedure	Result

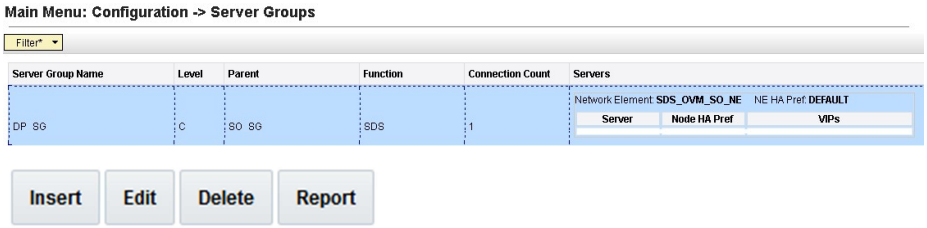
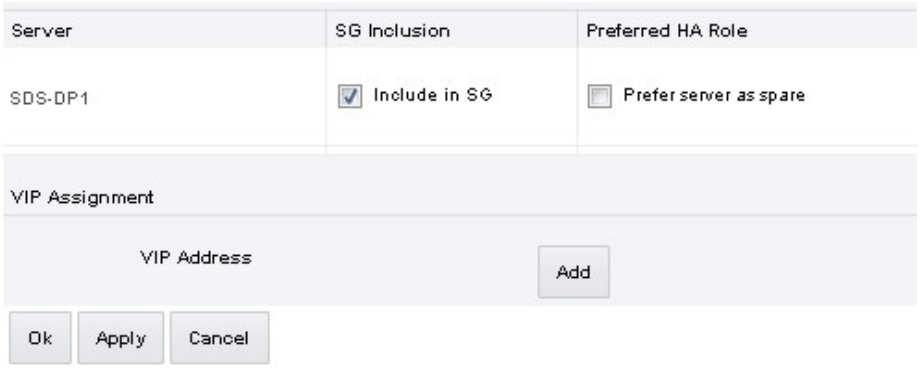
10 ☐	**DP Server**: Verify server health	Login into the DP server as the **admusr** user.
		Execute the following command on the Query server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running 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`

11 ☐	**Active SDS VIP**: Repeat	For additional DP servers, repeat steps 3 through 10 of this procedure.

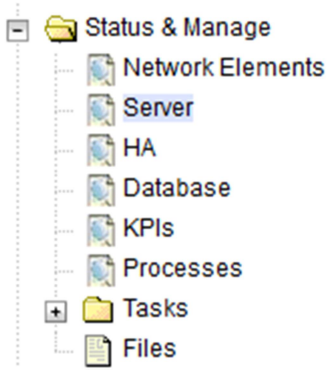
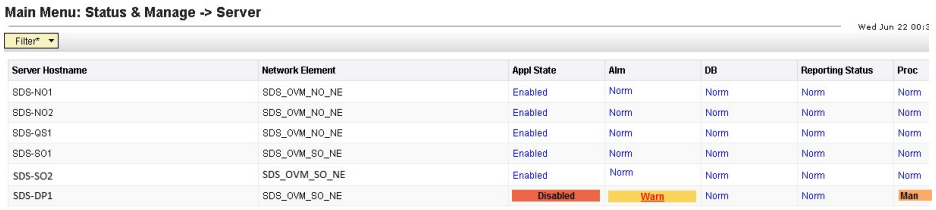
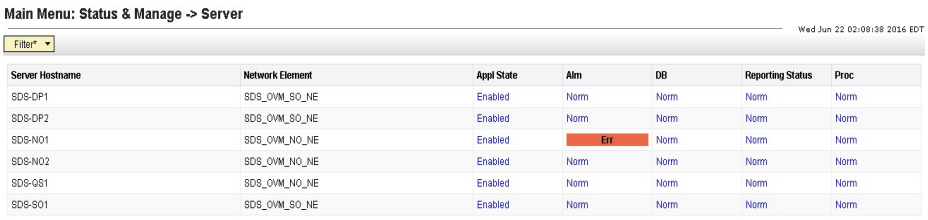
Procedure 16. Add DP Server to the SDS Server Group

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Add server to OAM Server Group	Navigate to **Main Menu->Configuration->Server Groups**.  Click **Insert**.  Fill in the following fields: Server Group Name: [Type Server Group Name] Level: C Parent: [Select System OAM Group Name] Function: SDS WAN Replication Connection Count: Use Default Value  Click **OK** when all fields are filled in.

Procedure 16. Add DP Server to the SDS Server Group

Step	Procedure	Result
2 ☐	**Active SDS VIP**: Add server to OAM Server Group	Select the new server group and click **Edit**.  In the portion of the screen that lists the servers for the server group, find the SDS-NOAM servers being configured. Mark the **Include in SG** checkbox.  Leave other boxes unchecked. Click **Apply**. A confirmation banner displays. 
3 ☐	**Active SDS VIP**: Repeat	For each subtending DP server, repeat steps 1 and 2 of this procedure. This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The servers establish DB replication with the active DP-SOAM server at the NE.

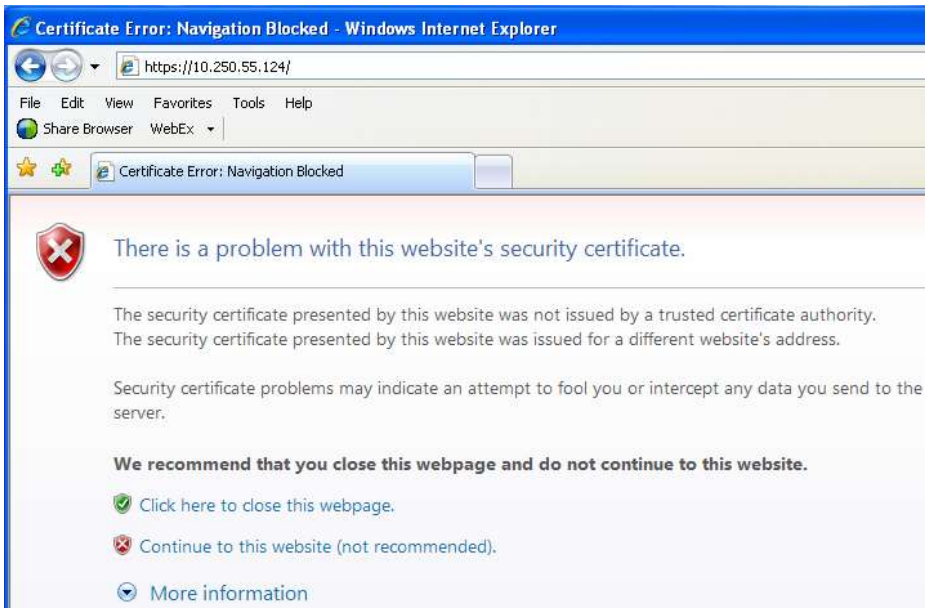
Procedure 16. Add DP Server to the SDS Server Group

Step	Procedure	Result
3 ☐	**SDS VIP**: Verify and restart the servers	Navigate to **Main Menu->Status & Manage->Server**.  Verify the DB and Reporting Status are **Norm** and the Proc status is **Man**.  Select the DP server and click **Restart**. Click **OK** on the confirmation screen.  A confirmation **Successfully restarted application** banner displays. Verify the Appl state is **Enabled** and the Alm, DB, Reporting Status, and Proc are **Norm**.  ***Note***: To refresh the server status screen before the 15-30 second default, navigate to the **Main Menu->Status & Manage->Server** screen again.
4 ☐	**Active SDS VIP**: Repeat	For each additional DP server, repeat step 3 of this procedure.

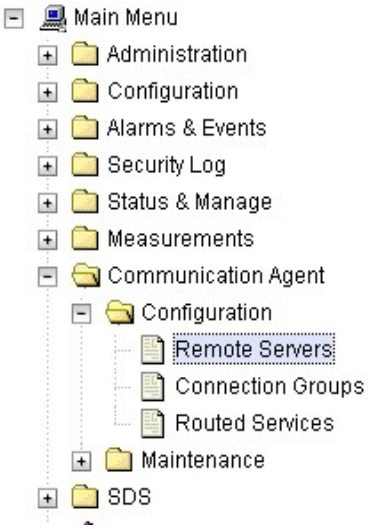
3.10 Configure ComAgent

This procedure configures ComAgent, which allows the SDS data processor servers and DSR message processor servers to communicate with each other. These steps cannot be executed until all SDS DP servers are configured.

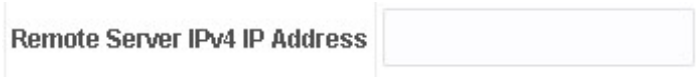
Procedure 17. Configure ComAgent (All DP-SOAM Sites)

Step	Procedure	Result
1 ☐	**Active SDS VIP**: Launch a web browser.	Connect to the XMI virtual IP address assigned to Active SDS site using **https://**. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended).** 
2 ☐	**Active SDS VIP**: Login	Establish a GUI session as the **default** user. 

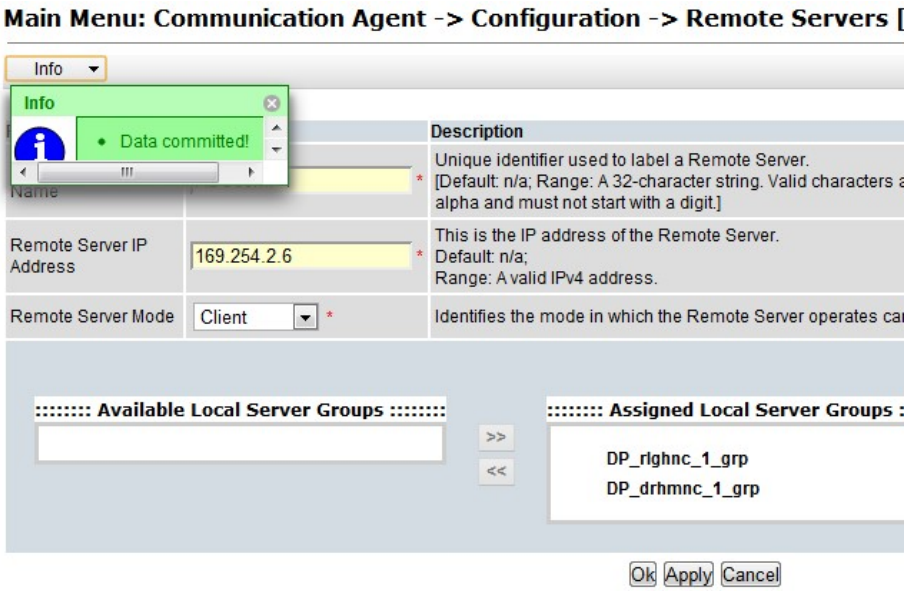
Procedure 17. Configure ComAgent (All DP-SOAM Sites)

Step	Procedure	Result
3 ☐	**Active SDS VIP**: Navigate to Remote Servers screen	Navigate to **Main Menu->Administration->Remote Servers**.  Click **Insert**.

Procedure 17. Configure ComAgent (All DP-SOAM Sites)

Step	Procedure	Result
4 ☐	**Active SDS VIP**: Configure the Remote server	Type the **Remote Server Name** for the DSR Message Processer server.  Type the **Remote Server IPv4 Address**.  ***Note***: This is the IMI IP address of the MP. Type the **Remote Server IPv6 Address**.  Select the **IP Address Preference**.  Select **Client** for the Remote Server Mode.  Select the **Local Server Group** for the SDS Data Processer server group.  Click **Apply**.

Procedure 17. Configure ComAgent (All DP-SOAM Sites)

Step	Procedure	Result
5 ☐	**Active SDS VIP**: Confirm data information	A confirmation banner displays. 
6 ☐	**Active SDS VIP**: Repeat	For each remote MP in the same SOAM NE, repeat steps 3 through 5 of this procedure.

3.11 Backups and Disaster Prevention

The preferred method for 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.

Appendix A. Create an XML File for Installing SDS Network Elements

SDS network elements are created using an XML configuration fileThe SDS software image (*.iso) contains two examples of XML configuration files for “NO” (Network OAM&P) and “SO” (System OAM) networks. These files are named **SDS_NO_NE.xml** and **SDS_SO_NE.xml** and are stored on the **/usr/TKLC/sds/vlan** directory. Create individual XML files for each of your SDS network elements. The format for each of these XML files is identical.

Below is an example of the SDS_NO_NE.xml file. The highlighted values are values you must update.

Note: The **Description** column in this example includes comments for this document only. **Do not include** the Description column in the actual XML file used during installation.

Table 2, SDS SML Network Element Configuration File (IPv4)

XML File Text	Description
<?xml version="1.0"?>	
<networkelement>	

XML File Text	Description
<name>**sds_mrsvnc**</name>	Unique identifier used to label a Network Element. [Range = 1-32 character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]
<ntpservers>	
<ntpserver>**10.250.32.10**</ntpserver>	IP Address of the first NTP server. There must be at least one NTP server IP address defined.
<ntpserver>**10.250.32.51**</ntpserver>	IP Address of second NTP server, if it exists; otherwise, this line must be deleted.
</ntpservers>	
<networks>	
<network>	
<name>XMI</name>	Name of customer external network. ***Note***: Do NOT change this name.
<vlanId>**3**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**10.250.55.0**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**10.250.55.1**</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. [Range = true/false]
</network>	
<network>	
<name>IMI</name>	Name of customer internal network. ***Note***: Do NOT change this name.
<vlanId>**4**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**169.254.100.0**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**169.254.100.3**</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
</network>	
</networks>	
</networkelement>	

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 3. List of Selected Time Zone Values

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

Time Zone Value	Description	Universal Time Code (UTC) Offset
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. Resource Profile

VM Name	VM Purpose	vCPUs	RAM (GB)	Storage (GB)
SDS NOAM	Database Processor for address resolution and subscriber location functions	4	12	125
SDS SOAM	Database Processor Site (node) Operation, Administration, Maintenance for address resolution and subscriber location functions	4	12	125
DP	Subscriber Database Processor for address resolution and subscriber location functions.	4	12	125
Query Server	Allows customers to query FABR subscriber data via a MySQL interface	4	12	125

VM Name	OAM (XMI)	Local (IMI)
SDS NOAM	eth0	eth1
SDS SOAM	eth0	eth1
DP	eth0	eth1
Query	eth0	eth1

Note: The Ethernet interfaces defined in the table are there as a guideline. Interfaces can be ordered as preferred, i.e., eth1 or eth2 could be associated with XMI if desired.

Appendix D. Common KVM/Openstack Tasks

Procedure 18. Import an OVA File

Step	Procedure	Result
1 ☐	Create VM flavors	Use the Appendix C Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the Admin section, or with the `nova flavor-create` command line tool. Make the flavor names as informative as possible. Since 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) represent the RAM allocation in GB, and the final three figures (060) represent the disk space in GB.

2 ☐	Unpack and import an image file using the glance utility	1. Copy the OVA file to the OpenStack control node.
		`$ scp SDS-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 SDS-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.
		SDS-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.
		sds-x.x.x-original
		7. Import the image using the **glance** utility from the command line.
		`$ glance image-create --name sds-x.x.x-original --visibility public --protected false progress --container-format bare --disk-format vmdk --file SDS-x.x.x-disk1.vmdk`
		This process takes about 5 minutes, depending on the underlying infrastructure.

Procedure 19. Create a Network Port

Step	Procedure	Result

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.
		NOAM-A-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=NOAM-A-xmi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>`
		`$ neutron port-create --name=NOAM-A-imi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>`
		View your newly created ports using the neutron tool.
		`$ neutron port-list`

Procedure 20. Create and Boot OpenStack Instance

Step	Procedure	Result

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.
		NOAM-A
		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.
		`$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> InstanceName`
		View the newly created instance using the nova tool.
		`$ nova list --all-tenants`
		The VM takes approximately 5 minutes to boot. At this point, the VM has no configured network interfaces and can only be accessed by the Horizon console tool.

Procedure 21. Configure Networking for OpenStack Instance

Step	Procedure	Result

1
☐
	Verify/ Configure the network interface	Check if interface is configured automatically.
		If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address. To verify, ping the XMI IP address provided with **nova boot**… command:
		`$ping <XMI-IP-Provided-During-Nova-Boot>`
		If the ping is successful, ignore the next part to configure the interface manually.
		Manually configure the interface, if not already done (Optional)
		1. Log into the **Horizon** GUI as the DSR tenant user.
		2. Go to the Compute/Instances section.
		3. Click on the **Name** field of the newly created instance.
		4. Select the Console tab.
		5. Login as the **admusr** user.
		6. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C.
		`$ 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 more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions:
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly.
		Re-run the `netAdm command`. It creates and configures the interface in one action.
		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 via both network and Horizon console.

Appendix E. Common OVM-Manager Tasks (CLI)

E-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 22. Set Up Server

Step	Procedure	Result

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:`

2 ☐	**OVM-M CLI**: Discover Oracle VM server	`discoverServer ipAddress=value password=value takeOwnership= { Yes | No }`
		Example:
		`OVM>discoverServer ipAddress=10.240.16.139 password=password takeOwnership=Yes`

3 ☐	**OVM-M CLI**: Create an ethernet-based network with the VM role	`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`

4 ☐	**OVM-M CLI**: Add a port from each Oracle VM server to the network	***Note***: 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`

Procedure 22. Set Up Server

Step	Procedure	Result

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`

Procedure 22. Set Up Server

Step	Procedure	Result
		BondPort id=0004fb00002000005a45a0761813d512 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 22. Set Up Server

Step	Procedure	Result
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`

Procedure 22. Set Up Server

Step	Procedure	Result
		name:SATA_WDC_WD5001ABYS-_WD-WCAS86571931 id:0004fb00001800008f6ea92426f2cfb8 name:SATA_WDC_WD5001ABYS-_WD-WCAS86257005 id:0004fb00001800008ccb1925cdbbd181 name:SATA_WDC_WD5001ABYS-_WD-WCAS86578538 id:0004fb0000180000e034b4662665161c name:FreeBSD (4) 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: OVM>refresh { AccessGroup | Assembly | FileServer | FileSystem | PhysicalDisk | Repository | Server | StorageArray | VirtualAppliance } instance For example, to refresh a physical disk: OVM>refresh PhysicalDisk id=0004fb000018000035ce16ee4d58dc4d 3. Refresh a file system: 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'
9 ☐	**OVM-M CLI**: Add Oracle VM servers to the server pool	OVM>add Server name=MyServer to ServerPool name=MyServerPool
10 ☐	**OVM-M CLI**: Create storage repository	1. Find the physical disk (LUN) to use for creating the storage repository. 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 2. Find a local file system on an Oracle VM server that has access to the LUN.

Procedure 22. Set Up Server

Step	Procedure	Result
		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 3. Create file system. OVM>create FileSystem name=VmsFs01 physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" on FileServer name="Local FS vms01.test.com" Command: create FileSystem name=VmsFs01 physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" 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 OVM> Add serverpool to repository OVM> add ServerPool name=TestPool001 to Repository

Procedure 22. Set Up Server

Step	Procedure	Result
		name=Vms01Repo Refresh the storage repository using the syntax: OVM> refresh Repository name=MyRepository

E-2. Create a VM

Procedure 23. Create a VM

Step	Procedure	Result
1 ☐	**OVM-M CLI**: Import the OVA	***Note***: Log into the OVM-M CLI for executing all the OVM commands. Refer to Procedure E-1 Set Up the Server. 1. Import the virtual appliance/OVA. OVM>importVirtualAppliance Repository name=MyRepository url="http:////example.com//myvirtualappliance.ova" Example: OVM>importVirtualAppliance Repository name=Vms01Repo url=http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova Command: importVirtualAppliance Repository name=Vms01Repo url=http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova Status: Success Time: 2016-09-09 07:33:11,777 EDT JobId: 1473420749759 Data: id:11cdf999eb name:SDS-8.0.0.0.0_80.11.0.ova ***Note***: Use the highlighted ID for referring to the newly created virtual appliance in any further commands.

Procedure 23. Create a VM

Step	Procedure	Result

2
☐
	OVM-M CLI:
	Create VM
		1. Show virtual appliance to get the VM ID.
		Note: The ID referred to in the following command is the virtual appliance ID from the above step.
		`OVM>show VirtualAppliance id=11cdf999eb`
		`Command: show VirtualAppliance id=11cdf999eb`
		`Status: Success`
		`Time: 2016-09-09 07:39:12,491 EDT`
		`Data:`
		`Origin = http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Repository = 0004fb000003000072973b7457792d93 [Vms01Repo]`
		`Virtual Appliance Vm 1 = 11cdf999eb_vm_vm [vm]`
		`Virtual Appliance VirtualDisk 1 = 11cdf999eb_disk_disk1 [disk1]`
		`Id = 11cdf999eb [SDS-8.0.0.0.0_80.11.0.ova]`
		`Name = SDS-8.0.0.0.0_80.11.0.ova`
		`Description = Import URL: http:////10.240.191.134//SDS-8.0.0.0.0_80.11.0.ova`
		`Locked = false`
		2. Create a VM from a virtual machine in a virtual appliance.
		Note: The virtual appliance VM name referred in the below command is the name from the above step.
		`OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name= 11cdf999eb_vm_vm`
		`Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11cdf999eb_vm_vm`
		`Status: Success`
		`Time: 2016-09-09 07:53:05,702 EDT`
		`JobId: 1473421832449`
		`Data: id:0004fb000006000009a08ec97ad5496b name:SDS-8.0.0.0.0_80.11.0.ova_vm`

Procedure 23. Create a VM

Step	Procedure	Result

3 ☐	**OVM-M CLI**: Add VM to server pool	1. Add VM to server pool.
		`OVM>add Vm instance to { AntiAffinityGroup | Server | ServerPool } instance`
		Example:
		`OVM>add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001`
		`Command: add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001`
		`Status: Success`
		`Time: 2016-08-30 02:15:00,859 EDT`
		`JobId: 1472537700721`
		Note: Refer E-3 Server Pool section for further information on Server Pool.

4 ☐	**OVM-M CLI**: Edit VM with required profile/resource	1. Edit VM with required resources. Refer Appendix C Resource Profile for recommended resource profile.
		Note: Use the VM ID/Name in any related commands.
		`OVM> edit Vm name=SDS-NOAM-A memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="SDS NOAM-A"`
		`Command: edit Vm name=SDS-NOAM-A memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="SDS NOAM-A"`
		`Status: Success`
		`Time: 2016-08-22 02:04:09,329 EDT`
		`JobId: 1471845849193`

5 ☐	**OVM-M CLI**: Attach VNIC	1. If VNIC is already created, attach it. First, get the VNIC ID:
		`OVM>show Vm name=SDS-NOAM-A`
		`Command: show Vm name=SDS NOAM-A`
		`Status: Success`
		`Time: 2016-08-24 06:42:00,115 EDT`
		`Data:`
		`Status = Running`
		`Memory (MB) = 6584`
		`Max. Memory (MB) = 6584`
		`Processors = 6`
		`Max. Processors = 6`
		`Priority = 50`
		`Processor Cap = 100`

Procedure 23. Create a VM

Step	Procedure	Result
		High Availability = No Operating System = Oracle Linux 6 Mouse Type = PS2 Mouse Domain Type = Xen HVM PV Drivers Keymap = en-us Start Policy = Use Pool Policy Origin = http://10.240.191.134/SDS-8.0.0.0.0_80.8.0.ova Disk Limit = 107 Huge Pages Enabled = No Config File Absolute Path = /dev/mapper/OVM_SYS_REPO_PART_3600605b00a15b2601cb8a56a1410036a/VirtualMachines/0004fb0000060000e07023e7051a923c/vm.cfg Config File Mounted Path = /OVS/Repositories/0004fb000003000072973b7457792d93/VirtualMachines/0004fb0000060000e07023e7051a923c/vm.cfg Server = 08:00:20:ff:ff:ff:ff:ff:ff:ff:00:10:e0:71:91:34 [compute01.test.com] Server Pool = 0004fb0000020000ff238819a2310353 [TestPool001] Repository = 0004fb000003000072973b7457792d93 [Vms01Repo] Vnic 1 = 0004fb000007000078f3fdb5bea01697 [00:21:f6:6f:b6:b1] VmDiskMapping 1 = 0004fb0000130000ac3e9f3d21e90188 [Mapping for disk Id (0004fb0000120000c95393297e1028e9.img)] VmDiskMapping 2 = 0004fb00001300002852a93587c1893a [Mapping for disk Id (EMPTY_CDROM)] Restart Action On Crash = Restart Id = 0004fb0000060000e07023e7051a923c [NOAM-A] Name = SDS NOAM-A Description = SDS NOAM-A Locked = false DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)] 2. Add VNIC to network. ***Note***: The VNIC ID referred to in the following command is the ID from the above step.

Procedure 23. Create a VM

Step	Procedure	Result
		OVM>list Network Command: list Network Status: Success Time: 2016-09-26 05:34:25,088 EDT Data: id:109560cfdc name:XSI1 id:10e361d8ee name:XSI2 id:107561a2ba name:XMI id:10333df5b6 name:IMI id:0af01080 name:10.240.16.128
6 ☐	**OVM-M CLI**: Create and attach remaining VNICs for the VM	1. Create VNIC on the network and attach to it. ***Note***: The network referred to in the following command is the network name from the above step. OVM>create Vnic network=IMI name=SDS-NOAM-A-IMI on Vm name=SDS-NOAM-A Command: create Vnic network=IMI name=SDS-NOAM-A-IMI on Vm name=SDS NOAM-AStatus: Success Time: 2016-08-22 05:38:34,252 EDT JobId: 1471858714114 Data: id:0004fb0000070000b51a093ec88ed87d name: SDS NOAM-A-IMI ***Note***: Repeat this step for all required interfaces (XSI1, XS2 etc.).

Procedure 23. Create a VM

Step	Procedure	Result

7
☐
	OVM-M CLI: Configure instance networking	1. Log into the **OVM-M** GUI/console.
		`https://<OVM-M-IP:port>/ovm/console/faces/login.jspx`
		2. Go to the servers and VMs tab.
		3. Select the host from the Server Pools.
		4. Go to **Virtual Machines**, select the VM, and click **Launch Console**.
		5. Login as the **admusr** user.
		6. Configure the required network interfaces, conforming to the interface-to-network mappings described at the bottom of Appendix C Resource Profile.
		`$ sudo netAdm set --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 more interfaces.
		If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions:
		`$ cd /etc/sysconfig/network-scripts`
		`$ sudo mv ifcfg-ethX /tmp`
		Keep ifcfg-ethX in /tmp until ethX is working correctly.
		Re-run the `netAdm command`. It creates and configures the interface in one action.
		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 via both network and console.

8
☐
	OVM-M CLI: Start VM	1. Start the VM.
		`OVM>start Vm name=SDS-NOAM-A`
		`Command: start Vm name=SDS-NOAM-A`
		`Status: Success`
		`Time: 2016-08-22 06:32:37,853 EDT`
		`JobId: 1471861954163`

E-3. 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. Since server pools have shared access to storage repositories, live migration of virtual machines is possible for load balancing or for scheduled maintenance, so that a virtual machine can be moved from one Oracle VM server to another without an interruption of service. Within a clustered server pool, virtual machines have high availability or HA. The clustering technology used within Oracle VM can take care of monitoring the status of all of the Oracle VM servers belonging to the server pool. If a pool member disappears for whatever reason, its virtual machines can be recovered and brought back up on another Oracle VM server, because all necessary resources are available on shared storage.

More information: http://docs.oracle.com/cd/E64076_01/E64081/E64081.pdf.

Appendix F. Application VIP Failover Options (OpenStack)

F-1. Application VIP Failover Options

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

- Allowed address pairs
- Disable port security

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

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

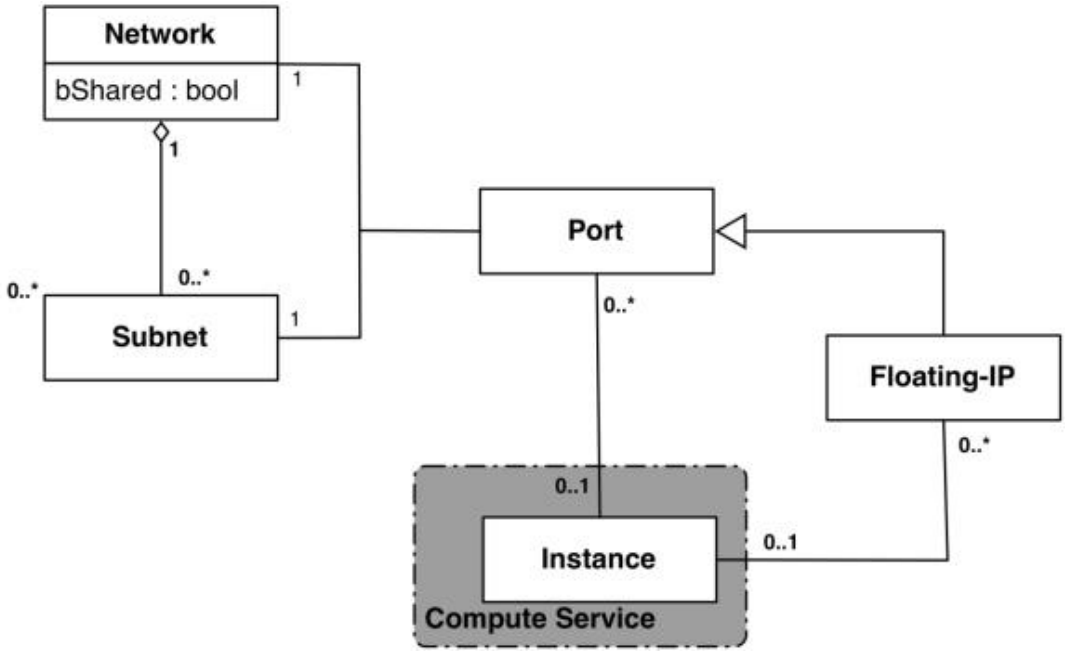


Figure 2. Neutron High-Level Data Model

Note how a port in the Neutron data model maps to at most one VM instance where internal to the VM instance, the port 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 via its command line utility, simply named `neutron`. However, be aware that all of the operations performed using the `neutron` command line utility can also be performed through the Neutron REST APIs, see the Networking v2.0 API documentation for more information.

F-2. Allowed Address Pairs

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

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

F-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.

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

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

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

where the bolded items have the following meaning:

- <Port ID>

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

- <VIP address to be added>

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

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

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

F-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.

F-6. Disable Port Security

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

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

OpenStack Configuration Requirements

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

ML2 Port Security Extension Wiki page

Note: Enabling the port security extension when there are already existing networks within the OpenStack cloud causes all network related requests into Neutron to fail due to a known bug in Neutron. There is a fix identified for this bug that is part of the Liberty release and is scheduled to be backported to the Kilo 2015.1.2 release. In the 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.

F-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.

F-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.

F-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 G. 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.