Oracle® Communications Diameter Signaling Router

Subscriber Data Server Cloud Installation Guide

Release 9.0.0.0.0
F79832-01
April 2023

Oracle Communications Diameter Signaling Router Subscriber Data Server Cloud Installation Guide, Release 9.0.0.0.0

F79832-01

Contents

1 Introduction

2 Application Installation

3 Configuration Procedures

A Appendix

My Oracle Support

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

Call the Customer Access Support 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 My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms and Terminology

Listed below is an alphabetized list of acronyms used in the document:

Table Acronyms and Terminology

Acronym	Definition
BNS	Broadband Networking Solutions
CSV	Comma Separated Values
ComAgent	Communication Agent. An EXG common infrastructure component delivered as part of a common plug-in that uses the COMCOL MX framework in support of communicating Stack Events between EXG application processes on different servers.
DA-MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
FABR	Full-Address Based Resolution
FOA	First Office Application
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
KVM	Kernel based Virtual Machine
MP	Message Processing or Message Processor
MTU	Maximum Transfer Unit
NAPD	Network Architecture Planning Document
NE	Network Element
NOAM	Network Operations, Administration and Maintenance
OAM	Operations, Administration and Maintenance
OS	Operating System
OVM-M	Oracle VM Manager
OVM-S	Oracle VM Server
POC	Point of Contact
PSE	Professional Services Engineer
SDS	Subscriber Database Server
SOAM	System Operations, Administration and Maintenance
SSH	Secure Shell
TPD	Tekelec Platform Distribution (Linux OS)
UI	User Interface
VIP	Virtual IP

Table (Cont.) Acronyms and Terminology

Acronym	Definition
VM	Virtual Management
VPN	Virtual Private Network
XMI	External Management Interface

Whats New in This Guide

No updates made to this document in this release.

1 Introduction

This document describes how to install Oracle Communications Subscriber Data Server (SDS) within a customer network. It uses the AppWorks 7.5 network installation and captures the initial network configuration steps for an SDS or Query Server NE for production use as part of the Diameter Signaling Router (DSR) solution.

This document describes the SDS product installation on a virtualized solution into VMs hosted by the VMware, Kernel-based Virtual Machine (KVM), and Oracle VM Server (OVM-S) hypervisors.

This document does not include the following configurations:

- Hardware installation
- Site survey
- Customer network configuration
- IP assignments
- Customer router configurations
- Configuration of any device outside of the SDS virtual machines

1.1 References

The following document references capture the source material used to create this document:

- *Diameter Signaling Router Cloud Benchmarking Guide*
- *Oracle VM Concepts Guide*

1.2 Pre-requisites

Ensure the following before initiating SDS installation:

- Review the latest customer specific Network Architecture Planning document.
- Ensure all the assigned values for the requested information related to SDS, DR SDS NO, Query Server, DP-SOAM, and DP installation are received.
- The values used to compile XML files (See, Creating an XML file for Installing SDS Network Elements for each SDS and DP-SOAM site's NE before performing this procedure are received.
- Conceptually understand DSR topology and SDS network configuration described in the latest customer-specific Network Architecture Planning document.
- The user must have an intermediate skill set with command prompt activities on an Open Systems computing environment such as Linux or Tekelec Platform Development (TPD).

1.3 XML Files

The XML files compiled for installation of each SDS and DP-SOAM site’s NE must be accessible for use in Disaster Recovery procedures. An Oracle Professional Services Engineer (PSE) provides a copy of the XML files used for installation to the designated Customer Operations POC.

> **Note:**
>
> Oracles Customer Service requires XML files for disaster recovery operations. The operator is responsible for maintaining and providing the XML files.

1.4 How to Use This Document

This document is primarily used as an initial installation guide, and its secondary purpose is as a reference for disaster recovery procedures. When executing this document for either purpose, before beginning a procedure, thoroughly read the instructional text (documented after the Procedure Section headings) and all associated Warnings or Notes for each procedure.

> **Note:**
>
> If any step fails, contact MOS.

2
Application Installation

Installing the SDS product is a task that requires multiple types of installations. This document covers the necessary configuration needed to complete product installation.

> **Note:**
>
> Refer to the online help or contact the Oracle Help Center for assistance with post installation configuration options.

Pre-requisites:

The following items or settings are required to perform installation:

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

2.1 Activity Logging

Log all activity while connected to the system using a convention that notates the **Customer Name**, **Site** or **Node location**, **Server hostname** and the **Date**. Post-installation, provide all logs to Oracle Communications for archiving.

2.2 Creating SDS Guests (VMware)

Perform the following procedure in Cloud Client to create SDS Guests from OVA (VMWare):

1. To add SDS OVA image, perform the following steps:
   a. Open the required Cloud Client.
   b. Add the SDS OVA image to the cloud catalog or repository. Follow the instructions provided by the cloud solutions manufacturer.
2. To create the SDS VM from the OVA image, perform the following steps:
   a. Navigate to the library or repository where the OVA image is present.
   b. Deploy the OVA image using Cloud or the Cloud Web Client.
   c. Name the **SDS NOAM VM** and select the datastore.
3. To configure the **SDS NOAM VM**, refer to the DSR Cloud Benchmarking Guide for the SDS NOAM using the Cloud Client or the Cloud Web Client.
4. To power on **SDS NOAM-A VM**, use the Cloud or Cloud Web Client.

5. To configure **SDS NOAM-A**, perform the following steps:
   a. Open the **SDS NOAM-A VM** console using the Cloud or Cloud web client.
   b. Login as **admusr**.
   c. When the ethX is the interface associated with the XMI network, configure the <ethX> device:

   ```
   $ sudo netAdm add --device=<ethX> --address=<IP Address in
   External management Network> --netmask=<Netmask> --onboot=yes --
   bootproto=none
   ```

   d. Add the default route for ethX:

   ```
   $ sudo netAdm add --route=default --gateway=<gateway address for
   the External management network> --device=<ethX>
   ```

> **Note:**
>
> While re-configuring virtual NICs under VMware, perform the following procedure:
>
> a. Remove the UDEV rules file under `/etc/udev/rules.d/70-persistent-net.rules` path.
> b. Shut down the guest and remove the interfaces.
> c. Power on the VM and add the interfaces one by one, in the desired order of enumeration.
> d. To get VMware to instantiate the device, click **OK** each time.

6. To verify network connectivity, ping the default gateway.

   ```
   $ ping -c3 <gateway address for the External management network>
   ```

> **Note:**
>
> Repeat these steps for each server before continuing to the next procedure. For example, NOAM-A, NOAM-B, DR SDS Servers, Query Server, and DP.

2.3 Creating SDS Guests from OVA (KVM or OpenStack)

Perform the following procedure in Cloud Client to create SDS Guests from OVA (KVM or OpenStack):

Pre-requisites:

- Create instance flavors.

- Use the *DSR Cloud Benchmarking Guide* values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the Admin section or the `nova flavor-create` command line tool.
- Name the flavors describing their respective function and ensure it is as informative as possible. Flavors define resource sizing. A standard convention is to name as **0406060**. Where the first two digits (04) represent the number of virtual CPUs, the next two digits (06) represent the RAM allocation in GB, and the final three digits (060) represent the disk space in GB.
- The default Large Receive Offload (LRO) option must be disabled on the host command line while using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes. For more information, see the Intel release notes.

  ```
  $ sudo ethtool -K <ETH_DEV> lro off
  ```

1. To add **SDS OVA** image, perform the following steps:
   a. Copy the OVA file to the OpenStack control node.

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

   b. Log into the OpenStack control node.

      ```
      $ ssh admusr@node
      ```

   c. Unpack the OVA file using tar in an empty directory.

      ```
      $ tar xvf SDS-x.x.x.ova
      ```

   d. Import the unpack the .vmdk VM image file.

      ```
      SDS-x.x.x-disk1.vmdk
      ```

   e. Source the OpenStack admin user credentials.

      ```
      $ . keystonerc_admin
      ```

   f. Select an informative name for the new image.

      ```
      sds-x.x.x-original
      ```

   g. To use VMDK format, import the image using the glance utility from the command line.

      ```
      $ glance image-create --name sds-x.x.x-original --is-public True --is-
      protected False --progress --container-format bare --disk-format vmdk
      --file SDS-x.x.x-disk1.vmdk
      ```

      > **Note:**
      >
      > This process takes about five minutes depending on the underlying infrastructure. To complete the VMDK format, go to Step 2.

h. To use QCOW2 format, perform the following steps:

   i. Convert VMDK to QCOW2 format using the qemu-img tool and create a qcow2 image file running the following command:

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

   For example:

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

   > **Note:**
   >
   > If the qemu-img tool is not already installed, install it using yum command.
   >
   > ```
   > sudo yum install qemu-img
   > ```

   ii. Import the converted QCOW2 image using the glance utility from the command line.

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

   > **Note:**
   >
   > This process takes about five minutes depending on the underlying infrastructure.

2. To name the new VM instance, perform the following steps:

   a. Create an informative name for the new instance.

   ```
   SDS-NOAM-A
   ```

   b. Review the network interface recommendation provided in *DSR Cloud Benchmarking Guide*.

3. In **OpenStack Control Node**, create and boot the VM instance from the glance image by performing the following steps:

   a. Retrieve the required configuration values, by running the following commands:

   - To obtain the image ID:

     ```
     $ glance image-list
     ```

Output:

```
811f0181-6e66-4cf0-9eb7-8058d86edf05
```

- To obtain flavor ID:

  ```
  $ nova flavor-list
  ```

- To obtain network ID(s):

  ```
  $ neutron net-list
  ```

  Output:

  ```
  cb2a0b22-2383-462d-bce5-73f3f5bb752d
  ```

b. Specify what information should convey by its name.

```
SDS-NOAM-A
SDS-NOAM-B
```

c. Create and boot the VM instance.

> **Note:**
>
> The instance must be owned by the DSR tenant user, not the **admin** user.

d. Source the credentials of the DSR tenant user and run 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> --config-drive
true <instance name>
```

> **Note:**
>
> Use one `--nic` argument for each IP or interface.
> IPv6 addresses should use the `v6-fixed-ip` argument, instead of `v4-fixed-ip`.

e. To verify if the new instance has been booted, view the newly created instance using the nova tool.

```
$ nova list | grep -i (xmi address)
```

> **Note:**
>
> The VM takes approximately five minutes to boot and can be accessed through both network interfaces and the Horizon console tool.

4. To configure VIP, in **OpenStack Control Node**, perform this step.

   > **Note:**
   >
   > This is an optional step. Refer to Application VIP Failover Options (OpenStack) for more information on VIP.

   If a NOAM or SOAM VIP is needed, run the following commands:

   a. Find the port ID associated with the instance's network interface.

      ```
      $ neutron port-list
      ```

      Output:

      ```
      aed2522e-cf52-4aa4-9e12-4acab7f8df04
      ```

   b. Add the VIP IP address to the address pairs list of the instance's network interface port.

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

5. Check if interface is configured.

   If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address provided in Step 3. To verify, ping the XMI IP address provided with the nova boot command from Step 3:

   ```
   $ ping <XMI-IP-Provided-During-Nova-Boot>
   ```

   If the ping is successful, ignore Step 6 to configure the interface manually.

6. To manually configure interface, in **OpenStack Dashboard (Horizon)**, perform the following steps:

   > **Note:**
   >
   > This is an optional step.
   > If the instance is already configured with an interface and has successfully pinged in Step 5, then ignore this step to configure the interface manually.

a. Log into the **Horizon** GUI as the tenant user.

b. Navigate to the **Compute/Instances** section.

c. Click **Name** field of the newly created instance.

d. Select **Console** tab.

e. Login as the **admusr** user.

f. Select an informative hostname for the new VM instance.

```
SDS-NOAM-A
SDS-SO2
```

g. Configure the network interfaces, by conforming to the OCDSR Network to Device Assignments defined in the *DSR Cloud Benchmarking Guide*.

```
$ sudo netAdm set --onboot=yes --device=eth0 --address=<xmi port ip>
--netmask=<xmi net mask>
$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi
gateway ip>
```

> **Note:**
>
> Under some circumstances, it may be necessary to configure more interfaces.

h. If `netAdm` fails to create the new interface (ethX) because it already exists in a partially configured state, run the following commands:

```
$ cd /etc/sysconfig/network-scripts
$ sudo mv ifcfg-ethX /tmp
```

> **Note:**
>
> Keep `ifcfg-ethX` in `/tmp` until ethX is working correctly.

i. To create and configure the interface in one action, re-run the `netAdm` command.

j. Reboot the VM.

```
$ sudo init 6
```

> **Note:**
>
> It takes approximately five minutes for the VM to complete rebooting.

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

7. Verify network connectivity, by pinging the default gateway.

   ```
   $ ping -c3 <gateway address for the External management network>
   ```

   > **Note:**
   >
   > Repeat these Step 2 through Step 7 for each server before continuing to the next procedure (for example, NOAM-A, NOAM-B, DR Servers, Query Server, and DP).

2.4 Creating SDS Guests from OVA (OVM-S or OVM-M)

This section provides procedure to import SDS OVA and prepare for VM creation.

Pre-requisites:
Provide values for the following variables:

- **<OVM-M IP>:** IP address to access a sh prompt on the OVM server.
- **<URL to OVA>:** Link to a source for downloading the product image (.ova).
- **<MyRepository name>:** Name of the repository in the OVM to hold the product image (.ova).
- **<Virtual Appliance OVA ID>**
- **<OVA VM name_vm_vm>**
- **<OVM network id for (each subnet)>**
- **<OVM network name for (each subnet)>**

1. To access command line of OVM, perform the following steps:

   > **Note:**
   >
   > Refer to Common OVM-Manager Tasks (CLI) for setting up the platform.

   a. Retrive the site-specific values for these variables.

      ```
      <OVM-M IP> = 100.64.62.221
      ```

   b. Use the respective value for `<OVM-M IP>` into the command.

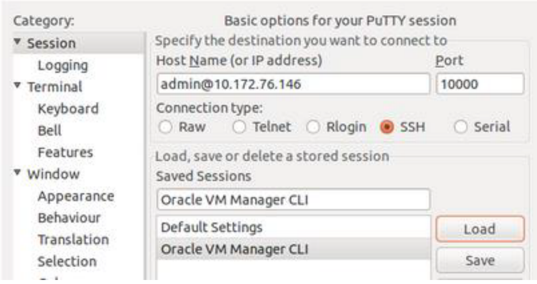
      ```
      ssh -l admin <OVM-M IP> -p 10000
      ```

      For example:

      ```
      ssl -l admin 100.64.62.221 -p 10000
      ```

      Alternatively, use a terminal emulation tool like putty.

Figure 2-1   Terminal Emulation Tool



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): admin@10.172.76.146

Port: 10000

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Oracle VM Manager CLI

Default Settings
Oracle VM Manager CLI

2. To import the OVA, using **OVM-M CLI** perform the following steps:

   a. Retrieve the site-specific values for these variables.

   ```
   <URL to OVA> = http://10.240.155.70/iso/SDS/8.6/ova/
   SDS-8.6.0.0.0_95.14.0.ova
   <MyRepository name> = XLab Utility Repo01
   ```

   b. Add the respective values for `<MyRepository name>` and `<URL to OVA>` in the command.

   ```
   OVM>importVirtualAppliance Repository name=’<MyRepository name>’
   url="<URL to OVA>”
   ```

   For example:

   ```
   OVM> importVirtualAppliance Repository name='XLab Utility Repo01'
   url=http://10.240.155.70/iso/SDS/8.6/ova/SDS-8.6.0.0.0_95.14.0.ova
   ```

   c. To validate success and examine the screen results to find site-specific text for variables in these locations, run the following command:

   ```
   importVirtualAppliance Repository name='XLab Utility Repo01'
   url=http://10.240.155.70/iso/SDS/8.6/ova/SDS-8.6.0.0.0_95.14.0.ova
   Status: Success
   Time: 2017-04-18 15:23:31,044 EDT
   JobId: 1492543363365
   Data: id: 1128a1c6ce name: SDS-8.6.0.0.0_95.14.0.ova
   ```

   d. Add the respective values for the following variable:

   ```
   <Virtual Appliance OVA ID> = 1128a1c6ce
   ```

3. To get the virtual appliance ID, using **OVM-M CLI** perform the following steps:

   > **Note:**
   >
   > The virtual appliance OVA ID is used in later steps.

a. Retrieve the site-specific text for these variables.

```
<Virtual Appliance OVA ID> = 1128a1c6ce
```

b. Add the respective values for <Virtual Appliance OVA ID> in the command.

```
OVM> show VirtualAppliance id=<Virtual Appliance OVA id>
```

For example:

```
OVM> show VirtualAppliance id=1128a1c6ce
```

c. To validate success and examine the screen results to find site-specific text for variables in these locations, run the following command:

```
show VirtualAppliance id=1128a1c6ce
Status: Success
Time: 2017-04-18 15:23:53,534 EDT
Data:
Origin = http://10.240.155.70/iso/SDS/8.6/ova/
SDS-8.6.0.0.0_95.14.0.ova
Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility
Repo01]
Virtual Appliance Vm 1 = 11145510c0_vm_vm [vm]
Virtual Appliance VirtualDisk 1 = 11145510c0_disk_disk1 [disk1]
Id = 11145510c0 [SDS-8.6.0.0.0_95.14.0.ova]
Name = SDS-8.6.0.0.0_95.14.0.ova
Description = Import URL: http://10.240.155.70/iso/SDS/8.6/ova/
SDS-8.6.0.0.0_95.14.0.ova
Locked = false
```

d. Add the respective values for this variable.

```
<OVA VM name_vm_vm> = 11145510c0_vm_vm
```

4. To determine the OVM network IDs, using **OVM-M CLI** perform the following steps:

> **Note:**
>
> This is established during the platform installation.
>
> ```
> OVM> list Network
> ```

a. Run the following command and validate success for:

- <OVM network ID>
- <OVM network name>

> **Note:**
>
> This screen results data is required to be referred in later steps.

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

b. Examine the screen results to find site-specific OVM values for each subnet.

c. Add the respective values for network ID variables. Then, change the examples as shown in the following table according to the values.

	OAM (XMI)	Local (IMI)
<OVM network name>	XMI-10	IMI Shared
<OVM network ID>	10345112c9	102e89a481

2.5 Configure Virtual Machines

The section provides procedure to create virtual machines.

> **Note:**
>
> Repeat this procedure for each of the SDS VM guests (NOAMs, DR Servers, SOAMs, Query servers, and DPs) that need to be created.

Pre-requisites:
Provide values for the following variables:

- `<OVA VM name_vm_vm>`
- `<ServerPool name>`
- `<VM name>`
- `<OVM network ID for XMI>`
- `<OVM network ID for IMI>`
- `<URL for OVM GUI>`

- `<VM IP in XMI>` from the NAPD
- `<Gateway for XMI>` from the NAPD
- `<NetMask for XMI>` from the NAPD
- `<VM ID>`
- `<vCPUs Production>`
- `<VNIC 1 ID>`
- `<interface name>` defined in DSR Cloud Benchmarking Guide

1. To create a VM for each guest from the VM in the OVA virtual appliance, using **OVM-M CLI** perform the following steps:
   a. Retrieve the site-specific text for these variables.

      ```
      <OVA VM name_vm_vm> = 11145510c0_vm_vm
      ```

   b. Add the respective values for `<OVA VM name>` in the command.

      ```
      OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=<OVA
      VM name>
      ```

      For example:

      ```
      OVM> createVmFromVirtualApplianceVm VirtualApplianceVm
      name=11145510c0_vm_vm
      ```

   c. Run the command and validate success.

      ```
      createVmFromVirtualApplianceVm VirtualApplianceVm
      name=11145510c0_vm_vm
      Status: Success
      Time: 2017-04-18 16:02:09,141 EDT
      JobId: 1492545641976
      Data: id: 0004fb00000600004a0e02bdf9fc1bcd
      name:DSR-8.6.0.0.0_95.14.0.ova_vm
      ```

   d. Examine the screen results to find site-specific text for variables in the required locations.
   e. Add the respective values for these variables.

      ```
      <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd
      ```

2. Add the VM to the server pool, using **OVM-M CLI**.
   a. Retrieve the site-specific text for these variables.

      ```
      <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd
      <ServerPool name> = XLab Pool 01
      ```

b. Add the respective values for `<VM ID>` and `<ServerPool name>` into the command.

```
OVM> add Vm id=<VM id> to ServerPool name=”<ServerPool name>”
```

For example:

```
OVM> add Vm id=0004fb00000600004a0e02bdf9fc1bcd to ServerPool
name="XLab Pool 01"
```

c. Run the command and validate success.

```
add Vm id=0004fb0000060000beb93da703830d3c to ServerPool name="XLab
Pool 01"
Status: Success
Time: 2017-04-19 21:05:10,950 EDT
JobId: 1492650310802
```

> **Note:**
>
> Refer to the Server Pool section for more information.

3. To apply required profile or resources, edit VM using **OVM-M CLI**.

a. Get the site-specific text for these variables.

```
<VM ID> = 0004fb00000600004a0e02bdf9fc1bcd
<VM name > = na-sdsnoam-na-2a
<vCPUs Production> = 4
```

> **Note:**
>
> Refer to DSR Cloud Benchmarking Guide for recommended resource.

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

b. Add the respective values for `<VM ID>`, `<VM name>`, and `<vCPUs Production>` into the command.

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

For example:

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

   c. Run the command and validate success.

```
edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-sdsnoam-
na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4
domainType=XEN_HVM description="na-sdsnoam-na-2a"
Status: Success
Time: 2017-04-18 17:55:25,645 EDT
JobId: 1492552525477
```

Now, the VM has a name and resources.

4. Determine VNIC ID, using **OVM-M CLI**.

   a. Retrive the site-specific text for this variable.

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

   b. Add the respective value for <VM name> in the command.

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

For example:

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

   c. Run the command and validate success.

```
Status = Stopped
Memory (MB) = 6144
Max. Memory (MB) = 6144
Processors = 4
Max. Processors = 4
Priority = 50
Processor Cap = 100
High Availability = No
Operating System = Oracle Linux 6
Mouse Type = PS2 Mouse
Domain Type = Xen HVM
Keymap = en-us
Start Policy = Use Pool Policy
Origin = http://10.240.155.70/iso/SDS/8.6/ova/
SDS-8.6.0.0.0_95.14.0.ova
Disk Limit = 4
Huge Pages Enabled = No
Config File Absolute Path = 192.168.5.5:/storage/ovm01/
repository/VirtualMachines/0004fb00000600004a0e02bdf9fc1bcd/
vm.cfg
Config File Mounted Path = /OVS/Repositories/
```

```
0004fb0000030000da5738315337bfc7/VirtualMachines/
0004fb00000600004a0e02bdf9fc1bcd/vm.cfg
Server Pool = 0004fb00000200009148c8926d307f05 [XLab Pool 01]
Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility Repo01]
Vnic 1 = 0004fb0000070000091e1ab5ae291d8a [Template Vnic]
VmDiskMapping 1 = 0004fb0000130000a1996c6074d40563 [Mapping for disk
Id (79def426328a4127b5bf9f7ae53d3f48.img)]
VmDiskMapping 2 = 0004fb00001300002db3d4b67a143ab5 [Mapping for disk
Id (EMPTY_CDROM)]
Restart Action On Crash = Restart
Id = 0004fb00000600004a0e02bdf9fc1bcd [na-sdsnoam-na-2a]
Name = na-sdsnoam-na-2a
Description = na-sdsnoam-na-2a
Locked = false
DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)]
```

d. Examine the screen results to find site-specific text for variables in the required locations.

e. Add the respective values for these variables.

```
<VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a
```

5. Determine network interfaces for the type of guest host.

Note:

Refer to the DSR Cloud Benchmarking Guide, for further information on which network interfaces need to be configured for each guest type.
The referring table sample:

	OAM (XMI)	Local (IMI)
Type of guest host	eth#	eth#

Note:

The VNICs must be created in the correct order so that the interfaces are associated with the correct network.

6. Attach XMI VNIC, if required by guest host type, using the **OVM-M CLI**.

a. Retreive the site-specific text for these variables:

```
<VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a
<OVM network ID for XMI> = 10345112c9
```

b. Add the respective values for <VNIC 1 ID> and <OVM network ID for XMI> in the command:

```
OVM> add Vnic ID=<Vnic 1 ID> to Network name=<OVM network ID for XMI>
```

For example:

```
OVM> add Vnic ID=0004fb0000070000091e1ab5ae291d8a to Network
name=10345112c9
```

c. Run the command and validate success.

```
add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network
name=10345112c9
Status: Success
Time: 2017-04-19 19:08:59,496 EDT
JobId: 1492643339327
```

7. To create and attach IMI VNIC, if required by guest host type, using **OVM-M CLI**, perform the following steps:

   a. Retrive the site-specific text for these variables:

   ```
   <VM name> = na-sdsnoam-na-2a
   <OVM network ID for IMI> = 102e89a481
   ```

   b. Add the respective values for <OVM network ID for IMI> and <VM name> into the command:

   ```
   OVM> create Vnic network=<OVM network ID for IMI> name=<VM name>-
   IMI on VM name=<VM name>
   ```

   For example:

   ```
   OVM> create Vnic network=102e89a481 name=na-sdsnoam-na-2a-IMI on
   Vm name=na-sdsnoam-na-2a
   ```

   c. Run the command and validate success.

   ```
   create Vnic network=102e89a481 name=na-sdsnoam-na-2a-IMI on Vm
   name=na-sdsnoam-na-2a
   Status: Success
   Time: 2017-04-19 21:21:57,363 EDT
   JobId: 1492651317194
   Data:
   id:0004fb00000700004f16dc3bfe0750a7 name:na-sdsnoam-na-2a-IMI
   ```

8. To start VM, using **OVM-M CLI**, perform the following steps:

   a. Retrieve the site-specific text for this variable:

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

   b. Add the respective values for <VM name> in the command.

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

For example:

```
OVM> start Vm name=na-sdsnoam-na-2a
```

c. Run the command and validate success.

```
start Vm name=na-sdsnoam-na-2a
Status: Success
Time: 2017-04-19 19:29:35,376 EDT
JobId: 1492644568558
```

9. To configure the XMI network interface for this VM, using **OVM-M GUI**, perform the following steps:

   a. Retreive the site-specific text for these variables:

   ```
   <URL for OVM GUI> = https://100.64.62.221:7002/ovm/console/faces/
   resource/resourceView.jspx
   <interface name> = from the table in DSR Cloud Benchmarking Guide
   <VM IP in XMI> = from the NAPD
   <Gateway for XMI> = from the NAPD
   <NetMask for XMI> = from the NAPD
   ```

   b. Access the CLI of the console for the VM, by logging into the **OVM-M GUI** by entering the <URL for OVM GUI> in a browser.

   c. Navigate to the Servers and VMs tab.

      i. Expand and select the <ServerPool name>.

      ii. From the **Perspective** list, select **Virtual Machines**.

      iii. Select the <VM name> from the rows listed and click the Launch Console icon.

      iv. In the **Console** window, log into the VM as the **admusr**.

   d. Add the respective values for <interface name>, <VM IP in XMI>, <Gateway for XMI>, and <NetMask for XMI> into the commands.
   Command for Netmask XMI:

   ```
   $ sudo netAdm set --onboot=yes --device=<interface name> --
   address=<VM IP in XMI> --netmask=<NetMask for XMI>
   ```

   For example:

   ```
   $ sudo netAdm set --onboot=yes --device=eth0 --address=10.75.158.189
   --netmask=255.255.255.128
   ```

   Command for Gateway XMI:

   ```
   $ sudo netAdm add --route=default --device=<interface name> –
   gateway=<Gateway for XMI>
   ```

For example:

```
$ sudo netAdm add --route=default --device=eth0 --
gateway=10.75.158.129
```

> **Note:**
>
> Run the above command, to validate success.

e. Verify network connectivity, by pinging Gateway of network.

```
$ ping -c3 <Gateway for XMI>
```

f. Reboot the VM.

```
$ sudo init 6
```

It takeS approximately 5 minutes for the VM to complete rebooting.

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

3 Configuration Procedures

3.1 Configure SDS NOAM Servers A and B (1st Site Only)

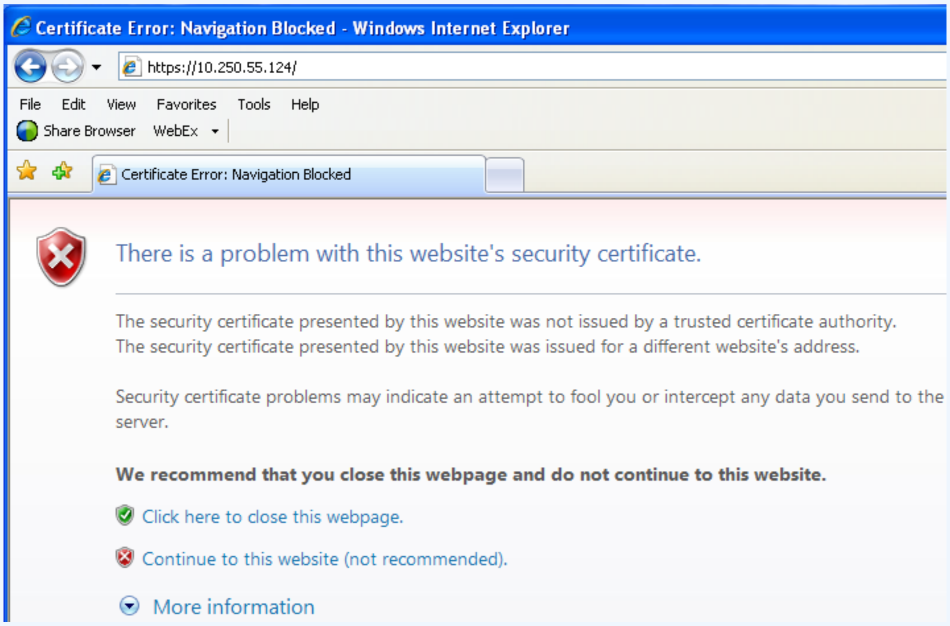
Pre-requisites:

- The SDS Network Element XML file for the Primary Provisioning SDS site must be created as described in Appendix A Creating an XML file for Installing SDS Network Elements.
- The Network Element XML files are present on the laptop's hard drive.
- The user must connect to the SDS GUI before configuring to the first SDS server.

Perform the following steps in **SDS NOAM-A**:

1. Launch the approved web browser and connect to the **SDS NOAM-A XMI** IP address.

> **Note:**
>
> If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.



Certificate Error: Navigation Blocked - Windows Internet Explorer

https://10.250.55.124/

There is a problem with this website's security certificate.

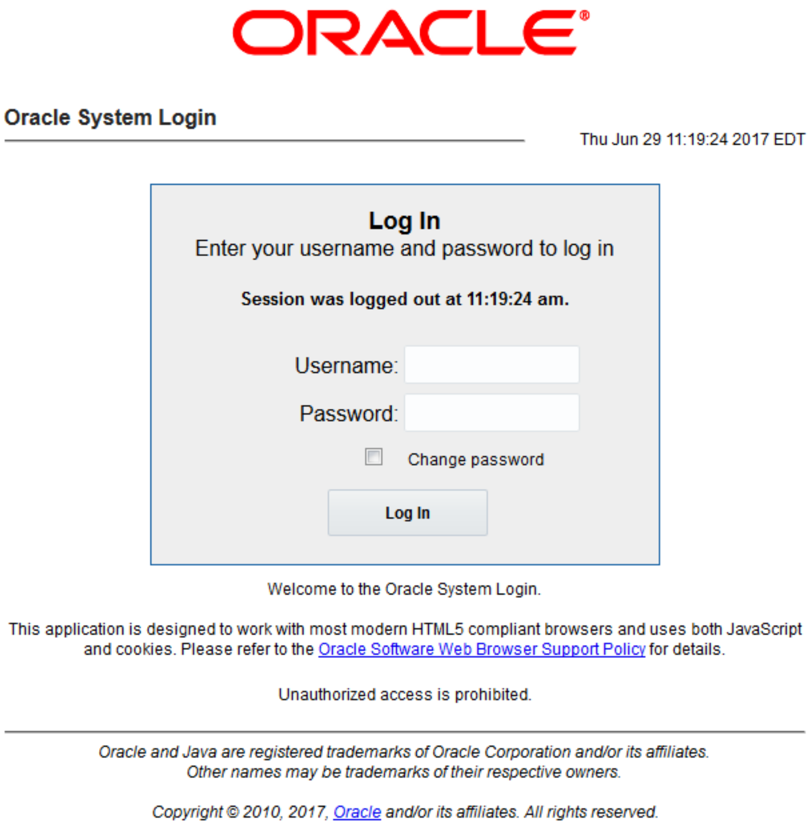
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

2. To login, establish a GUI session as the **guiadmin** user on the NOAM-A server, by using the XMI IP address.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

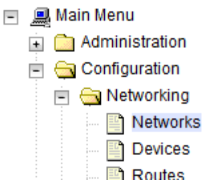
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

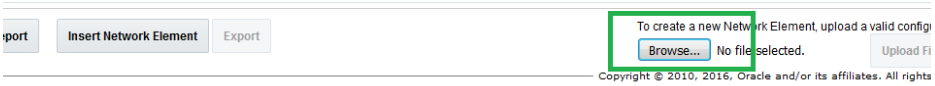
Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To create the **SDS NOAM-A** network element, using the XML file, perform the following steps:

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



   b. Click **Browse** and type the pathname of the NOAM network XML file.



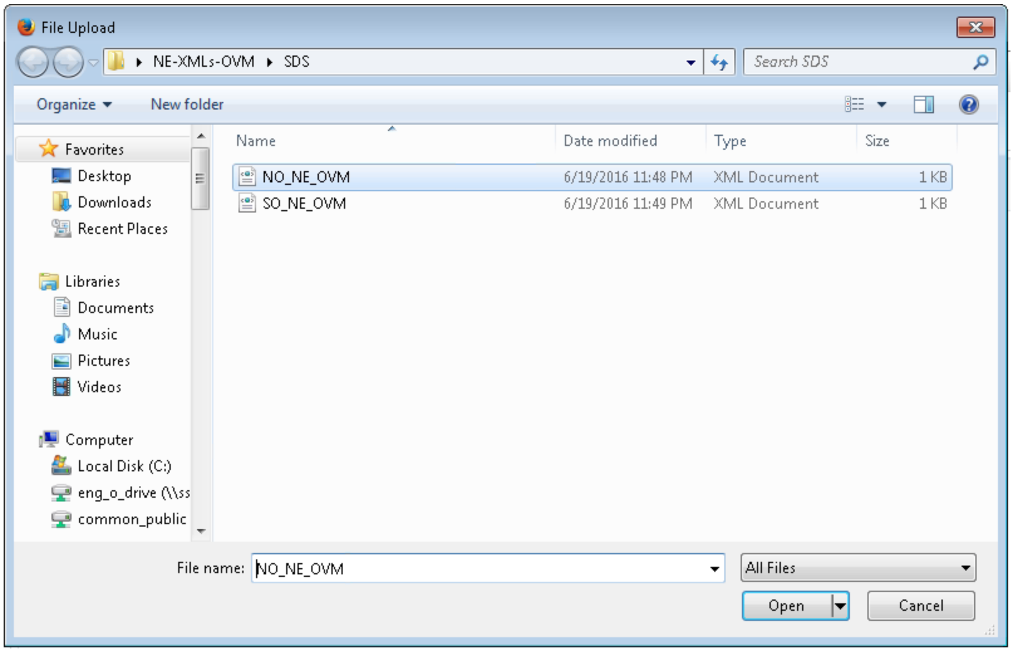
To create a new Network Element, upload a valid configu

No file selected.

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights

> **Note:**
>
> This step assumes that the XML files were previously prepared as described in Creating an XML file for Installing SDS Network Elements.

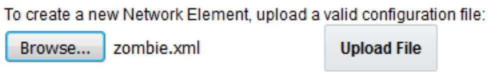
c. Select the location of the XML file and click **Open**.



Name	Date modified	Type	Size
NO_NE_OVM	6/19/2016 11:48 PM	XML Document	1 KB
SO_NE_OVM	6/19/2016 11:49 PM	XML Document	1 KB

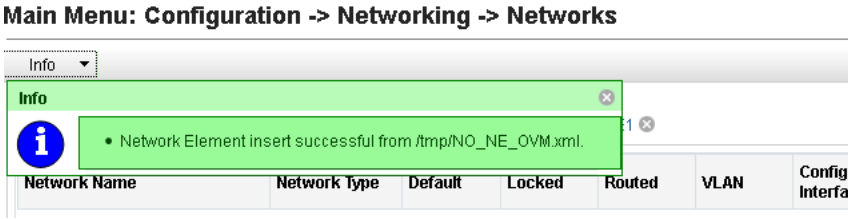
File name: NO_NE_OVM

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


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

zombie.xml

If the values in the XML file pass, an information banner displays.


Main Menu: Configuration -> Networking -> Networks

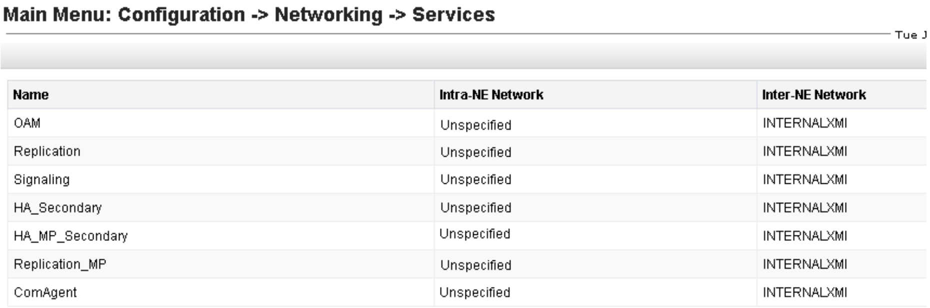
- Network Element insert successful from /tmp/NO_NE_OVM.xml.

Network Name	Network Type	Default	Locked	Routed	VLAN	Config Interfa

> **Note:**
>
> Left-click on the Info banner to display the banner.

4. To map services to networks, perform the following steps:

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



Main Menu: Configuration -> Networking -> Services

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

b. Click **Edit**.

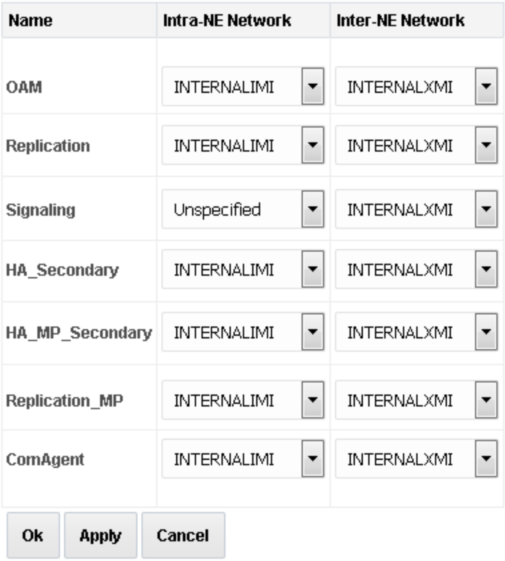
c. Set the services as shown in the table below:

Table 3-1 Services - IMI and XMI Network

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

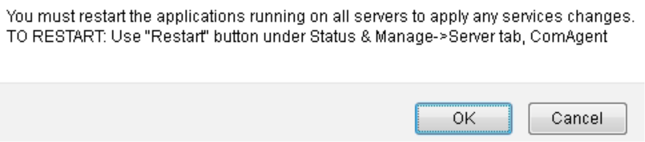
For example: If your IMI network is named IMI and your XMI network is named XMI, then your services configuration should look like the following:

Figure 3-1 Example for Services Configuration



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

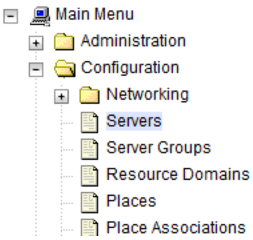
d. Click **OK** to apply the Service-to-Network selections. Dismiss any popup notifications.



You must restart the applications running on all servers to apply any services changes.
TO RESTART: Use "Restart" button under Status & Manage->Server tab, ComAgent

5. To insert the 1st VM, perform the following steps:

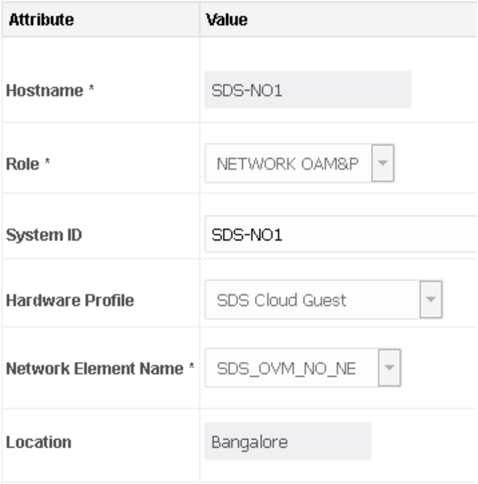
   a. Navigate to **Configuration > Servers**.



   b. To insert the new NOAM server into either the server or first server’s table, click **Insert**.

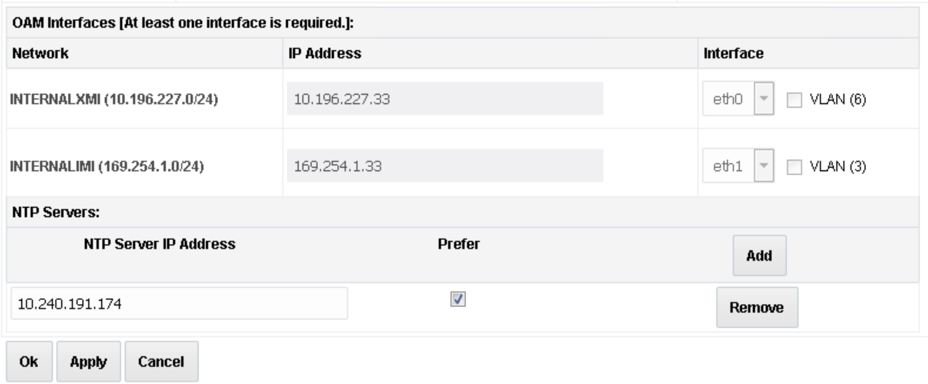
   c. Configure the following fields with these values:

      - **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



Attribute	Value
Hostname *	SDS-NO1
Role *	NETWORK OAM&P
System ID	SDS-NO1
Hardware Profile	SDS Cloud Guest
Network Element Name *	SDS_OVM_NO_NE
Location	Bangalore

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



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

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.33	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.33	eth1 □ VLAN (3)

NTP Servers:

NTP Server IP Address	Prefer	
10.240.191.174	☑	Remove

d. Enter the server IP addresses for the XMI network, select **ethX** for the interface and leave the **VLAN** checkbox unchecked.

e. Enter the server IP addresses for the IMI network, select **ethX** for the interface and leave the **VLAN** checkbox unchecked.

> **Note:**
>
> For OpenStack, these IP addresses must be the addresses used during instance booting and networking.

f. Add the following NTP servers:

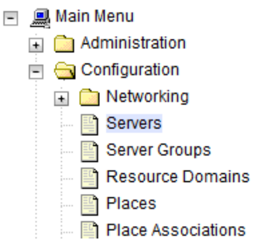
NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server (Optional)	No
Valid NTP Server (Optional)	No

g. Optionally, mark the Prefer checkbox to prefer one server over the other.

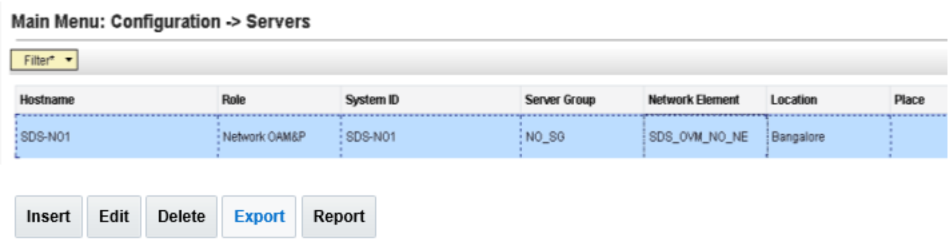
h. Click **OK**, post entering all the server data.

6. To export the initial configuration, perform the following steps:

a. Navigate to **Configuration > Servers**.



b. From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server. Navigate to the Info tab to verify if the file has been created.



Main Menu: Configuration -> Servers

Hostname	Role	System ID	Server Group	Network Element	Location	Place
SDS-NO1	Network OAM&P	SDS-NO1	NO_SG	SDS_OVM_NO_NE	Bangalore	

7. To copy server configuration file to `/var/tmp` directory, perform the following steps:
   a. Obtain a terminal window to the **SDS NOAM-A** server, logging in as the admusr user.
   b. 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`.
      For 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.
> 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.
>
> > **Note:**
> >
> > If you are on the console, wait to be prompted to reboot the server. 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. To set the time zone, which is optional, and reboot the server, perform the following steps:

   a. To change the system time zone, from the command line prompt, run `set_ini_tz.pl`. The following command example uses the **America/New_York** time zone.

   ```
   $ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York"
   >/dev/null 2>&1
   $ sudo init 6
   ```

   b. 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.
   Wait for server to reboot.

9. To verify server health, perform the following steps:

   a. Log into the NOAM1 as the **admusr** user.

b. Run the following command on the 1st NOAM server and ensure 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
```

c. Exit from the command line to return to the server console.

```
$ exit
sds-mrsvnc-a login:
```

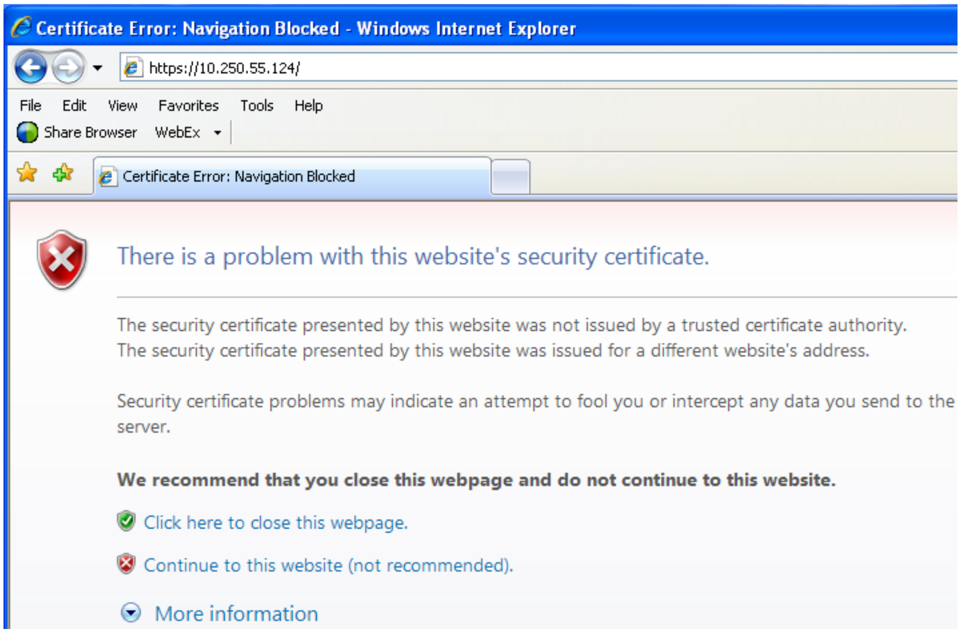
10. To configure **DR SDS NOAM-B**, repeat the above Step 5 to Step 10 of this procedure in **SDS NOAM-B**.

3.2 OAM Pairing (1st SDS NOAM Site Only)

Configuring the SDS Server Group:

1. 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)**.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

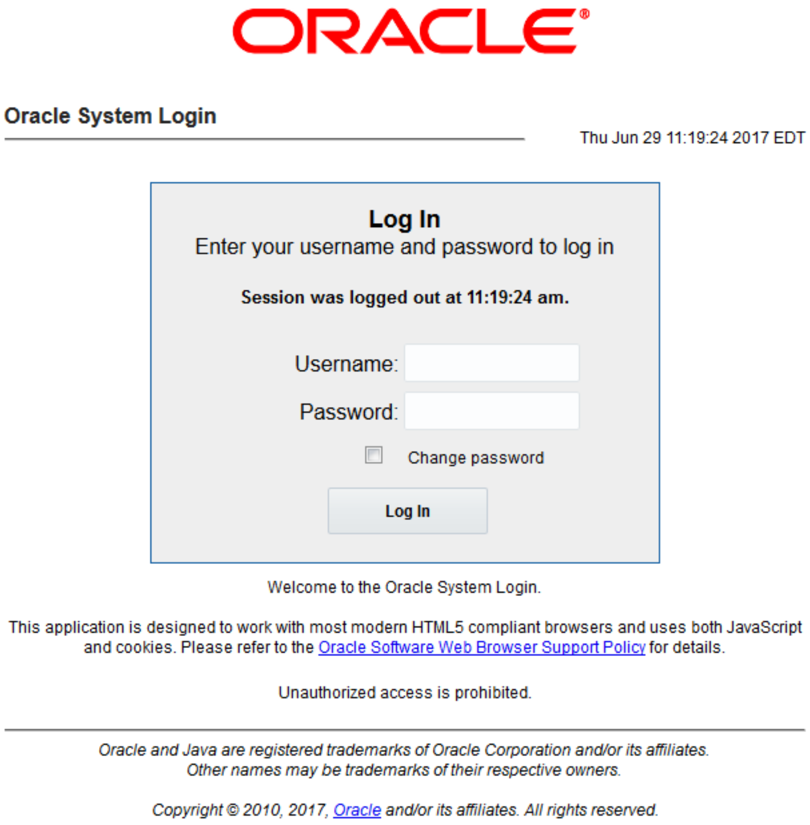
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login to SDS NOAM-A, establish a GUI session as the guiadmin user on the NOAM-A server.



ORACLE®

Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In

Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

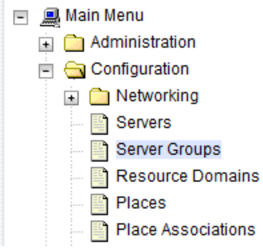
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To enter group data in SDS NOAM-A, perform the following steps:

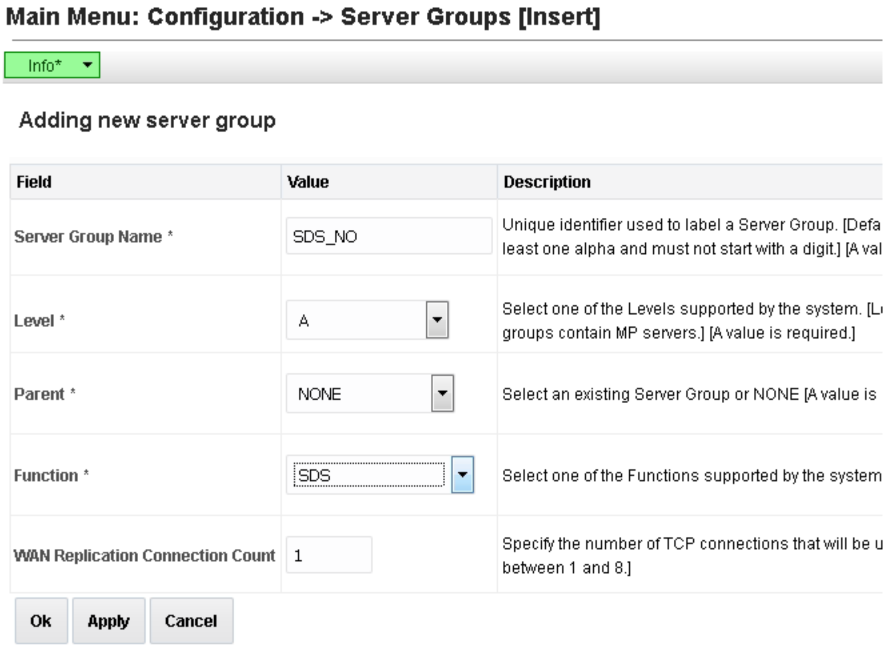
   a. Navigate to **Configuration > Server Groups**.



   b. 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]

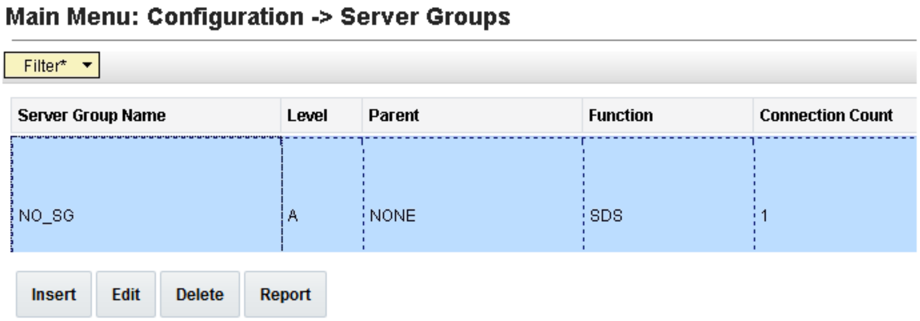
Adding new server group

Field	Value	Description
Server Group Name *	SDS_NO	Unique identifier used to label a Server Group. [Defa least one alpha and must not start with a digit.] [A val
Level *	A	Select one of the Levels supported by the system. [L groups contain MP servers.] [A value is required.]
Parent *	NONE	Select an existing Server Group or NONE [A value is
Function *	SDS	Select one of the Functions supported by the system
WAN Replication Connection Count	1	Specify the number of TCP connections that will be u between 1 and 8.]

c. Click **OK** when all fields are configured.

4. To add server to OAM Server Group, in **SDS NOAM-A** perform the following steps:

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

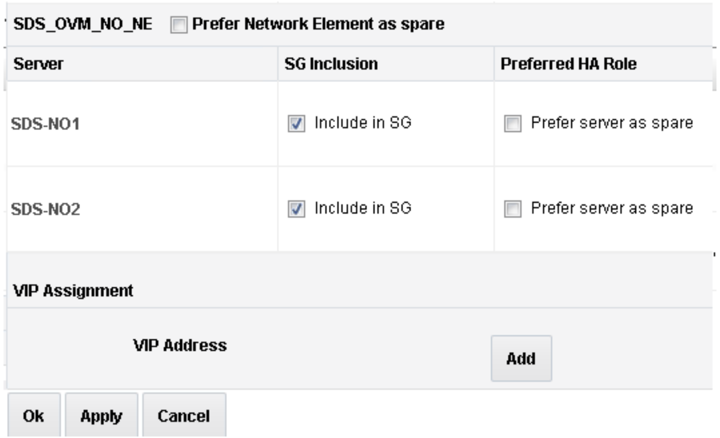


Main Menu: Configuration -> Server Groups

Server Group Name	Level	Parent	Function	Connection Count
NO_SG	A	NONE	SDS	1

   b. In the portion of the screen that lists the servers for the server group, find the SDS-NOAM servers being configured.

   c. Select **Include in SG** checkbox.



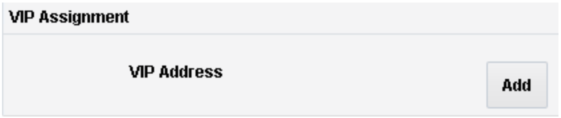
SDS_OVM_NO_NE ☐ Prefer Network Element as spare

Server	SG Inclusion	Preferred HA Role
SDS-NO1	☑ Include in SG	☐ Prefer server as spare
SDS-NO2	☑ Include in SG	☐ Prefer server as spare

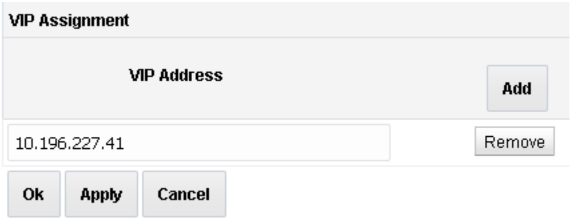
d. Click **Apply**.

5. To add VIP address, in **SDS NOAM-A** perform the following steps:

   a. Click **Add**.



   b. Enter the IP address in the textbox under **VIP Address** and click **Apply**.

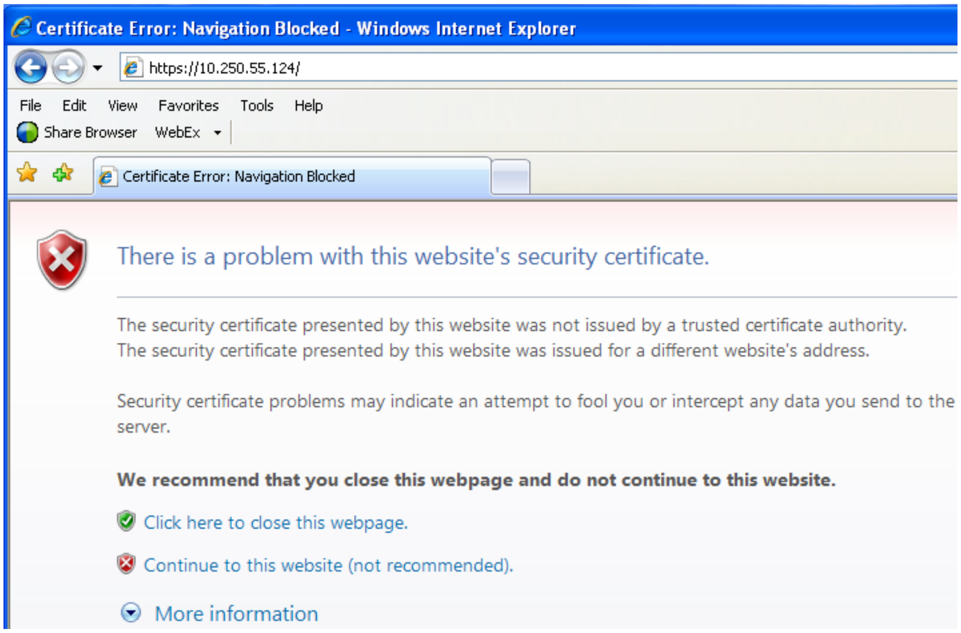


10.196.227.41

   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. 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).**



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

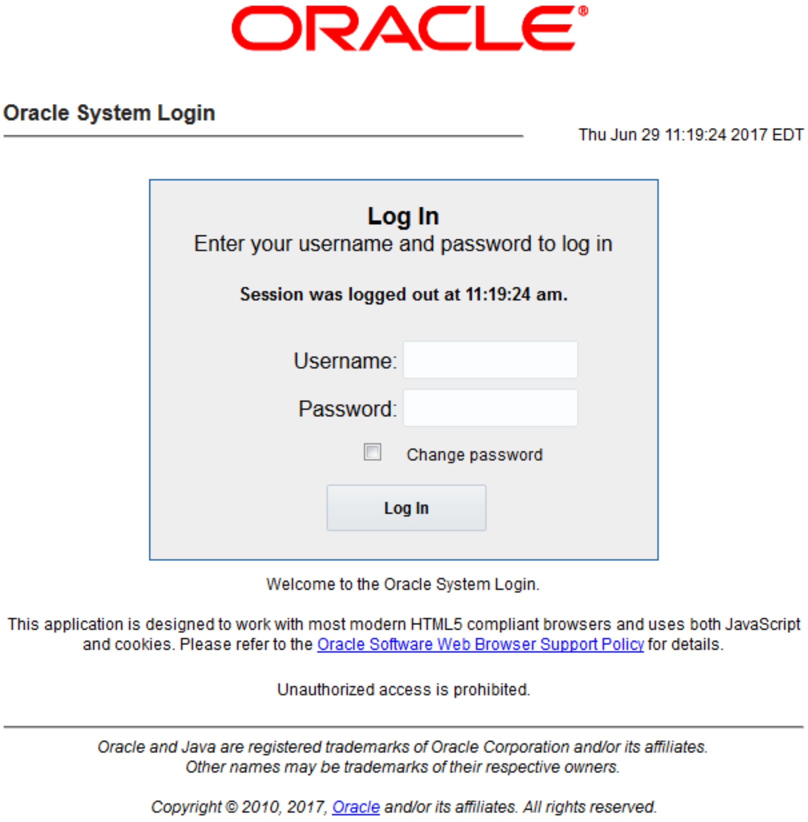
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

7. To login to **SDS VIP**, establish a GUI session as the guiadmin user on the NOAM-A server by using the XMI IP address.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:
Password:
□ Change password

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

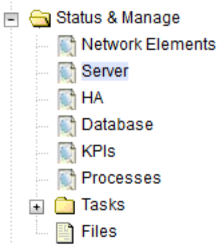
Unauthorized access is prohibited.

*Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.*

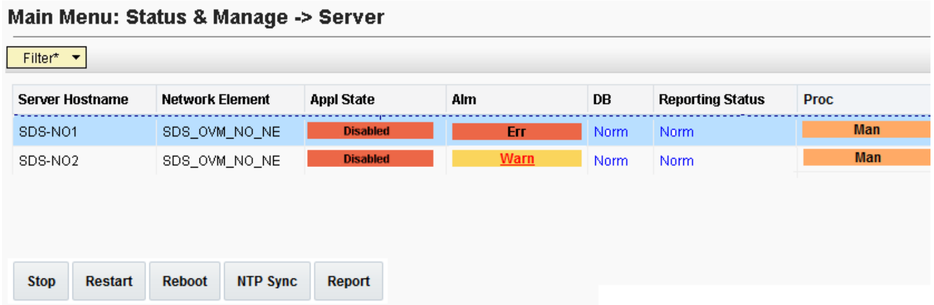
Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

8. To verify and restart the servers, in **SDS VIP** perform the following steps:

a. Navigate to **Status & Manage > Server**.



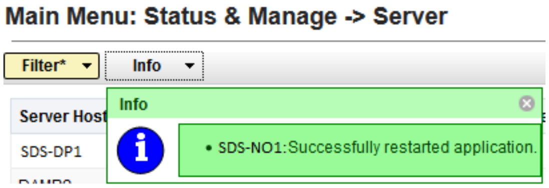
b. Verify if the DB status is **Norm** and the Proc status is **Man**.


Main Menu: Status & Manage -> Server

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Disabled	Err	Norm	Norm	Man
SDS-NO2	SDS_OVM_NO_NE	Disabled	Warn	Norm	Norm	Man

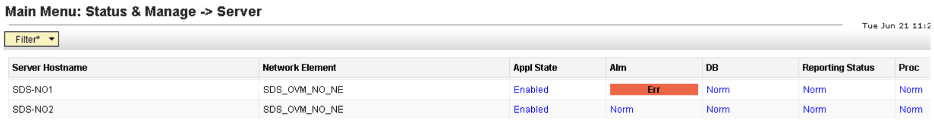
c. Select the **SDS NOAM-A** server and click **Restart**.

d. Click **OK** on the confirmation screen.
A confirmation banner displays.


Main Menu: Status & Manage -> Server

- SDS-NO1:Successfully restarted application.

e. Verify if the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.


Main Menu: Status & Manage -> Server

Tue Jun 21 11:2

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Enabled	Err	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm

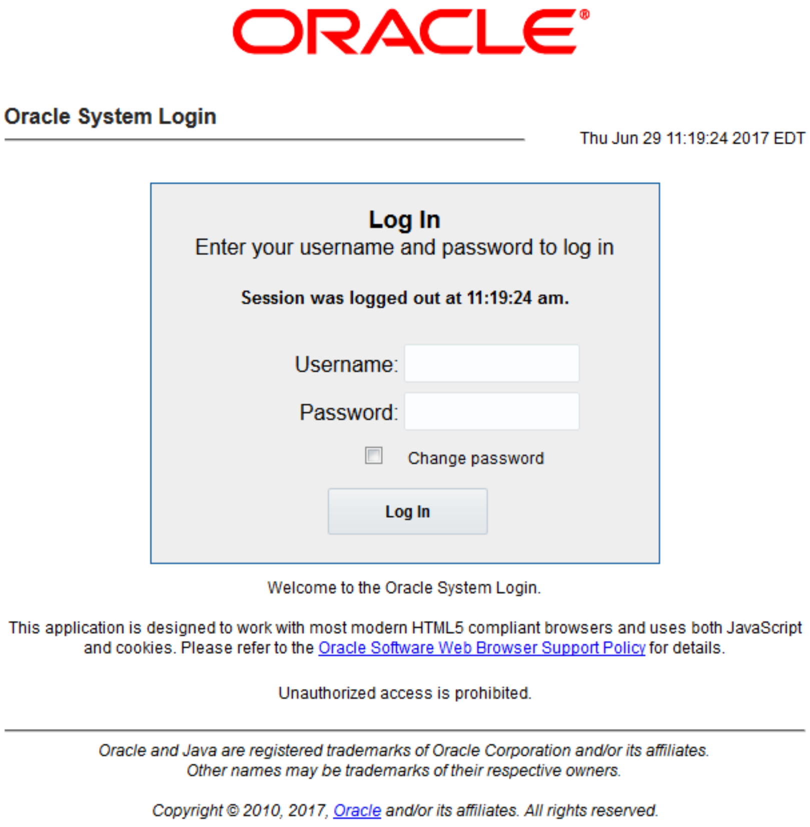
> **Note:**
>
> To refresh the server status screen before the 15-30 second default, navigate to the **Status & Manage > Server** screen again.

9. To configure **SDS NOAM-B**, repeat the above 8 steps in **SDS NOAM-B**.

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).

Verifying SDS Server Alarm Status

1. To establish GUI session on the NOAM VIP, use the NOAM VIP address and login as the **guiadmin** user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

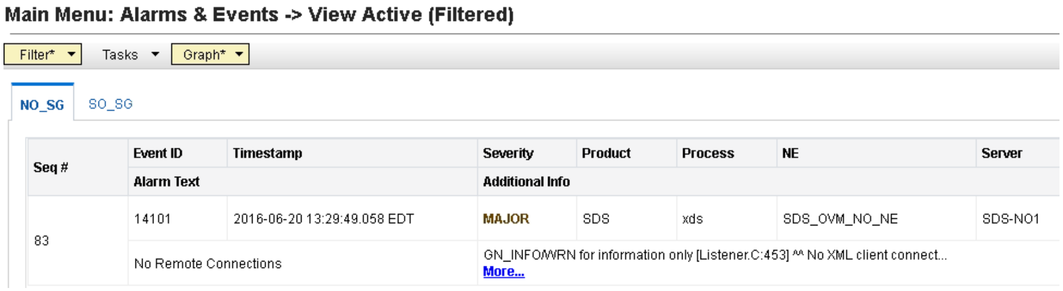
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

Wait for remote database alarm to clear.

2. Navigate to **Alarms & Events > View Active**.
3. Verify if event ID **14101**, which has no remote connections, is the only alarm present on the system at the time.

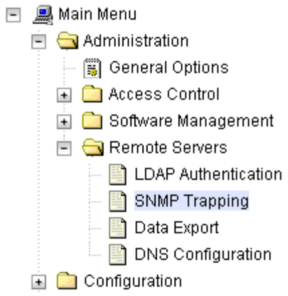


Main Menu: Alarms & Events -> View Active (Filtered)

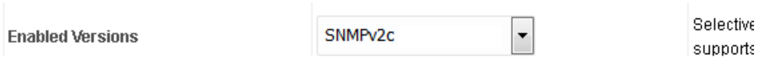
Seq #	Event ID	Timestamp	Severity	Product	Process	NE	Server
	Alarm Text		Additional Info				
83	14101	2016-06-20 13:29:49.058 EDT	MAJOR	SDS	xds	SDS_OVM_NO_NE	SDS-NO1
	No Remote Connections		GN_INFO/WRN for information only [Listener.C:453] ^^ No XML client connect... More...				

Configuring SNMP for Traps from Individual Servers

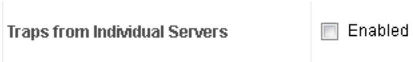
1. To establish GUI session on the NOAM VIP, use the NOAM VIP address and login as the **guiadmin** user.
2. In SDS VIP, navigate to SNMP Trapping screen and perform the following steps:
   a. Navigate to **Administration > Remote Servers > SNMP Trapping**.



   b. Click **Insert**.
   c. Change the Enabled Versions to **SNMPv2c**.


Enabled Versions: SNMPv2c

   d. Mark the Traps from Individual Servers checkbox as **Enabled**.


Traps from Individual Servers: □ Enabled

   e. Click **OK**.

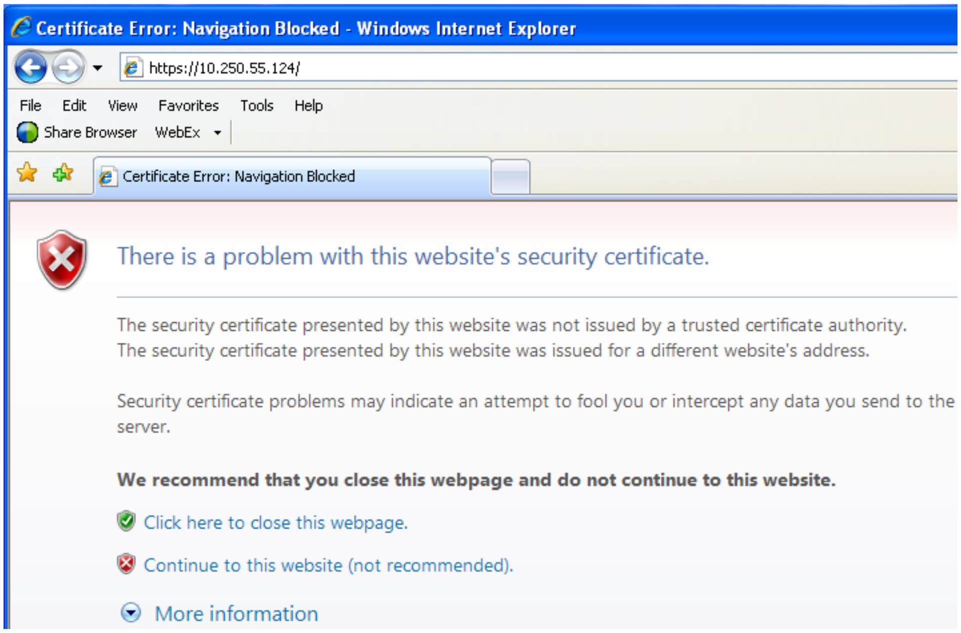
3.3 Query Server Installation (All SDS NOAM Sites)

During the Query Server installation procedure, various errors are displayed at different stages of the procedure. While running a step, ignore errors related to values other than those referenced by that step.
Configuring Query Server (All SDS NOAM Sites)

Perform the following steps in **Active SDS VIP**:

1. Launch a web browser and connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

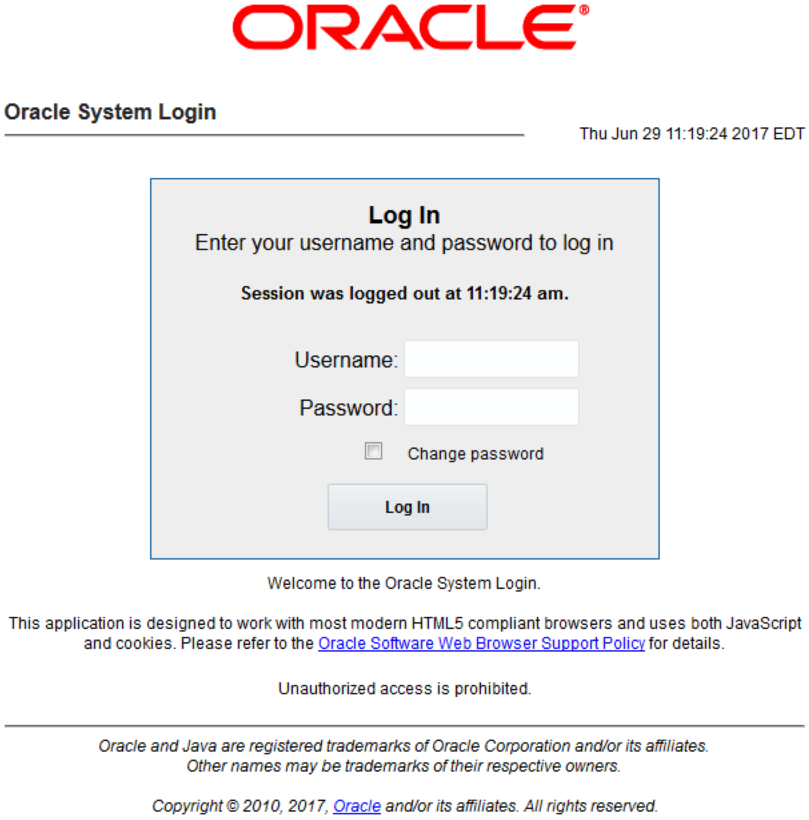
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login, establish a GUI session as the default user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In

Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Welcome to the Oracle System Login.

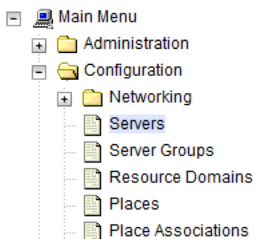
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

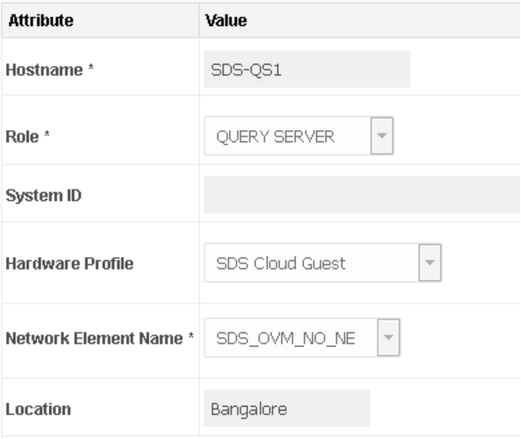
3. To configure Query server, perform the following steps:
   a. Navigate to **Configuration** and click **Servers**.



b. Click **Insert** to insert the new NOAM server into the server or first server's table.

c. Fill in the fields as follows:

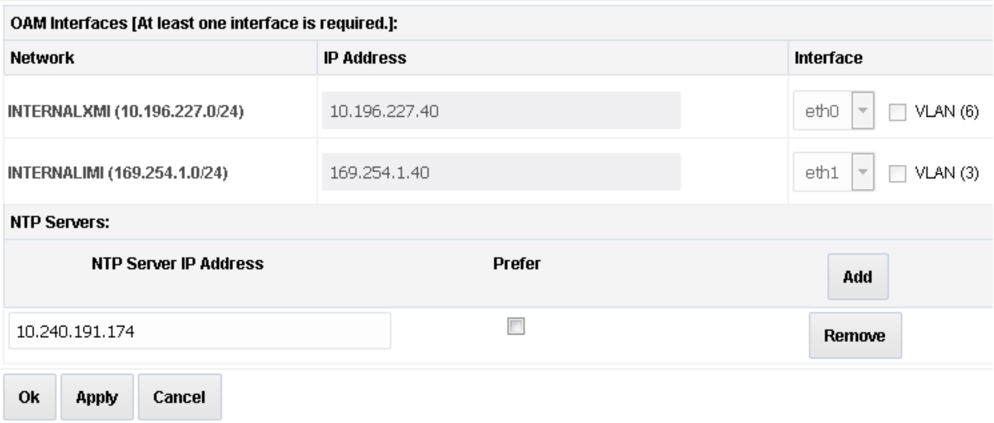
   - **Hostname:** Assigned Hostname
   - **Role:** Query Server
   - **System ID:** Leave Blank
   - **Hardware Profile:** SDS Cloud Guest
   - **Network Element Name:** [Select NE from list where Query server is physically located]
   - **Location:** Optional



Attribute	Value
Hostname *	SDS-QS1
Role *	QUERY SERVER
System ID	
Hardware Profile	SDS Cloud Guest
Network Element Name *	SDS_OVM_NO_NE
Location	Bangalore

4. Insert the Query server.

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



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

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.40	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.40	eth1 □ VLAN (3)

NTP Servers:

NTP Server IP Address	Prefer	Add
10.240.191.174	□	Remove

a. Enter the server IP addresses for the XMI network, select **ethX** for the interface and retain the **VLAN** checkbox unchecked.

b. Enter the server IP addresses for the IMI network, select **ethX** for the interface and retain the **VLAN** checkbox unchecked.

> **Note:**
>
> For OpenStack, use the IP addresses used during instance booting and networking.

c. Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server (Optional)	No
Valid NTP Server (Optional)	No

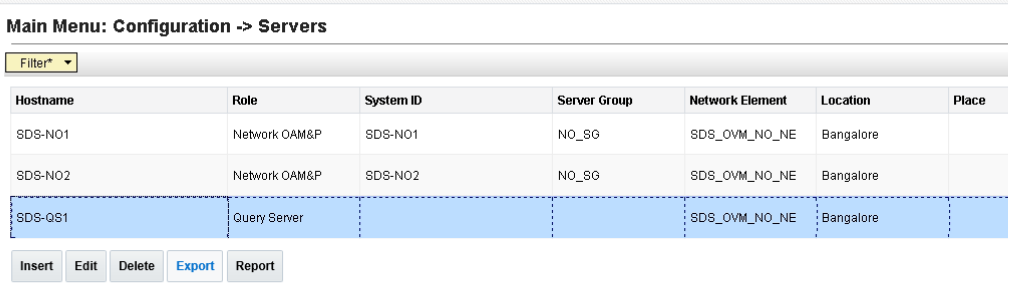
d. Optionally, mark the Prefer checkbox to prefer one server over the other.

e. Click **OK**, once all the server data is entered.

5. To export the initial configuration, perform the following steps:

a. From the GUI screen, select **SDS** server.

b. Click **Export**, to generate the initial configuration data for that server.



Main Menu: Configuration -> Servers

Hostname	Role	System ID	Server Group	Network Element	Location	Place
SDS-NO1	Network OAM&P	SDS-NO1	NO_SG	SDS_OVM_NO_NE	Bangalore	
SDS-NO2	Network OAM&P	SDS-NO2	NO_SG	SDS_OVM_NO_NE	Bangalore	
SDS-QS1	Query Server			SDS_OVM_NO_NE	Bangalore	

c. Navigate to the **Info** tab to confirm that the file is created.

6. To copy server configuration file to `/var/tmp` directory, perform the following steps:

   a. Obtain a terminal window to the active **SDS VIP** server, login as the **admusr** user.

   b. 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`.
      For 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 runs 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.
      >   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 process can take anywhere from 3 up to 20 minutes to complete.
      > - If you are on the console, wait to be prompted to reboot the server. Do not reboot the server. It is rebooted later in this procedure.

7. Verify the script run is completed successfully by checking the following file:

   ```
   $ cat /var/TKLC/appw/logs/Process/install.log
   ```

> **Note:**
>
> Ignore the warning to remove the USB key as no USB key is present. No response is received until the reboot prompt is issued.

8. Set the time zone (optional) and reboot the server by performing the following steps:
   a. To change the system time zone from the command line prompt, run `set_ini_tz.pl`. The following command example uses the America/New_York time zone.

   ```
   $ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/
   null 2>&1
   $ sudo init 6
   ```

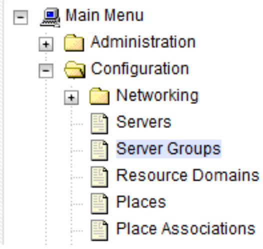
   b. Set the time zone as per the installation requirement. Refer to List of Frequently Used Time Zones.
   Wait for server to reboot.
9. To verify server health, perform the following steps:
   a. Log into the NOAM1 as the **admusr** user.
   b. Run the following command on the first NOAM server and ensure no there are no error responses:

   ```
   $ 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
   ```

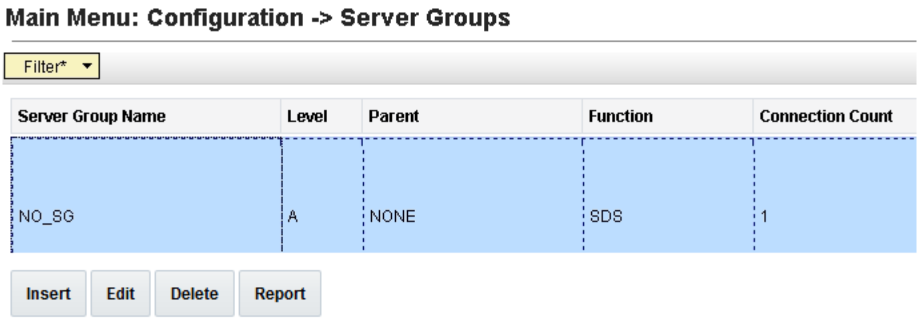
Adding Query Server to the SDS Server Group

Perform the following steps in **Active SDS VIP**:

1. To add server to OAM Server Group, perform the following steps:
   a. Navigate to **Configuration** and click **Server Groups**.



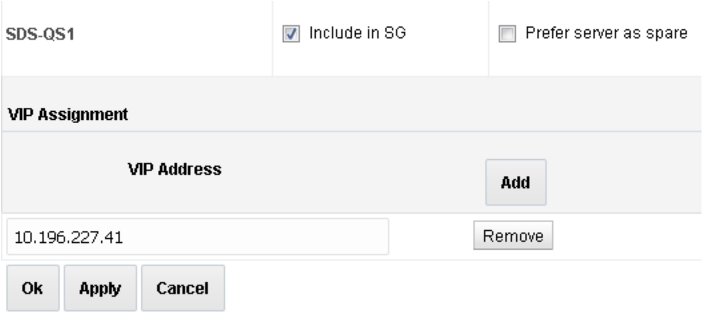
b. Select the new server group and click **Edit**.



Main Menu: Configuration -> Server Groups

Server Group Name	Level	Parent	Function	Connection Count
NO_SG	A	NONE	SDS	1

c. In the window where the servers for the server group are listed, find the Query server being configured and select **Include in SG** checkbox.



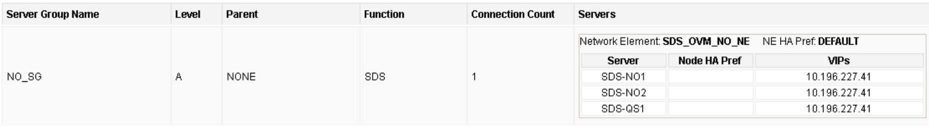
SDS-QS1 ☑ Include in SG □ Prefer server as spare

VIP Assignment

VIP Address: 10.196.227.41

d. Retain all other boxes unchecked.

e. Click **OK**.
Wait for process to complete.



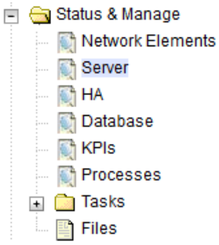
Server Group Name	Level	Parent	Function	Connection Count	Servers
NO_SG	A	NONE	SDS	1	Network Element: **SDS_OVM_NO_NE** NE HA Pref: **DEFAULT**

Server	Node HA Pref	VIPs
SDS-NO1		10.196.227.41
SDS-NO2		10.196.227.41
SDS-QS1		10.196.227.41

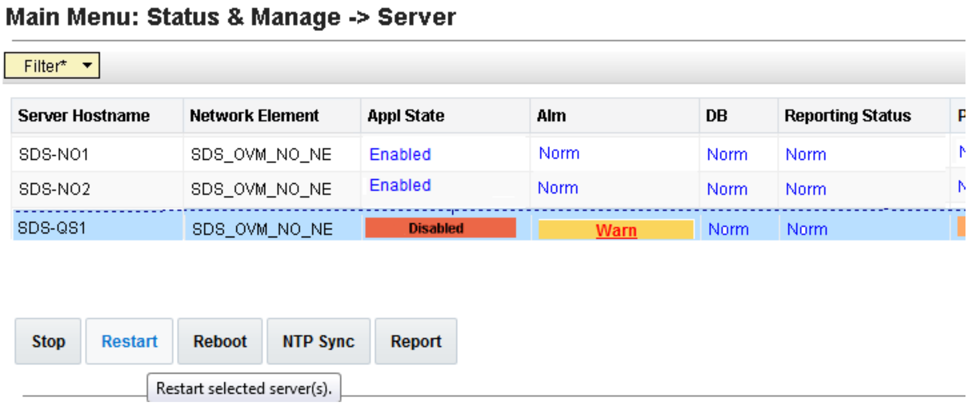
This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The server establishes DB replication with the active SDS server.

2. To verify and restart the servers, perform the following steps:

a. Navigate to **Status & Manage** and click **Server**.



b. Verify if the `DB status` is **Norm** and the `Proc status` is **Man**.

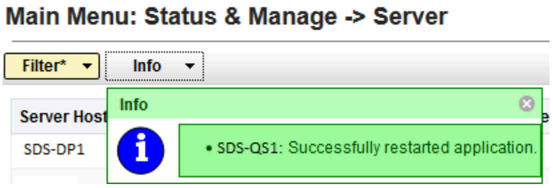


Main Menu: Status & Manage -> Server

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	P
SDS-NO1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	N
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	N
SDS-QS1	SDS_OVM_NO_NE	Disabled	Warn	Norm	Norm	

c. Select the Query server and click **Restart**.

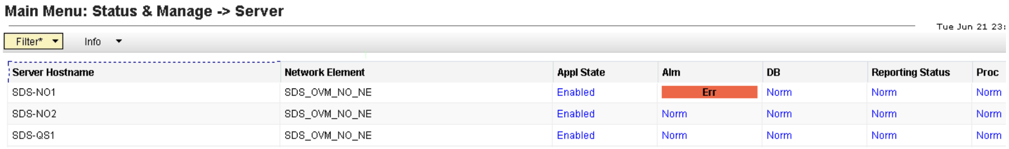
d. Click **OK** on the confirmation screen.
A confirmation banner displays.



Main Menu: Status & Manage -> Server

• SDS-QS1: Successfully restarted application.

e. Verify the `Appl state` is **Enabled** and the `Alm`, `DB`, `Reporting Status`, and `Proc` is **Norm**.



Main Menu: Status & Manage -> Server

Tue Jun 21 23:

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Enabled	Err	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-QS1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm

> **Note:**
>
> To refresh the server status screen before the 15-30 second default, navigate to **Status & Manage** and click **Server screen** again.

3.4 OAM Installation for DR SDS NOAM Site (Optional)

Pre-requisites:

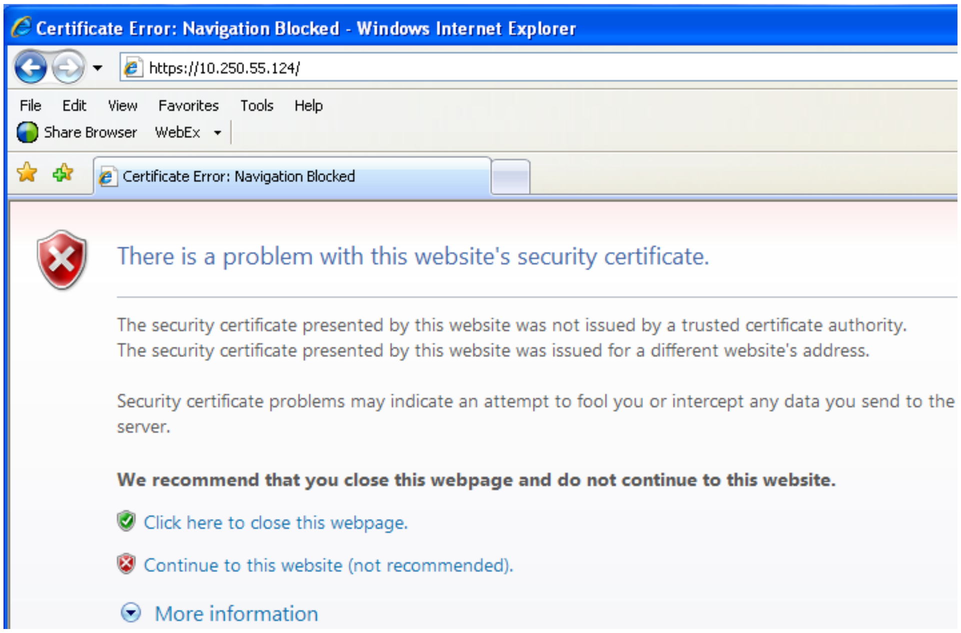
- Ensure the SDS Network Element XML file for Disaster Recovery Provisioning SDS site has been created as described in Creating an XML file for Installing SDS Network Elements.
- All the Network Element XML files are on the laptop’s hard drive.

- Ensure an established connection is present to the SDS GUI before configuring the first SDS server.

Configuring DR NOAM Servers (DR SDS NOAM Site Only)
Perform the following steps in **DR SDS NOAM-A**:

1. Launch a web browser and connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File
Edit
View
Favorites
Tools
Help
Share Browser
WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

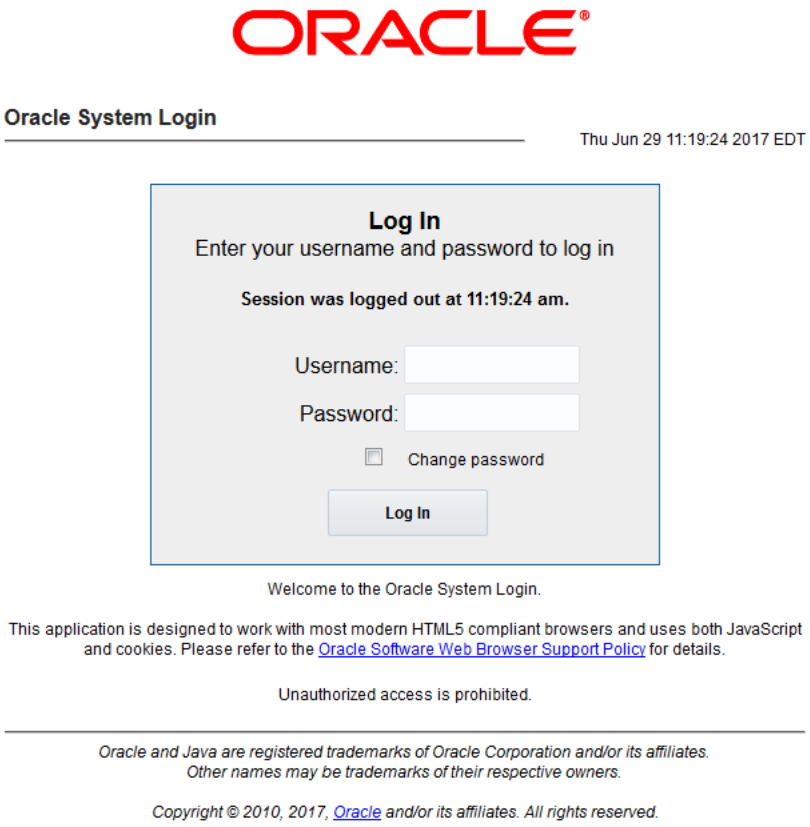
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login, establish a GUI session as the **guiadmin** user on the NOAM-A server.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In

Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

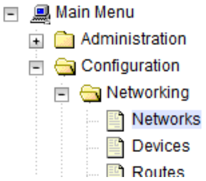
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

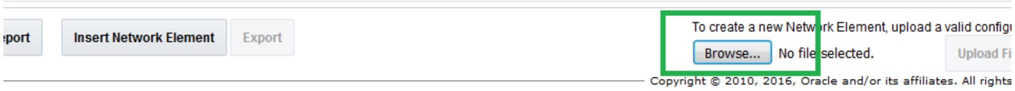
Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To create the SDS VIP network element using the XML file, perform the following steps:

   a. Navigate to **Configuration**, select **Networking**, and click **Networks**.



   b. Click **Browse** and enter pathname of the NOAM network XML file.



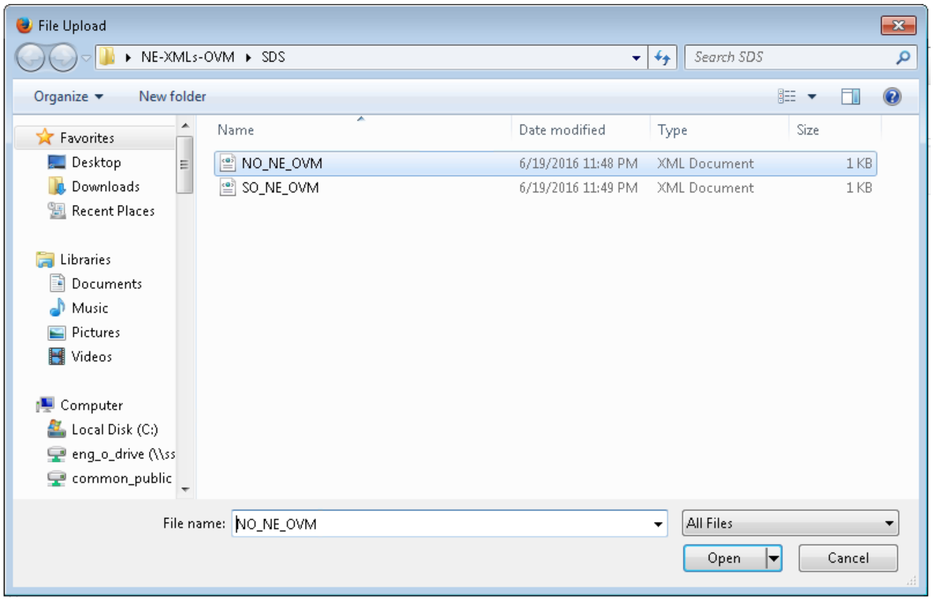
To create a new Network Element, upload a valid configu

No file selected.

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights

> **Note:**
>
> This step assumes that the XML files were previously prepared as described in Appendix A Creating an XML file for Installing SDS Network Elements.

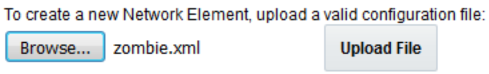
   c. Select the location of the XML file and click **Open**.



Name	Date modified	Type	Size
NO_NE_OVM	6/19/2016 11:48 PM	XML Document	1 KB
SO_NE_OVM	6/19/2016 11:49 PM	XML Document	1 KB

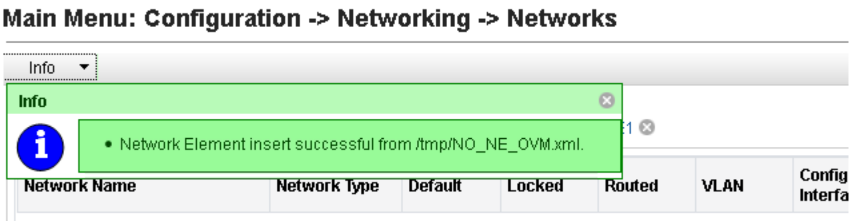
File name: NO_NE_OVM

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



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

If the values in the XML file pass, an information banner displays.



Main Menu: Configuration -> Networking -> Networks

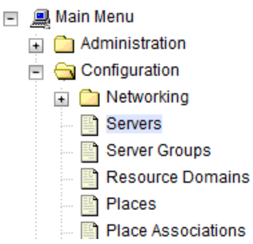
- Network Element insert successful from /tmp/NO_NE_OVM.xml.

Network Name	Network Type	Default	Locked	Routed	VLAN	Config Interfa

> **Note:**
>
> Left-click on the Info banner to display the banner.

4. To insert the DR NOAM-A and DR NOAM-B servers, perform the following steps:

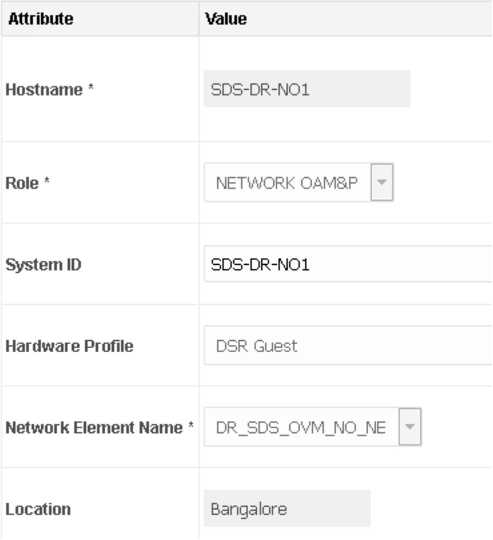
a. Navigate to **Configuration** and select **Servers**.



b. To insert the new NOAM server into the the server or first servers table, click **Insert**.

c. Fill in the fields as follows:

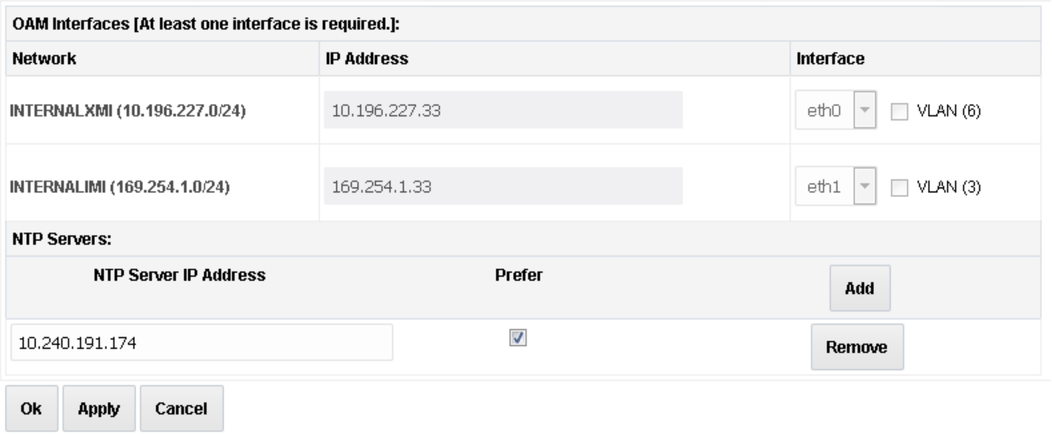
- **Hostname:** Assigned Hostname
- **Role:** NETWORK OAM&P
- **System ID:** Assigned Hostname
- **Hardware Profile:** SDS Cloud Guest
- **Network Element Name:** [Select NE from list]
- **Location:** Optional



Attribute	Value
Hostname *	SDS-DR-NO1
Role *	NETWORK OAM&P
System ID	SDS-DR-NO1
Hardware Profile	DSR Guest
Network Element Name *	DR_SDS_OVM_NO_NE
Location	Bangalore

5. To insert the first VM, perform the following steps:

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



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

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.33	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.33	eth1 □ VLAN (3)

NTP Servers:

NTP Server IP Address	Prefer	Add
10.240.191.174	☑	Remove

a. Enter the server IP addresses for the XMI network, select **ethX** for the interface and retain the **VLAN** checkbox unchecked.

b. Enter the server IP addresses for the IMI network, select **ethX** for the interface and retain the **VLAN** checkbox unchecked.

> **Note:**
>
> For OpenStack, use the IP addresses used during instance booting and networking.

c. Click **Add** in the NTP server's box.

d. Add the following NTP servers:

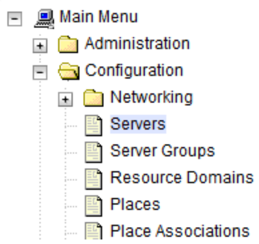
NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server (Optional)	No
Valid NTP Server (Optional)	No

e. Optionally, mark the Prefer checkbox to prefer one server over the other.

f. Click **OK**, once entering all the server data is completed.

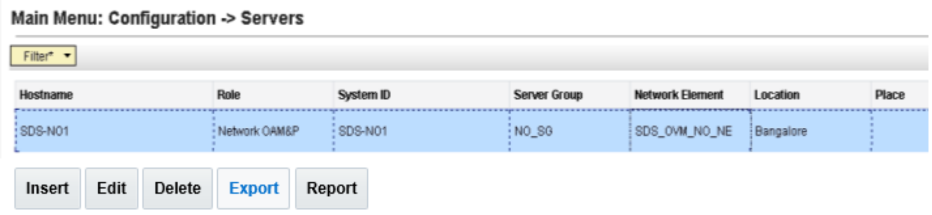
6. To export the initial configuration, perform the following steps:

a. Navigate to **Configuration**, and select **Servers**.



b. From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server.

c. Navigate to the **Info** tab to confirm the file is created.


Main Menu: Configuration -> Servers

Hostname	Role	System ID	Server Group	Network Element	Location	Place
SDS-N01	Network OAM&P	SDS-N01	NO_SG	SDS_OVM_NO_NE	Bangalore	

7. To copy server configuration file to `/var/tmp` directory, perform the following steps:

a. Obtain a terminal window to the SDS NOAM-A server, logging in as the **admusr** user.

b. 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`.
For 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 runs 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.

Wait for configuration to complete.

The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory. It implements the configuration in the file and prompts the user to reboot the server.

A broadcast message is sent to the terminal. This process can take anywhere from 3 up to 20 minutes to complete.

If you are on the console, wait to be prompted to reboot the server. Do not reboot the server. It is rebooted later in this procedure.

8. Verify if the script is 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. To verify server health, perform the following steps:

   a. Log into the NOAM1 as the **admusr** user.

b. Run the following command on the first NOAM server and ensure 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
```

c. Exit from the command line to return to the server console.

```
$ exit
sds-mrsvnc-a login:
```

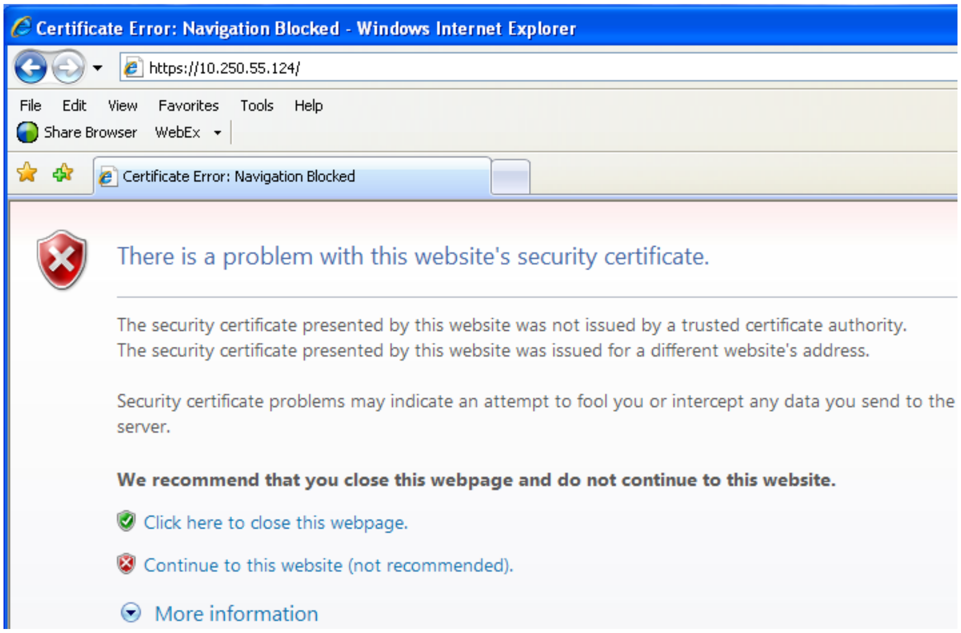
10. To configure DR SDS NOAM-B, repeat the above steps from Step 3 to Step 9 of this procedure, in **DR SDS NOAM-B**.

3.5 OAM Pairing for DR SDS NOAM Site (Optional)

During the OAM pairing procedure, various errors may display at different stages of the procedure. While executing a step, ignore errors related to values other than those referenced by that step.
Pairing the DR OAM Servers (DR SDS NOAM Site Only)

1. To launch a web browser, in **Primary SDS VIP**, connect to the XMI virtual IP address assigned to Primary SDS NOAM-A site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

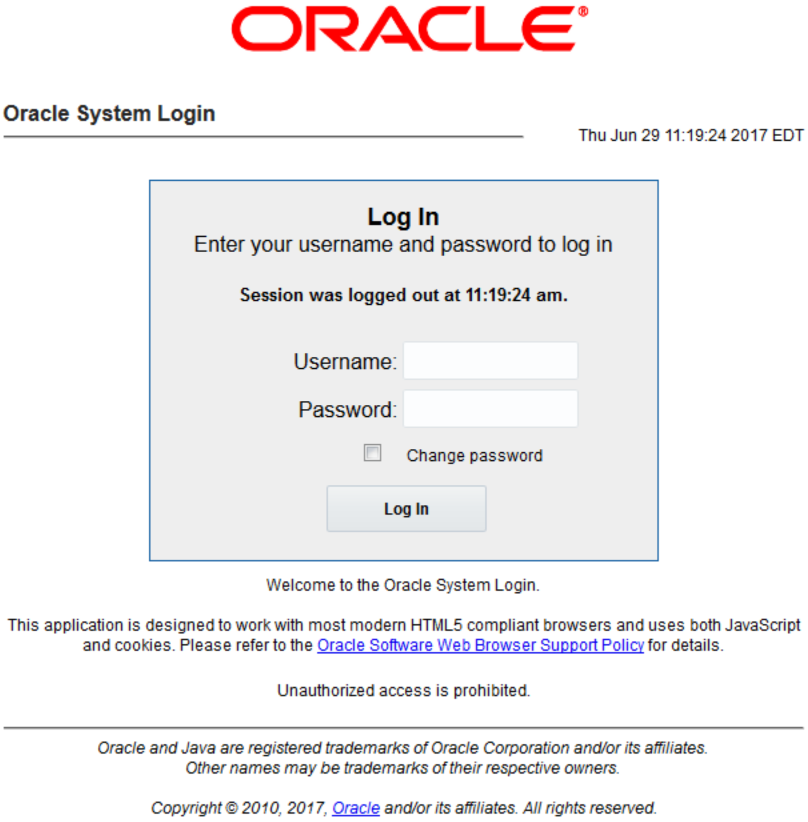
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login, in **Primary SDS VIP**, establish a GUI session as the default user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

□ Change password

Welcome to the Oracle System Login.

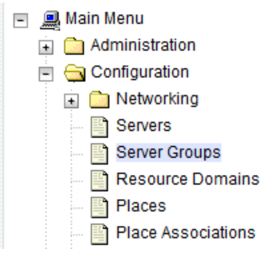
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

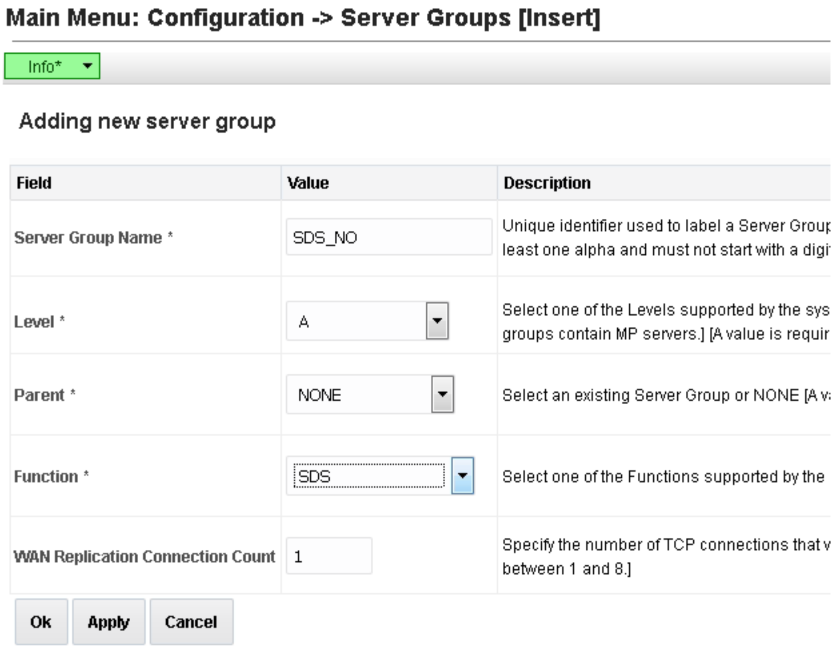
3. To enter group data, in **DR SDS NOAM-A**, perform the following steps:
   a. Navigate to **Configuration**, select **Server Groups**.



b. Click **Insert**.

c. Fill in the following fields:

- **Server Group Name:** [Enter DR Server Group Name]
- **Level:** A
- **Parent:** None
- **Function:** SDS
- **WAN Replication Connection Count:** Use Default Value



Main Menu: Configuration -> Server Groups [Insert]

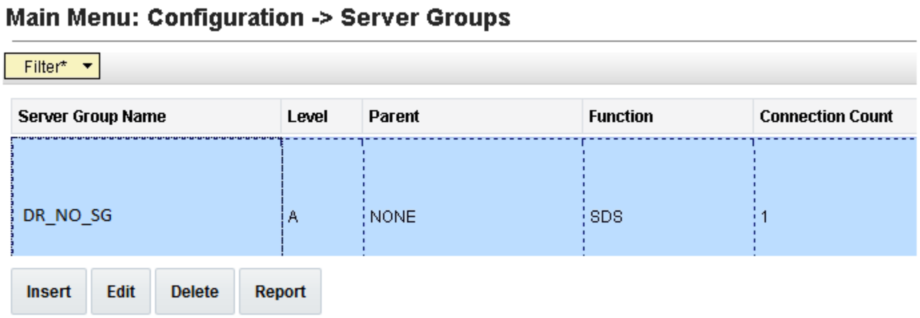
Adding new server group

Field	Value	Description
Server Group Name *	SDS_NO	Unique identifier used to label a Server Grour least one alpha and must not start with a digi
Level *	A	Select one of the Levels supported by the sys groups contain MP servers.] [A value is requir
Parent *	NONE	Select an existing Server Group or NONE [A v
Function *	SDS	Select one of the Functions supported by the
WAN Replication Connection Count	1	Specify the number of TCP connections that v between 1 and 8.]

d. Click **OK**, once all fields are entered.

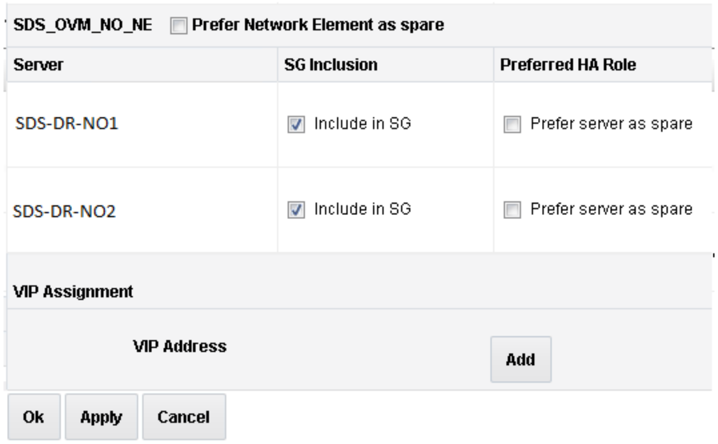
4. To add server to OAM Server Group, in **DR SDS NOAM-A**, perform the following steps:

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



Server Group Name	Level	Parent	Function	Connection Count
DR_NO_SG	A	NONE	SDS	1

b. In the window where the servers for the server group are listed, find the Query server being configured and select **Include in SG** checkbox.



SDS_OVM_NO_NE ☐ Prefer Network Element as spare

Server	SG Inclusion	Preferred HA Role
SDS-DR-NO1	☑ Include in SG	☐ Prefer server as spare
SDS-DR-NO2	☑ Include in SG	☐ Prefer server as spare

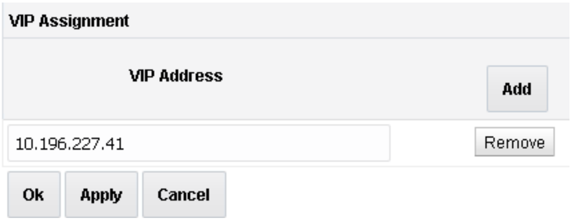
c. Retain other boxes unchecked.

d. Click **Apply**.

5. To add VIP address, in **DR SDS NOAM-A**, perform the following steps:

a. Click **Add**.

b. Enter VIP Address and click **Apply**.

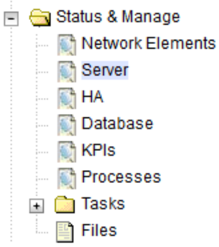


VIP Address: 10.196.227.41

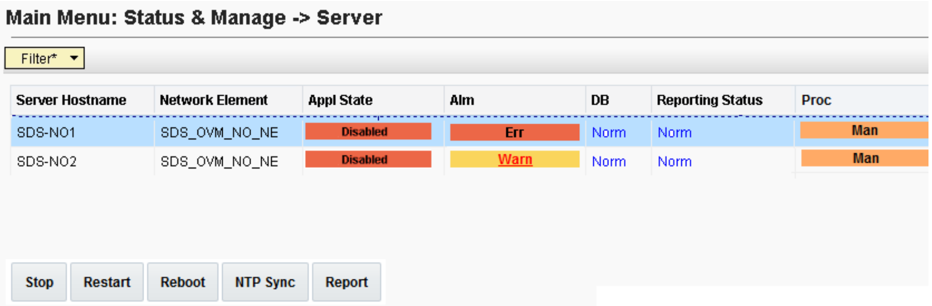
This process takes a minimum duration of five minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/ slave relationship for High Availability (HA).

6. To verify and restart the servers, in **DR SDS VIP**, perform the following steps:

a. Navigate to **Status & Manage**, select **Server**.



b. Verify the DB status is **Norm**, and the Proc status is **Man**.

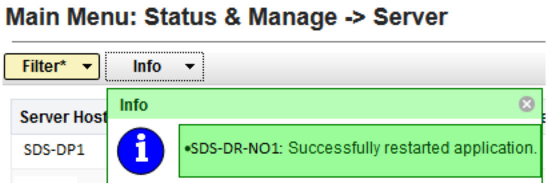


Main Menu: Status & Manage -> Server

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Disabled	Err	Norm	Norm	Man
SDS-NO2	SDS_OVM_NO_NE	Disabled	Warn	Norm	Norm	Man

c. Select the SDS NOAM-A server and click **Restart**.

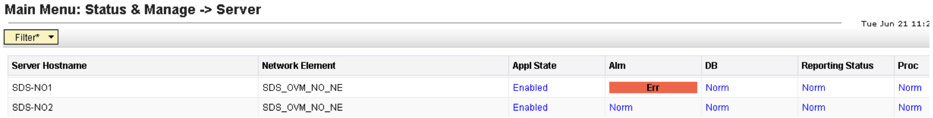
d. Click **OK** on the confirmation screen.
A confirmation banner displays.



Main Menu: Status & Manage -> Server

•SDS-DR-NO1: Successfully restarted application.

e. Verify the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.



Main Menu: Status & Manage -> Server

Tue Jun 21 11:2

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Enabled	Err	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm

Note:

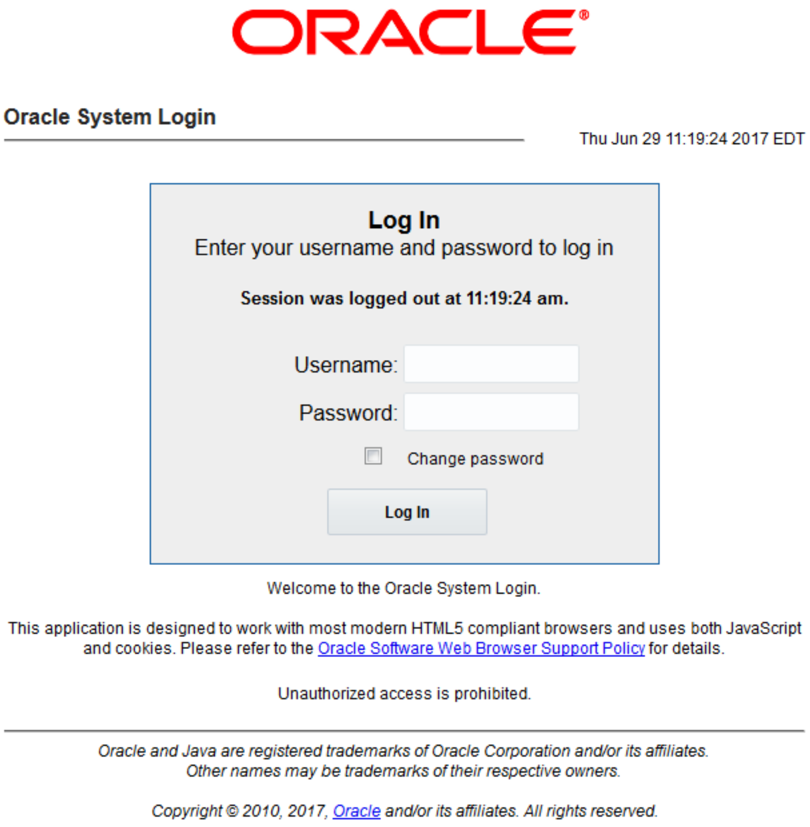
To refresh the server status screen before the default time of 15-30 seconds, navigate to **Status& Manage**, select **Server** screen again.

7. Repeat the above steps of this procedure to configure **SDS NOAM-B** in **DR SDS NOAM-B**.

   This process takes at least five minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master/ slave relationship for High Availability (HA).

Verifying SDS Server Alarm Status

1. To establish GUI session on the NOAM VIP, in **SDS VIP**, perform the following steps:
   a. Establish a GUI session on the NOAM by using the NOAM VIP address.
   b. Login as the **guiadmin** user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In

Enter your username and password to log in

Session was logged out at 11:19:24 am.

Welcome to the Oracle System Login.

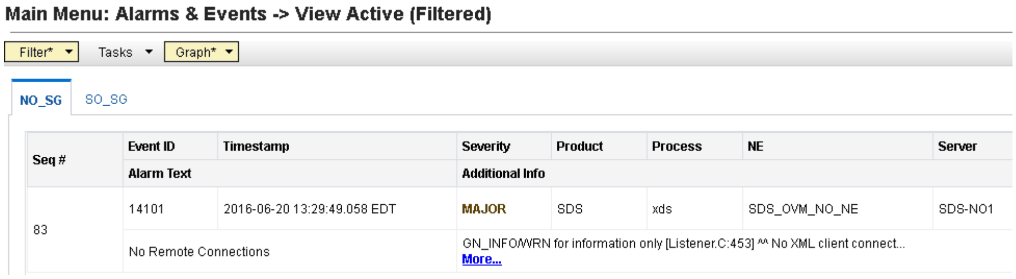
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

2. Wait for remote database alarm to clear, in **SDS VIP**. Then, perform the following steps:
   a. Navigate to **Alarms & Events**, and select **View Active**.
   b. Ensure that the event ID **14101** (with no remote connections) is the only alarm present on the system at this time.



Main Menu: Alarms & Events -> View Active (Filtered)

Seq #	Event ID	Timestamp	Severity	Product	Process	NE	Server
	Alarm Text		Additional Info				
83	14101	2016-06-20 13:29:49.058 EDT	MAJOR	SDS	xds	SDS_OVM_NO_NE	SDS-NO1
	No Remote Connections		GN_INFO/WRN for information only [Listener.C:453] ^^ No XML client connect... More...				

3. To add Query server for the DR SDS server, in **SDS VIP**, perform the following steps:

a. Repeat all steps in Query Server Installation (All SDS NOAM Sites) section.

b. Use the DR SDS NOAM NE and server group instead of the primary SDS NOAM NE and server group.

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

Pre-requisites:

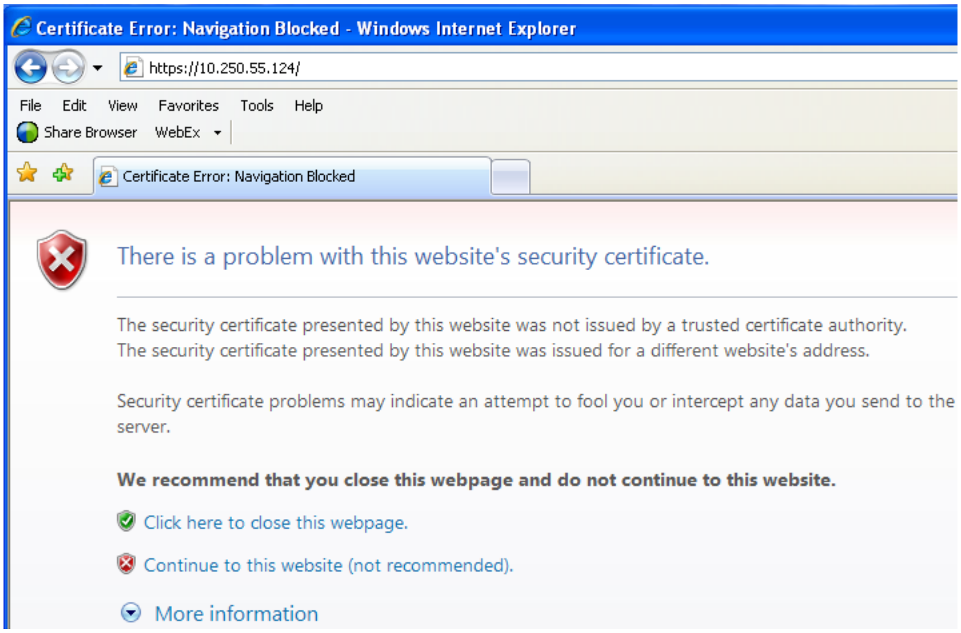
- Ensure the DP-SOAM Network Element XML file for the DP-SOAM site is created as described in Creating an XML file for Installing SDS Network Elements.
- All the Network Element XML files are on the laptop's hard drive.

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.

Installing OAM for DP-SOAM Servers

1. To launch a web browser, in **Active SDS VIP**, connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File
Edit
View
Favorites
Tools
Help
Share Browser
WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

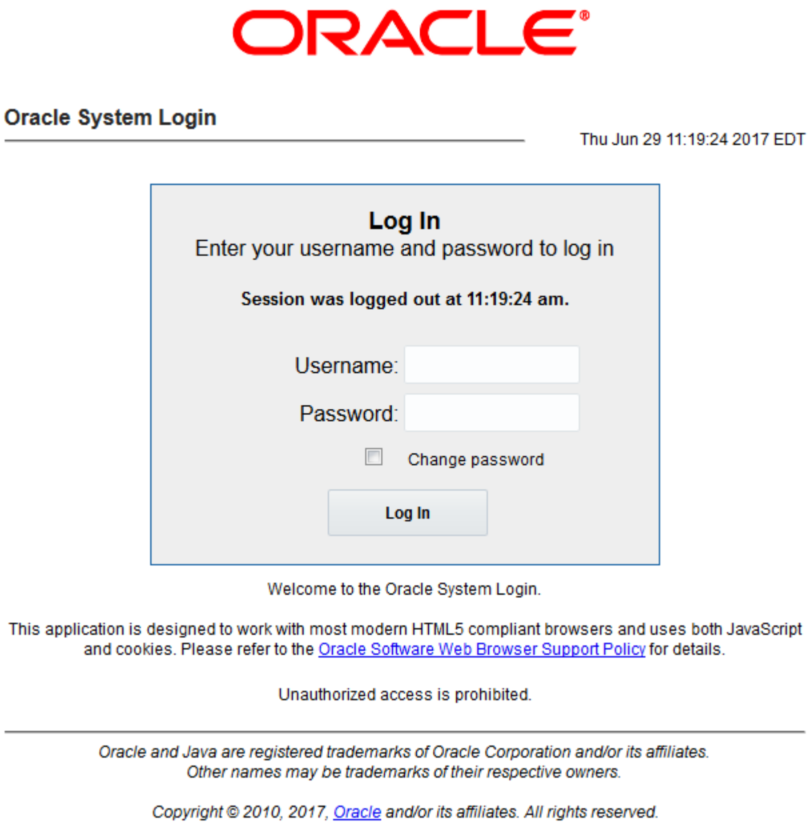
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login to **Active SDS VIP**, establish a GUI session as the **guiadmin** user on the NOAM-A server.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

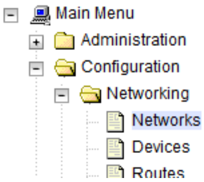
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

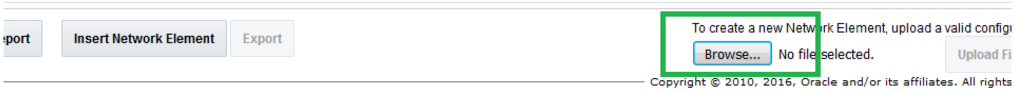
Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To configure the DP SOAM network element, in **Active SDS VIP**, perform the following steps:

   a. Navigate to **Configuration**, select **Networking** and click **Networks**.



   b. Click **Browse** and enter the pathname of the NOAM network XML file.

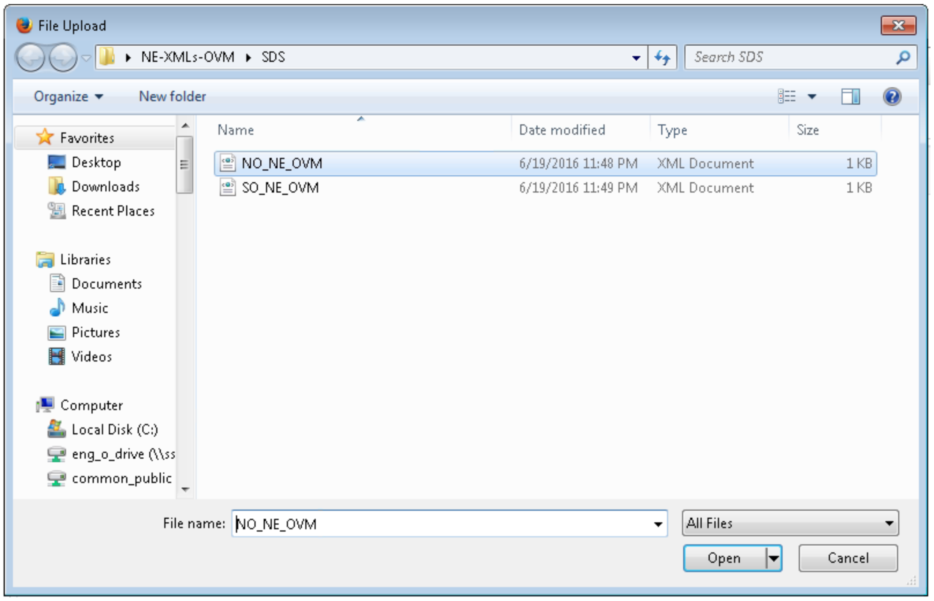


To create a new Network Element, upload a valid config

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights

> **Note:**
>
> This step assumes that the XML files were previously prepared as described in Creating an XML file for Installing SDS Network Elements.

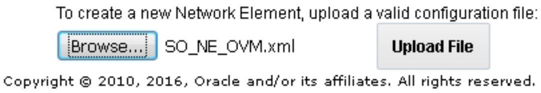
   c. Select the location of the XML file and click **Open**.



Name	Date modified	Type	Size
NO_NE_OVM	6/19/2016 11:48 PM	XML Document	1 KB
SO_NE_OVM	6/19/2016 11:49 PM	XML Document	1 KB

File name: NO_NE_OVM

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

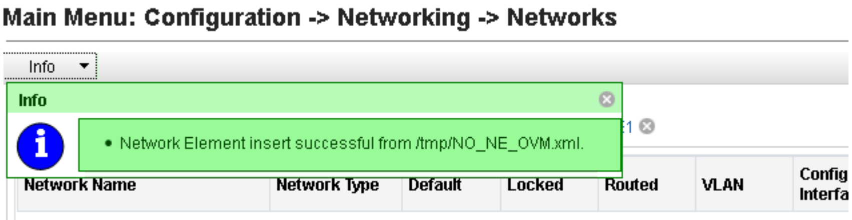


To create a new Network Element, upload a valid configuration file:

Browse... SO_NE_OVM.xml Upload File

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

If the values in the XML file pass and the upload is successful, an information banner displays.



Main Menu: Configuration -> Networking -> Networks

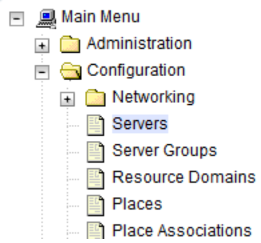
- Network Element insert successful from /tmp/NO_NE_OVM.xml.

Network Name	Network Type	Default	Locked	Routed	VLAN	Config Interfa

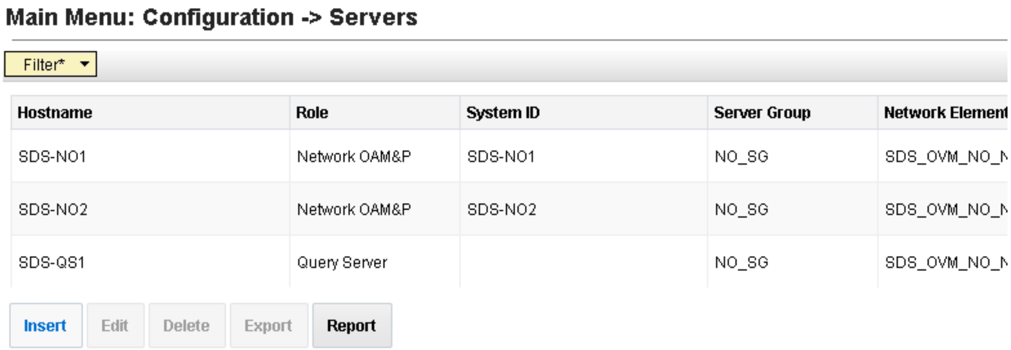
> **Note:**
>
> Left-click mouse on the Info banner to display the banner.

4. To configure the SOAM server, in **Active SDS VIP**, perform the following steps:

   a. Navigate to **Configuration**, and select **Servers**.



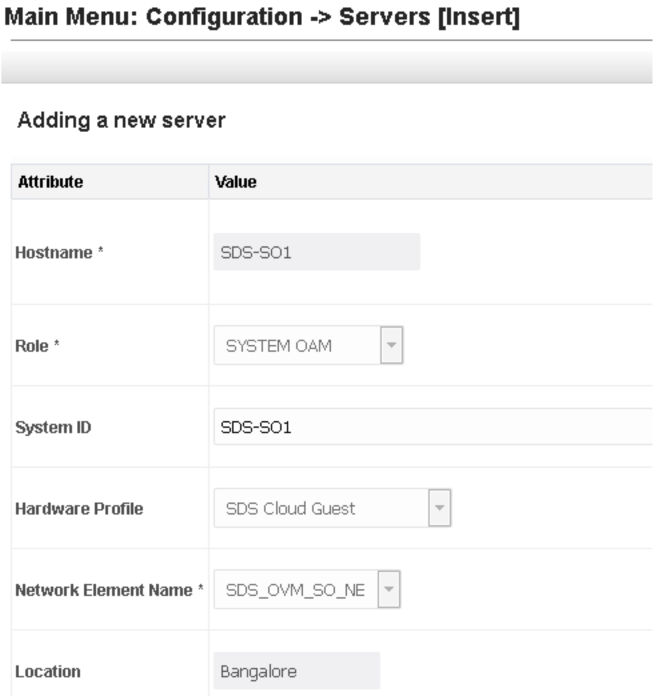
b. Click **Insert** to insert the new SOAM server into server’s table.



Hostname	Role	System ID	Server Group	Network Element
SDS-NO1	Network OAM&P	SDS-NO1	NO_SG	SDS_OVM_NO_N
SDS-NO2	Network OAM&P	SDS-NO2	NO_SG	SDS_OVM_NO_N
SDS-QS1	Query Server		NO_SG	SDS_OVM_NO_N

c. 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



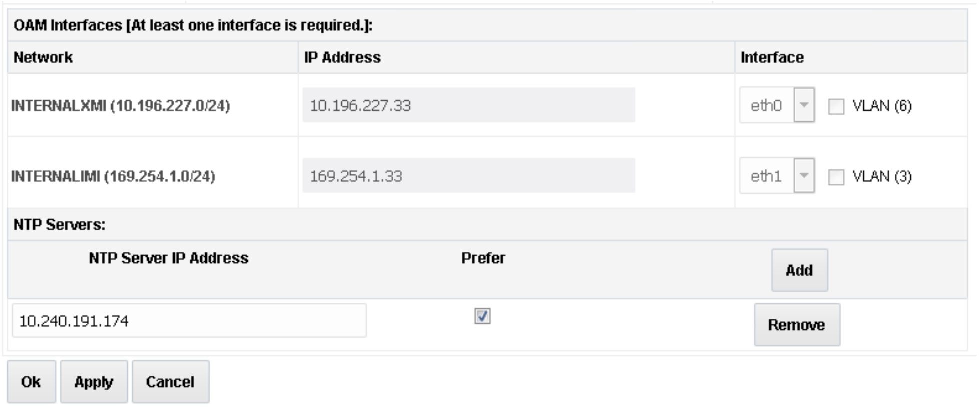
Main Menu: Configuration -> Servers [Insert]

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

5. The network interface fields are now available with selection choices based on the chosen hardware profile and the network element. To insert the network element in **Active SDS VIP**, perform the following steps:

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



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

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.33	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.33	eth1 □ VLAN (3)

NTP Servers:

NTP Server IP Address	Prefer	Add
10.240.191.174	☑	Remove

   a. Enter the server IP addresses for the XMI network, select **ethX** for the interface, and retain the **VLAN** checkbox unchecked.
   b. Enter the server IP addresses for the IMI network, select **ethX** for the interface, and retain the **VLAN** checkbox unchecked.

> **Note:**
>
> For OpenStack, use the IP addresses used during instance booting and network.

c. Add the following NTP servers:

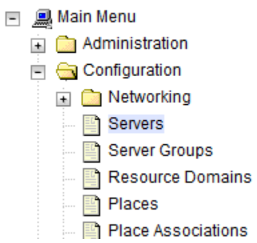
NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server (Optional)	No
Valid NTP Server (Optional)	No

d. Optionally, mark the Prefer checkbox to prefer one server over the other.

e. Click **OK**, once all the server data is entered.

6. To export the initial configuration, in **Active SDS VIP**, perform the following steps:

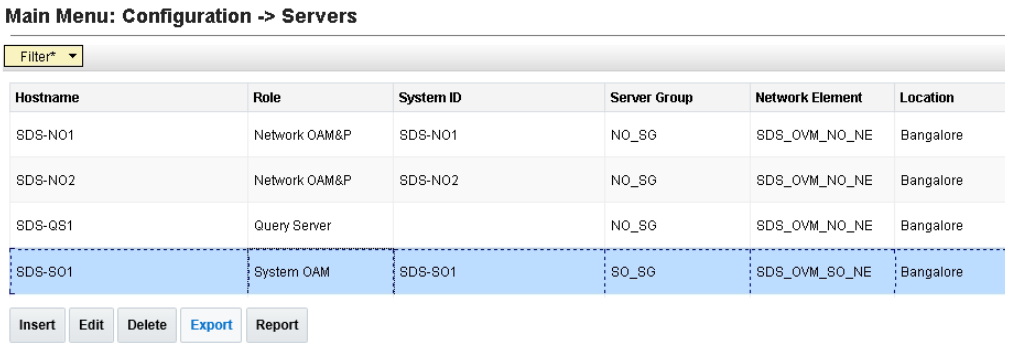
a. Navigate to **Configuration**, and then select **Servers**.



b. From the GUI screen, select the SDS server.

c. Click **Export**, to generate the initial configuration data for that server.

d. Navigate to the **Info** tab to confirm the file has been created.



Main Menu: Configuration -> Servers

Hostname	Role	System ID	Server Group	Network Element	Location
SDS-NO1	Network OAM&P	SDS-NO1	NO_SG	SDS_OVM_NO_NE	Bangalore
SDS-NO2	Network OAM&P	SDS-NO2	NO_SG	SDS_OVM_NO_NE	Bangalore
SDS-QS1	Query Server		NO_SG	SDS_OVM_NO_NE	Bangalore
SDS-SO1	System OAM	SDS-SO1	SO_SG	SDS_OVM_SO_NE	Bangalore

7. To copy server configuration file to `/var/tmp` directory, in **Active SDS VIP**, perform the following steps:

a. Obtain a terminal window to the SDS NOAM-A server, loggin as the **admusr** user.

b. 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`.

For 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 runs 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.

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 process can take between 3 to 20 minutes to complete.

If you are on the console, wait to be prompted to reboot the server. Do not reboot the server. It is rebooted later in this procedure.

8. Verify if the script is completed successfully, in **SDS SOAM Server**, 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. Optionally, to set the time zone and reboot the server, in **SDS SOAM Server**, perform the following steps:

a. To change the system time zone, from the command line prompt, run `set_ini_tz.pl`. The following command example uses the America/New_York time zone.

```
$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/
null 2>&1
$ sudo init 6
```

b. Replace, as appropriate, with the time zone selected for this installation. See List of Frequently Used Time Zones for a complete list of valid time zones.

Wait for server to reboot.

10. To verify server health, in **SDS NOAM-A**, perform the following steps:

a. Log into the NOAM1 as the **admusr** user.

b. Run the following command on the first NOAM server and ensure 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. To configure DR SDS NOAM-B, repeat the above steps from Step 4 to Step 10 of this procedure on **SDS NOAM-B.**

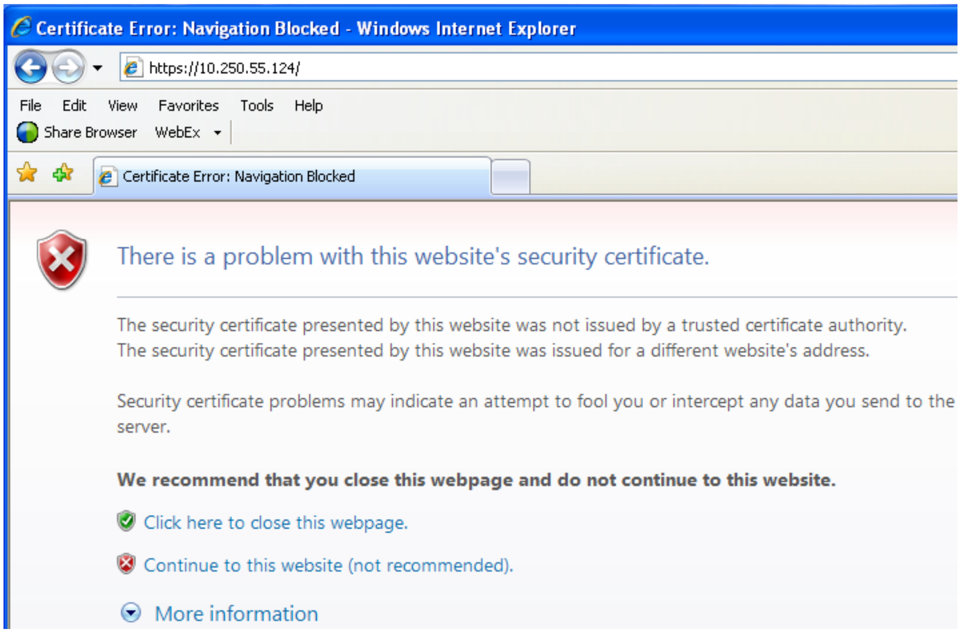
3.7 OAM Pairing for DP-SOAM Sites (All DP-SOAM Sites)

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

Pairing the OAM Servers for DP-SOAM Sites

1. To launch a web browser, in **Active SDS VIP**, connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

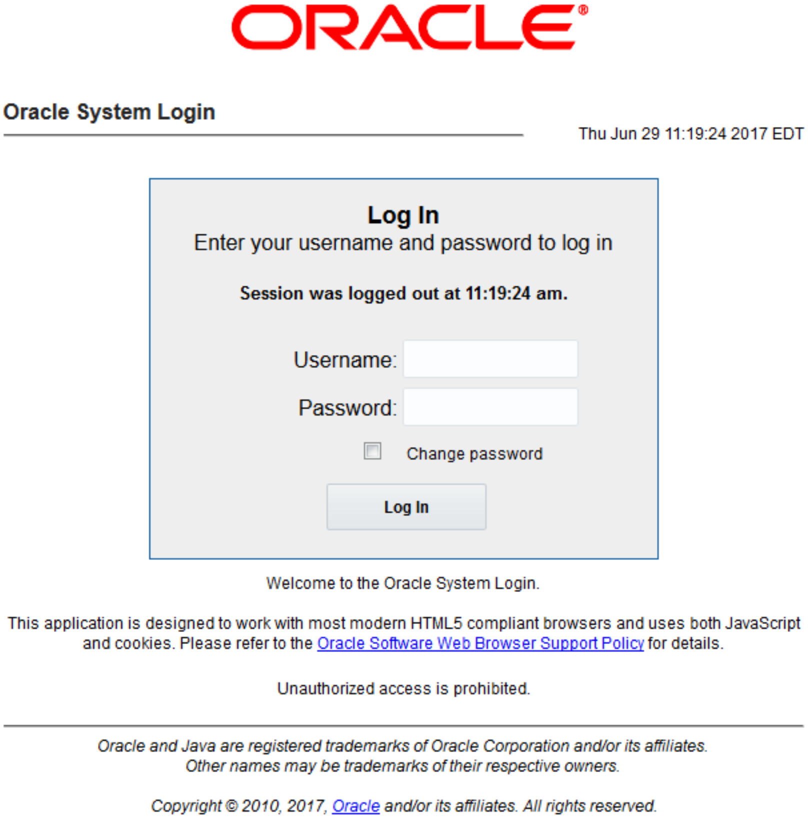
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login to **Active SDS VIP**, establish a GUI session as the default user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Welcome to the Oracle System Login.

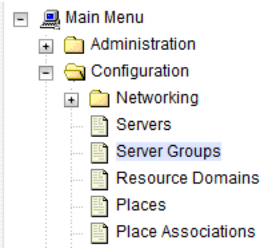
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

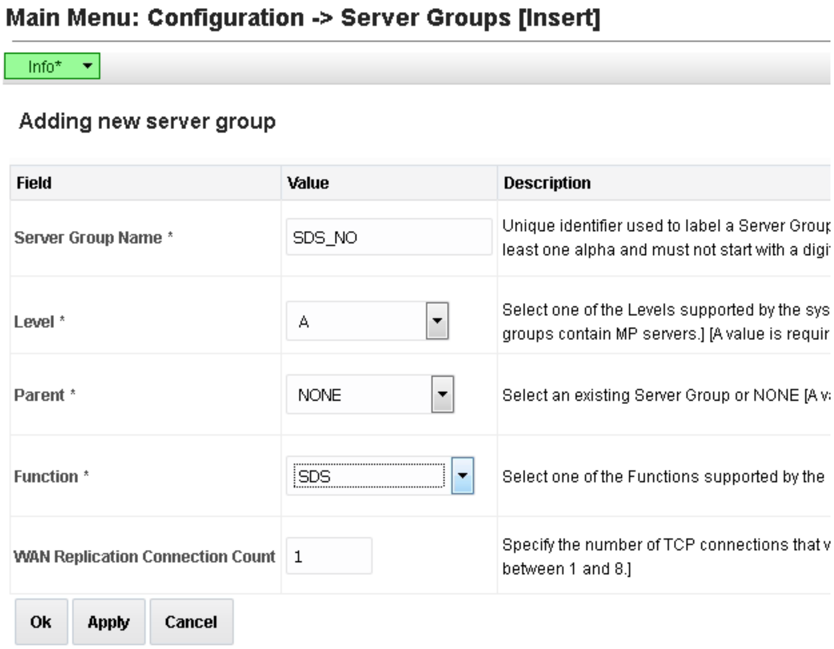
3. To enter group data, in **Active SDS VIP**, perform the following steps:
   a. Navigate to **Configuration**, and select **Server Groups**.



b. Click **Insert**.

c. Fill in the following fields:

   - **Server Group Name:** [Enter Server Group Name]
   - **Level:** B
   - **Parent:** [Select SDS Server Group Name]
   - **Function:** SDS
   - **WAN Replication Connection Count:** Use Default Value



Main Menu: Configuration -> Server Groups [Insert]

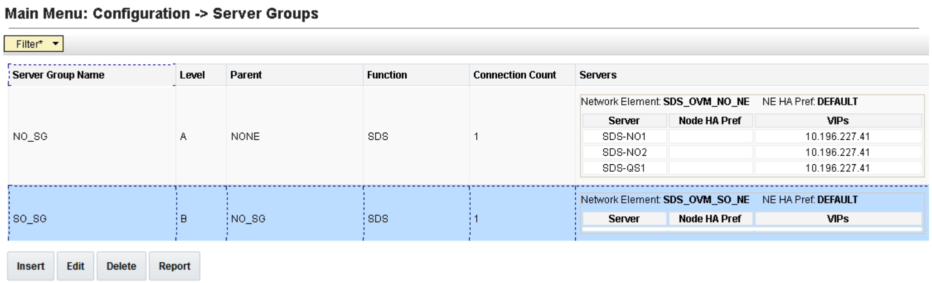
Adding new server group

Field	Value	Description
Server Group Name *	SDS_NO	Unique identifier used to label a Server Group least one alpha and must not start with a digi
Level *	A	Select one of the Levels supported by the sys groups contain MP servers.] [A value is requir
Parent *	NONE	Select an existing Server Group or NONE [A v
Function *	SDS	Select one of the Functions supported by the
WAN Replication Connection Count	1	Specify the number of TCP connections that v between 1 and 8.]

d. Click **Ok**, once all fields are filled.

4. To add server to OAM Server Group, in **SDS SOAM-A**, perform the following steps:

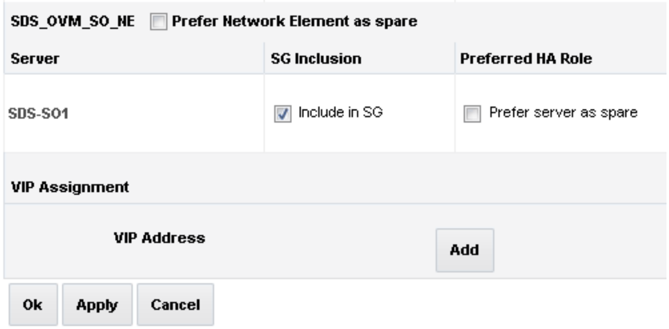
   a. Select the new server group and click **Edit**.



Main Menu: Configuration -> Server Groups

Server Group Name	Level	Parent	Function	Connection Count	Servers
NO_SG	A	NONE	SDS	1	Network Element: **SDS_OVM_NO_NE** NE HA Pref: **DEFAULT** Server / Node HA Pref / VIPs SDS-NO1 / / 10.196.227.41 SDS-NO2 / / 10.196.227.41 SDS-QS1 / / 10.196.227.41
SO_SG	B	NO_SG	SDS	1	Network Element: **SDS_OVM_SO_NE** NE HA Pref: **DEFAULT** Server / Node HA Pref / VIPs

b. In the window where the servers for the server group are listed, find the Query server being configured and select the **Include in SG** checkbox.



SDS_OVM_SO_NE □ Prefer Network Element as spare

Server	SG Inclusion	Preferred HA Role
SDS-SO1	☑ Include in SG	□ Prefer server as spare

VIP Assignment

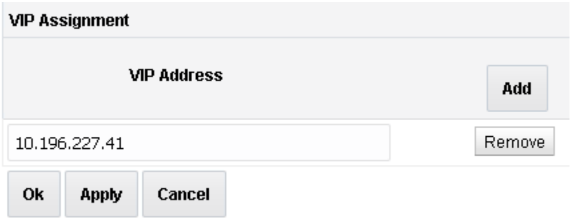
c. Leave other boxes unchecked.

d. Click **Apply**.

5. To add VIP address, in **SDS SOAM-A**, perform the following steps:

a. Click **Add**.

b. Enter the VIP Address and click **OK**.



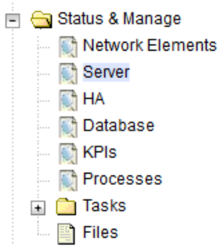
VIP Assignment

VIP Address: 10.196.227.41

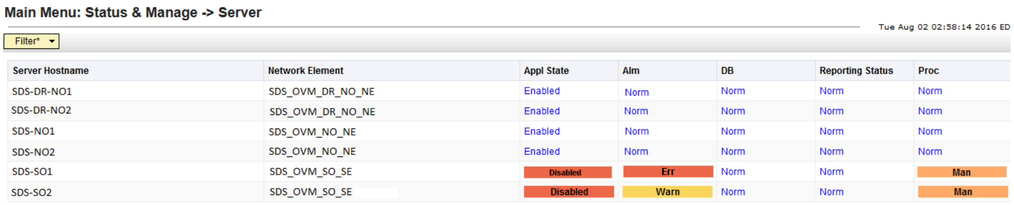
This process takes at least five minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master-slave relationship for High Availability (HA).

6. To verify and restart the servers, in **Active SDS VIP**, perform the following steps:

a. Navigate to **Status & Manage**, and select **Server**.



b. Verify if the DB status is **Norm** and the Proc status is **Man**.

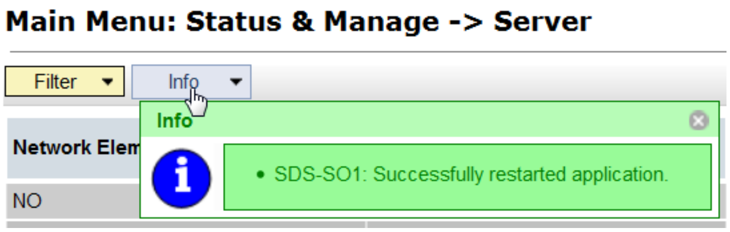

Main Menu: Status & Manage -> Server

Tue Aug 02 02:58:14 2016 ED

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-DR-NO1	SDS_OVM_DR_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-DR-NO2	SDS_OVM_DR_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-NO1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-SO1	SDS_OVM_SO_SE	Disabled	Err	Norm	Norm	Man
SDS-SO2	SDS_OVM_SO_SE	Disabled	Warn	Norm	Norm	Man

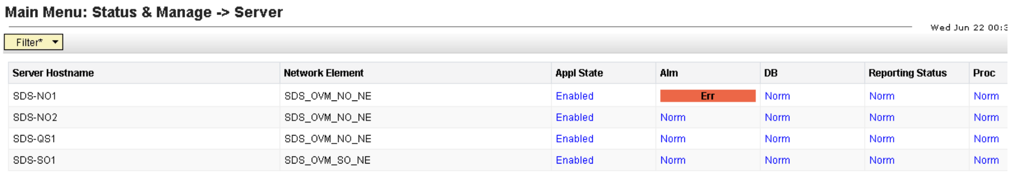
c. Select the DP SOAM-A server and click **Restart**.

d. Click **OK** on the confirmation screen.
A confirmation banner displays.


Main Menu: Status & Manage -> Server

- SDS-SO1: Successfully restarted application.

e. Verify the Appl state is **Enabled** and the DB and Reporting Status is **Norm**.


Main Menu: Status & Manage -> Server

Wed Jun 22 00:3

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Enabled	Err	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-QS1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-SO1	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm

> **Note:**
>
> To refresh the server status screen before the default time of 15 to 30 seconds, navigate to **Status & Manage**, and select **Server** screen again.

7. Configure **SDS SOAM-B**. Repeat the above steps of this procedure to configure **SDS SOAM-B**.

   This process takes at least five minutes, depending on the underlying infrastructure. The server pairs within the server group and establishes a master-slave relationship for High Availability (HA).

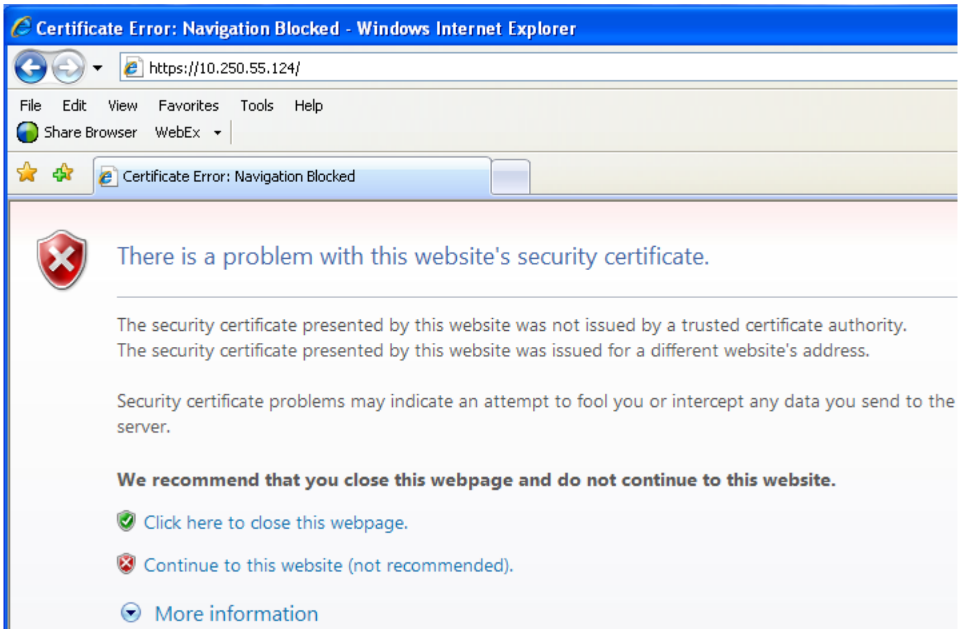
3.8 DP Installation (All DP-SOAM Sites)

> **Note:**
>
> During the Data Processor (DP) installation procedure, various errors are displayed at different stages. While executing a step, ignore errors related to values other than the ones referenced by that step.

Configuring the Database Processor (DP) Server

1. To launch a web browser, in **Active SDS VIP**, connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

   
   Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File
Edit
View
Favorites
Tools
Help
Share Browser
WebEx
Certificate Error: Navigation Blocked

   There is a problem with this website's security certificate.

   The security certificate presented by this website was not issued by a trusted certificate authority.
   The security certificate presented by this website was issued for a different website's address.

   Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

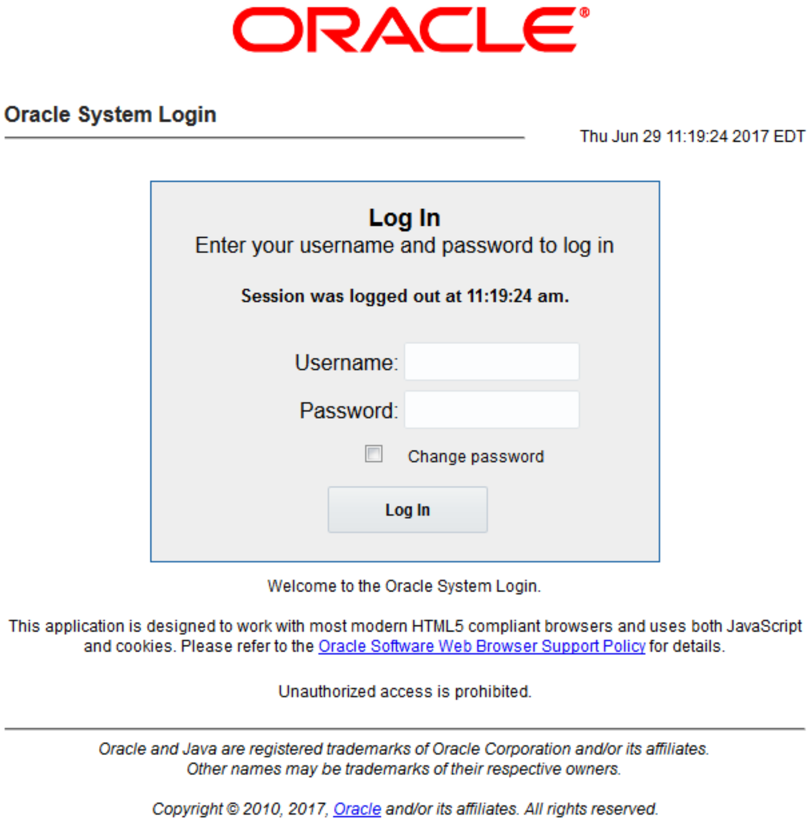
   We recommend that you close this webpage and do not continue to this website.

   Click here to close this webpage.

   Continue to this website (not recommended).

   More information

2. To login, in **Active SDS VIP**, establish a GUI session as the **guiadmin** user on the NOAM-A server.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

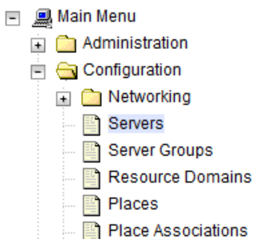
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To configure DP server, in **Active SDS VIP**, perform the following steps:

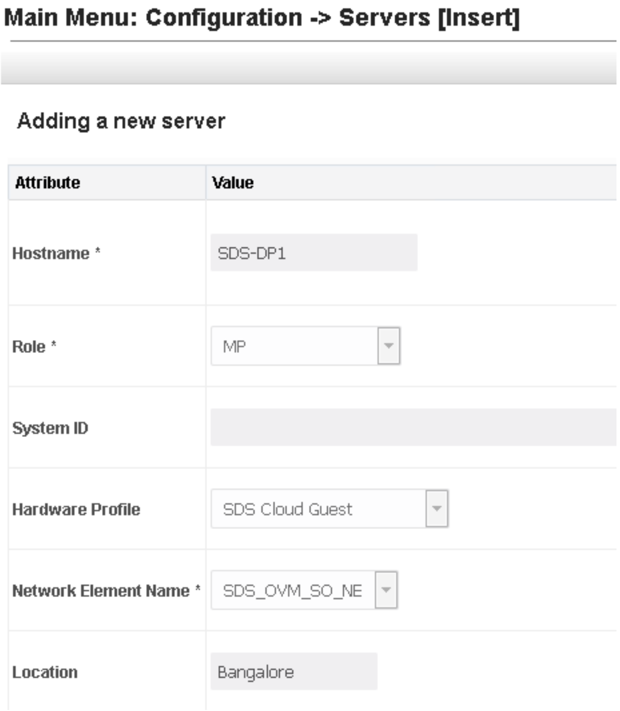
   a. Navigate to **Configuration**, and select **Servers**.



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

   c. 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



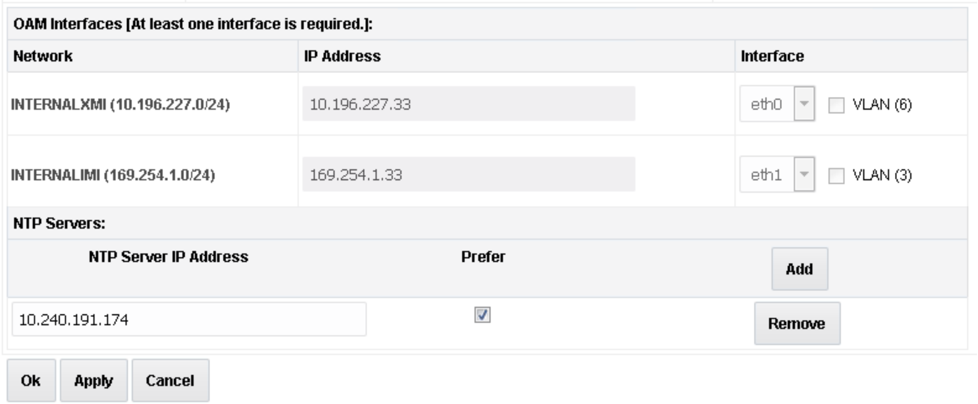
Main Menu: Configuration -> Servers [Insert]

Adding a new server

Attribute	Value
Hostname *	SDS-DP1
Role *	MP
System ID	
Hardware Profile	SDS Cloud Guest
Network Element Name *	SDS_OVM_SO_NE
Location	Bangalore

4. The network interface fields are now available with selection choices based on the hardware profile and the network element. To insert the DP server in **Active SDS VIP**, perform the following steps:

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



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

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.33	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.33	eth1 □ VLAN (3)

NTP Servers:

NTP Server IP Address	Prefer	Add
10.240.191.174	☑	Remove

   a. Enter the server IP addresses for the XMI network, select **ethX** for the interface, and retain the **VLAN** checkbox unchecked.

   b. Enter the server IP addresses for the IMI network, select **ethX** for the interface, and retain the **VLAN** checkbox unchecked.

> **Note:**
>
> For OpenStack, use the IP addresses used during instance booting and networking.

c. Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server (Optional)	No
Valid NTP Server (Optional)	No

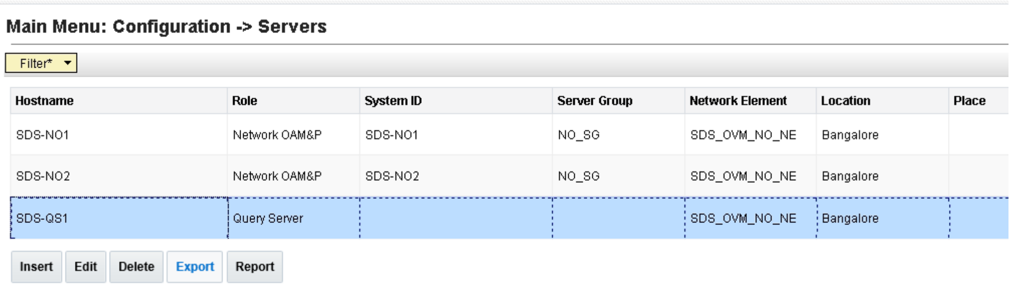
d. Optionally, mark the Prefer checkbox to prefer one server over the other.

e. Click **OK**, once all the server data is entered.

5. To export the initial configuration, in **Active SDS VIP**, perform the following steps:

   a. From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server.

   b. Navigate to the Info tab to confirm the file is created.



Main Menu: Configuration -> Servers

Hostname	Role	System ID	Server Group	Network Element	Location	Place
SDS-NO1	Network OAM&P	SDS-NO1	NO_SG	SDS_OVM_NO_NE	Bangalore	
SDS-NO2	Network OAM&P	SDS-NO2	NO_SG	SDS_OVM_NO_NE	Bangalore	
SDS-QS1	Query Server			SDS_OVM_NO_NE	Bangalore	

6. To login and change directory, in **Active SDS VIP**, perform the following steps:

   a. Obtain a terminal window to the active SDS VIP server, logging in as the **admusr** user.

   b. Change directory to filemgmt:

```
$ cd /var/TKLC/db/filemgmt
```

7. In Active SDS VIP, 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`. *For 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.

In **DP Server**, wait for configuration to complete.

The automatic configuration daemon looks for the file `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 process can take between 3 to 20 minutes to complete.

If you are on the console, wait to be prompted to reboot the server. Do not reboot the server. It is rebooted later in this procedure.

8. Verify if the script is 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. Optionally, to set the time zone and reboot the server, perform the following steps:

   a. Change the system time zone, from the command line prompt, by running `set_ini_tz.pl`. The following command example uses the America/New_York time zone.

      ```
      $ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York"
      >/dev/null 2>&1
      $ sudo init 6
      ```

   b. Replace with appropriate the time zone selected for this installation. For a complete list of valid time zones, see List of Frequently Used Time Zones.

   Wait for server to reboot.

10. To verify server health, in DP Server, perform the following steps:

    a. Log into the NOAM1 as the **admusr** user.

    b. Run the following command on the first NOAM server and ensure no errors are returned:

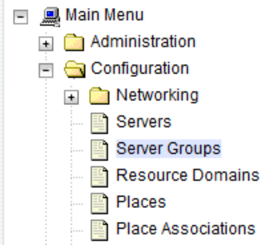
       ```
       $ sudo syscheck
       Running modules in class hardware...
       OK
       Running modules in class disk...
       OK
       Running modules in class net...
       OK
       ```

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

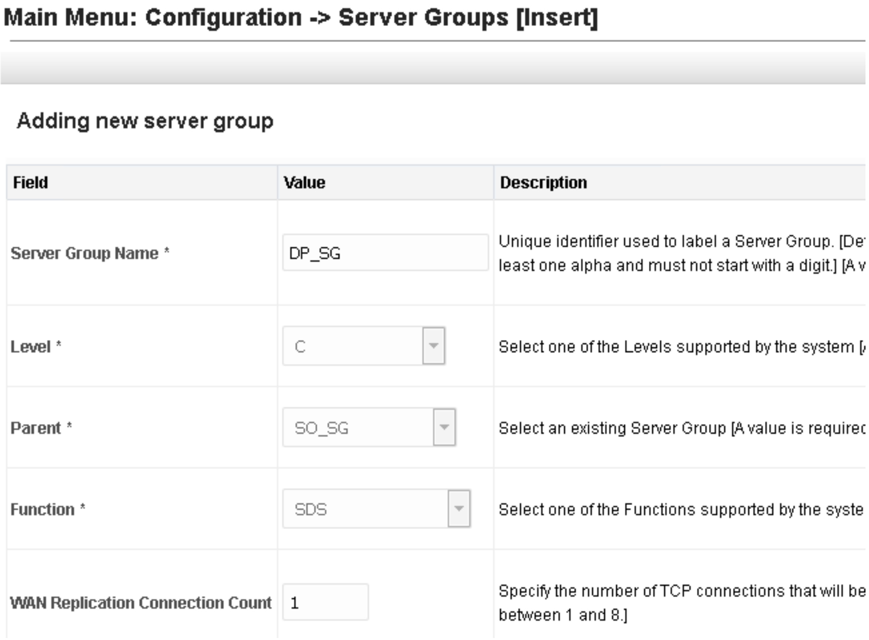
11. For additional DP servers, repeat steps 3 through 10 of this procedure in **Active SDS VIP**.

Adding DP Server to the SDS Server Group

1. To add server to OAM Server Group, in Active SDS VIP, perform the following steps:
   a. Navigate to **Configuration** and select **Server Groups**.



   b. Click **Insert**.
   c. Fill in the following fields:
      - **Server Group Name:** [Enter Server Group Name]
      - **Level:** C
      - **Parent:** [Select System OAM Group Name]
      - **Function:** SDS
      - **WAN Replication Connection Count:** Use Default Value



Main Menu: Configuration -> Server Groups [Insert]

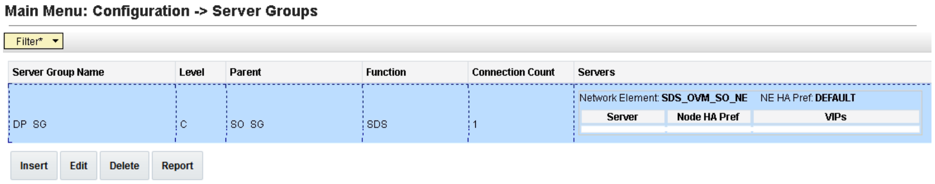
Adding new server group

Field	Value	Description
Server Group Name *	DP_SG	Unique identifier used to label a Server Group. [De least one alpha and must not start with a digit.] [A v
Level *	C	Select one of the Levels supported by the system [
Parent *	SO_SG	Select an existing Server Group [A value is requirec
Function *	SDS	Select one of the Functions supported by the syste
WAN Replication Connection Count	1	Specify the number of TCP connections that will be between 1 and 8.]

d. Click **OK**, once all fields are entered.

2. To add server to OAM Server Group, in **Active SDS VIP**, perform the following steps:

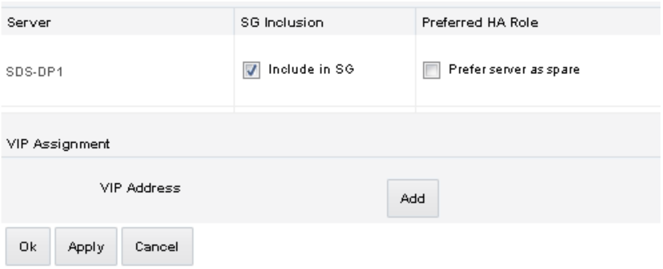
a. Select the new server group and click **Edit**.



Main Menu: Configuration -> Server Groups

Server Group Name	Level	Parent	Function	Connection Count	Servers
DP SG	C	SO SG	SDS	1	Network Element: SDS_OVM_SO_NE NE HA Pref: DEFAULT Server · Node HA Pref · VIPs

b. In the window where the servers for the server group are listed, find the Query server being configured and select the **Include in SG** checkbox.

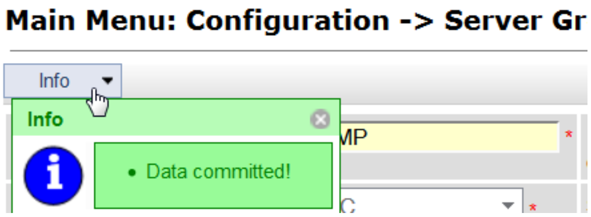


Server	SG Inclusion	Preferred HA Role
SDS-DP1	☑ Include in SG	☐ Prefer server as spare

VIP Assignment

c. Leave other boxes unchecked.

d. Click **Apply**.
A confirmation banner displays.



Main Menu: Configuration -> Server Gr

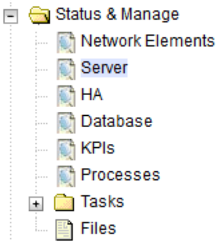
- Data committed!

3. For each subtending DP server, repeat Step 1 and Step 2 of this procedure, in **Active SDS VIP**.

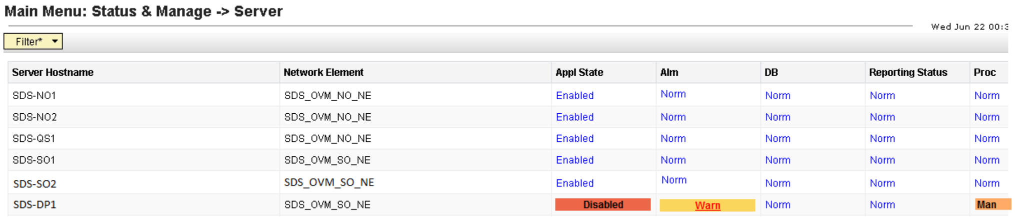
   This process takes a minimum of 5 minutes, depending on the underlying infrastructure. The servers establish DB replication with the active DP-SOAM server at the NE.

4. To verify and restart the servers, in **SDS VIP**, perform the following steps:

   a. Navigate to **Status & Manage**, and select **Server**.



   b. Verify the DB and Reporting Status are **Norm** and the Proc status is **Man**.



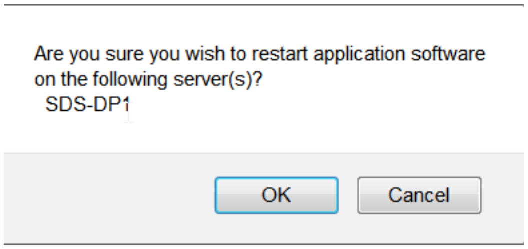
Main Menu: Status & Manage -> Server

Wed Jun 22 00:3

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-NO1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-QS1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-SO1	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-SO2	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-DP1	SDS_OVM_SO_NE	Disabled	Warn	Norm	Norm	Man

   c. Select the DP server and click **Restart**.

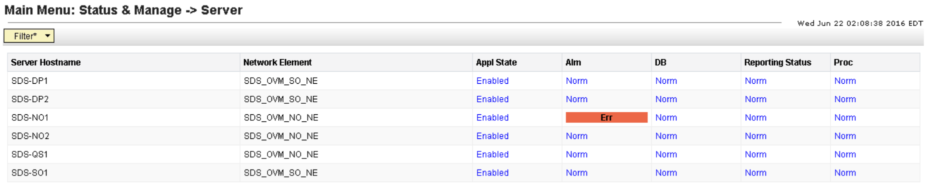
   d. Click **OK** on the confirmation screen.



Are you sure you wish to restart application software on the following server(s)?
SDS-DP1

   A confirmation Successfully restarted application banner displays.

   e. Verify the Appl state is **Enabled** and the Alm, DB, Reporting Status, and Proc are **Norm**.



Main Menu: Status & Manage -> Server

Wed Jun 22 02:08:38 2016 EDT

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
SDS-DP1	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-DP2	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-NO1	SDS_OVM_NO_NE	Enabled	Err	Norm	Norm	Norm
SDS-NO2	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-QS1	SDS_OVM_NO_NE	Enabled	Norm	Norm	Norm	Norm
SDS-SO1	SDS_OVM_SO_NE	Enabled	Norm	Norm	Norm	Norm

> **Note:**
>
> To refresh the server status screen before the default set time of 15 to 30 seconds, navigate to the **Status & Manage**, and select **Server** screen again.

5. For each additional DP server, repeat Step 3 of this procedure, in **Active SDS VIP**.

3.9 Configure ComAgent

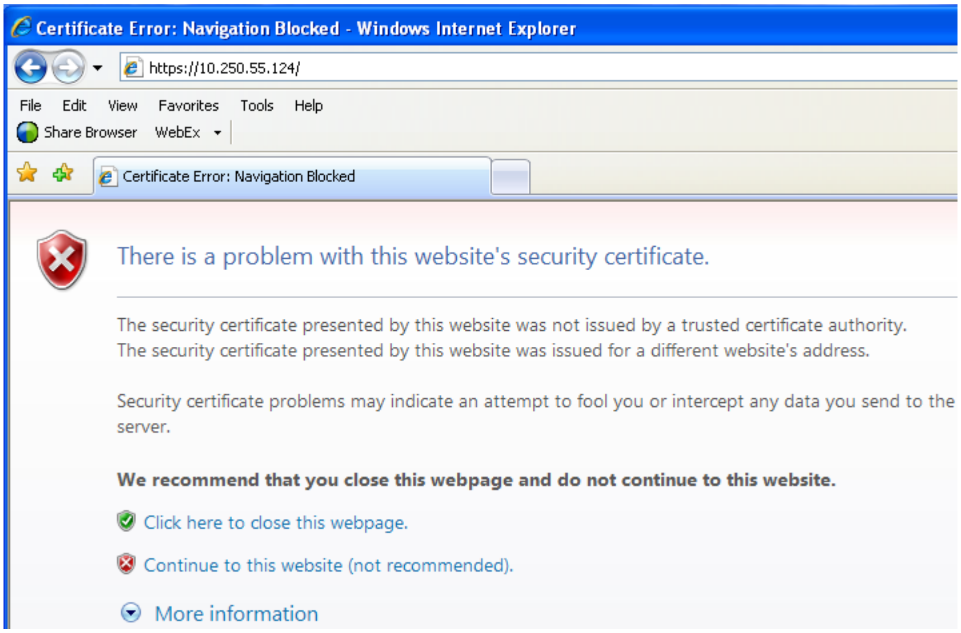
This procedure configures ComAgent, allowing the SDS data processor servers and DSR message processor servers to communicate.

> **Note:**
>
> The following steps cannot be executed until all SDS DP servers are configured.

Configuring ComAgent (All DP-SOAM Sites)
Perform the following steps in **Active SDS VIP**:

1. Open a web browser and connect to the XMI virtual IP address assigned to active SDS site using https://xx.xxx.xx.xxx/

   If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://10.250.55.124/
File Edit View Favorites Tools Help
Share Browser WebEx
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

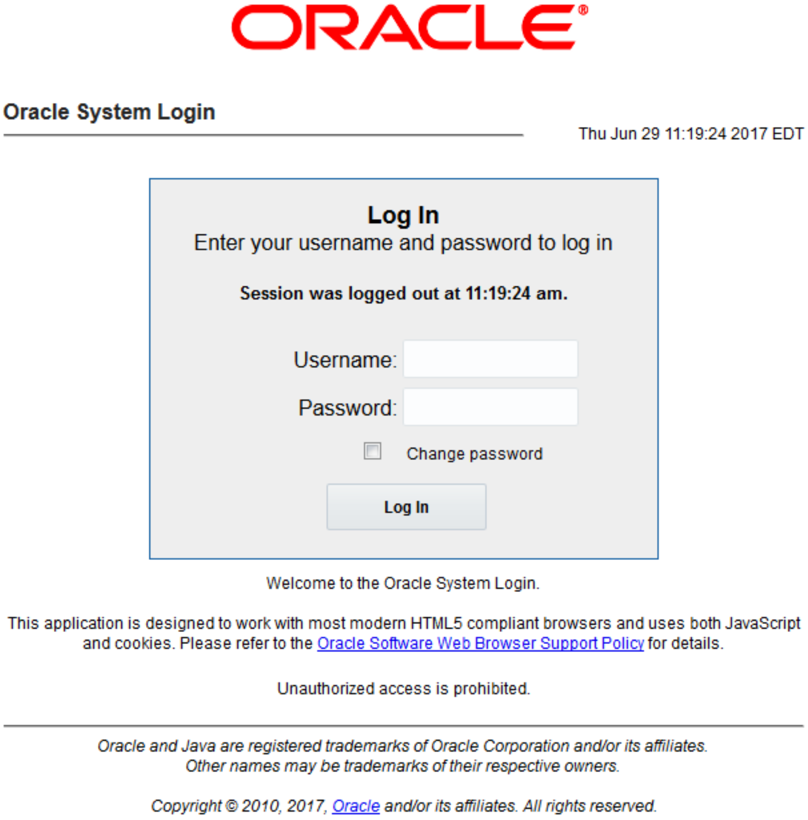
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. To login, establish a GUI session as the default user.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:
Password:
□ Change password

Welcome to the Oracle System Login.

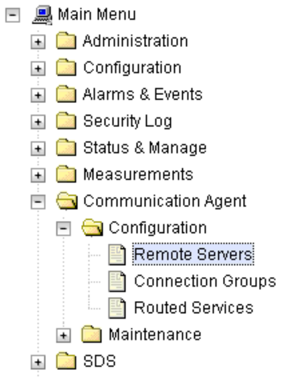
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To navigate to **Remote Servers** screen, perform the following steps:
   a. Navigate to **Administration**, and select **Remote Servers**.



b. Click **Insert**.

4. To configure the Remote server, perform the following steps:

   a. Enter the **Remote Server Name** for the DSR Message Processer server.

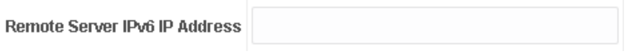
Remote Server Name *

   b. Enter the **Remote Server IPv4 Address**.

Remote Server IPv4 IP Address

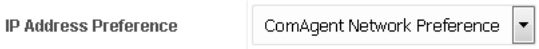
> **Note:**
>
> This is the IMI IP address of the MP.

   c. Enter the **Remote Server IPv6 Address**.



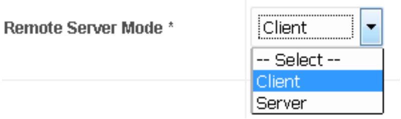
Remote Server IPv6 IP Address

   d. Select the **IP Address Preference**.



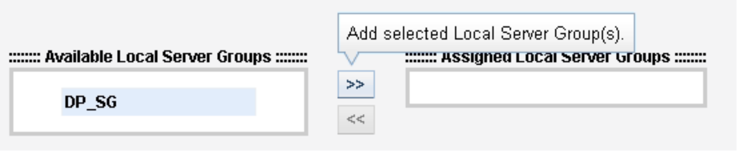
IP Address Preference: ComAgent Network Preference

   e. Select **Client** for the Remote Server Mode.



Remote Server Mode *: Client

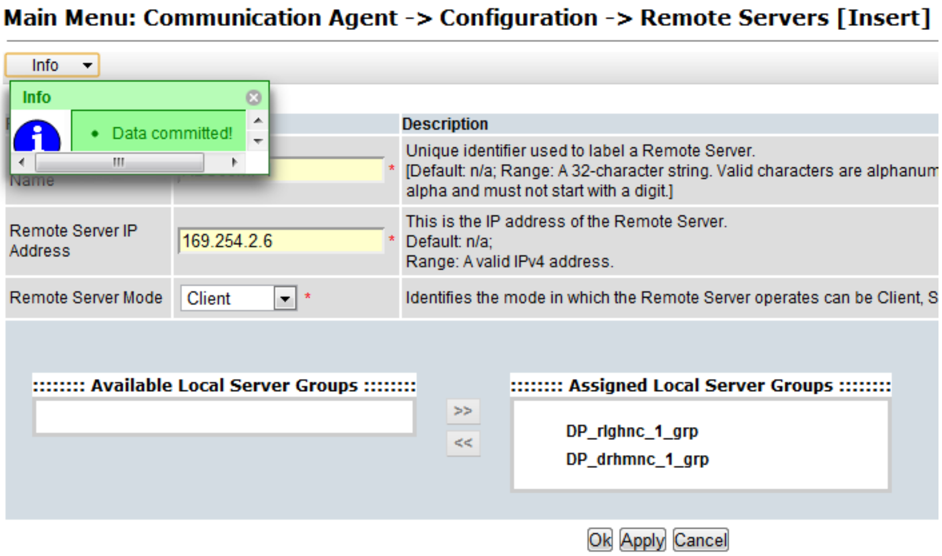
   f. Select the **Local Server Group** for the SDS Data Processer server group.


Add selected Local Server Group(s).
:::::::: Available Local Server Groups ::::::::
DP_SG
>>
<<
:::::::: Assigned Local Server Groups ::::::::

   g. Click **Apply**.

5. Confirm data information.

   A confirmation banner displays.



Main Menu: Communication Agent -> Configuration -> Remote Servers [Insert]

		Description
Name		Unique identifier used to label a Remote Server. [Default: n/a; Range: A 32-character string. Valid characters are alphanum alpha and must not start with a digit.]
Remote Server IP Address	169.254.2.6 *	This is the IP address of the Remote Server. Default: n/a; Range: A valid IPv4 address.
Remote Server Mode	Client *	Identifies the mode in which the Remote Server operates can be Client, S

:::::::: Available Local Server Groups ::::::::

:::::::: Assigned Local Server Groups ::::::::
DP_rlghnc_1_grp
DP_drhmnc_1_grp

6. For each remote MP in the same SOAM NE, repeat Step 3 to Step 5 of this procedure.

3.10 Backup and Disaster Prevention

Snapshotting is the preferred method for backing up cloud system VM instances. Once the DSR and optional sub-systems are installed and configured, before adding traffic, use the appropriate cloud tool (VMware Manager or the OpenStack Horizon GUI) to take snapshots of critical VM instances. It is important to snapshot the control instances, such as the NOAM and SOAM.

> **Note:**
>
> It is recommended to follow this procedure to back up the NOAM and SOAM database.

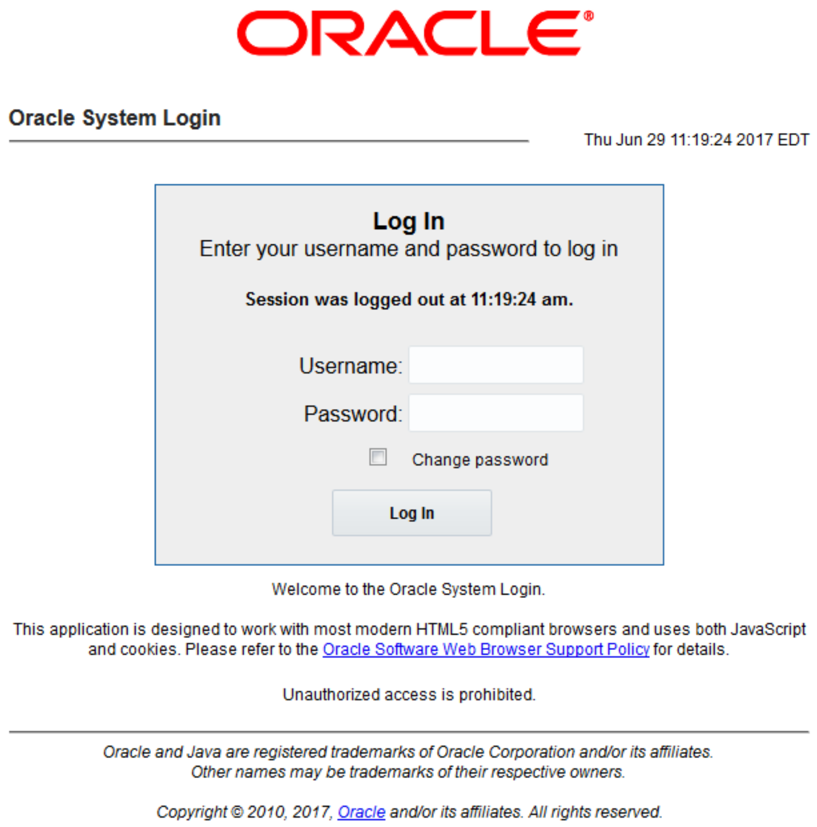
1. Identify Backup Server.

   Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:

   - Cloud Infrastructure Manager Server or Controller

- SDS NOAM

2. To login, in **NOAM VIP**, establish a GUI session as the **guiadmin** user on the NOAM.



Oracle System Login

Thu Jun 29 11:19:24 2017 EDT

Log In
Enter your username and password to log in

Session was logged out at 11:19:24 am.

Username:

Password:

□ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

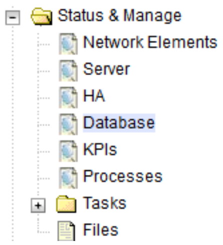
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

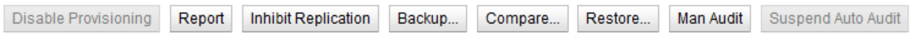
Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

3. To backup configuration data for the system, in **NOAM VIP**, perform the following steps:

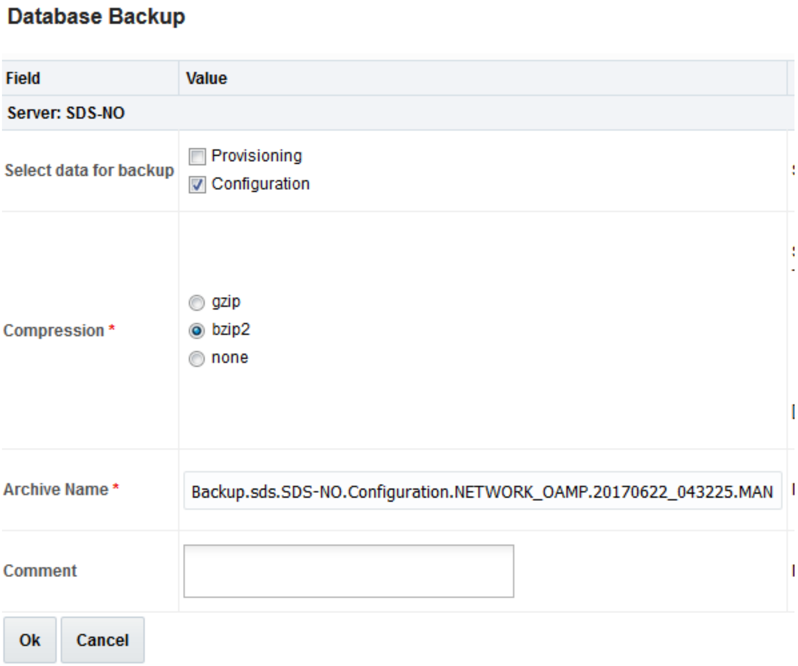
   a. Navigate to **Status & Manage**, and select **Database**.



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



   c. Ensure **Configuration** checkbox is marked.



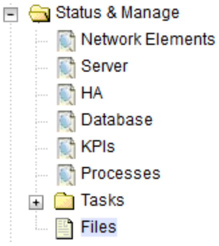
Database Backup

Field	Value
Server: SDS-NO	
Select data for backup	□ Provisioning ☑ Configuration
Compression *	○ gzip ● bzip2 ○ none
Archive Name *	Backup.sds.SDS-NO.Configuration.NETWORK_OAMP.20170622_043225.MAN
Comment	

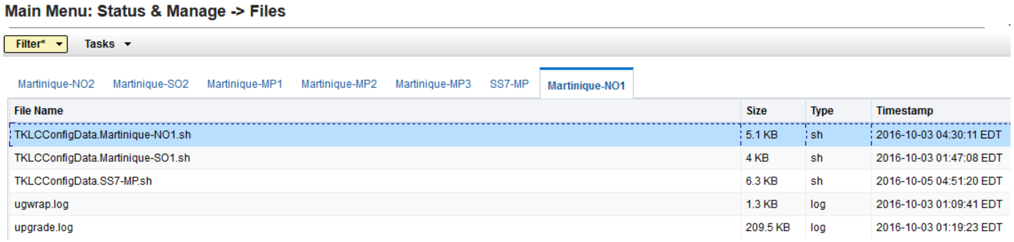
d. Enter a filename for the backup and click **OK**.

4. To verify the backup file existence, in **NOAM VIP**, perform the following steps:

a. Navigate to **Status & Manage**, and select **Files**.



b. Select the active NOAM tab.



Main Menu: Status & Manage -> Files

File Name	Size	Type	Timestamp
TKLCConfigData.Martinique-NO1.sh	5.1 KB	sh	2016-10-03 04:30:11 EDT
TKLCConfigData.Martinique-SO1.sh	4 KB	sh	2016-10-03 01:47:08 EDT
TKLCConfigData.SS7-MP.sh	6.3 KB	sh	2016-10-05 04:51:20 EDT
ugwrap.log	1.3 KB	log	2016-10-03 01:09:41 EDT
upgrade.log	209.5 KB	log	2016-10-03 01:19:23 EDT

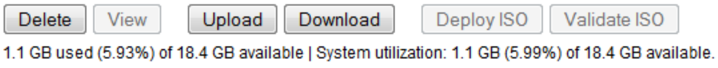
The files on this server are displayed.

c. Verify the existence of the backup file.

5. To download the file to a local machine, in **NOAM VIP**, perform the following steps:

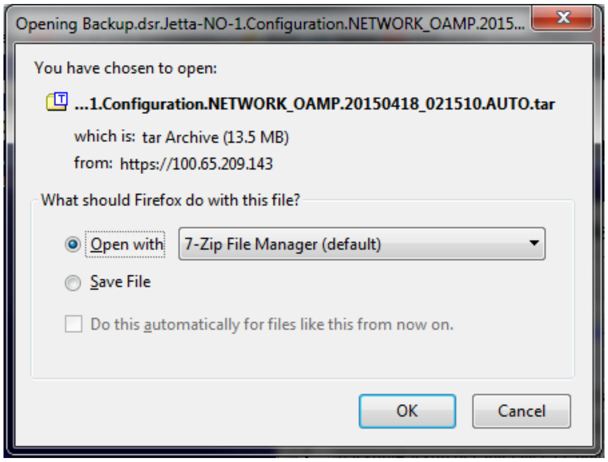
a. Select the backup file.

b. Click **Download**.



1.1 GB used (5.93%) of 18.4 GB available | System utilization: 1.1 GB (5.99%) of 18.4 GB available.

c. Select **OK** to confirm the download.



Opening Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.2015...

You have chosen to open:

...1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar

which is: tar Archive (13.5 MB)

from: https://100.65.209.143

What should Firefox do with this file?

● Open with 7-Zip File Manager (default)

○ Save File

□ Do this automatically for files like this from now on.

6. Upload the image to secure location.

   Save the backed-up image to a secure location where the system administrator can fetch server backup files while performing disaster recovery.

3.11 Configure the Desired MTU value

By default, SDS defines MTU size of all its management and/or signaling networks as 1500 bytes. If the configured virtual network(s) on cloud is VXLAN based and MTU size defined or negotiated on it is 1500 bytes, then accommodate VXLAN header (size 65 bytes) within these 1500 bytes.
Configuring the desired MTU value

This procedure configures the desired MTU value.

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

1. To verify MTU on SDS system, run the following command:

   ```
   iqt -pE NetworkDeviceOption
   ```

   Output:

   ```
   DeviceOption_ID=0 Keyword=MTU Device_ID=0 Value=1500
   DeviceOption_ID=1 Keyword=bootProto Device_ID=0 Value=none
   ```

```
DeviceOption_ID=2 Keyword=onboot Device_ID=0 Value=yes
DeviceOption_ID=3 Keyword=MTU Device_ID=1 Value=1500
DeviceOption_ID=4 Keyword=bootProto Device_ID=1 Value=none
DeviceOption_ID=5 Keyword=onboot Device_ID=1 Value=yes
DeviceOption_ID=6 Keyword=MTU Device_ID=2 Value=1500
DeviceOption_ID=7 Keyword=bootProto Device_ID=2 Value=none
DeviceOption_ID=8 Keyword=onboot Device_ID=2 Value=yes
DeviceOption_ID=9 Keyword=MTU Device_ID=3 Value=1500
DeviceOption_ID=10 Keyword=bootProto Device_ID=3 Value=none
DeviceOption_ID=11 Keyword=onboot Device_ID=3 Value=yes
DeviceOption_ID=12 Keyword=MTU Device_ID=4 Value=1500
DeviceOption_ID=13 Keyword=bootProto Device_ID=4 Value=none
DeviceOption_ID=14 Keyword=onboot Device_ID=4 Value=yes
```

2. To change the MTU value on SDS system (optional), run the following command:

   For example: If the MTU value is 1500 bytes, to change it to 1435 bytes, run the command:

   ```
   sudo iset -fValue=1435 NetworkDeviceOption where “Keyword='MTU'”
   === changed 256 records ===
   ```

   Wait for few minutes.

3. To verify the MTU value SDS system, run the command:

   ```
   ip addr
   ```

   Output:

   ```
   1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
   valid_lft forever preferred_lft forever
   2: control: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast
   state UP qlen 1000
   link/ether 02:79:b5:f7:65:0e brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.32/24 brd 192.168.1.255 scope global control
   inet6 fe80::79:b5ff:fef7:650e/64 scope link
   valid_lft forever preferred_lft forever
   3: xmi: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1435 qdisc pfifo_fast state
   UP qlen 1000
   link/ether 02:90:04:c6:3b:e1 brd ff:ff:ff:ff:ff:ff
   inet 10.75.198.37/25 brd 10.75.198.127 scope global xmi
   inet 10.75.198.4/25 scope global secondary xmi
   inet6 2606:b400:605:b821:90:4ff:fec6:3be1/64 scope global dynamic
   valid_lft 2591870sec preferred_lft 604670sec
   inet6 fe80::90:4ff:fec6:3be1/64 scope link
   valid_lft forever preferred_lft forever
   4: imi: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1435 qdisc pfifo_fast state
   UP qlen 1000
   link/ether 02:3b:48:96:3c:61 brd ff:ff:ff:ff:ff:ff
   inet 192.168.100.32/24 brd 192.168.100.255 scope global imi
   ```

```
inet6 fe80::3b:48ff:fe96:3c61/64 scope link
valid_lft forever preferred_lft forever
```

4. To verify on all nodes, run the command:

   ```
   iqt -pE NetworkDeviceOption
   ```

   Output:

   ```
   DeviceOption_ID=0 Keyword=MTU Device_ID=0 Value=1435
   DeviceOption_ID=1 Keyword=bootProto Device_ID=0 Value=none
   DeviceOption_ID=2 Keyword=onboot Device_ID=0 Value=yes
   DeviceOption_ID=3 Keyword=MTU Device_ID=1 Value=1435
   DeviceOption_ID=4 Keyword=bootProto Device_ID=1 Value=none
   DeviceOption_ID=5 Keyword=onboot Device_ID=1 Value=yes
   DeviceOption_ID=6 Keyword=MTU Device_ID=2 Value=1435
   DeviceOption_ID=7 Keyword=bootProto Device_ID=2 Value=none
   DeviceOption_ID=8 Keyword=onboot Device_ID=2 Value=yes
   DeviceOption_ID=9 Keyword=MTU Device_ID=3 Value=1435
   DeviceOption_ID=10 Keyword=bootProto Device_ID=3 Value=none
   DeviceOption_ID=11 Keyword=onboot Device_ID=3 Value=yes
   DeviceOption_ID=12 Keyword=MTU Device_ID=4 Value=1435
   DeviceOption_ID=13 Keyword=bootProto Device_ID=4 Value=none
   DeviceOption_ID=14 Keyword=onboot Device_ID=4 Value=yes
   ```

A
Appendix

A.1 Creating an XML file for Installing SDS Network Elements

Create SDS Network Elements by using an XML configuration file. The 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 stored on the `/usr/TKLC/sds/vlan` directory. The customer is required to create individual XML files for each of their 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 that the user 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 A-1 SDS XML SDS Network Element Configuration File (IPv4)

XML File Text	Description
<name>sds_mrsvnc</name>	A unique identifier to label a Network Element. Range from 1 up to 32 characters string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and not start with a digit.
<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. The range allowed is "2" up to "4094".
<ip>10.250.55.0</ip>	The network address of this VLAN is 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 is a valid IP address.

Table A-1 (Cont.) SDS XML SDS Network Element Configuration File (IPv4)

XML File Text	Description
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. It can be either true or false.

Table A-2 SDS XML SDS Network Element Configuration File (IPv6)

XML File Text	Description
<name>sds_mrsvnc</name>	A unique identifier to label a Network Element the range is "1" up to "32" character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and not start with a digit.
<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 the allowed range is "2" up to "4094".
<ip>2606:b400:605:b804::</ip>	The network address of this VLAN is a valid IP address.
<mask>/64</mask>	Subnetting to apply to servers within this VLAN.
<gateway>2606:B400:605:B804: D27E:28FF:FEB3:4FE2</gateway>	The gateway router interface address associated with this network is a valid IP address.
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. It can be either true or false.

A.2 List of Frequently Used Time Zones

This table lists valid time zone strings that can be used for the time zone setting in a CSV file or as the time zone parameter required when manually setting a DSR time zone.

Table A-3 List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07

Table A-3 (Cont.) List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico City	Central Time — most locations	UTC-06
Africa/Monrousing		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01
Asia/Hong Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time — west British Columbia	UTC-08
America/Edmonton	Mountain Time — Alberta, east British Columbia & west Saskatchewan	UTC-07
America/Toronto	Eastern Time — Ontario — most locations	UTC-05
America/Montreal	Eastern Time — Quebec — most locations	UTC-05
America/Sao Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia — most locations	UTC+08
Australia/Sydney	New South Wales — most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto Rico		UTC-04
Europe/Moscow	Moscow+00 — west Russia	UTC+04
Asia/Manila		UTC+08

Table A-3 (Cont.) List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

A.3 Common KVM or OpenStack Tasks

A.3.1 Importing an OVA File

1. Create VM flavors.

   Use the *DSR Cloud Benchmarking Guide* values to create flavors for each type of VM. Flavors are created using the Horizon GUI in the **Admin** section or with the `nova flavor-create` command line tool. Ensure the flavor names are as informative as possible.

   Flavors describe resource sizing, and a standard convention is to use a name like “0406060”, where the first two digits (04) represent the number of virtual CPUs and the next two digits (06) represent the RAM allocation in GB. The final three digits (060) represent the disk space in GB.

2. Unpack and import an image file using the glance utility.

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

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

   b. Log into the OpenStack control node.

   ```
   $ ssh admusr@node
   ```

   c. In an empty directory unpack the OVA file using tar.

   ```
   $ tar xvf SDS-x.x.x.ova
   ```

   > **Note:**
   >
   > One of the unpacked files have a .vmdk suffix. This is the VM image file that must be imported.
   > `SDS-8.6.x.x.x-disk1.vmdk`

   d. Source the OpenStack admin user credentials.

   ```
   $ . keystonerc_admin
   ```

e. Select an informative name for the new image.

```
sds-x.x.x-original
```

f. 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 five minutes depending on the underlying infrastructure.

A.3.2 Creating Network Ports for the NO Network Interfaces

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 six or more interfaces and corresponding network ports.

1. 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

2. Identify the neutron network ID associated with each IP or interface using the neutron command line tool.

   ```
   $ neutron net-list
   ```

3. Identify the neutron subnet ID associated with each IP or interface using the neutron command line tool.

   ```
   $ neutron subnet-list
   ```

4. 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=NO1-xmi --tenant-id <tenant id> --fixed-ip
   subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>
   $ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip
   subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>
   ```

5. View your newly created ports using the neutron tool.

   ```
   $ neutron port-list
   ```

A.3.3 Creating and Boot OpenStack Instance from a Glance Image

1. Retrieve the following configuration values:

   Retrieve image ID, run the command:

   ```
   $ glance image-list
   ```

   Retrieve flavor ID, run the command:

   ```
   $ nova flavor-list
   ```

   Retrieve network IDs, run the command:

   ```
   $ neutron net-list
   ```

   For example: 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. Obtain the credentials of the DSR tenant user and issue the following command.

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

   ```
   $ nova boot --image <image ID> --flavor <flavor id> --nic net-
   id=<first network id>,v4-fixed-ip=<first ip address> --nic net-
   id=<second network id>,v4-fixed-ip=<second ip address> InstanceName
   ```

3. View the newly created instance using the nova tool.

   ```
   $ nova list --all-tenants
   ```

   The VM takes approximately five minutes to boot. At this stage, the VM has no configured network interfaces and can be accessed only through the Horizon console tool.

A.3.4 Configure Networking for OpenStack Instance

To verify or configure the network interface, perform the following steps:

1. Verify if the 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 the `nova boot` command:

   ```
   $ ping <XMI-IP-Provided-During-Nova-Boot>
   ```

   If the ping is successful, ignore the next part to configure the interface manually.

2. Manually configure the interface, if not already done.

   a. Log into the Horizon GUI as the DSR tenant user.

   b. Navigate to the **Compute/Instances** section.

   c. Click **Name field** of the newly created instance.

   d. Select **Console** tab.

   e. Login as the admusr user.

   f. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments as defined in Appendix A Creating an XML file for Installing SDS Network Elements.

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

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

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

   ```
   $ cd /etc/sysconfig/network-scripts
   $ sudo mv ifcfg-ethX /tmp
   ```

3. To create and configure the interface in one action, re-run the `netAdm` command.

4. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.

   ```
   $ sudo init 6
   ```

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

A.4 Application VIP Failover Options (OpenStack)

A.4.1 Application VIP Failover Options

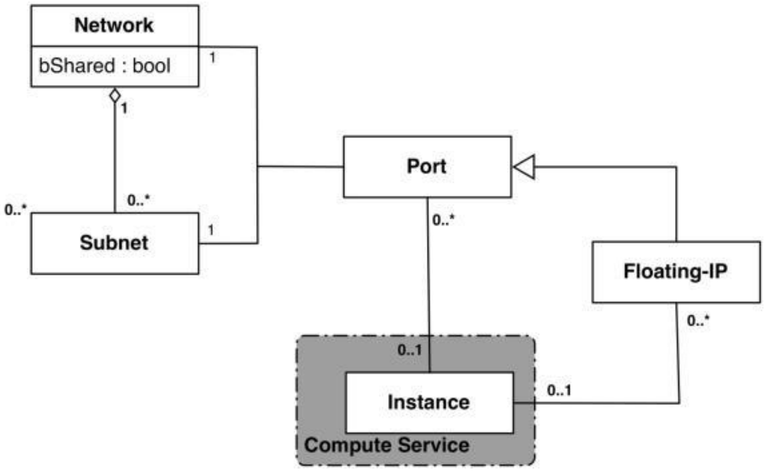
Within an OpenStack cloud environment, there are several options for allowing applications to manage their own virtual IP (VIP) addresses as traditionally done in telecommunications applications. This document describes two of those options:

- 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 onutilizing application managed virtual IP addresses within an OpenStack VM instance.

Both 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 A-1 Neutron High-Level Data Model



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.
- 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. This is since Neutron is not aware of the VIPs being applied by the application to VM instance network interfaces without an interaction between the application (or a higher-level management element) and Neutron. Hence, 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.

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

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

A.4.2 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, so on) to define additional IP addresses to be associated with a Neutron port. In this way, if an application within the VM instance sends an outgoing packet with one of those additional IP addresses, then Neutron anti-spoofing rules enforcement logic does not drop those packets. The Neutron allowed-address-pairs extension is available starting with the OpenStack Havana release.

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

A.4.3 OpenStack Configuration Requirements

The Neutron allowed-address-pairs extension must be enabled for this option to work. For most OpenStack cloud deployments this extension should be enabled by default, to verify 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 highlighted line.

A.4.4 Before a VM Instance has been Booted: Allowed Address Pairs

To associate additional allowed IP addresses with a port before it is associated with a VM instance, then create the port and 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 as follows:

```
# 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:

- **<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.

For example: 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 run the following command:

```
# 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 is created, when you boot the VM instance use a nova boot command:

```
# 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 mustt be replaced by appropriate values for your VM. If the port to be associated with the VM instance is not named, then 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.

A.4.5 After a VM Instance has been Booted: Allowed Address Pairs

If a VM instance has already been booted, that is, instantiated, and you need to associate one or more additional IP addresses with the Neutron port assigned to the VM instance then run the following command:

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

Where:

- **<Port ID>**
  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence like `$(neutron port-show -f value -F id <Port Name>)` to replace the `<Port ID>` placeholder.
- **<VIP address to be added>**
  Identifies the IP address, a virtual IP address in this case, that should additionally be associated with the port where this can be a single IP address. For example, 10.133.97.135/32, or a range of IP addresses as indicated by a value such as 10.133.97.128/30.

  For example: 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 runthe following command:

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

A.4.6 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 done with the allowed-address-pairs extension, to disable the Neutron anti-spoofing filter rules for a given port. This option allows all IP packets originating from the VM instance to be propagated no matter whether the source IP address in the packet matches the IP address associated with the Neutron port or not. This option relies upon the Neutron port security extension that is available starting with the OpenStack Kilo release.

OpenStack Configuration Requirements

The Neutron port security extension must be enabled for this method to work. For procedure to enable the port security extension, see ML2 Port Security Extension

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, so on, 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, so on)
- Re-add the appropriate network interfaces to the VMs.

Note:

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

A.4.7 Before a VM Instance has been Booted: Port Security

To disable port security for a port before it is associated with a VM instance, create the port and specify the time that port security should be disabled. The command to create a new port with port security disabled is as follows:

```
# 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:

- **<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. This is 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.

For example: 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 run following command:

```
# 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, run the following command when you boot the VM instance:

```
# 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 must be replaced by values appropriate for your VM. If the port to be associated with the VM instance is not named, then 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 command with the port's ID value.

A.4.8 After a VM Instance has been Booted: Port Security

To disable port security for a port after it has already been associated with a VM instance, run 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 verify), then run the following command for each of the security group(s) associated with the VM instance:

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

where:

- **<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.

For example: To remove the default security group from a VM instance named `testvm4` then run the following command:

```
# 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 must be updated to disable port security on those ports. The command to disable port security for a specific Neutron port is:

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

where, **<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>)`.

For example: To indicate to Neutron that port security should be disabled for a port with an ID of 6d48b5f2-d185-4768-b5a4-c0d1d8075e41, then run 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, the application managed VIPs can now be added to the network interface within the VM instance associated with the port. The network traffic using that VIP address should now propagate.

A.4.9 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.

For example: The following command line operations are 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 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.

Section Title

(Optional) Enter conceptual text here.

Example A-1   Example Title

(Optional) Enter an example here.

A.5 Common OVM-Manager Tasks (CLI)

A.5.1 Setting Up the Server

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

Perform the following steps using using OVM-M CLI:

1. Log into the OVM-M command line interface.

   ```
   ssh -l admin <OVM-M IP> -p 1000
   ```

   For example:

   ```
   [root@manager01 ~]# ssh -l admin 10.240.16.138 -p 10000
   admin@10.240.16.138's password:
   ```

2. To discover Oracle VM server, run the command:

   ```
   discoverServer ipAddress=value password=value takeOwnership= { Yes | No }
   ```

   For example:

   ```
   OVM>discoverServer ipAddress=10.240.16.139 password=password
   takeOwnership=Yes
   ```

3. To create an ethernet-based network with the VM role, run the command:

   ```
   create Network [ roles= { MANAGEMENT | LIVE_MIGRATE |
   CLUSTER_HEARTBEAT | VIRTUAL_MACHINE | STORAGE } ] name=value
   [ description=value ] [ on Server instance ]
   ```

   For example:

   ```
   OVM>create Network name=XMI roles=VIRTUAL_MACHINE
   ```

4. To add a port from each Oracle VM server to the network, perform the following steps:

   > **Note:**
   >
   > Skip this step and proceed to Step 5 for bonded interfaces.

   a. 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]
      ```

   b. Add a port from each Oracle VM Server to the network.

      ```
      OVM>add Port instance to { BondPort | Network } instance
      ```

      For example:

      ```
      OVM>add Port id=0004fb0000200000d2e7d2d352a6654e to Network
      name=MyVMNetwork
      ```

5. To create Bondport, for Bonded Interfaces, perform the following steps:

   a. Find the ID of an Ethernet port.

      ```
      OVM>list Port
      Status: Success
      Time: 2016-08-22 04:43:02,565 EDT
      Data:
      id:0004fb000020000045b4e8dc0b3acc6 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
```

b. Create Bondport on required interfaces.

```
OVM>create BondPort
ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443
e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server
name=compute01.test.com
```

Command:

```
create BondPort
ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443
e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server
name=compute01.test.com
Status: Success
```

6. To add VLAN Interface to network, for VLAN tagged networks, perform the following steps:

a. 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
```

b. Create VLAN interface.

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

c. Add remaining VLAN interfaces to the same bond accordingly:

```
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
```

d. 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
```

7. To create unclustered server pool, run the command:

   ```
   OVM>create ServerPool clusterEnable=No name=MyServerPool
   description='Unclustered server pool'
   ```

   > **Note:**
   >
   > To create clustered server pool, ignore this step and proceed to next.

8. Optionally, to create clustered server pool, perform the following steps:

   a. To create a clustered server pool, 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:0004fb0000050000809e28f4fab56b1 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:0004fb000018000732be086afb26911 name:FreeBSD (7)
id:0004fb000018000067ce80973e18374e name:FreeBSD (8)
id:0004fb000018000035ce16ee4d58dc4d name:FreeBSD (1)
id:0004fb0000180000685511 7242d9a537 name:FreeBSD (6)
id:0004fb0000180000a9c7a87ba52ce5ec name:FreeBSD (5)
id:0004fb0000180000ebabef9838188d78 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)
```

b. Refresh the file system or physical disk to be used for the server pool file system.

```
OVM>refresh { AccessGroup | Assembly | FileServer | FileSystem |
PhysicalDisk | Repository | Server | StorageArray |
VirtualAppliance } instance
```

For example: To refresh a physical disk, run the command:

```
OVM>refresh PhysicalDisk id=0004fb000018000035ce16ee4d58dc4d
```

For example: To refresh a file system, run the command:

```
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. To add Oracle VM servers to the server pool, run the command:

```
OVM>add Server name=MyServer to ServerPool name=MyServerPool
```

10. To create storage repository, perform the following steps:

a. 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
```

b. Find a local file system on an Oracle VM server that has access to the LUN.

```
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
```

c. 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
```

d. 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
```

e. Add server pool to repository.

```
OVM> add ServerPool name=TestPool001 to Repository name=Vms01Repo
Refresh the storage repository using the syntax:
OVM> refresh Repository name=MyRepository
```

A.5.2 Server Pool

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

A.6 Emergency Response

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

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

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

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

A.7 Locate Product Documentation on the Oracle Help Center

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

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