ORACLE Communications
5200 Paramount Parkway
Morrisville, NC 27560 USA
888-FOR-TKLC

Installation User's Guide

Oracle® Communications

SDS 7.1 Cloud Installation Guide

E64816-03

May 2016

This procedure is intended for execution by ORACLE Communications personnel only! The user should always download the latest version from DOC CENTER before executing.

CHANGE HISTORY

Date	ENG Version	ECO Revision	Author	Description	Approved (Yes/No)
5/20/2015	0.1		C. Cooper	Hardware references removal	No
5/29/2015	0.2		C. Cooper	Updates per installation testing	No
6/08/2015	0.3 – 0.12		C. Cooper	Updates per working session	No
6/29/2015	1 – 3		C.Cooper	Updates per formal review	No
6/30/2015	4		C. Cooper		Yes
8/24/2015	5		A. Gold	Updates for 7.1.1	No
10/14/2015	6		A. Gold	Updates per review	No
10/16/2015	7		A. Gold	Final updates.	Yes
05/18/2016	8		A. gold	Updates for 7.2	No

TABLE OF CONTENTS

List of Tables

List of Figures

1.0 INTRODUCTION

1.1 Purpose and Scope

This document describes how to install the Oracle® Communications Diameter Signal Router Full Address Resolution prouct also known as "Eagle XG Subscriber Data Server (SDS)" within a customer network. It makes use of the AppWorks 66.0 network installation and is intended to cover the initial network configuration steps for a SDS/Query Server NE for production use as part of the DSR 7.2 solution.

This document only describes the SDS product SW installation on a Virtualized solution. It does not cover hardware installation, site survey, customer network configuration, IP assignments, customer router configurations, or the configuration of any device outside of the SDS virtual machines.

1.2 References

External (*Customer Facing*)**:**

[1] *TEKELEC Acronym Guide*, MS005077, Latest Revision

[2] Diameter Signaling Router Cloud Installation Guide, E64814, Latest Revision

Internal (*ORACLE Communications Personnel Only*)**:**

[3] *DSR IP Network Planning for AT&T Mobility – LTE*, MS006641, Latest Revision

1.3 Acronyms

Acronym	Meaning
CSV	Comma Separated Values
DR	Disaster Recovery
FABR	Full Address Based Resolution
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAM	Network Operations, Administration & Maintenance
SDS	Subscriber Data Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
VIP	Virtual IP
XMI	External Management Interface

Table 1 - Acronyms

1.4 Assumptions

This procedure assumes the following;

- The user has reviewed the latest Customer specific DSR Network Planning document [3] and has received assigned values for all requested information related to SDS, Query Server, DP-SOAM and DP installation.
- The user has taken assigned values from the latest Customer specific DSR Network Planning document [3] and used them to compile XML files (See **0**) for each SDS and DP-SOAM site's NE prior to attempting to execute this procedure.
- The user conceptually understands DSR topology and SDS network configuration as described in the latest Customer specific DSR Network Planning document [3].
- The user has at least an intermediate skill set with command prompt activities on an Open Systems computing environment such as Linux or TPD.

1.5 XML Files (for installing NE)

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

1.6 How to use this Document

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

1) Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.

2) Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

If a procedural STEP fails to execute successfully, STOP and contact Oracle's Tekelec Customer Service (*US: 1-888-367-8552, Intl: +1-919-460-2150)* for assistance before attempting to continue.

2.0 PRE-INSTALLATION SETUP

2.1 Installation Prerequisites

The following items/settings are required in order to perform installation:

- A laptop or desktop computer equipped as follows;
  - Administrative privileges for the OS.
  - An approved web browser.

- TPD "admusr" user password.

2.2 Activity Logging

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

3.0 INSTALLATION OVERVIEW

3.1 Installing SDS on the Customer Network

Installing the SDS product is a task which requires multiple installations of varying types. The user should be aware that this document only covers the necessary configuration required to complete product install. Refer to the online help or contact the Oracle's Tekelec Customer Care Center for assistance with post installation configuration options.

SDS Installation: List of Procedures

In general, unless following a cross reference or otherwise instructed differently, the procedures listed here are meant to be executed in numeric order.

Table 2 - SDS Installation: List of Procedures

4.0 APPLICATION INSTALL

4.1 Create SDS Guests

Procedure 1: Create SDS Guests From OVA (VMware)

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

5. ☐	**Cloud Client:**
	
	Configure SDS Server A.
		1. Access the **SDS SERVER A VM console** via the **Cloud client** or **Cloud web client**.
		2. Login as **admusr**.
		3. Set the <**ethX**> device:
		4. **Note:** Where **ethX** is the interface associated with the **XMI** network
		`$ sudo netAdm add --device=<ethX> --address=<IP Address in External management Network> --netmask=<Netmask> --onboot=yes --bootproto=none`
		5. Add the default route for **ethX**:
		`$ sudo netAdm add --route=default --gateway=<gateway address for the External management network> --device=<ethX>`
		
		Note: When reconfiguring virtual NICs under VMware, the proper procedure is to remove the UDEV rules file (/etc/udev/rules.d/70-persistent-net.rules), shut down the guest and remove the interfaces. Power on the VM, then add the interfaces one by one, in the desrired order of enumeration, each time clicking « OK » to get VMware to instantiate the device.

Procedure 1: Create SDS Guests From OVA (VMware)

Step	Procedure	Result
6. ☐	Verify Network connectivity.	1. Ping the **default** gateway. `$ ping -c3 <gateway address for the External management network>`
7. ☐	• **Repeat these steps 1 - 6 for each server before continuing on to the next procedure.** ***(e.g. Server A, Server B, Query Server, DP)***	
THIS PROCEDURE HAS BEEN COMPLETED		

Procedure 2: Create SDS Guests From OVA (KVM/OpenStack)

Step	Procedure	Result
1. ☐	**Preparation**	1. Create instance flavors. a. Use the Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the “Admin” section, or with the “nova flavor-create” command line tool. Make the flavor names as informative as possible. As flavors describe resource sizing, a common convention is to use a name like “0406060” where the first two figures (04) represent the number of virtual CPUs, the next two figures (06) might represent the RAM allocation in GB and the final three figures (060) might represent the disk space in GB. 2. If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, please note that the default LRO (Large Receive Offload) option must be disabled on the host command line. Please see the Intel release notes for more details. This action can be performed with the following command. `a. $ sudo ethtool -K <ETH_DEV> lro off` 3.

Procedure 2: Create SDS Guests From OVA (KVM/OpenStack)

Step	Procedure	Result
2. ☐	**Add SDS OVA image.**	1. Copy the OVA file to the OpenStack control node. i. `$ scp SDS-7.2.x.x.x.ova admusr@node:~` 2. Login to the OpenStack control node. i. `$ ssh admusr@node` 3. In an empty directory unpack the OVA file using “tar” i. `$ tar xvf SDS-7.2.x.x.x.ova` 4. One of the unpacked files will have a “.vmdk” suffix. This is the VM image file that must be imported. i. SDS-7.2.x.x.x-disk1.vmdk 5. Source the OpenStack “admin” user credentials. i. `$ . keystonerc_admin` 6. Select an informative name for the new image. i. “sds-7.2.x.x.x-original” 7. Import the image using the “glance” utility from the command line. i. `$ glance image-create --name sds-7.2.x.x.x-original --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file SDS-7.2.x.x.x-disk1.vmdk` ii. This process will take about 5 minutes, depending on the underlying infrastructure.
3. ☐	**Name the new VM instance.**	Create an informative name for the new instance: “SDS-NO1”. Examine the network interface recommendations at the bottom of the Resource Profile in Appendix C.

Procedure 2: Create SDS Guests From OVA (KVM/OpenStack)

Step	Procedure	Result
4. ☐	**Create and boot the VM instance from the glance image.**	1. Get the following configuration values. a. The image ID. i. `$ glance image-list` b. The flavor ID. i. `$ nova flavor-list` c. The network ID(s) i. `$ neutron net-list` d. An informative name for the instance. i. "SDS-NO1" ii. "SDS-NO2" 2. Create and boot the VM instance. a. The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Use one "—nic" argument for each IP/interface. Note that IPv6 addresses should use the "v6-fixed-ip" argument instead of "v4-fixed-ip". b. `$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>` c. View the newly created instance using the nova tool. i. `$ nova list --all-tenants` The VM will take approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.
5. ☐	**Configure VIP (optional).**	1. If a NOAM/SOAM VIP is needed, execute the following commands. 2. Find the port id associated with the instances' network interface. a. `$ neutron port-list` 3. Add the VIP IP address to the address pairs list of the instances network interface port. a. `$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>` If necessary, see Allowed Address Pairs in Appendix E for more information

Procedure 2: Create SDS Guests From OVA (KVM/OpenStack)

Step	Procedure	Result
6. ☐	**Configure instance networking.**	1. Log in to the "Horizon" GUI as the DSR tenant user. 2. Go to the Compute/Instances section. 3. Click on the "Name" field of the newly created instance. 4. Select the "Console" tab. 5. Login as the admusr. 6. Select an informative hostname for the new VM instance. a. "SDS-NO1". b. "SDS-SO2". 7. Use sudo to change the machine hostname from the default value. a. Edit /etc/hosts. i. Append the hostname to the IPv4 line. 1. "127.0.0.1 localhost localhost4 NO1" ii. Append the hostname to the IPv6 line. 1. "::1 localhost localhost6 NO1" b. Edit /etc/syconfig/hostname. i. Change the "HOSTNAME=XXXX" line to the new hostname. ii. "HOSTNAME=SDS-NO1" c. Set the hostname on the command line. i. `$ sudo hostname SDS-NO1` 8. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. a. `$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi port ip> --netmask=<xmi net mask>` b. `$ sudo netAdm add --onboot=yes --device=eth1 --address=<imi port ip> --netmask=<imi net mask>` c. `$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>` d. Under some circumstances, it may be necessary to configure more interfaces. e. If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions. i. `$ cd /etc/sysconfig/network-scripts` ii. `$ sudo mv ifcfg-ethX /tmp` 1. Keep ifcfg-ethX in /tmp until ethX is working correctly. iii. Re-run the netAdm command. It will create and configure the interface in one action. 9. Reboot the VM. It will take approximately 5 minutes for the VM to complete rebooting. a. `$ sudo init 6` The new VM should now be accessible via both netwok and Horizon console.

Procedure 2: Create SDS Guests From OVA (KVM/OpenStack)

Step	Procedure	Result
7. ☐	Verify Network connectivity.	Ping the **default** gateway. `$ ping -c3 <gateway address for the External management network>`
8. ☐	• **Repeat these steps 1 - 6 for each server before continuing on to the next procedure.** ***(e.g. Server A, Server B, Query Server, DP)***	
THIS PROCEDURE HAS BEEN COMPLETED		

5.0 CONFIGURATION PROCEDURES

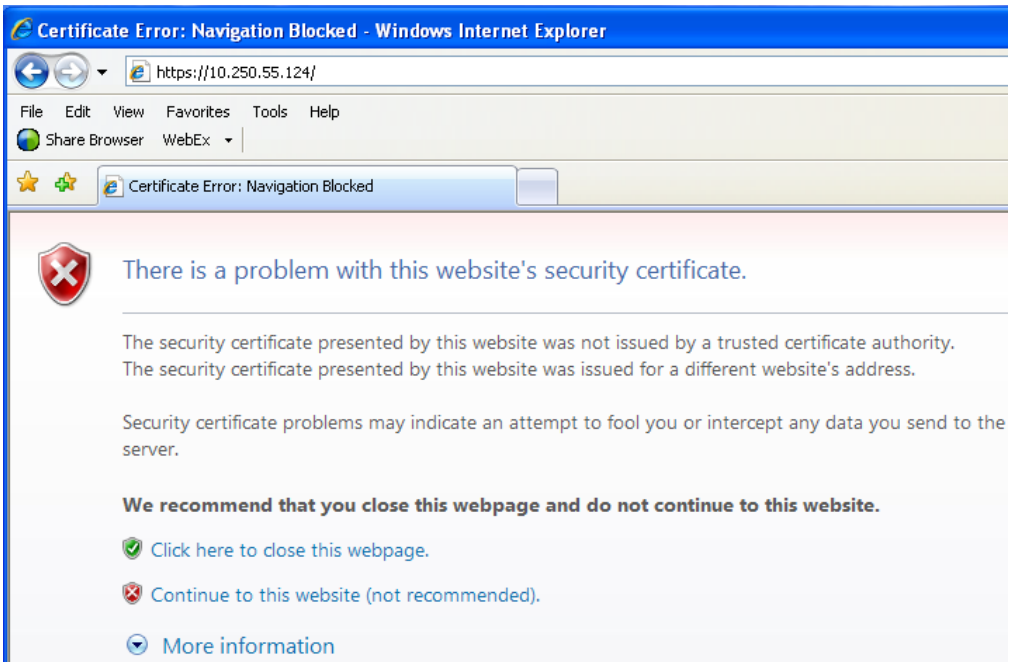
5.1 Configuring SDS Servers A and B

Assumptions:

- This procedure assumes that the SDS Network Element XML file for the Primary Provisioning SDS site has previously been created, as described in **0.**
- This procedure assumes that the Network Element XML files are on the laptop's hard drive.

This procedure requires that the user connects to the SDS GUI prior to configuring the first SDS server.

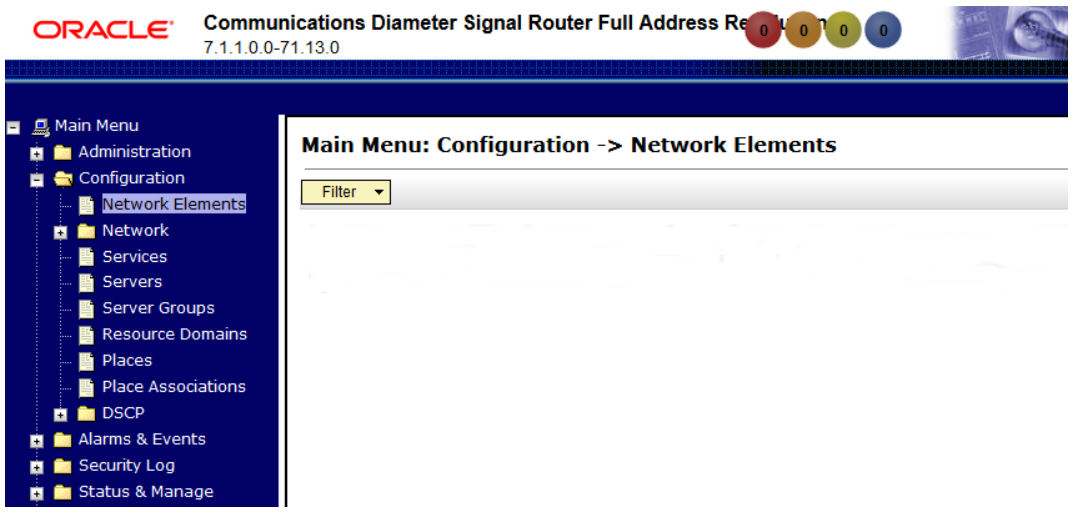
Procedure 3: Configuring SDS Servers A and B

Step	Procedure	Result
1. ☐	**SDS Server A:** Launch an approved web browser and connect to the SDS SERVER A XMI IP address. **NOTE:** *If presented with the "security certificate" warning screen shown to the right,* ***choose the following option:*** ***"Continue to this website (not recommended)".***	

Procedure 3: Configuring SDS Servers A and B

Step	Procedure	Result
2. ☐	**SDS Server A:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 3.1 Configuring the Network Element

3. ☐	**SDS Server A:** Select… **<u>Main Menu</u>** → **Configuration** → ***Network Elements*** …as shown on the right.	

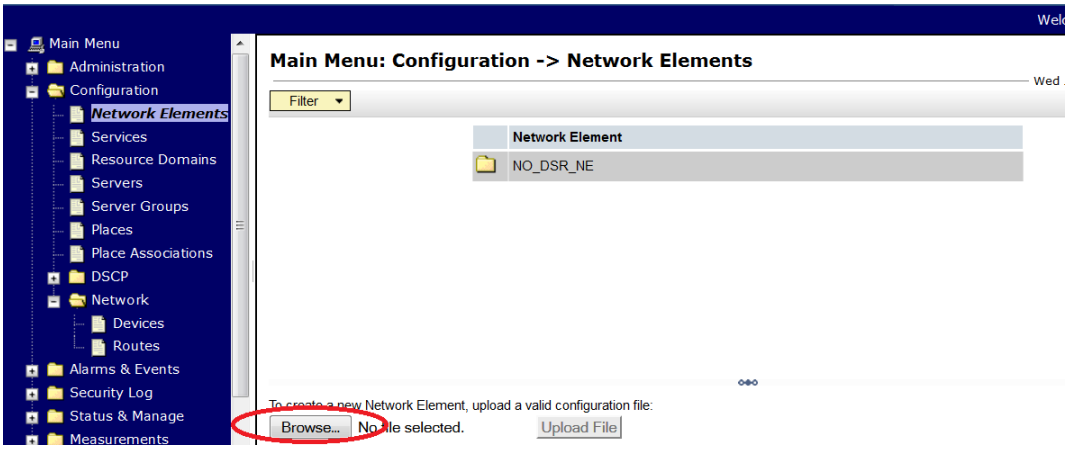
Procedure 3.1 Configuring the Network Element

4. ☐

SDS Server A:

From the **Configuration / Network Elements** screen…

Select the **"Browse"** dialogue button (scroll to bottom left corner of screen).



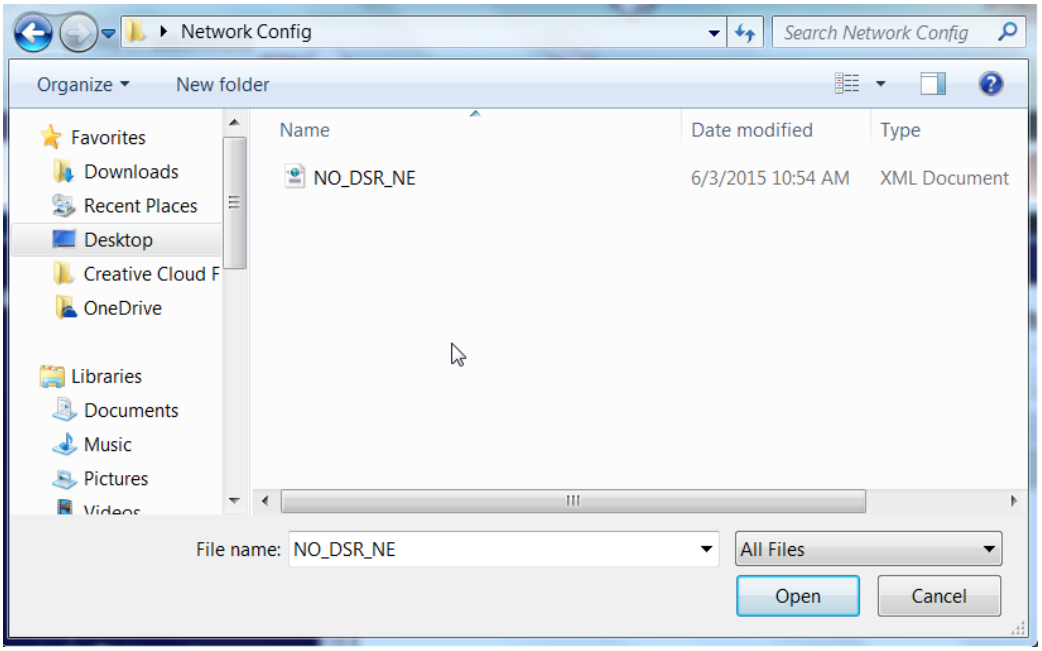
5. ☐

SDS Server A:

Note: This step assumes that the **xml** files were previously prepared, as described in **0**.

1) Select the location containing the site **.xml** file.

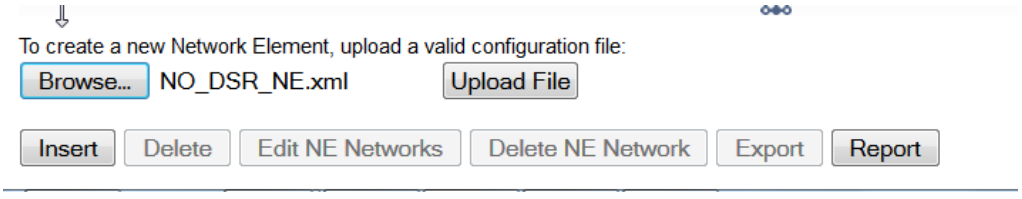
2) Select the **.xml** file and click the **"Open"** dialogue button.



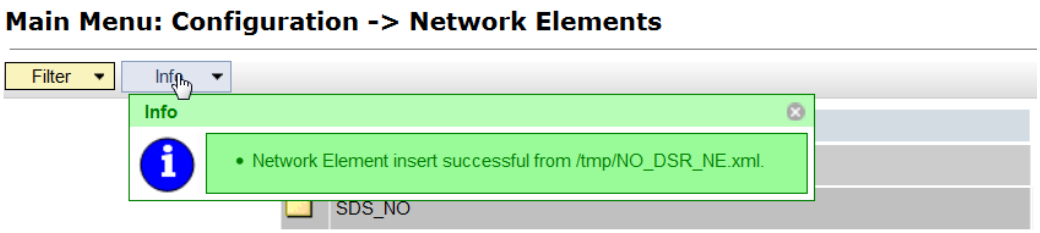
6. ☐

SDS Server A:

Select the **"Upload File"** dialogue button (bottom left corner of screen).



Procedure 3.1 Configuring the Network Element

7. ☐	**SDS Server A:** If the values in the **.xml** file pass validation rules, the user will receive a banner information message showing that the data has been successfully validated and committed to the DB. **NOTE:** *You may have to left mouse click the **"Info"** banner option in order to see the banner output.*	

Procedure 3.2 Configuring Services

8. ☐

SDS Server A:

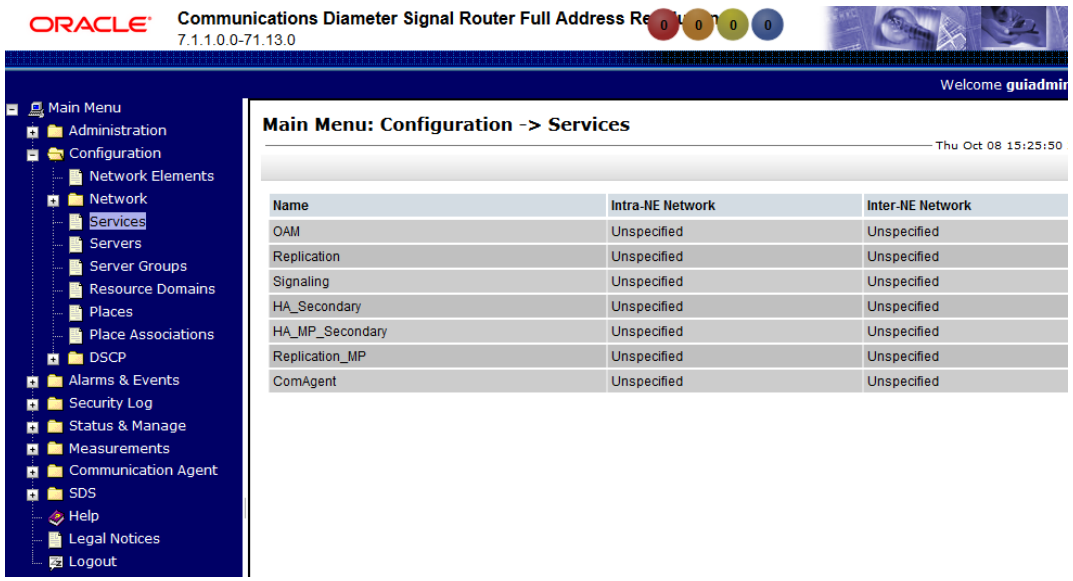
Select…

Main Menu
→ **Configuration**
→ ***Services***

…as shown on the right.

1) The user will be presented with the "**Services**" configuration screen as shown on the right.

2) Select the **"Edit"** dialogue button.



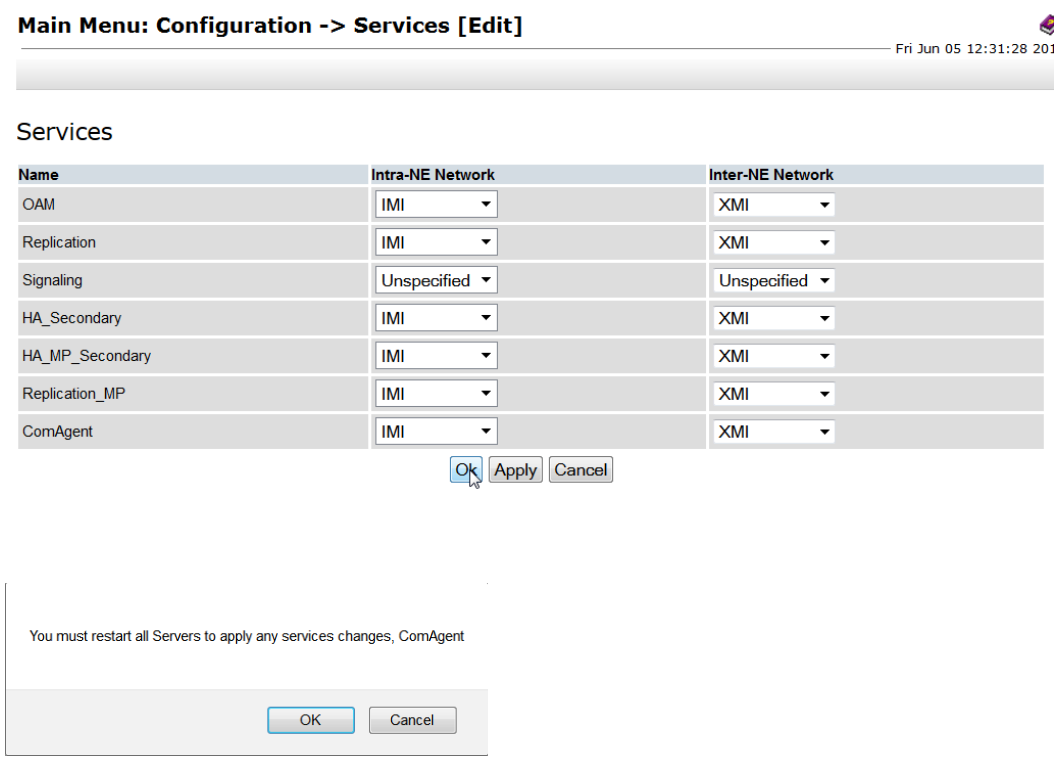
9. ☐

SDS Server A:

1) With the exception of **"Signaling"** which is left **"Unspecified"**, set other services values so that all **Intra-NE Network** traffic is directed across **IMI** and all **Inter-NE Network** traffic is across **XMI**.

2) Select the **"Ok"** dialogue button.

3) Select the **"Ok"** popup dialogue button.

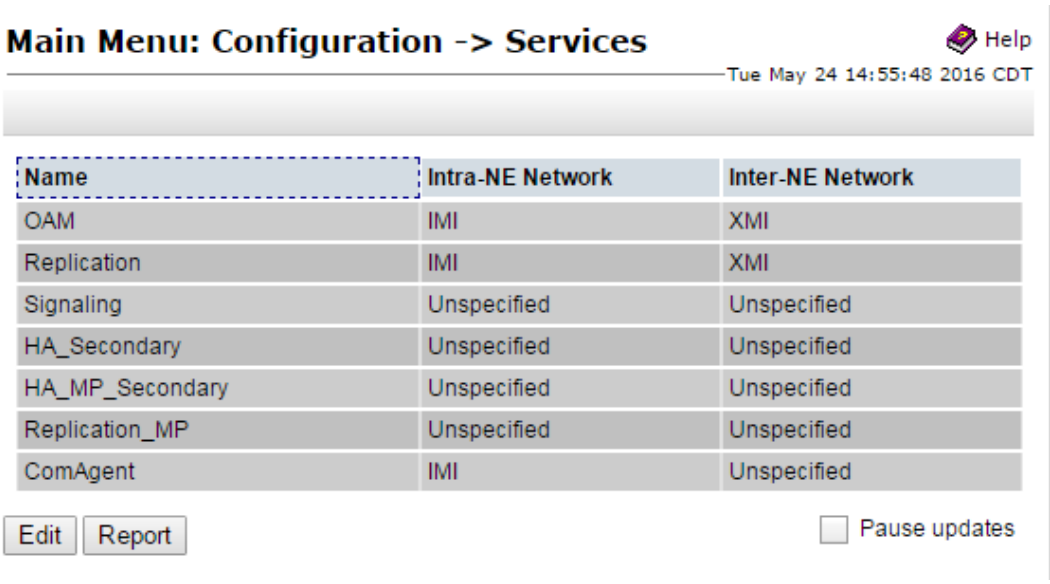


Procedure 3.2 Configuring Services

10. ☐

SDS Server A:

The user will be presented with the "**Services**" configuration screen as shown on the right



Procedure 3.3 Configuring the SDS Server

11. ☐

Note: This step thru the last step of this procedure need to be done for both SDS Server A and SDS Server B.

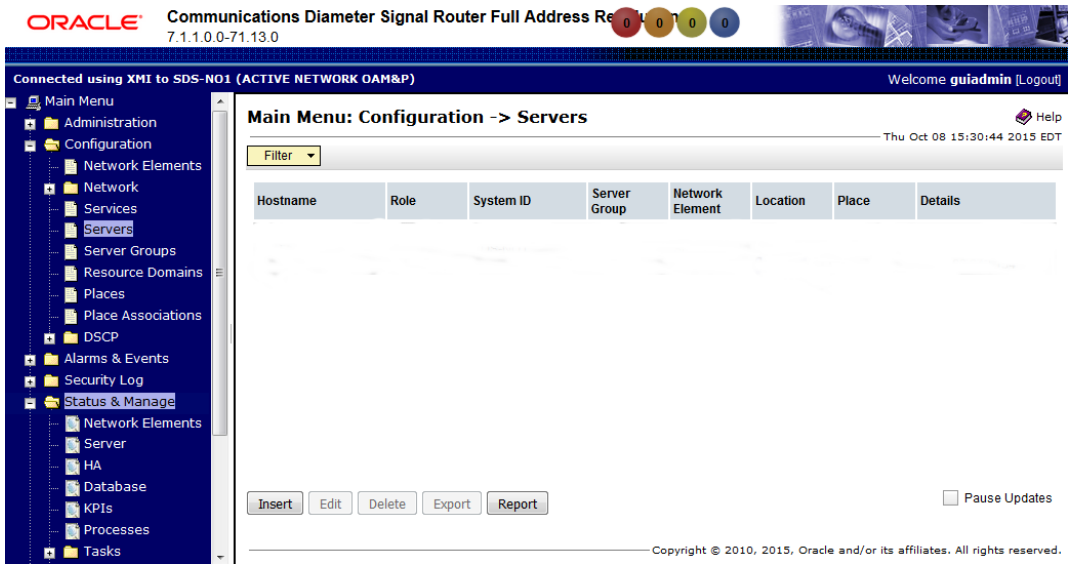
SDS Server A or B:

Select…

Main Menu
→ **Configuration**
→ ***Servers***

…as shown on the right.

Select the **"Insert"** dialogue button.



Procedure 3.3 Configuring the SDS Server

12. ☐

SDS Server A or B:

1) Input the assigned "**hostname"** for the SDS Server (A or B).

2) Select **"NETWORK OAM&P"** for the server **"Role"** from the pull-down menu.

3) Input the assigned hostname again as the "**System ID**" for the SDS Server (A or B).

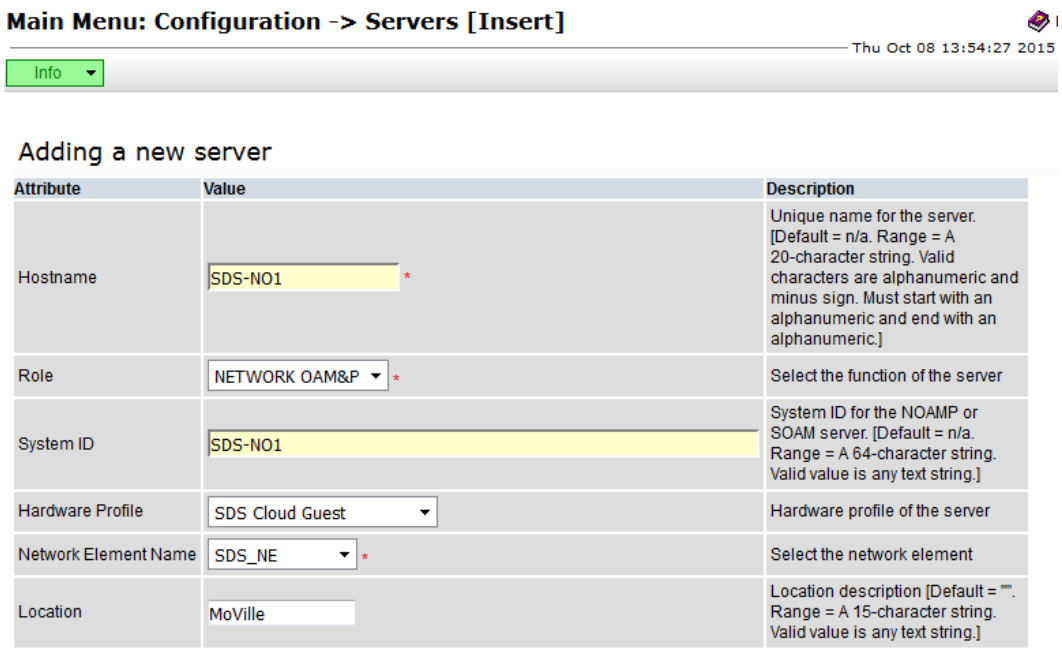
4) Select "**SDS Cloud Guest**" for the **Hardware Profile**.

5) Select the **Network Element Name** for the SDS from the pull-down menu.

NOTE: *After the Network Element Name is selected, the Interfaces fields will be displayed, as seen in step* **13***.*

6) Enter the site location.

NOTE: *Location is an optional field.*



Procedure 3.3 Configuring the SDS Server

13. ☐

SDS Server A or B:

1) Enter the XMI and IMI IP addresses for the SDS Server.

OpenStack Note: These must be the addresses used during instance booting and networking.

2) Set the **XMI** and **IMI Interfaces** to Ethernet interfaces associated with the **XMI and IMI Virtual networks**. **DO NOT**check the **VLAN** checkboxs.

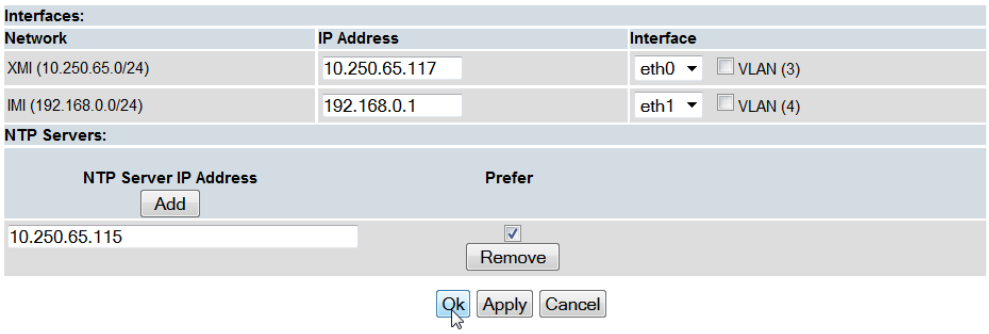
3) Click the "**NTP Servers:**" **"Add"** dialogue button.

4) Enter the **NTP Server IP Address** for an NTP Server.

5) If you have another **NTP Server IP address**, repeat (1) and (2) to enter it.

6) Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other.

7) Click the **"Ok"** dialogue button.



Procedure 3.4 Applying the SDS Server Configuration File

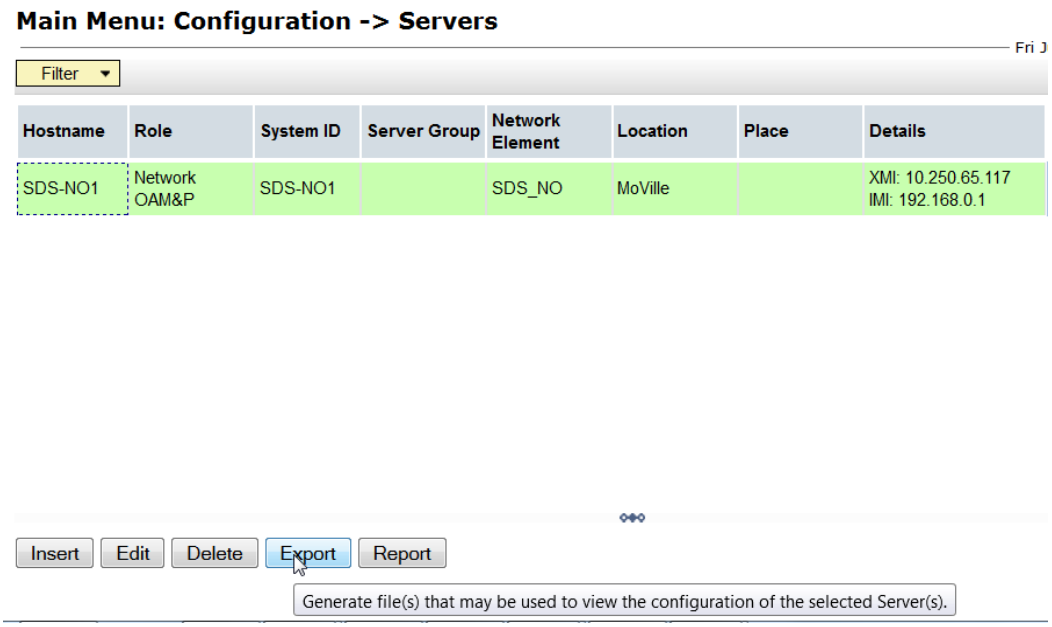
14. ☐

SDS Server A or B:

1) Use the cursor to select the **SDS Server** entry added in **Steps 11 - 13**.

The row containing the desired **SDS Server** should now be highlighted in **GREEN**.

2) Select the **"Export"** dialogue button.



15. ☐

SDS Server A or B:

Copy the **server** configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname from the file name.

NOTE: *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

Example Server A:

TKLCConfigData<hostname>.sh ➔ will translate to ➔TKLCConfigData.sh

```
[admusr@hostname1260476099 ~]$ cp
/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh
/var/tmp/TKLCConfigData.sh
[admusr@hostname1260476099 ~]$
```

Example Server B:

Obtain a terminal session on **Server A** as admusr. Log in as admusr on the **Server A** shell, and issue the following commands:

```
[admusr@sds-mrsvnc-a ~]$ scp \
/var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh \
<ipaddr>:/var/tmp/TKLCConfigData.sh
```

Note: ipaddr is the IP address of Server B associated with the xmi network.

Procedure 3.4 Applying the SDS Server Configuration File

16. ☐	**SDS Server A or B:**
	After the script completes, a broadcast message will be sent to the terminal.
	
	NOTE: *The user should be aware that the time to complete this step varies by server and may take from 3-20 minutes to complete.*
		***** NO OUTPUT FOR ≈ 3-20 MINUTES *****
		`Broadcast message from root (Thu Dec 1 09:41:24 2011):`
		
		`Server configuration completed successfully!`
		
		`See /var/TKLC/appw/logs/Process/install.log for details.`

17. ☐	**SDS Server A or B:** Set the time zone (optional) and initiate a reboot of the **SDS Server**.	To change the system time zone, from the command line prompt, execute ***set_ini_tz.pl***. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see List of Frequently Used Time Zones, Appendix B. **$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1** `[admusr@hostname1260476099 ~]$` **`sudo init 6`**
18. ☐	**SDS Server A or B:** After the server has completed reboot… Verify that the server console returns to a login prompt.	`sds-mrsvnc-a login:` **`admusr`** `Password:` ***<admusr_password>***

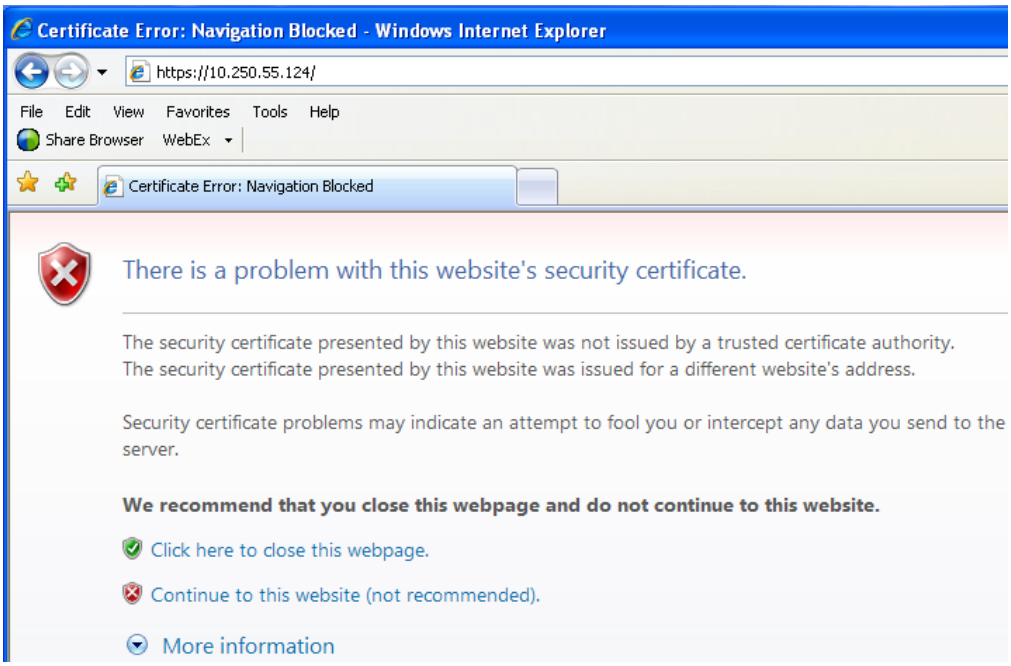
19. ☐	**SDS Server A or B:**
	Execute a **"syscheck"** to verify the current health of the server.
		`[admusr@sds-mrsvnc-a ~]$` **`sudo syscheck`**
		`Running modules in class system...`
		`OK`
		
		`Running modules in class proc...`
		`OK`
		
		`Running modules in class net...`
		`OK`
		
		`Running modules in class hardware...`
		`OK`
		
		`Running modules in class disk...`
		`OK`
		
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[admusr@sds-mrsvnc-a ~]$`

Procedure 3.4 Applying the SDS Server Configuration File		
20. ☐	**SDS Server A or B:** Exit from the command line to return the server console to the login prompt.	`[admusr@sds-mrsvnc-a ~]$ exit` `sds-mrsvnc-a login:`
21. ☐	• **Configure SDS Server B by repeating steps 112 - 200 of this procedure**.	
THIS PROCEDURE HAS BEEN COMPLETED		

5.2 OAM Pairing

The user should be aware that during the OAM Pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 4: Pairing the OAM Servers (1st SDS site only)

Step	Procedure	Result
1. ☐	**SDS Server A:** Launch an approved web browser and connect to the XMI IP address assigned to **SDS Server A** using "https://"	
2. ☐	**SDS Server A:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 4.1 Configuring the SDS Server Group

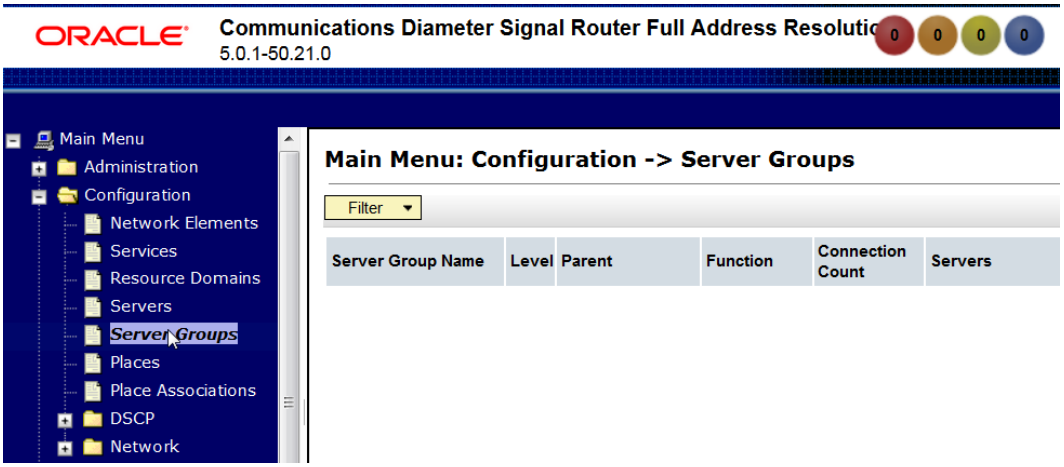
3. ☐

SDS Server A:

Select…

Main Menu
→ **Configuration**
→ ***Server Groups***

…as shown on the right.



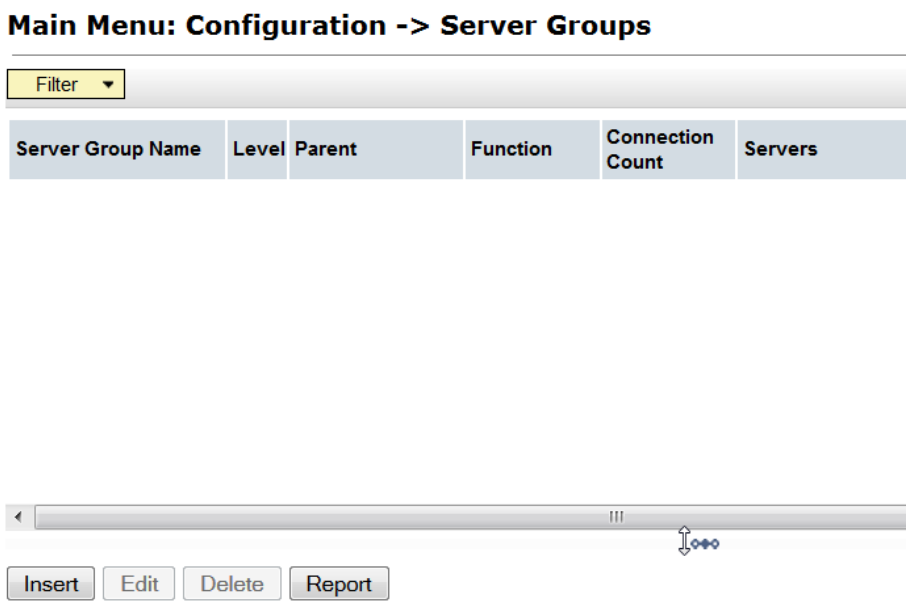
4. ☐

SDS Server A:

1) The user will be presented with the **"Server Groups"** configuration screen as shown on the right.

2) Select the **"Insert"** dialogue button from the bottom left corner of the screen.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Insert"** dialogue button visible.*

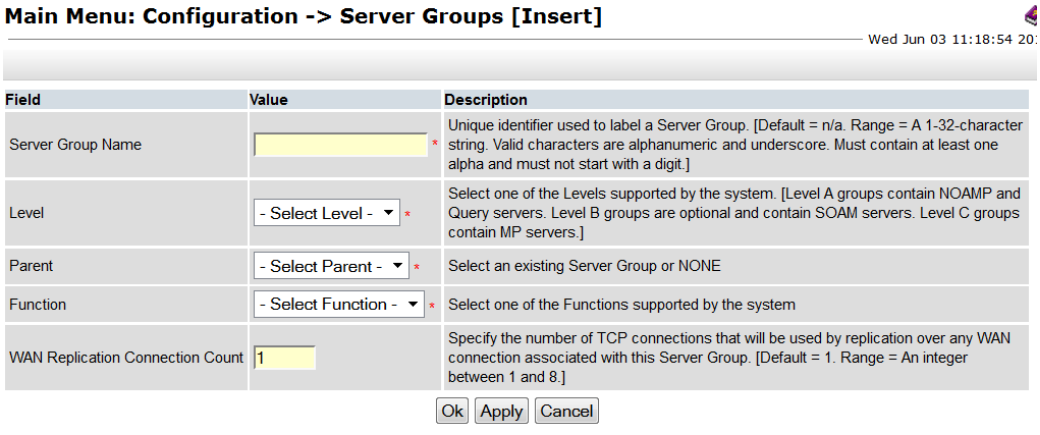


5. ☐

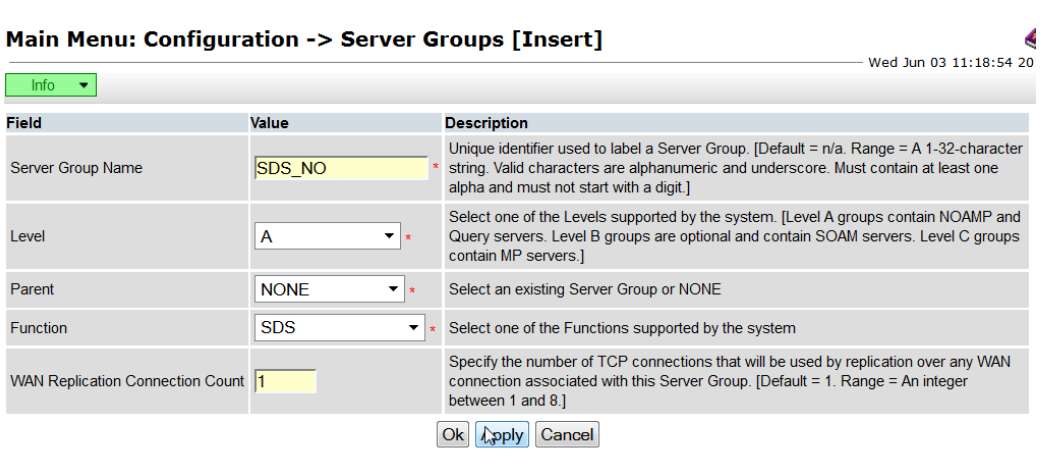
SDS Server A:

The user will be presented with the **"Server Groups [Insert]"** screen as shown on the right.

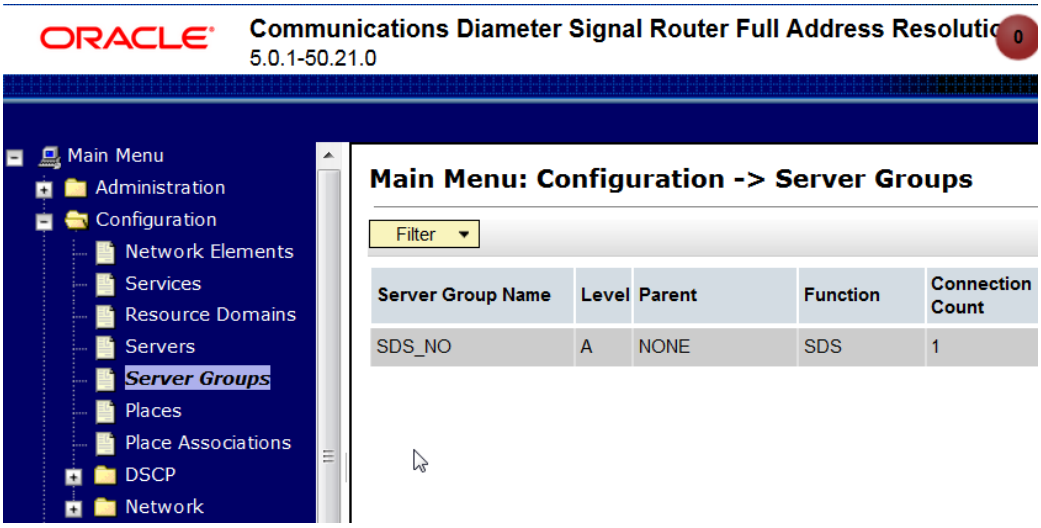
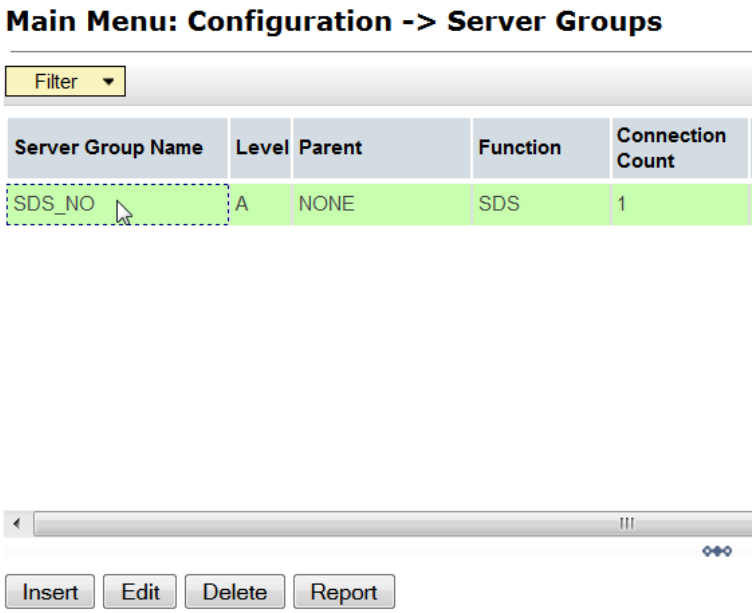
NOTE: *Leave the "**WAN Replication Connection Count**" blank (it will default to 1).*



Procedure 4: Pairing the OAM Servers (1st SDS site only)

Step	Procedure	Result
6. ☐	**SDS Server A:** Input the **Server Group Name**. Select **"A"** on the **"Level"** pull-down menu. Select **"None"** on the **"Parent"** pull-down menu. Select **"SDS"** on the **"Function"** pull-down menu. Select the "**Ok**" dialogue button.	

Procedure 4.2 Adding a Server to an OAM Server Group

7. ☐	**SDS Server A:** The **Server Group** entry added in **Steps 5 - 6** should now appear on the **"Server Groups"** configuration screen as shown on the right.	
8. ☐	**SDS Server A:** **1)** Select the **Server Group** entry added in **Steps 5 - 7**. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Edit"** dialogue button from the bottom left corner of the screen. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Edit"** dialogue button visible.*	

Procedure 4.2 Adding a Server to an OAM Server Group

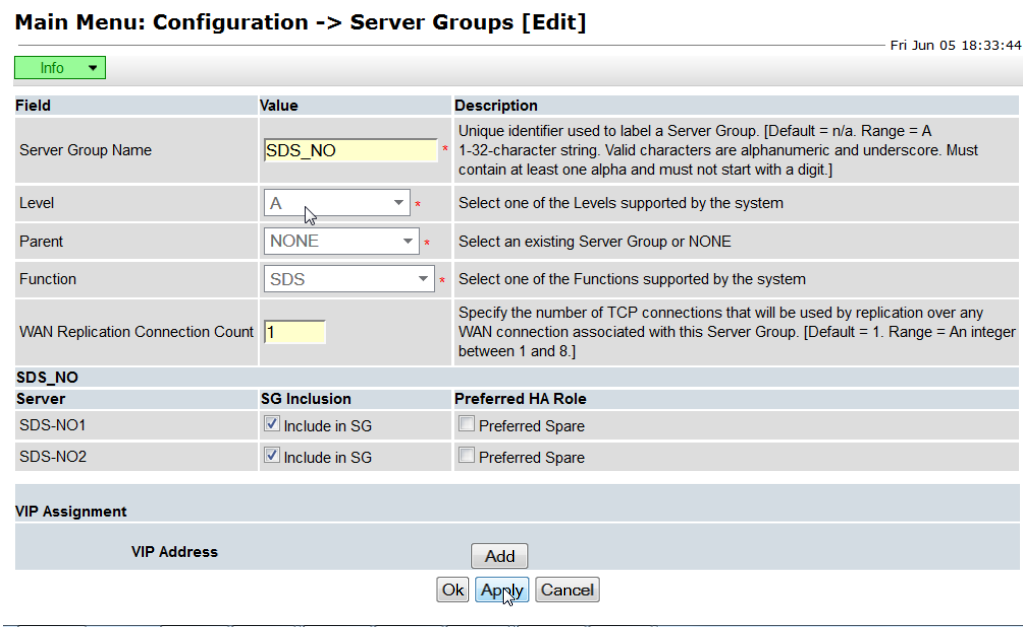
9. ☐

SDS Server A:

The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.

1) Select the **"A"** server and the **"B"** server if configured from the list of **"Servers"** by clicking the check box next to their names.

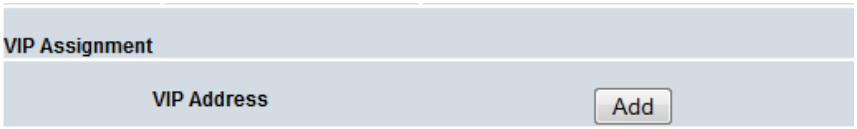
2) Select the **"Apply"** dialogue button.



10. ☐

SDS Server A:

Click the **"Add"** dialogue button for the **VIP Address**.

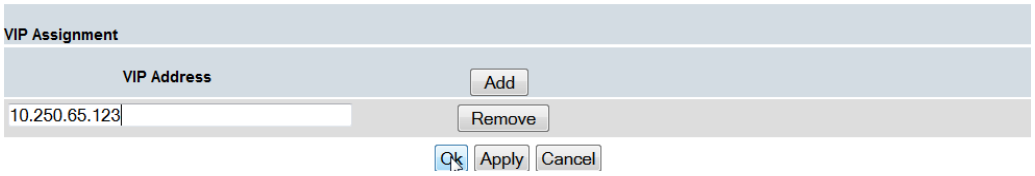


11. ☐

SDS Server A:

1) Input the **VIP Address.**

2) Select the **"Apply"** dialogue button.



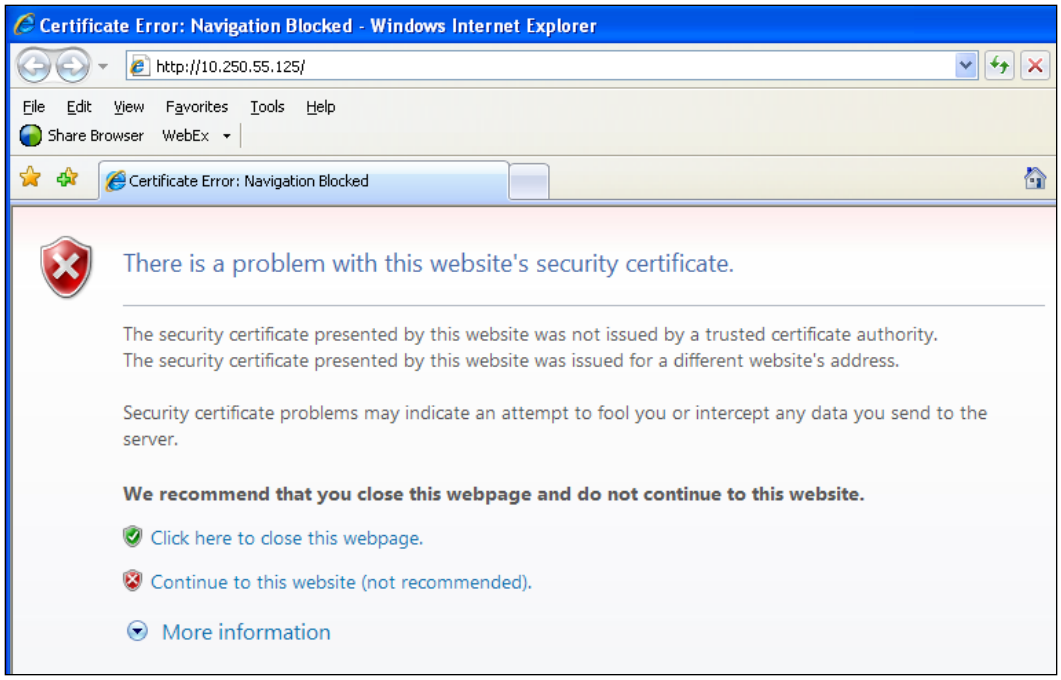
12. ☐

IMPORTANT:

Wait at least **5 minutes** before proceeding on to the next Step.

- Now that the server(s) have been paired within a Server Group they must establish a master/slave relationship for High Availability (HA). It may take several minutes for this process to be completed.
- Allow a minimum of **5 minutes** before continuing to the next Step.

Procedure 4.2 Adding a Server to an OAM Server Group

13. ☐	**SDS VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** assigned in **STEP 11** to the **SDS Server Group** using **"https://".**	
14. ☐	**SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 4.2 Adding a Server to an OAM Server Group

15. ☐

SDS VIP:

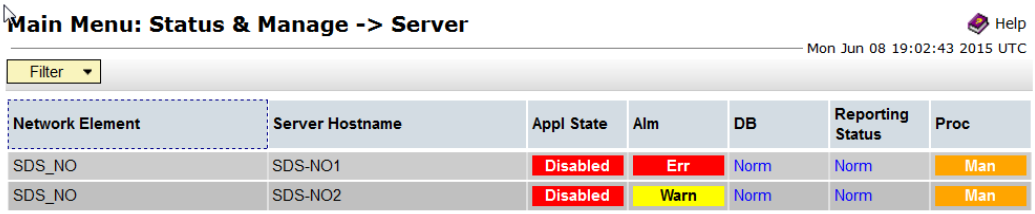
Select…

Main Menu
→ Status & Manage
→ *Server*

…as shown on the right.

1) The **"A"** and **"B"** SDS servers should now appear in the right panel.

2) Verify that the **"DB"** status shows **"Norm"** and the **"Proc"** status shows **"Man"** for both servers before proceeding to the next Step.



Procedure 4.2 Adding a Server to an OAM Server Group

16. ☐

SDS VIP:

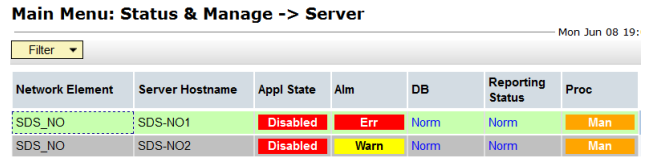
1) Using the mouse, select **SDS Server A**. The line entry should now be highlighted in **GREEN**.

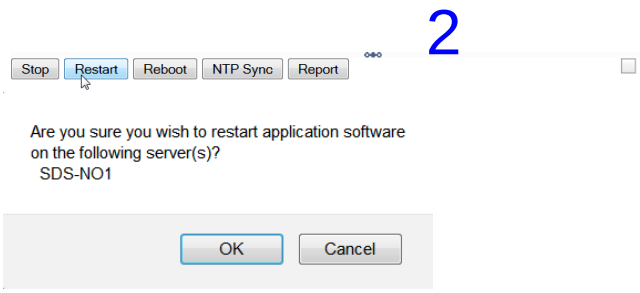
2) Select the **"Restart"** dialogue button from the bottom left corner of the screen.

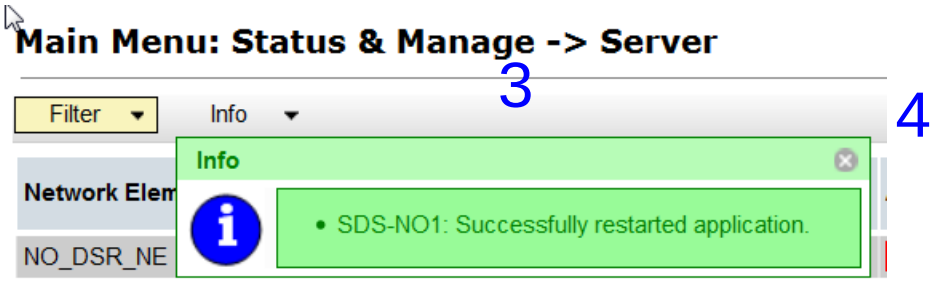
3) Click the **"OK"** button on the confirmation dialogue box.

4) The user should be presented with a confirmation message (in the banner area) for **SDS Server A** stating: **"Successfully restarted application"**.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*







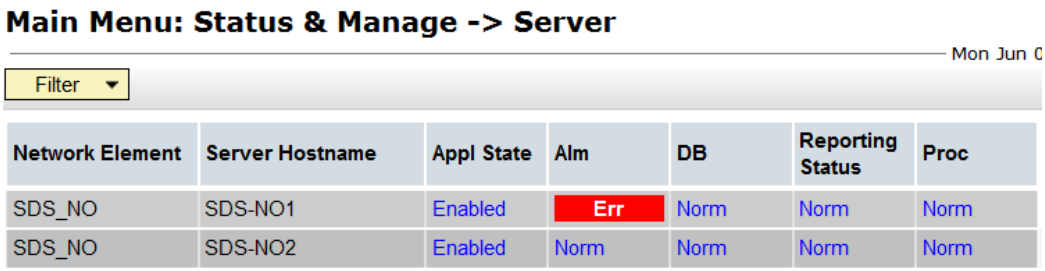
Procedure 4.2 Adding a Server to an OAM Server Group

17. ☐

SDS VIP:

Verify that the **"Appl State"** now shows **"Enabled"** and that the **"DB, Reporting Status & Proc"** status columns all show **"Norm"** for **SDS Server A** before proceeding to the next Step.

NOTE: *If user chooses to refresh the Server status screen in advance of the default setting (15-30 sec.). This may be done by simply reselecting the **"Status & Manage → Server"** option from the Main menu on the left.*



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

18. ☐

- **Configure SDS Server B by repeating steps 16 - 17 of this procedure**.

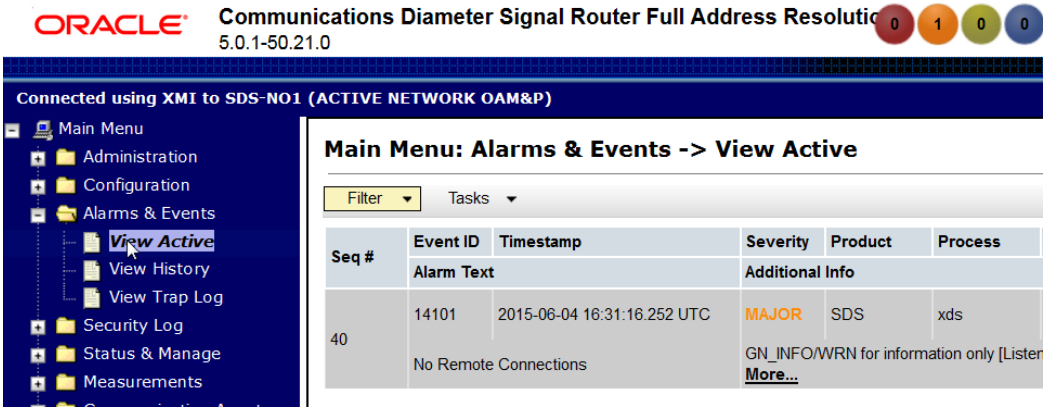
19. ☐

IMPORTANT:

Wait at least **5 minutes** before proceeding on to the next Step.

- Now that the server(s) have been restarted they must establish a master/slave relationship for High Availability (HA). It may take several minutes for this process to be completed.
- Allow a minimum of **5 minutes** before continuing to the next Step.

Procedure 4.3 Verifying the SDS Server Alarm status

20. ☐	**SDS VIP:** If there is a context switch, you may be required to login again. Login to the GUI using the default user and password.	
21. ☐	**SDS VIP:** Select… **<u>Main Menu</u>** → **Alarms & Events** → ***View Active*** …as shown on the right. Verify that **Event ID 14101** (“*No Remote Connections”***)** is the only alarm present on the system at this time.	

Procedure 4.4 Configuring SNMP for Traps from Individual Servers

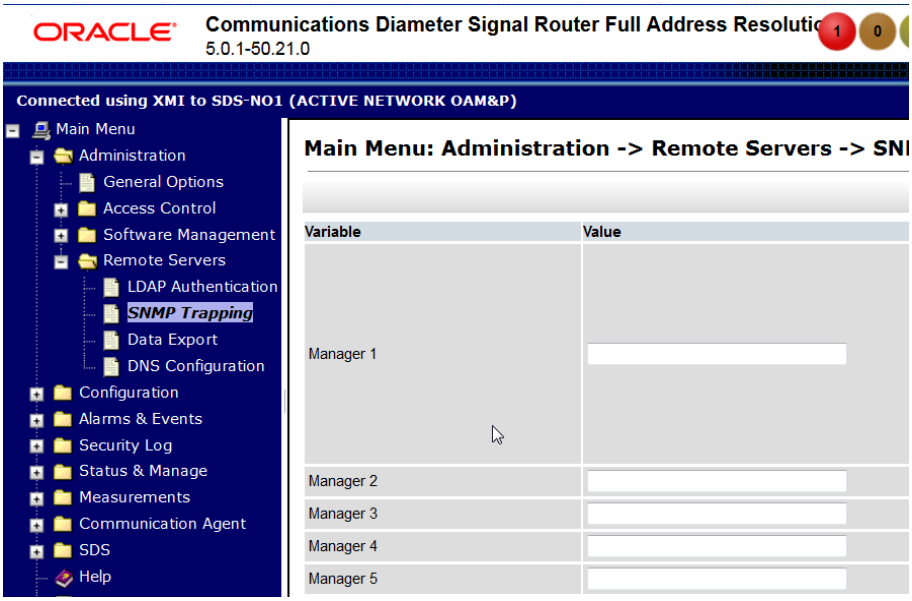
22. ☐

SDS VIP:

Select…

Main Menu
→ Administration
→ Remote Servers
→ SNMP Trapping

…as shown on the right.

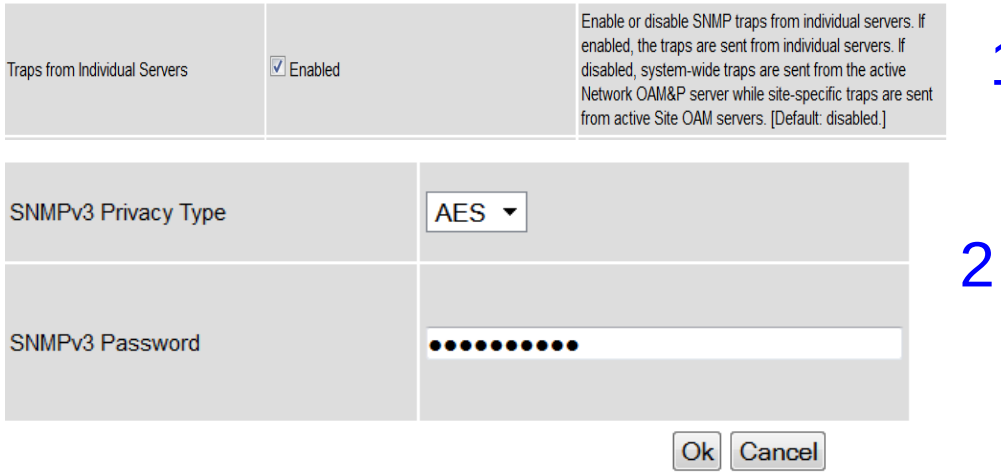


23. ☐

SDS VIP:

1) Using the cursor, place a "check" in the check box for **"Traps from Individual Servers"**.

2) Click the **"Ok"** dialogue button located at the bottom of the right panel.

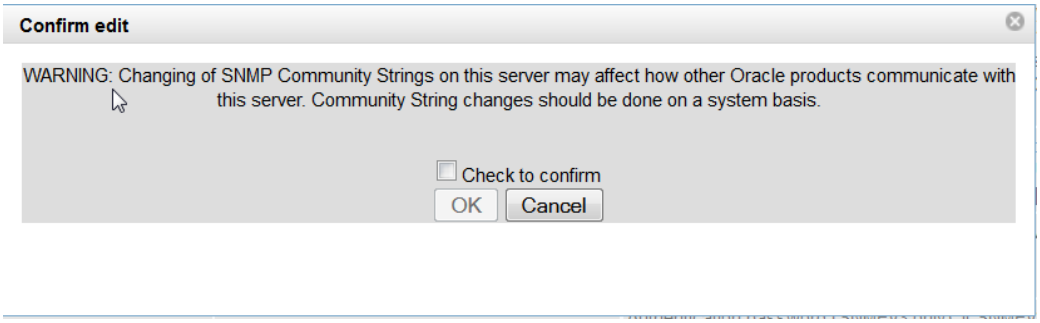


24. ☐

SDS VIP:

1) Using the cursor, place a "check" in the check box for **"Check to confirm"**.

2) Click the **"OK"** dialogue button.

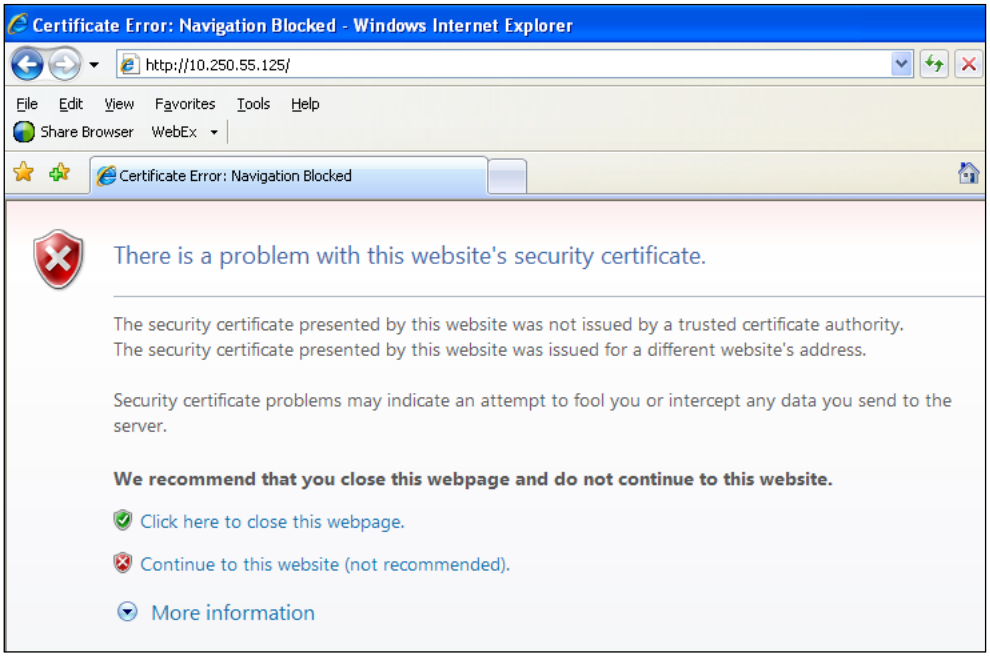
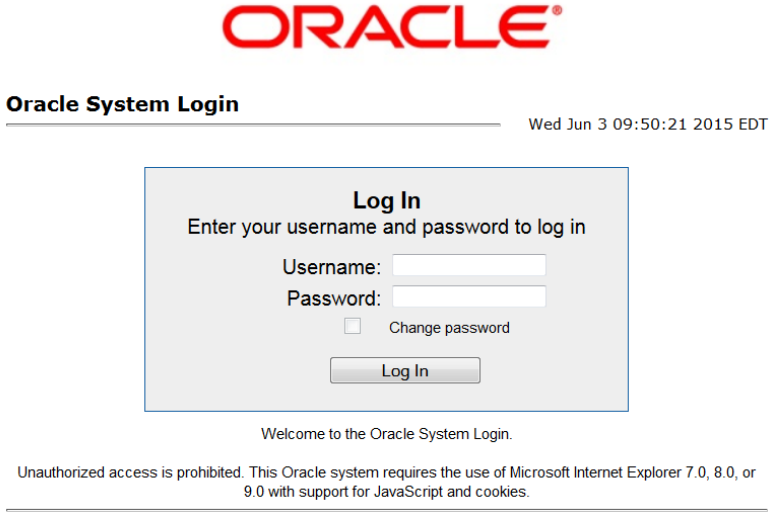


THIS PROCEDURE HAS BEEN COMPLETED

5.3 Query Server Installation

The user should be aware that during the Query Server installation procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 5: Configuring the Query Server

Step	Procedure	Result
1. ☐	**Active SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to **Active SDS site** using "https://"	
2. ☐	**Active SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 5.1 Configuring the Query Server

3. ☐

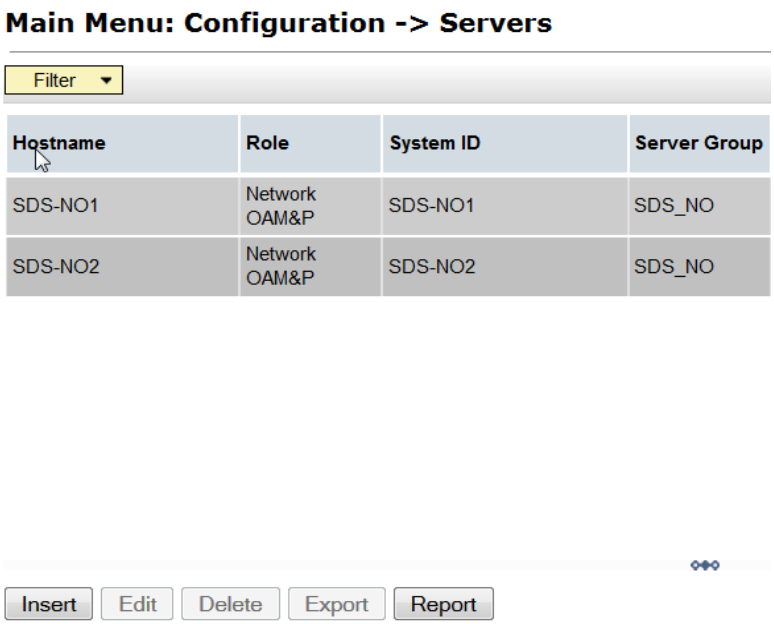
Active SDS VIP:

Select…

Main Menu
→ **Configuration**
→ ***Servers***

…as shown on the right.

Select the **"Insert"** dialogue button.



4. ☐

Active SDS VIP:

1) Input the assigned "**hostname"** for the Query Server.

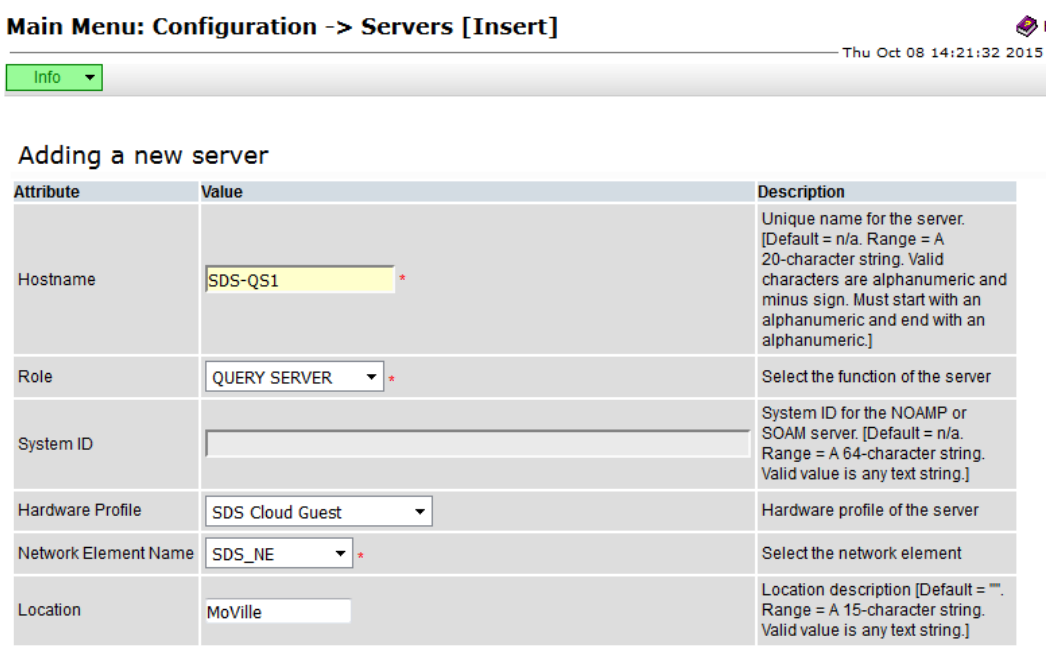
2) Select **"QUERY SERVER"** for the server **"Role"** from the pull-down menu.

3 Select "**SDS Cloud Guest**" for the **Hardware Profile**.

4) Select the **Network Element Name** of the **SDS site** where the Query Server is physically located from the list of available NEs in the pull-down menu.

5) Enter the site location.

NOTE: *Location is an optional field.*



Procedure 5.1 Configuring the Query Server

5. ☐

1) Enter the **IMI** IP addresses for the **Query Server**.

2) Set the **IMI Interfaces** to "**ethX**" and **DO NOT check** each the **VLAN** checkbox
.

3) Enter the **XMI IP address** for the **Query Server**.

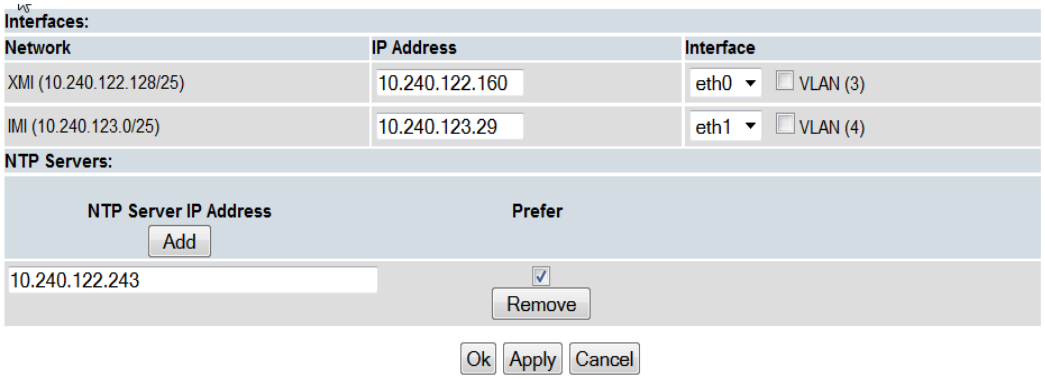
4) Set the **XMI Interface** to "**ethX**" and **DO NOT** check the **VLAN** box.

5) Click the "**NTP Servers:**" **"Add"** dialogue button.

6) Enter the **NTP Server IP Address** for an NTP Server.

7) If you have another **NTP Server IP address**, repeat (1) and (2) to enter it.

8) Click the **"Ok"** dialogue button.



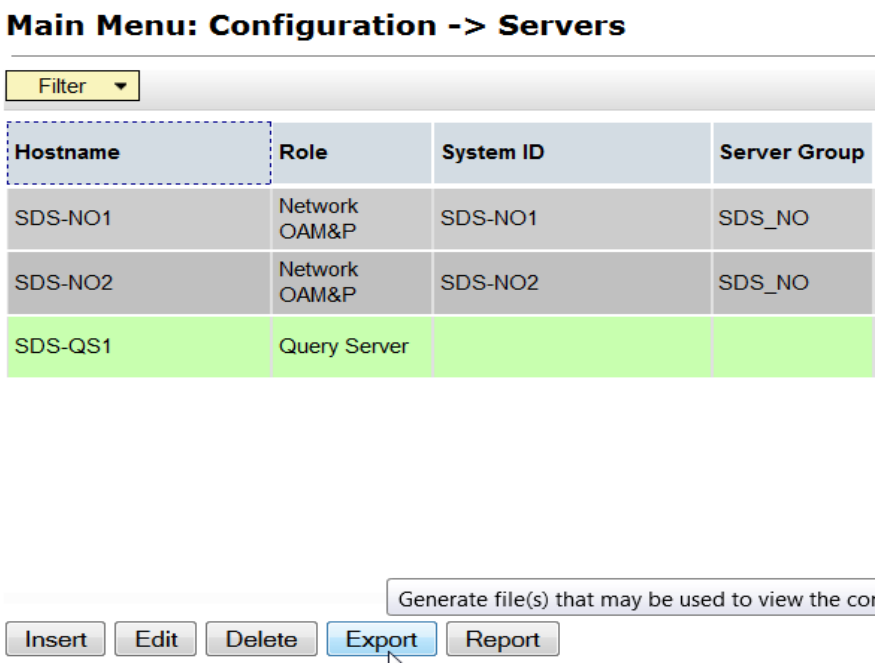
Procedure 5.2 Applying the Query Server Configuration file

6. ☐

Active SDS VIP:

1) Select the "**Query Server"** in the configuration Menu.

2) Select the **"Export"** dialogue button.



7. ☐

Active SDS VIP:

Copy the Query Server configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname from the file name.

NOTE: *The server will poll the* ***/var/tmp*** *directory for the presence of the configuration file and automatically execute it when found.*

Example:

TKLCConfigData.<hostname>.sh ➔ will translate to ➔TKLCConfigData.sh

Obtain a terminal session on the **Active SDS VIP** as admusr. Log in as admusr on the **Active SDS VIP** shell, and issue the following commands:

```
[admusr@sds-mrsvnc-a ~]$ scp \
/var/TKLC/db/filemgmt/TKLCConfiguData.<hostname>.sh \
<ipaddr>:/var/tmp/TKLCConfigData.sh
```

Note: ipaddr is the IP address of Query Server associated with the xmi network.

Procedure 5.2 Applying the Query Server Configuration file

8. ☐

Query Server:

Log into the Query Server as root. After the script completes, a broadcast message will be sent to the terminal.

NOTE: *The user should be aware that the time to complete this step varies by server and may take from 3-20 minutes to complete.*

***** NO OUTPUT FOR ≈ 3-20 MINUTES *****

```
Broadcast message from root (Mon Dec 14 16:17:13 2009):

Server configuration completed successfully!
See /var/TKLC/appw/logs/Process/install.log for details.
```

Obtain a terminal session on the **Query Server** as admusr. Log in as admusr on the **Query Server** shell, and issue the following commands:

```
[admusr@hostname1260476099 ~]$ cat
/var/TKLC/appw/logs/Process/install.log
```

9. ☐

Query Server:

Set time zone (optional) and initiate a reboot of the Query Server.

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

Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see List of Frequently Used Time Zones, Appendix B.

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

[admusr@hostname1262121944 ~]$ sudo init 6
```

10. ☐

Query Server:

After the server has completed reboot…

Verify that the server console returns to a login prompt.

```
qs-mrsvnc-1 login: admusr
Password: <admusr_password>
```

11. ☐

Query Server:

Execute a **"syscheck"** to verify the current health of the server.

```
[admusr@qs-mrsvnc-1 ~]$ 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
[admusr@qs-mrsvnc-1 ~]$
```

Procedure 5.3 Adding the Query Server to the SDS Server Group

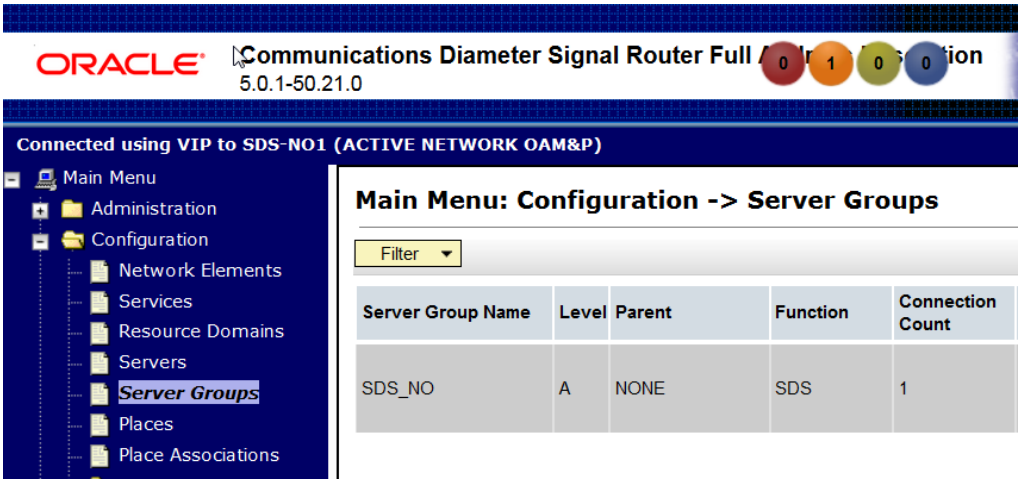
12. ☐

Active SDS VIP:

Select…

Main Menu
→ **Configuration**
→ ***Server Groups***

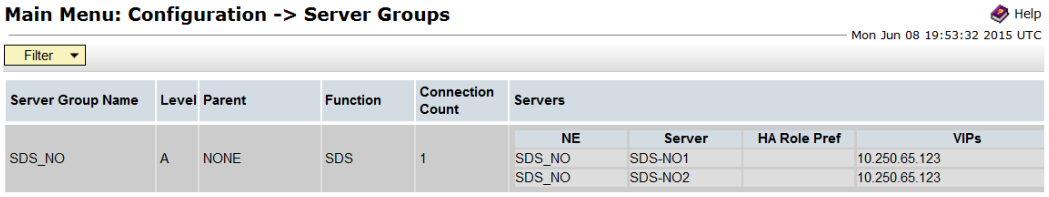
…as shown on the right.



13. ☐

Active SDS VIP:

The user will be presented with the **"Configuration → Server Groups"** screen as shown on the right



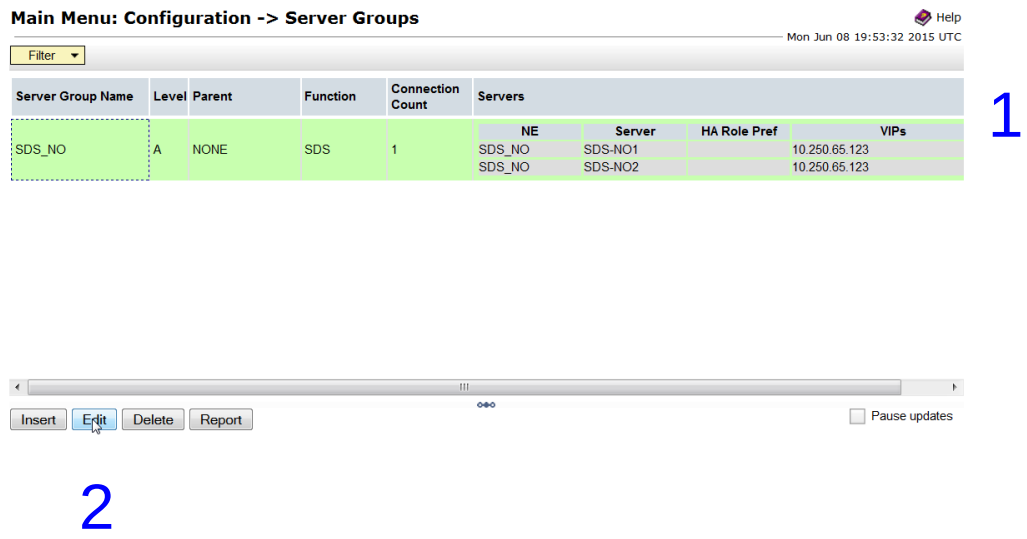
14. ☐

Active SDS VIP:

1) Using the mouse, select the SDS Server Group associated with the Query Server being installed.

2) Select the **"Edit"** dialogue button from the bottom left corner of the screen.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Edit"** dialogue button visible.*



Procedure 5.3 Adding the Query Server to the SDS Server Group

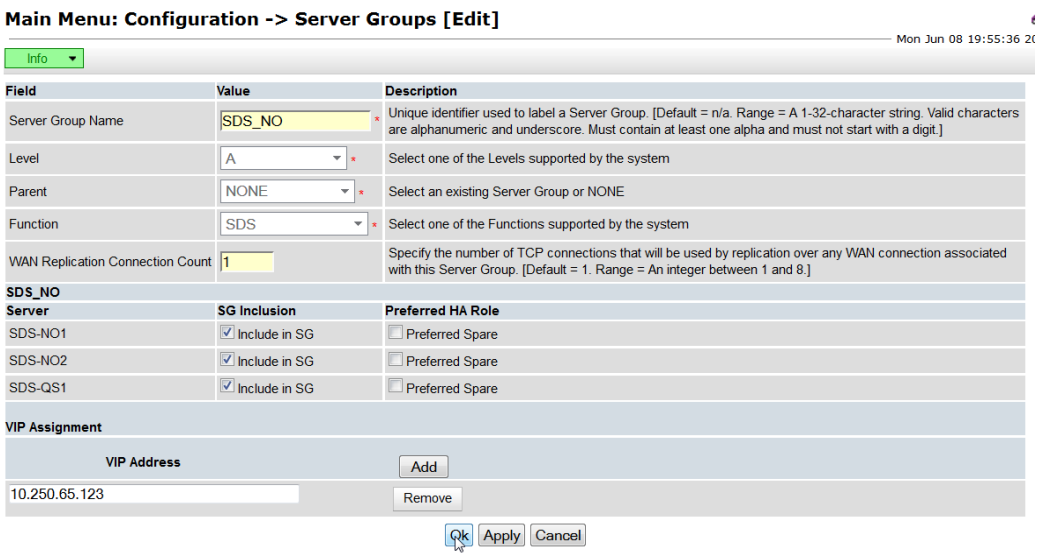
15. ☐

Active SDS VIP:

The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.

1) Select the **"Query Server"** from the list of **"Available Servers in Network Element"** by clicking on the check box next to its name.

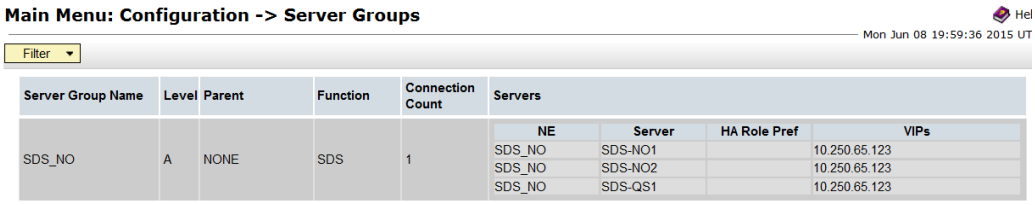
2) Click the **"Ok"** dialogue button.



16. ☐

Active SDS VIP:

The user should be presented with a screen as show on the right.



17. ☐

IMPORTANT:

Wait at least **5 minutes** before proceeding on to the next Step.

- Now that the Query Server has been paired within its SDS Server Group, it must establish DB replication with the Active SDS server. It may take several minutes for this process to be completed.
- Allow a minimum of **5 minutes** before continuing to the next Step.

Procedure 5.4 Restarting the Query Server Application

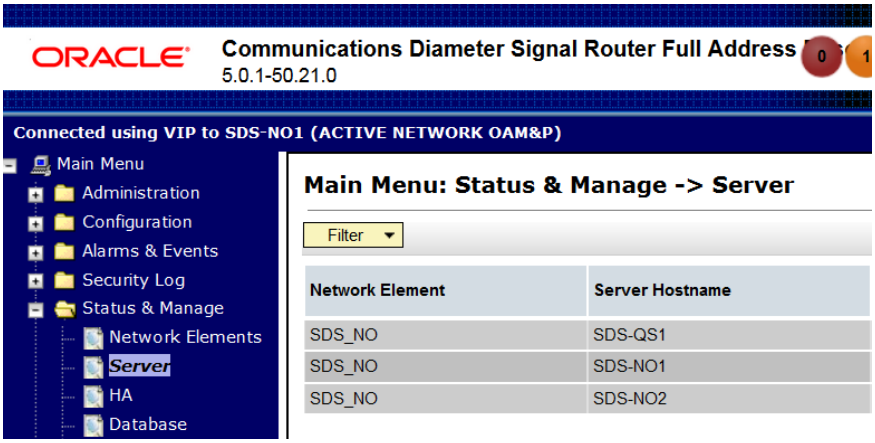
18. ☐

Active SDS VIP:

Select…

Main Menu
→ **Status & Manage**
→ ***Server***

…as shown on the right.

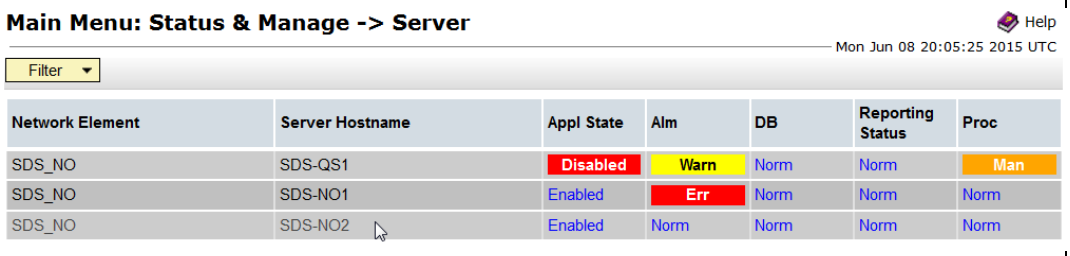


19. ☐

Active SDS VIP:

Verify that the **"DB and Reporting Status"** status columns show **"Norm"** for the Query Server at this point. The **"Proc"** column should show **"Man"**.

NOTE: *If user chooses to refresh the Server status screen in advance of the default setting (15-30 sec.). This may be done by simply reselecting the* ***"Status & Manage → Server"*** *option from the Main menu on the left.*



Procedure 5.4 Restarting the Query Server Application

20. ☐

Active SDS VIP:

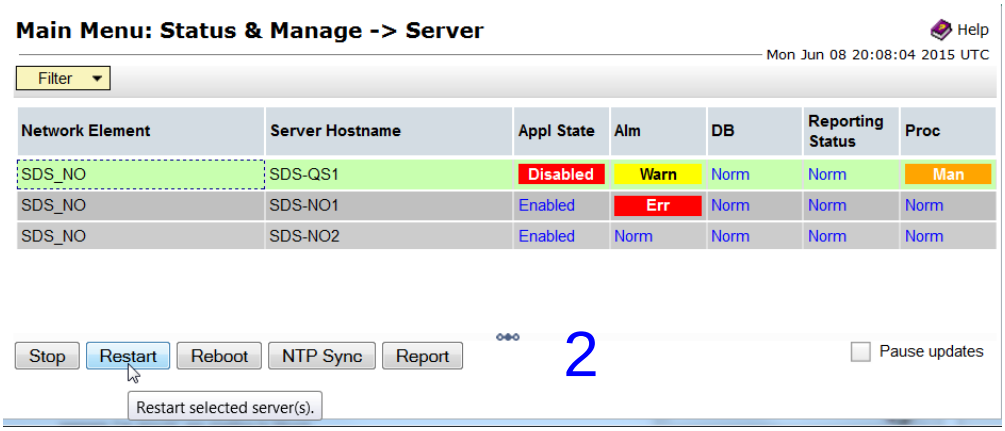
1) Using the mouse, select the **"Query Server"** hostname. The line entry should now be highlighted in **GREEN**.

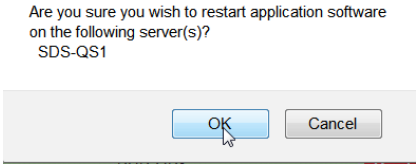
2) Select the **"Restart"** dialogue button from the bottom left corner of the screen.

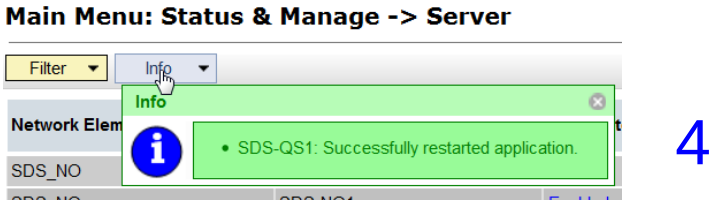
3) Click the **"OK"** button on the confirmation dialogue box.

4) The user should be presented with a confirmation message (in the banner area) for the **"Query Server"** stating: **"Successfully restarted application"**.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*







Procedure 5.4 Restarting the Query Server Application

21. ☐	**Active SDS VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for the **"Query Server"**. **NOTE:** *If user chooses to refresh the Server status screen in advance of the default setting (15-30 sec.). This may be done by simply reselecting the **"Status & Manage → Server"** option from the Main menu on the left.*	**Main Menu: Status & Manage -> Server** Mo Filter **Network Element** | **Server Hostname** | **Appl State** | **Alm** | **DB** | **Reporting Status** | **Proc** SDS_NO | SDS-QS1 | Enabled | Norm | Norm | Norm | Norm SDS_NO | SDS-NO1 | Enabled | Err | Norm | Norm | Norm SDS_NO | SDS-NO2 | Enabled | Norm | Norm | Norm | Norm

THIS PROCEDURE HAS BEEN COMPLETED

5.4 OAM Installation for DP-SOAM sites (All DP-SOAM sites)

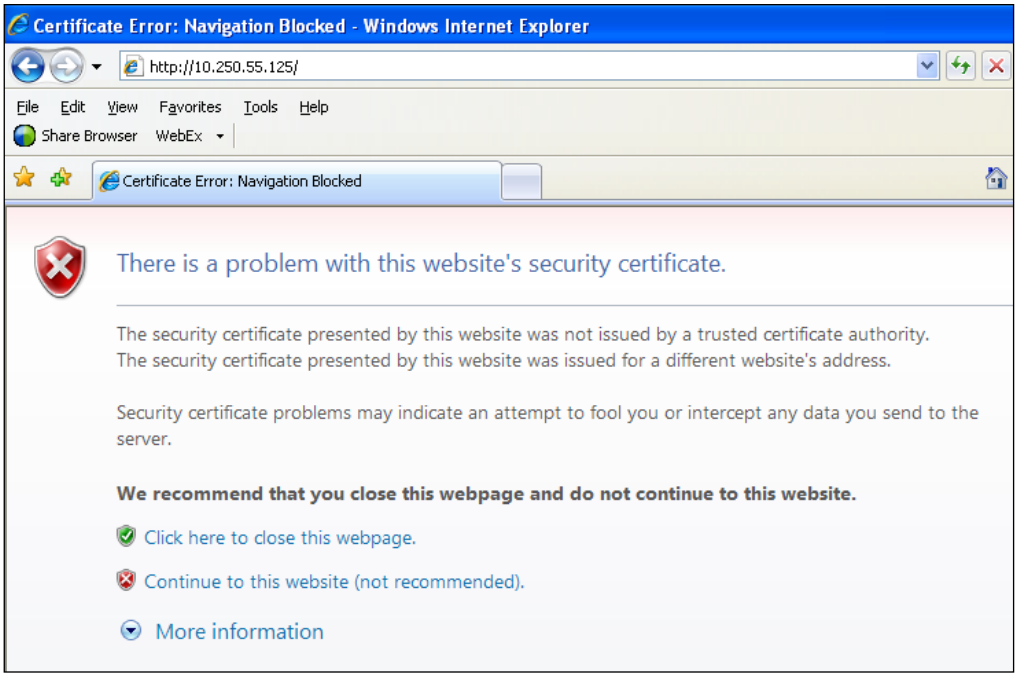
Assumptions:

- This procedure assumes that the DP-SOAM Network Element XML file for the DP-SOAM site has previously been created, as described in **0.**
- This procedure assumes that the Network Element XML files are on the laptop's hard drive.

This procedure is for installing the DP-SOAM software on the OAM server located at each DSR Signaling Site. The DP-SOAM and DSR OAM servers run in 2 virtual machines.

This procedure assumes that the DSR 7.2 or later OAM has already been installed in a virtual environment, as described in as described in [2] DSR Cloud Installation Guide.

Procedure 6 Configuring the Network Element (DP-SOAM)

1. ☐	**Active SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to **Active SDS site** using "https://"	

Procedure 6 Configuring the Network Element (DP-SOAM)

2. ☐

Active SDS VIP:

The user should be presented the login screen shown on the right.

Login to the GUI using the default user and password.

3. ☐

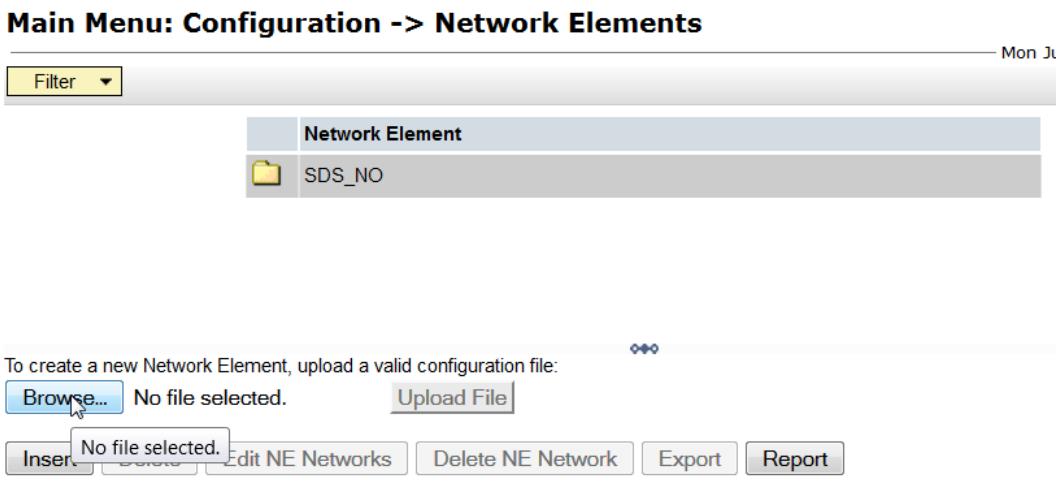
Active SDS VIP:

Select…

Main Menu
→ **Configuration**
→ ***Network Elements***

…as shown on the right.

Select the **"Browse"** dialogue button (scroll to bottom left corner of screen).



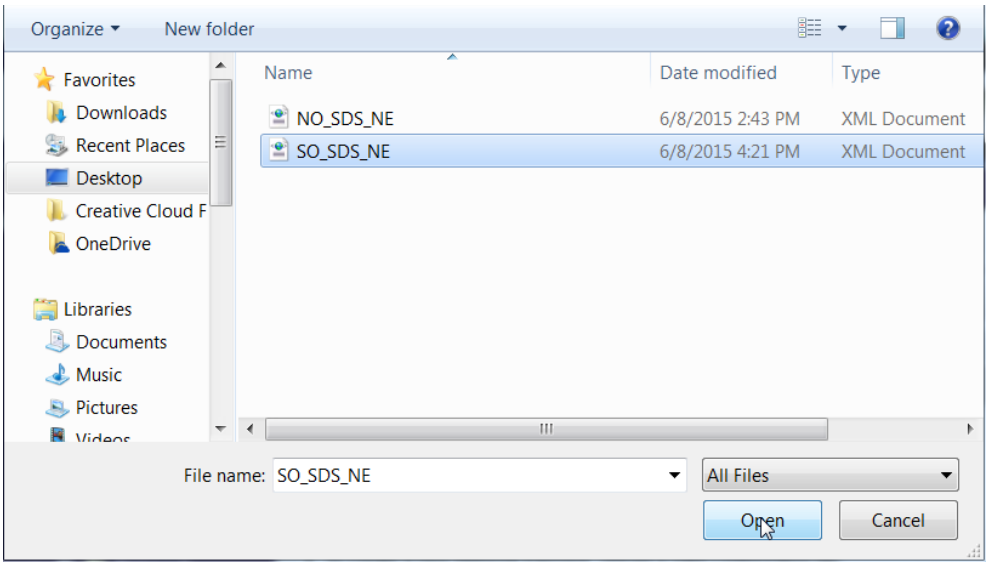
4. ☐

Active SDS VIP:

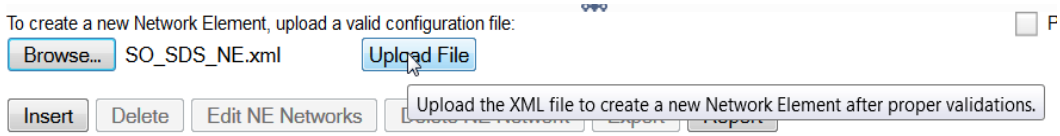
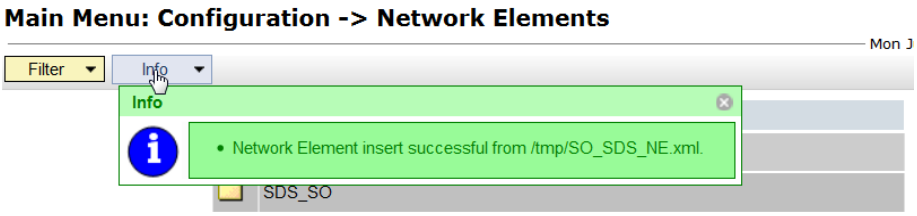
Note: This step assumes that the **xml** files were previously prepared, as described in **0**.

1) Select the location containing the site **.xml** file.

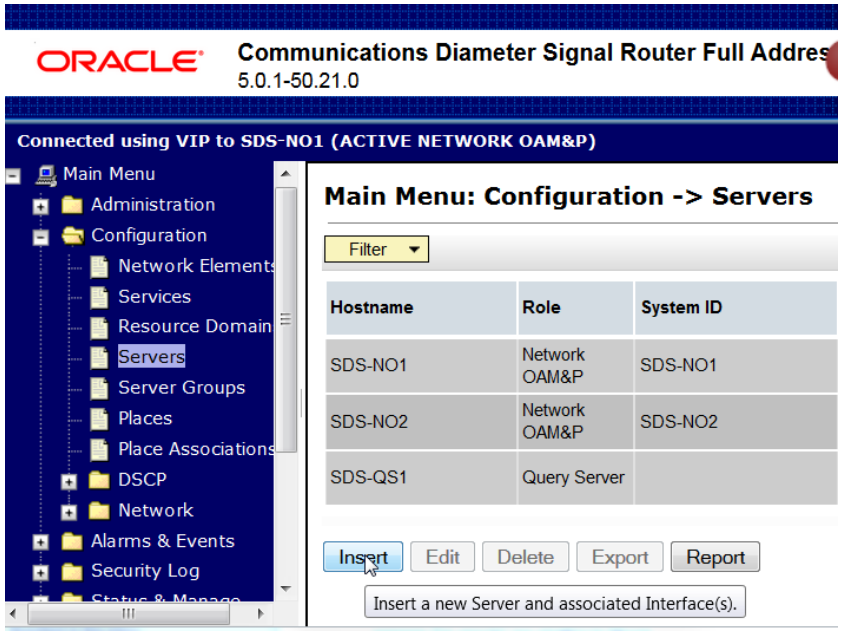
2) Select the **.xml** file and click the **"Open"** dialogue button.



Procedure 6 Configuring the Network Element (DP-SOAM)

5. ☐	**Active SDS VIP:** Select the **"Upload File"** dialogue button (bottom left corner of screen).	
6. ☐	**Active SDS VIP:** If the values in the **.xml** file pass validation rules, the user will receive a banner information message showing that the data has been successfully validated and committed to the DB.	

Procedure 6.1 Configuring the SOAM Server

7. ☐	**Active SDS VIP:** Select… **<u>Main Menu</u>** **→ Configuration** ***→ Servers*** …as shown on the right. Select the **"Insert"** dialogue button (bottom left corner of screen).	

Procedure 6.1 Configuring the SOAM Server

8. ☐

Active SDS VIP:

1) Input the assigned "**hostname"** for OAM Server.

2) Select ***"SYSTEM OAM"*** for the **Role** from the pull-down menu.

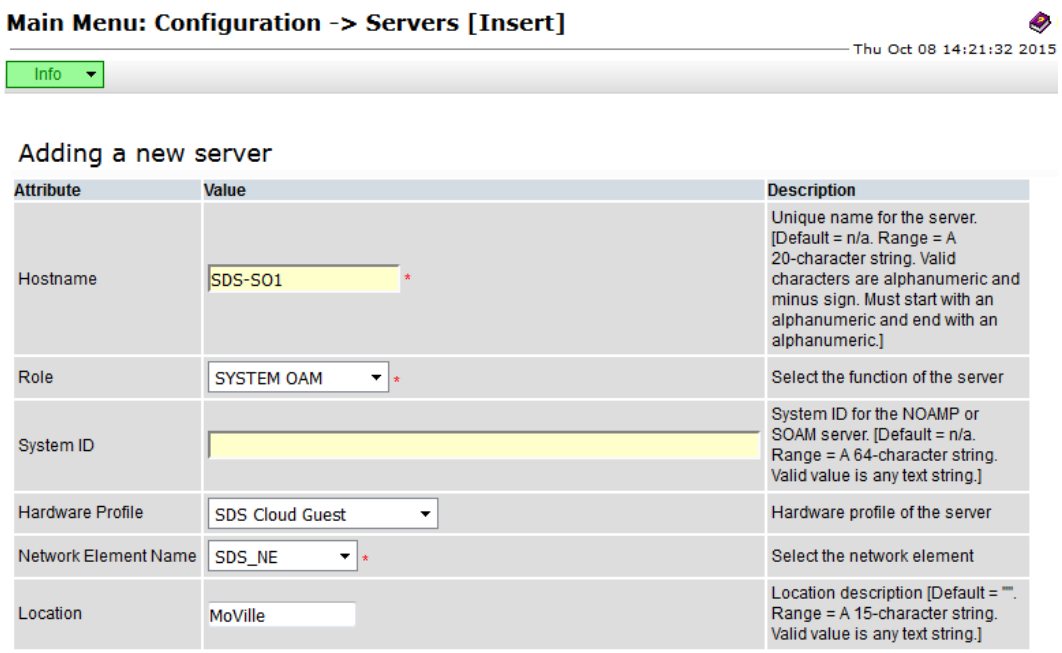
3) Input the assigned hostname again as the "**System ID**" for the SO Server (A or B).

4 Select "**SDS Cloud Guest**" for the **Hardware Profile**.

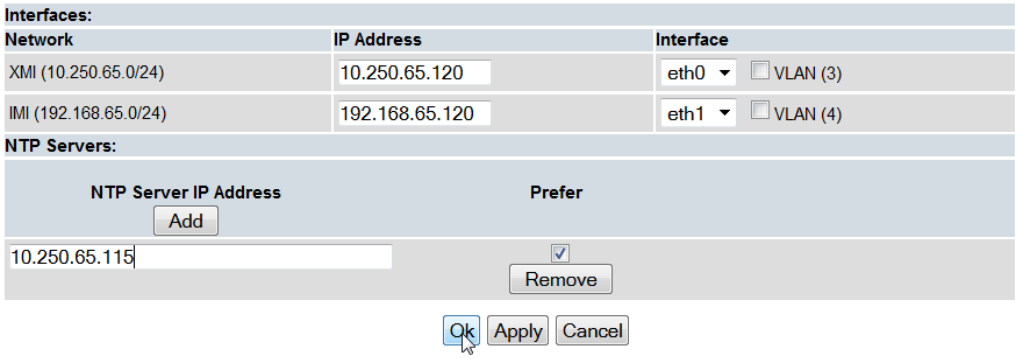
5) Select the **Network Element Name** for the SDS from the pull-down menu.

6) Enter the site location.

NOTE: *Location is an optional field.*



Procedure 6.1 Configuring the SOAM Server

9. ☐	**1)** Enter the **XMI IP address** and **IMI IP address** for the **DP-SOAM Server**. **2)** Set the **XMI Interface** to "**ethX**" and do NOT check the **VLAN** box. **3)** Set the **IMI Interface** to "**ethX**" and do NOT check the **VLAN** box. **4)** Click the "**NTP Servers:**" **"Add"** dialogue button. **5)** Enter the **NTP Server IP Address** for an NTP Server. **6)** If you have another **NTP Server IP address**, repeat (1) and (2) to enter it. **7)** Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other. **8)** Click the **"Ok"** dialogue button.	

Procedure 6.2 Applying the SOAM Server Configuration file

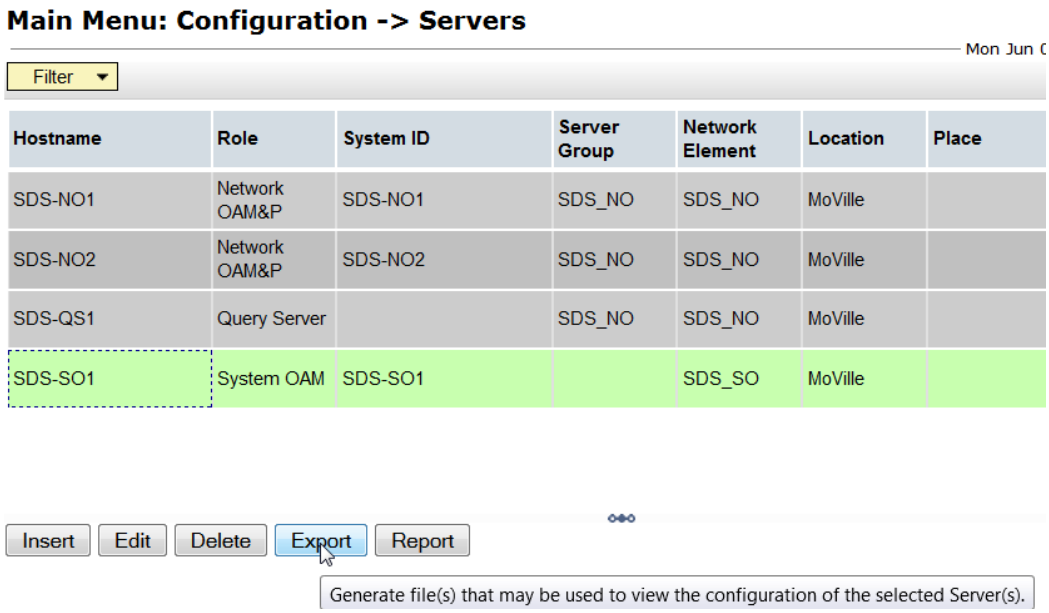
10. ☐

Active SDS VIP:

1) Select the "**System OAM**".

…as shown on the right.

2) Select the **"Export"** dialogue button (bottom left corner of screen).



11. ☐

Repeat **Steps 7 - 10** of this procedure for the **DP-SOAM B Server**.

12. ☐

Active SDS Server:

Access the server console.

- Connect to the **Active SDS VIP** console.

13. ☐

Active SDS Server:

1) Access the command prompt.

2) Log into the OAM server as the "**admusr**" user.

```
hostname1260476035 login: admusr
Password: <admusr_password>
```

14. ☐

Active SDS Server:

Copy the configuration file to the **"/var/tmp"** directory on the remote **SOAM A or B** server.

NOTE: *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

Example:

TKLCConfigData<hostname>.sh ➔ will translate to ➔TKLCConfigData.sh

```
[admusr@sds-mrsvnc-a ~]$ scp \
/var/TKLC/db/filemgmt/TKLCConfiguData.<hostname>.sh \
<ipaddr>:/var/tmp/TKLCConfigData.sh
```

Note: ipaddr is the IP address of **SOAM A or B** associated with the xmi network.

Procedure 6.2 Applying the SOAM Server Configuration file

15. ☐

SOAM Server:

After the script completes, a broadcast message will be sent to the terminal.

NOTE: *The user should be aware that the time to complete this step varies by server and may take from 3-20 minutes to complete.*

```
*** NO OUTPUT FOR ≈ 3-20 MINUTES ***
Broadcast message from root (Mon Dec 14 16:17:13 2009):

Server configuration completed successfully!
See /var/TKLC/appw/logs/Process/install.log for details.
```

Obtain a terminal session on the **SOAM Server** as admusr. Log in as admusr on the **SOAM Server** shell, and issue the following commands:

```
[admusr@hostname1260476099 ~]$ cat
/var/TKLC/appw/logs/Process/install.log
```

16. ☐

SOAM Server:

Set time zone (optional) and initiate a reboot of the OAM server.

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

Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see List of Frequently Used Time Zones, Appendix B.

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

[admusr@hostname1260476221 ~]$ sudo init 6
```

17. ☐

SOAM Server:

Execute a **"syscheck"** to verify the current health of the server.

```
[admusr@so-carync-a ~]$ 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
[admusr@so-carync-a ~]$
```

18. ☐

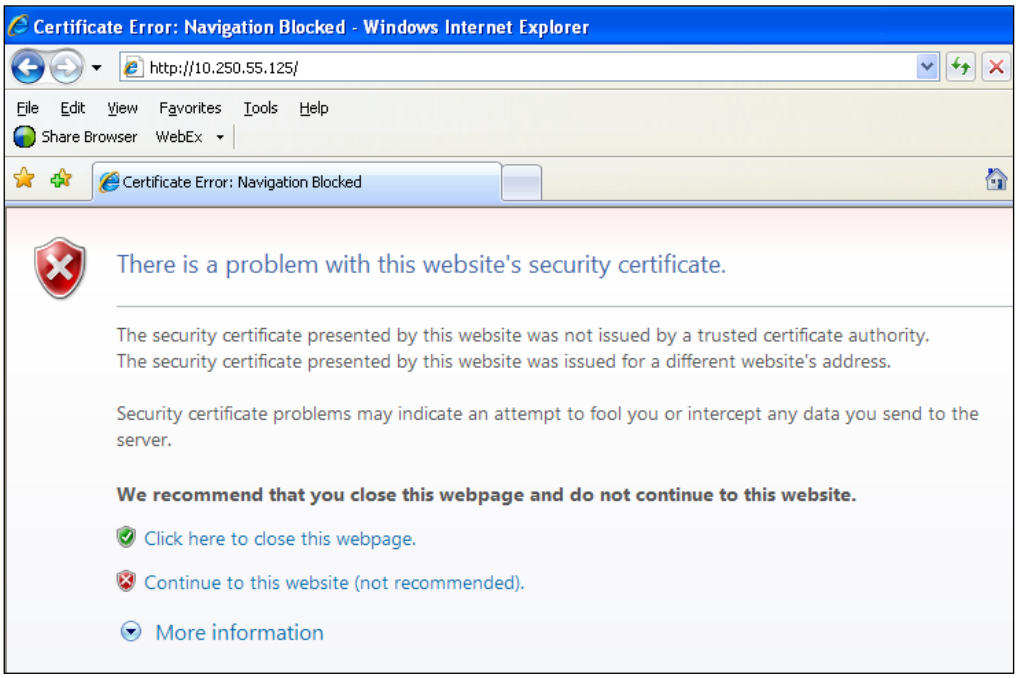
If you have just completed this procedure for the **SOAM Server A** in the enclosure then repeat **Steps 112 - 177** this procedure for **SOAM Server B**.

THIS PROCEDURE HAS BEEN COMPLETED

5.5 OAM Pairing for DP-SOAM sites (All DP-SOAM sites)

The user should be aware that during the OAM Pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 7: Pairing the OAM Servers for DP-SOAM sites

Step	Procedure	Result
1. ☐	**Active SDS VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active SDS site** using "https://"	
2. ☐	**Active SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 7.1 Configuring the SOAM Server Group (SOAM)

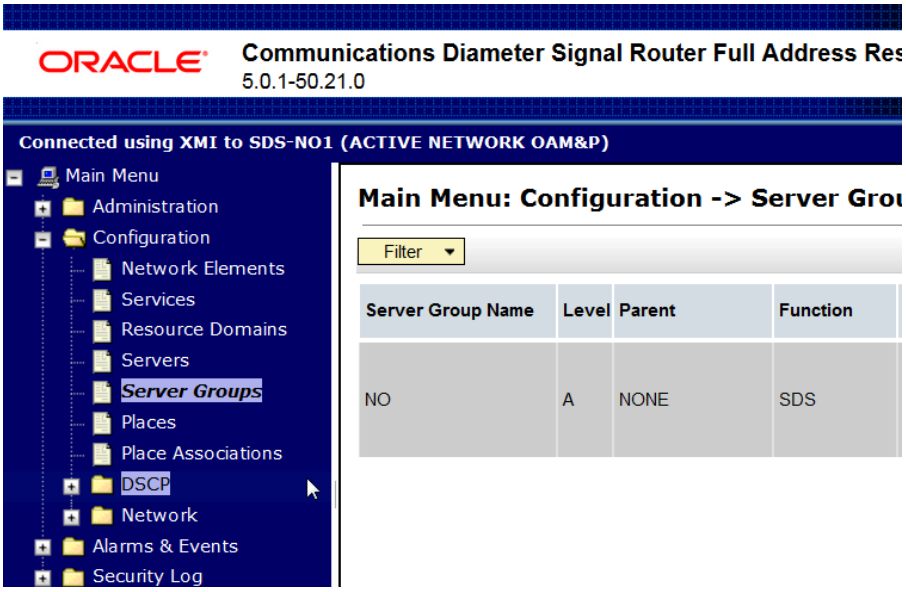
3. ☐

Active SDS VIP:

Select…

Main Menu
→ **Configuration**
→ ***Server Groups***

…as shown on the right.



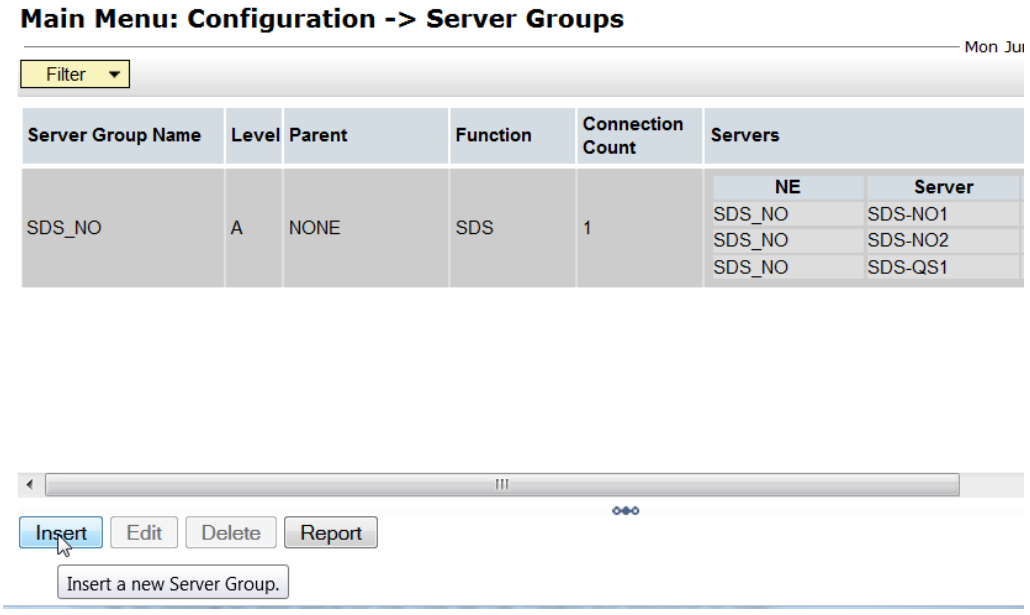
4. ☐

Active SDS VIP:

1) The user will be presented with the **"Server Groups"** configuration screen as shown on the right.

2) Select the **"Insert"** dialogue button from the bottom left corner of the screen.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Insert"** dialogue button visible.*



Procedure 7.1 Configuring the SOAM Server Group (SOAM)

5. ☐

Active SDS VIP:

The user will be presented with the **"Server Groups [Insert]"** screen as shown on the right.

NOTE: *Leave the "**WAN Replication Connection Count**" blank (it will default to 1).*

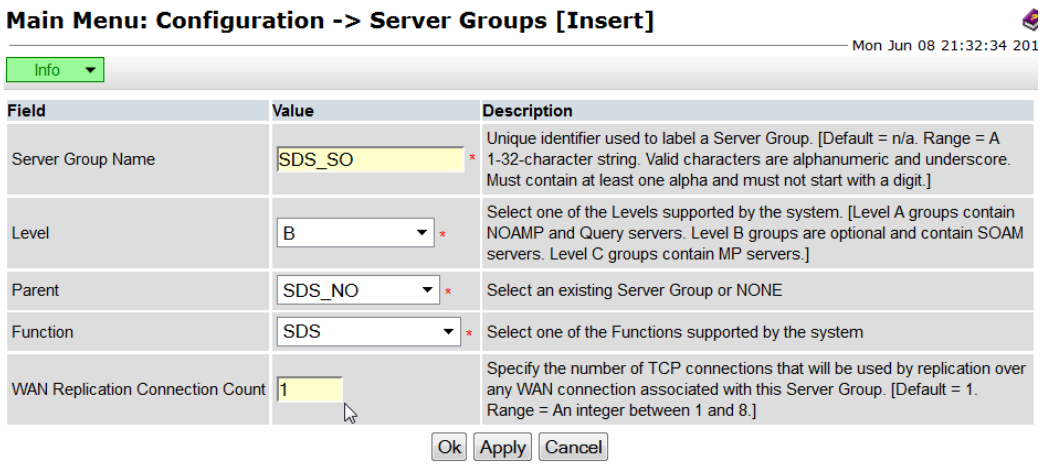
1) Input the **Server Group Name**.

2) Select **"B"** on the **"Level"** pull-down menu...

3) Select the 1st SDS Site's server group, as entered in **Procedure 3, Step 6,** on the **"Parent"** pull-down menu...

4) Select **"SDS"** on the **"Function"** pull-down menu.

5) Select the **"Ok"** dialogue button.



Procedure 7.2 Adding a Server to the OAM Server Group (SOAM)

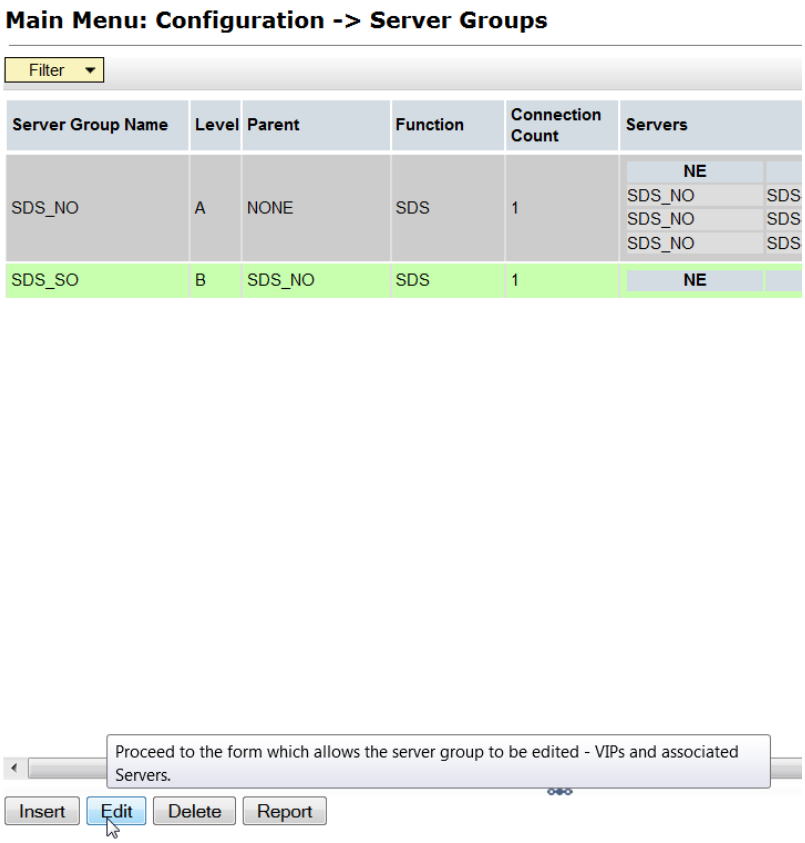
6. ☐

SDS Server A:

1) Select the **Server Group** entry applied in **Step 13**. The line entry should now be highlighted in **GREEN**.

2) Select the **"Edit"** dialogue button from the bottom left corner of the screen.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Edit"** dialogue button visible.*



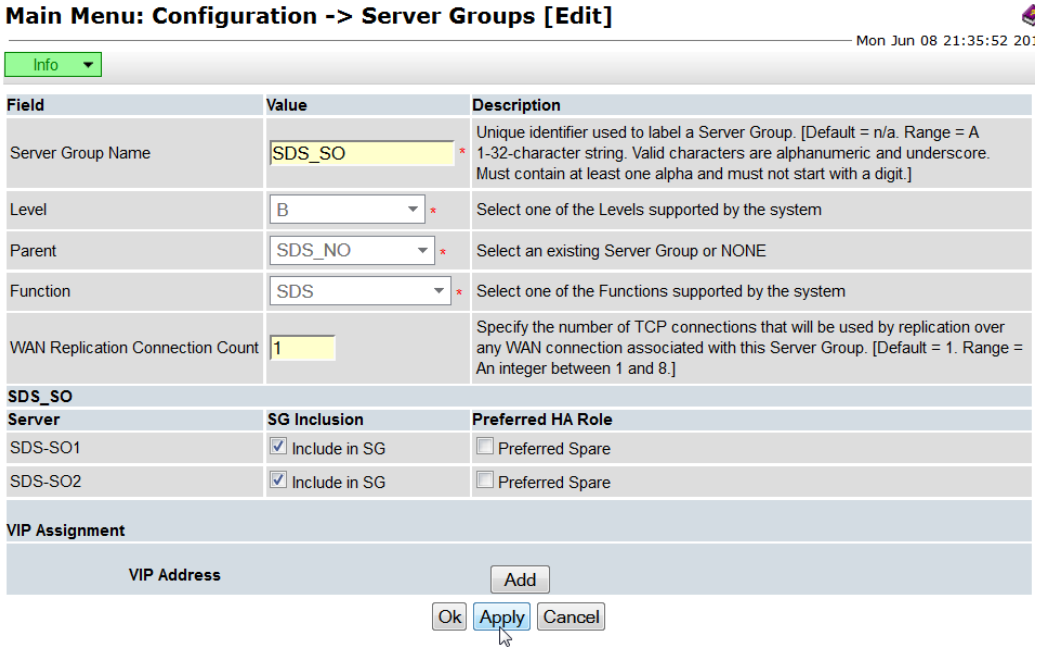
7. ☐

Active SDS VIP:

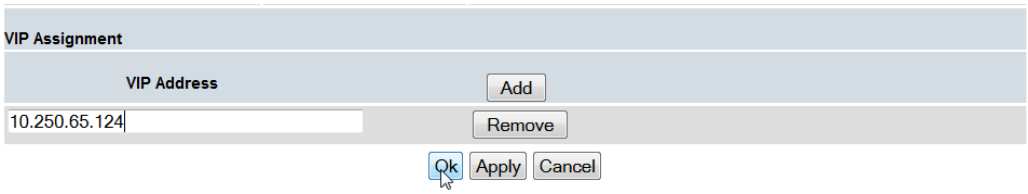
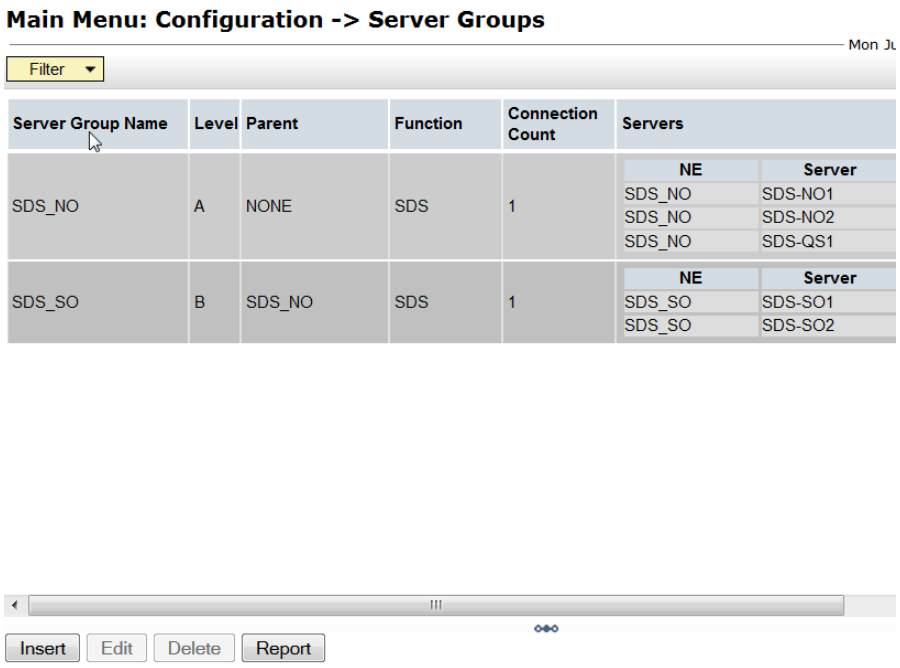
The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.

Select the **"A"** server and the **"B"** server from the list of **"Servers"** by clicking the check box next to their names.

Select the **"Apply"** dialogue button.



Procedure 7.2 Adding a Server to the OAM Server Group (SOAM)

8. ☐	**Active SDS VIP:** Click the **"Add"** dialogue button for the **VIP Address**. Input the **VIP Address** Click the **"Ok"** dialogue button.	
9. ☐	**SDS Server A:** The user will be presented with the **"Server Groups"** configuration screen as shown on the right.	
10. ☐	**IMPORTANT:** Wait at least **5 minutes** before proceeding on to the next Step.	• Now that the server(s) have been paired within a Server Group they must establish a master/slave relationship for High Availability (HA). It may take several minutes for this process to be completed. • Allow a minimum of **5 minutes** before continuing to the next Step.

Procedure 7.3 Restarting the OAM Server Application (SOAM)

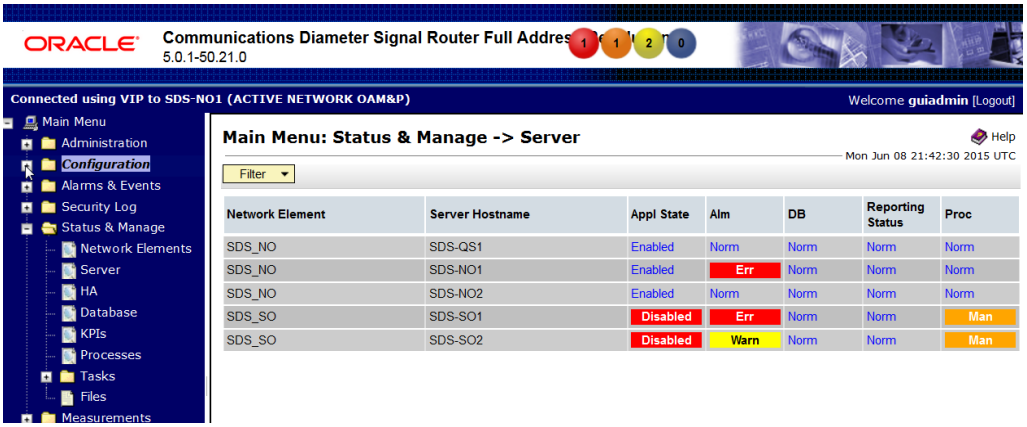
11. ☐

Active SDS VIP:

Select…

Main Menu
→ Status & Manage
→ *Server*

…as shown on the right.

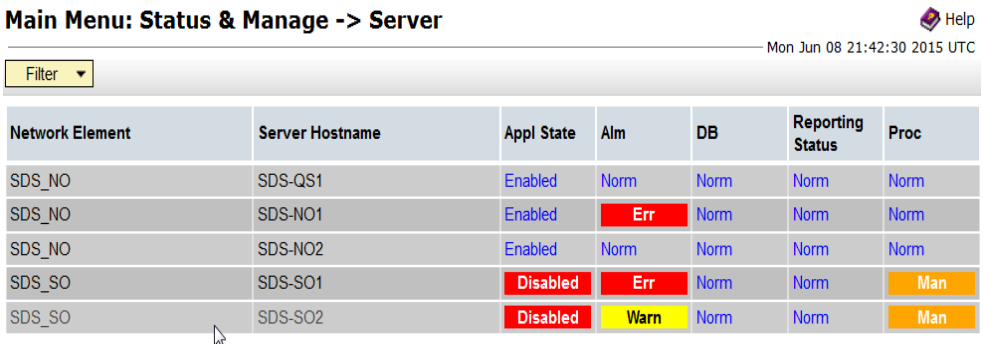


12. ☐

Active SDS VIP:

1) The **"A"** and **"B"** DP-SOAM servers should now appear in the right panel.

2) Verify that the "DB" status shows "Norm" and the "Proc" status shows "Man" for both servers before proceeding to the next Step.



Procedure 7.3 Restarting the OAM Server Application (SOAM)

13. ☐

Active SDS VIP:

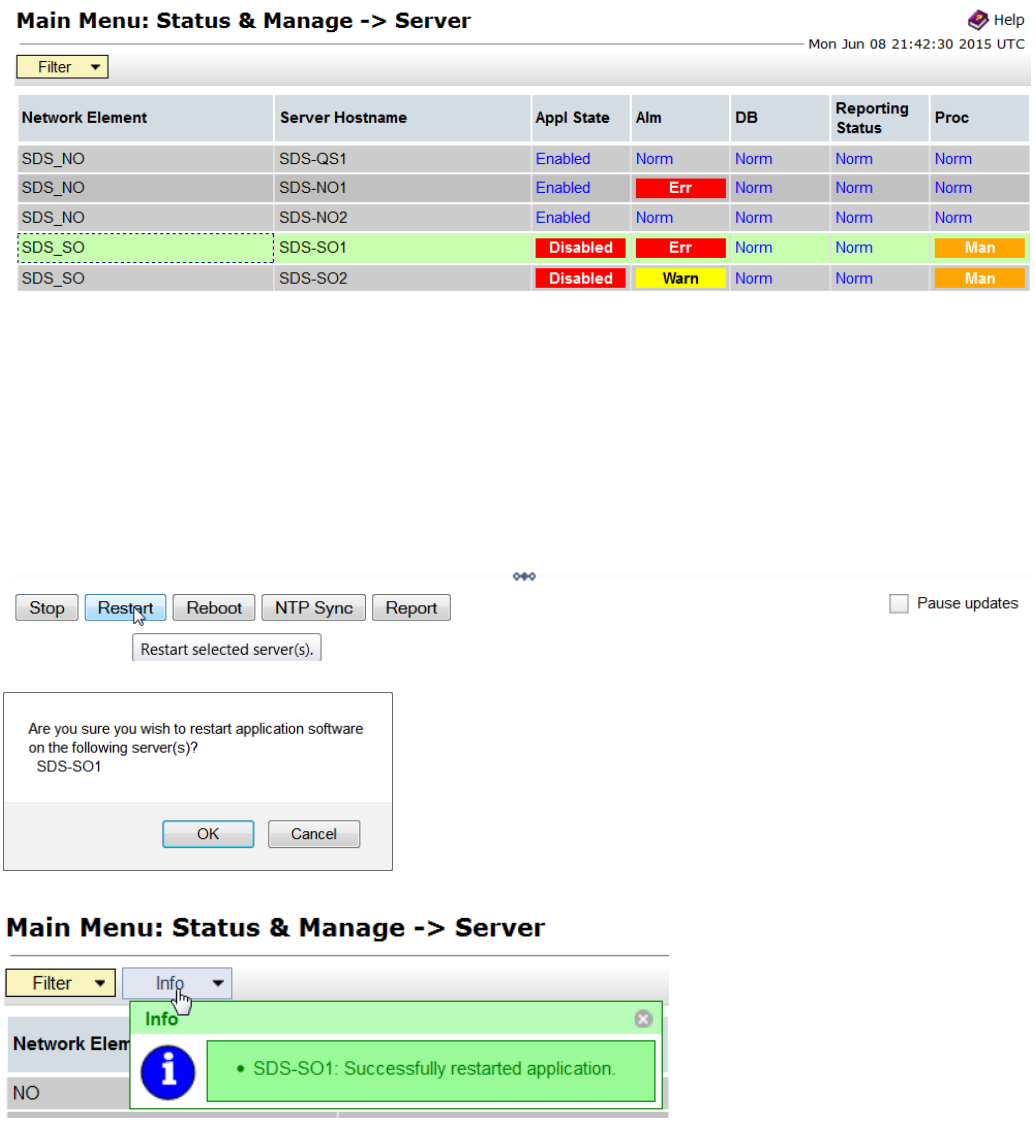
1) Using the mouse, select **DP-SOAM Server A**. The line entry should now be highlighted in **GREEN**.

2) Select the **"Restart"** dialogue button from the bottom left corner of the screen.

3) Click the **"OK"** button on the confirmation dialogue box.

4) The user should be presented with a confirmation message (in the banner area) for **DP-SOAM Server A** stating: **"Successfully restarted application"**.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*



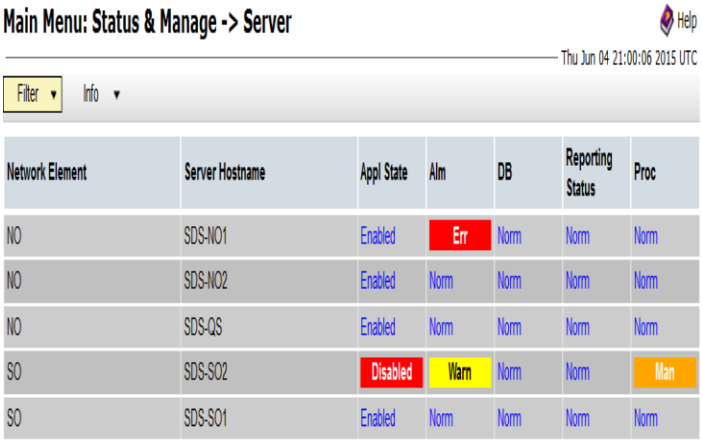
Procedure 7.3 Restarting the OAM Server Application (SOAM)

14. ☐

Active SDS VIP:

Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status, & Proc"** status columns all show **"Norm"** for **OAM Server A** before proceeding to the next Step.

NOTE: *If user chooses to refresh the Server status screen in advance of the default setting (15-30 sec.). This may be done by simply reselecting the **"Status & Manage → Server"** option from the Main menu on the left.*



Network Element	Server Hostname	Appl State	Alm	DB	Reporting Status	Proc
NO	SDS-NO1	Enabled	Err	Norm	Norm	Norm
NO	SDS-NO2	Enabled	Norm	Norm	Norm	Norm
NO	SDS-QS	Enabled	Norm	Norm	Norm	Norm
SO	SDS-SO2	Disabled	Warn	Norm	Norm	Man
SO	SDS-SO1	Enabled	Norm	Norm	Norm	Norm

15. ☐

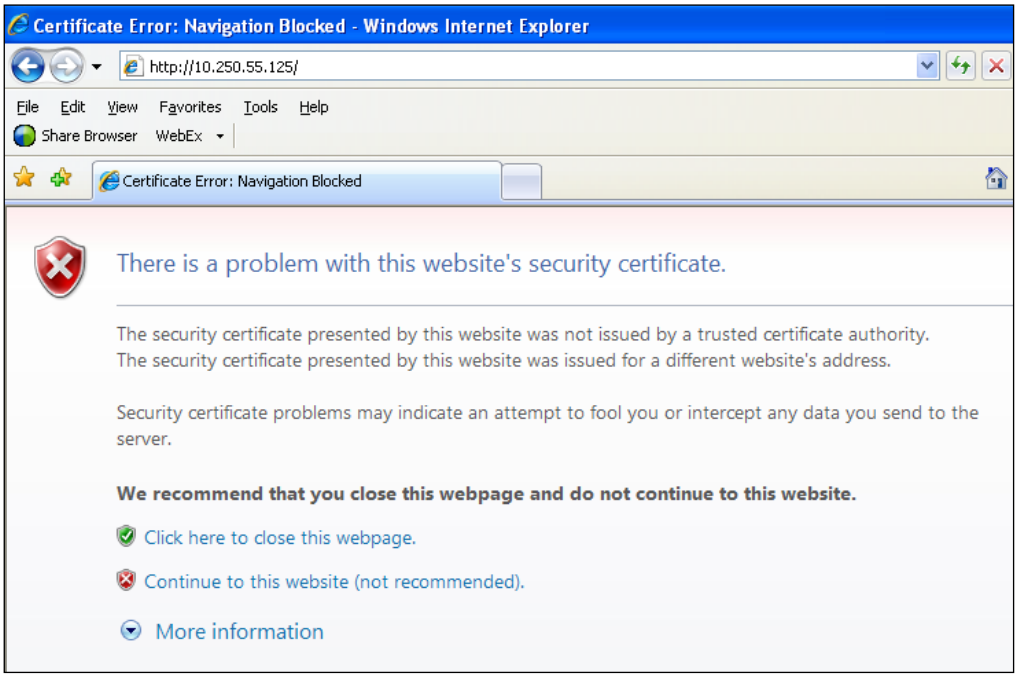
Repeat **Steps 13 and 14** of this procedure for the **DP-SOAM Server B**.

THIS PROCEDURE HAS BEEN COMPLETED

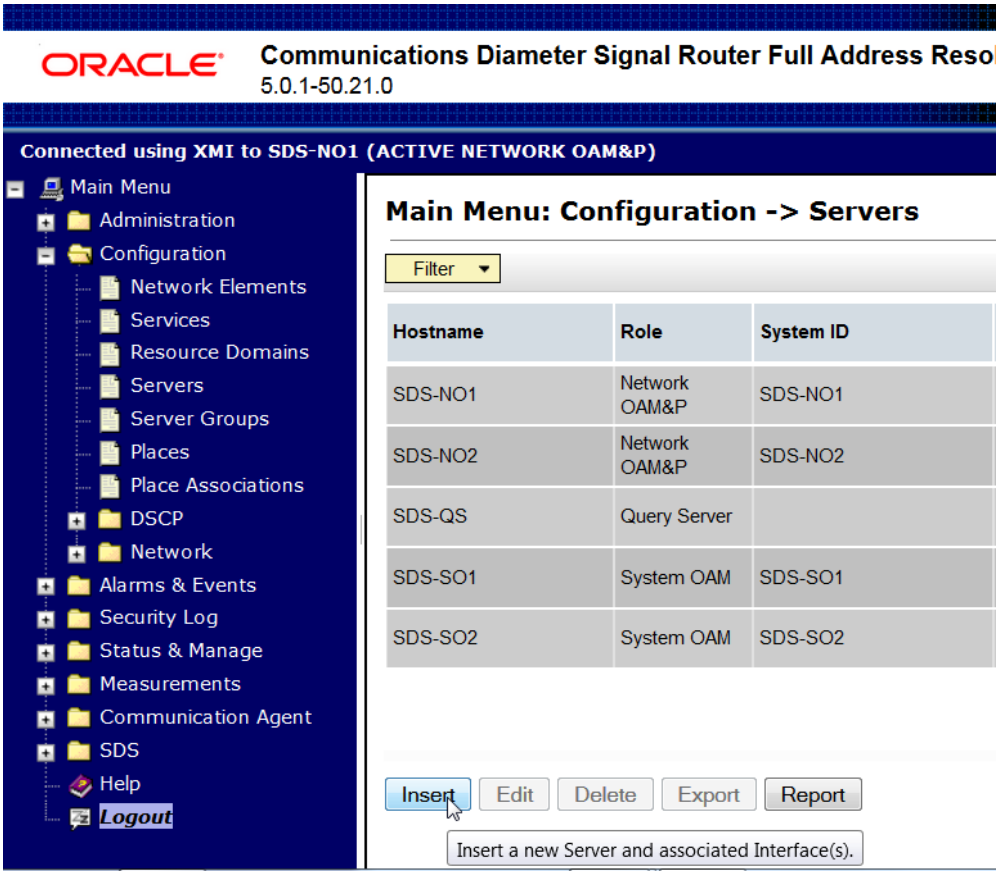
5.6 DP Installation (All DP-SOAM sites)

The user should be aware that during the Data Processor (DP) installation procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

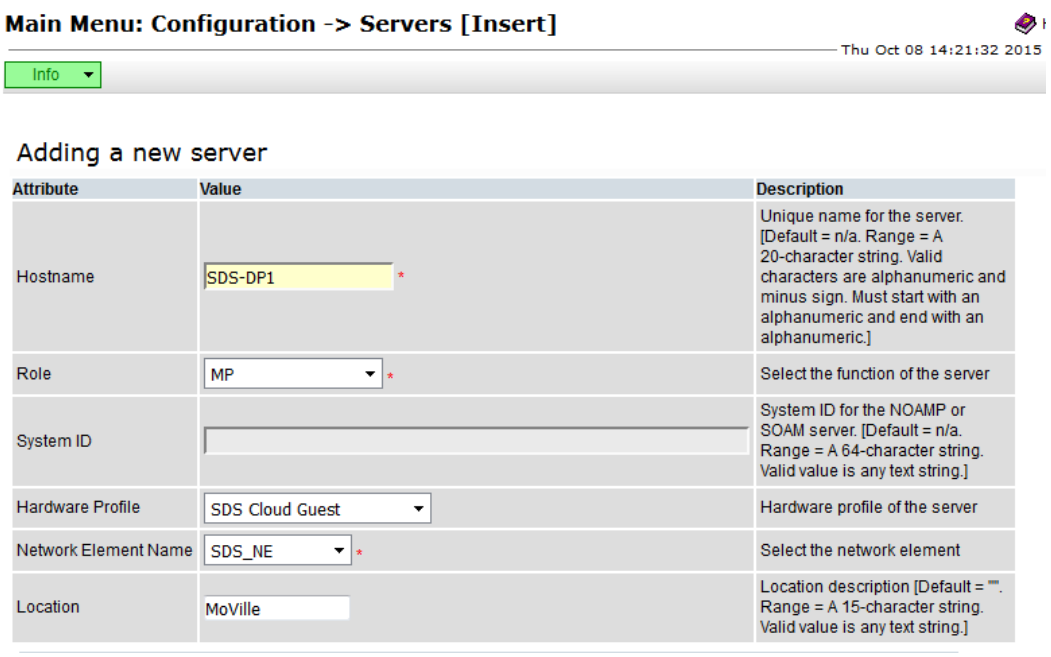
Procedure 8.0 Configuring the Database Processor Server (DP)

1. ☐	**Active SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to **Active SDS site** using "https://"	
2. ☐	**Active SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 8.0 Configuring the Database Processor Server (DP)

3. ☐	**Active SDS VIP:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right. Select the **"Insert"** dialogue button.	

Procedure 8.0 Configuring the Database Processor Server (DP)

4. ☐	**Active SDS VIP:** **1)** Input the assigned "**hostname"** for the Database Processor **(DP)**. **2)** Select **"MP"** for the server **Role** from the pull-down menu. **3)** Select **"SDS Cloud Guest"** for the **Hardware Profile**. **4)** Select the **Network Element Name** of the **DP-SOAM site** where the **DP** is physically located from the list of available NEs in the pull-down menu **5)** Enter the site location. **NOTE:** *Location is an optional field.*	

Procedure 8.0 Configuring the Database Processor Server (DP)

5. ☐

1) Enter the **XMI IP address** and **IMI IP address** for the **DP-SOAM Server**.

2) Set the **XMI Interface** to "**ethX**" and **DO NOT** check the **VLAN** box.

3) Set the **IMI Interface** to "**ethX**" and **DO NOT** check the **VLAN** box.

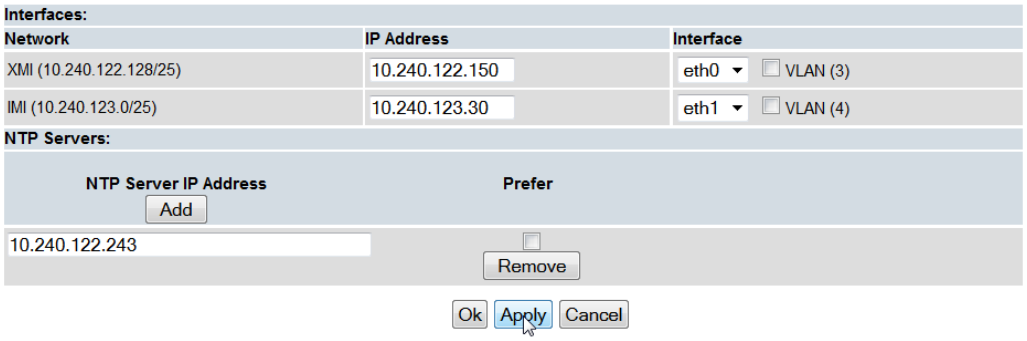
4) Click the "**NTP Servers:**" **"Add"** dialogue button.

5) Enter the **NTP Server IP Address** for an NTP Server.

6) If you have another **NTP Server IP address**, repeat (1) and (2) to enter it.

7) Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other.

8) Click the **"Ok"** dialogue button...



Procedure 8.1 Applying the Database Processor Configuration file (DP)

6. ☐

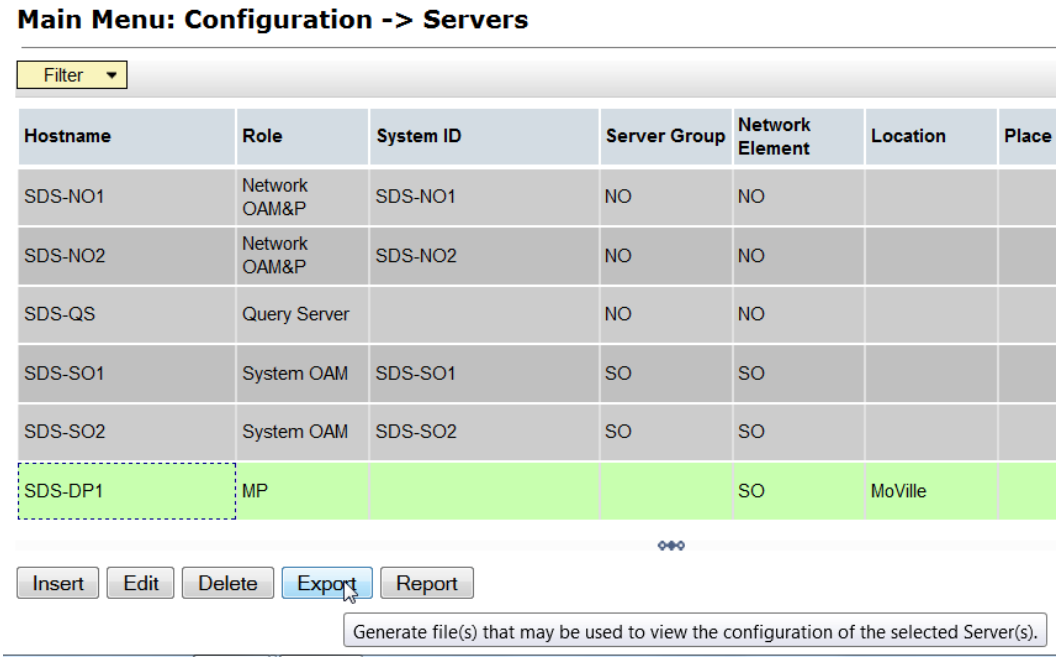
Active SDS VIP:

On the **"Configuration →Servers" screen**, find the newly added DP server in the list.

Note: The DP server will have a "**MP**" role.

1) Using the mouse, select the newly added DP server entry. The line entry containing the server with a "**MP**" role should now be highlighted in **GREEN**.

2) Select the **"Export"** dialogue button from the bottom left corner of the screen.



7. ☐

- Repeat **Steps 3 - 6** of this procedure for each additional **DP** server.

8. ☐

Active SDS Server:

Access the server console.

- Connect to the **Active SDS VIP** console.

9. ☐

Active SDS Server:

1) Access the command prompt.

2) Log into the OAM server as the "**admusr**" user.

```
hostname1260476035 login: admusr
Password: <admusr_password>
```

10. ☐

Active SDS Server:

Change directory to filemgmt

```
[admusr@sds-mrsvnc-a ~]$ cd /var/TKLC/db/filemgmt
```

Procedure 8.1 Applying the Database Processor Configuration file (DP)		

11. ☐	**Active SDS Server:**
	
	Copy the **SDS DP** configuration file to the **"/var/tmp"** directory on the remote server.
	
	NOTE: *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*
		Example:
		TKLCConfigData<.hostname>.sh ➔ will translate to ➔TKLCConfigData.sh
		
		`[admusr@sds-mrsvnc-a ~]$ scp \`
		`/var/TKLC/db/filemgmt/TKLCConfiguData.<hostname>.sh \`
		`<ipaddr>:/var/tmp/TKLCConfigData.sh`
		
		Note: ipaddr is the IP address of DP server associated with the xmi network.

12. ☐	**DP Server:**
	
	After the script completes, a broadcast message will be sent to the terminal.
	
	NOTE: *The user should be aware that the time to complete this step varies by server and may take from 3-20 minutes to complete.*
		***** NO OUTPUT FOR ≈ 3-20 MINUTES *****
		
		`Broadcast message from root (Mon Dec 14 15:47:33 2009):`
		
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		
		Obtain a terminal session on the **DP Server** as admusr. Log in as admusr on the **DP Server** shell, and issue the following commands:
		
		`[admusr@hostname1260476099 ~]$ cat`
		`/var/TKLC/appw/logs/Process/install.log`

13. ☐	**DP Server:**
	
	Set time zone (optional) and initiate a reboot of the DP.
		To change the system time zone, from the command line prompt, execute ***set_ini_tz.pl***. The following command example uses the America/New_York time zone.
		
		Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see List of Frequently Used Time Zones, Appendix B.
		
		`$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York"`
		`>/dev/null 2>&1`
		
		`[admusr@hostname1260476035 ~]$ sudo init 6`

Procedure 8.1 Applying the Database Processor Configuration file (DP)		

14. ☐	**DP Server:**
	
	Execute a **"syscheck"** to verify the current health of the server.
		Obtain a terminal session on the **DP Server** as admusr. Log in as admusr on the **DP Server** shell, and issue the following commands:
		
		`[admusr@dp-carync-1 ~]$ 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`
		`[admusr@dp-carync-1 ~]$`

15. ☐	Repeat **Steps 8 - 14** of this procedure for each subtending **DP** server.	

Procedure 8.2 Configuring the Database Processor Server Group (DP)

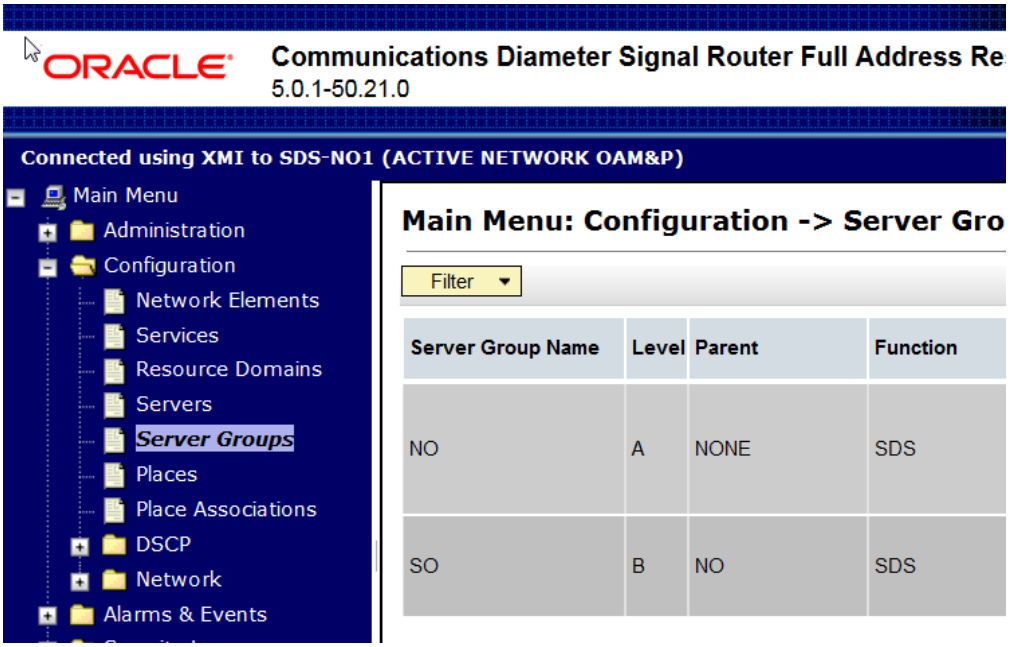
16. ☐

Active SDS VIP:

Select…

Main Menu
→ **Configuration**
→ ***Server Groups***

…as shown on the right.



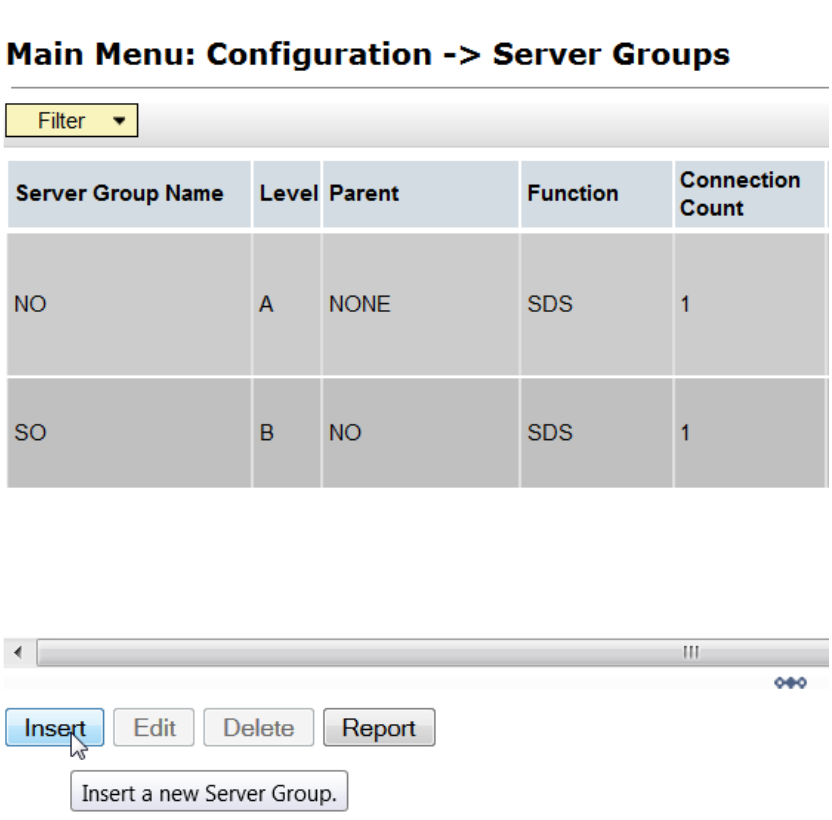
17. ☐

Active SDS VIP:

1) The user will be presented with the **"Server Groups"** configuration screen as shown on the right.

2) Select the **"Insert"** dialogue button from the bottom left corner of the screen.

NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Insert"** dialogue button visible.*



Procedure 8.2 Configuring the Database Processor Server Group (DP)

18. ☐

Active SDS VIP:

1) Input the **Server Group Name**.

Note: Each DP will have its own server group. Group names may be differentiated by assigning each a unique name.

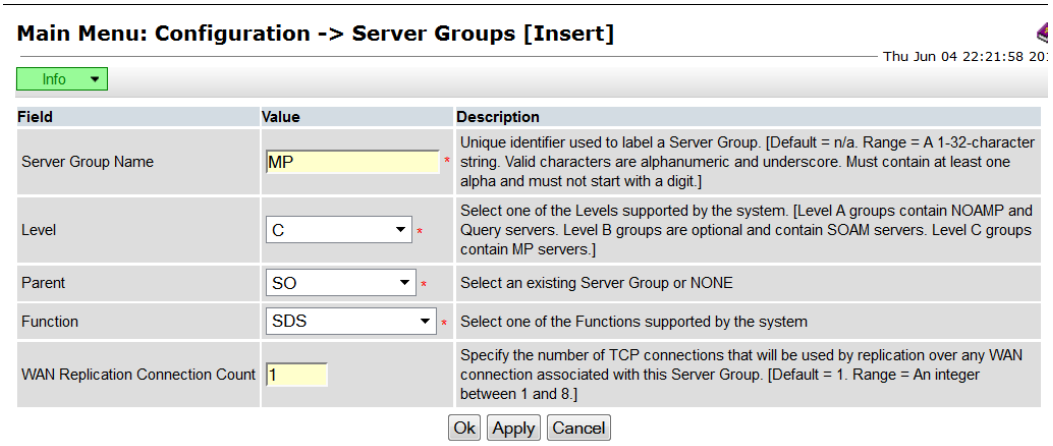
2) Select **"C"** on the **"Level"** pull-down menu.

3) Select **System OAM group** on the **"Parent"** pull-down menu.

4) Select **"SDS"** on the **"Function"** pull-down menu.

NOTE: *Leave the "**WAN Replication Connection Count**" blank it will default to 1.*

5) Select the **"OK"** dialogue button.

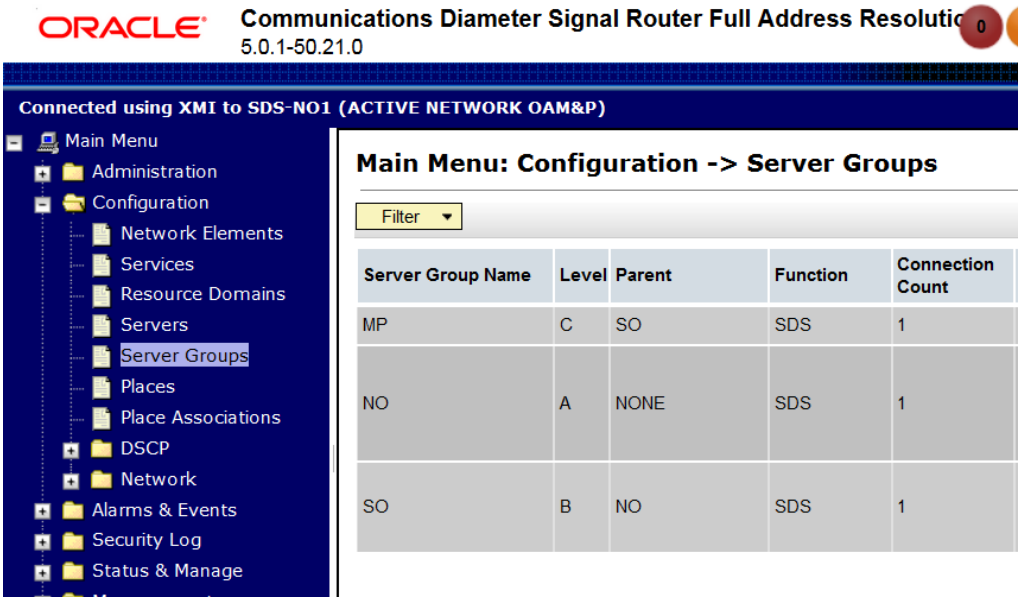


Procedure 8.3 Adding the Database Processor into the DP Server Group (DP)

19. ☐

Active SDS VIP:

The user will be presented with the **"Configuration → Server Groups"** screen as shown on the right

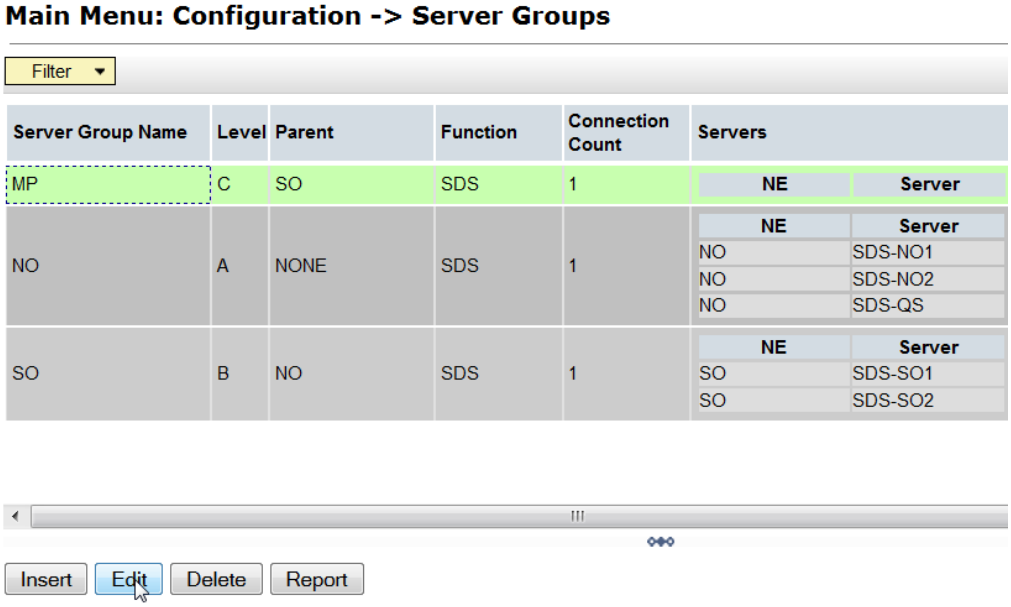


20. ☐

Active SDS VIP:

1) Using the mouse, select the MP Server Group associated with the **DP** being installed.

2) Select the **"Edit"** dialogue button from the bottom left corner of the screen.



Procedure 8.3 Adding the Database Processor into the DP Server Group (DP)

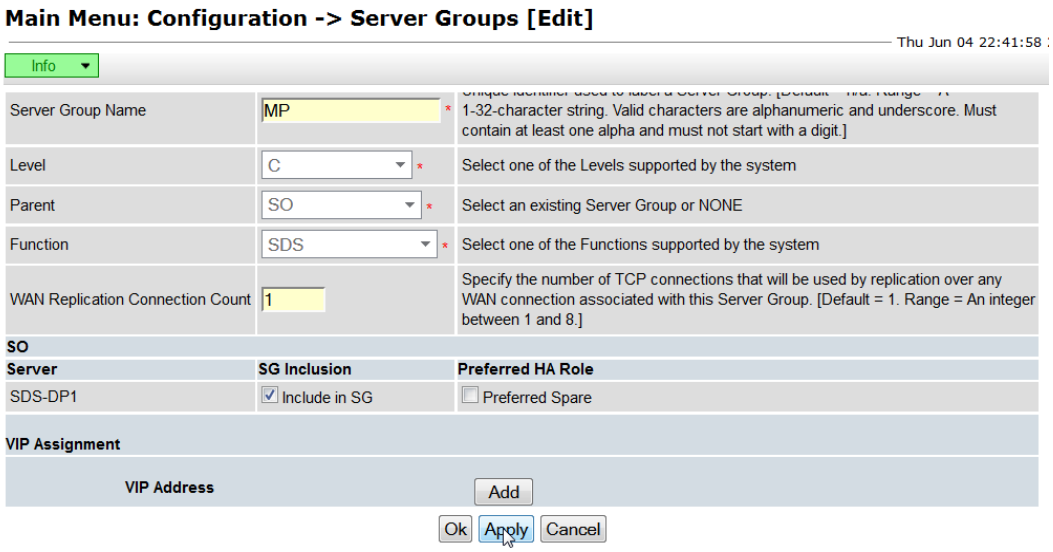
21. ☐

Active SDS VIP:

The user will be presented with the **"Configuration → Server Groups [Edit]"** screen as shown on the right

Select the **"DP"** server from the list of **"Servers"** by clicking the check box next its name.

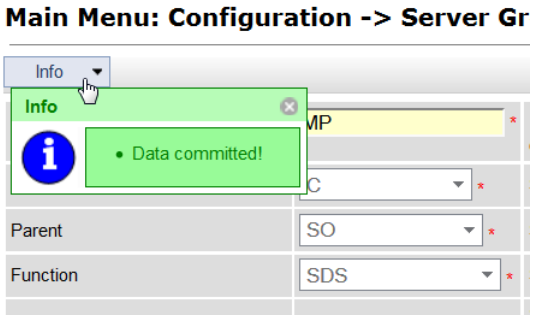
Select the **"Apply"** dialogue button.



22. ☐

Active SDS VIP:

The user should be presented with a banner information message stating **"Data committed"**.



23. ☐

Repeat **Steps 16 - 22** of this procedure for each subtending **DP** server, *using a unique server group for each **DP***.

24. ☐

IMPORTANT:

Wait at least **5 minutes** before proceeding on to the next Step.

- Now that the Database Processor(s) have been placed within their respective Server Groups, each must establish DB replication with the Active DP-SOAM server at the NE. It may take several minutes for this process to be completed.
- Allow a minimum of **5 minutes** before continuing to the next Step.

Procedure 8.4 Restarting the Database Processor Application (DP)

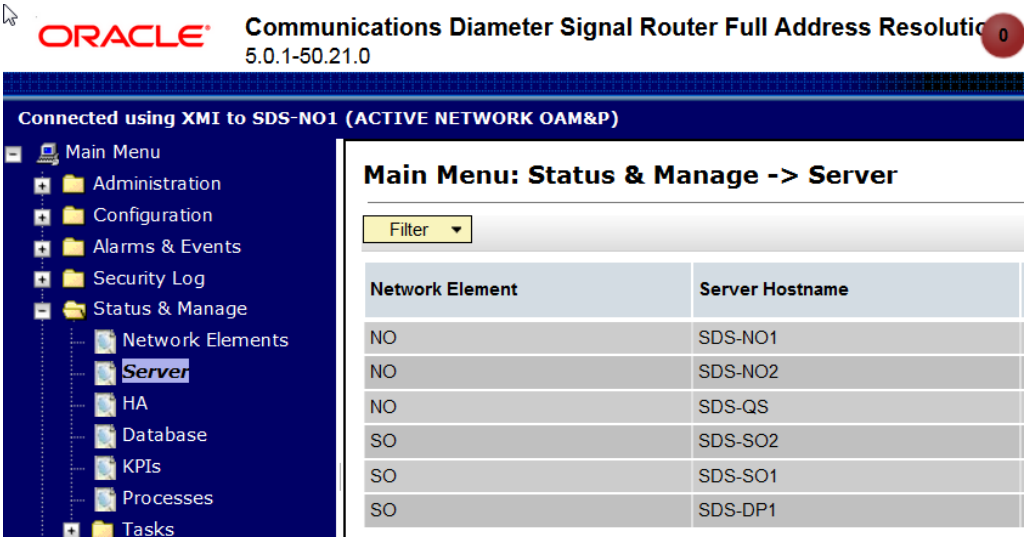
25. ☐

Active SDS VIP:

Select…

Main Menu
→ **Status & Manage**
→ ***Server***

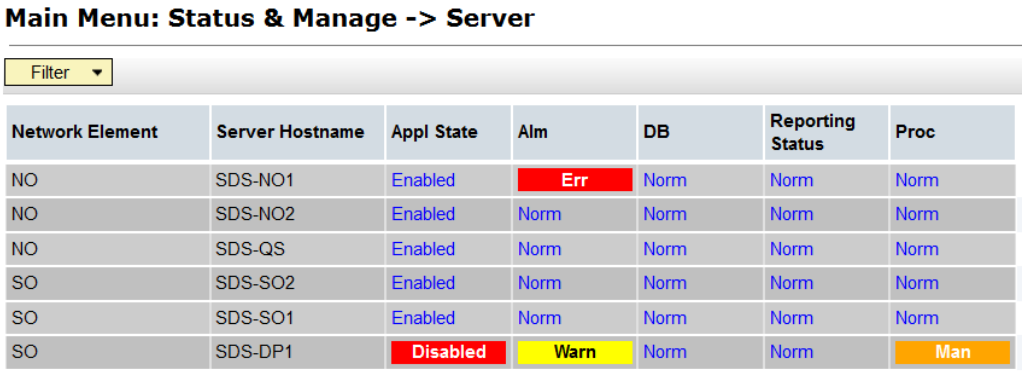
…as shown on the right.



26. ☐

Active SDS VIP:

Verify that the **"DB & Reporting"** status columns all show **"Norm"** for the **DP** at this point. The **"Proc"** column should show **"Man"**.



Network Element	Server Hostname	Appl State	Alm	DB	Reporting Status	Proc
NO	SDS-NO1	Enabled	Err	Norm	Norm	Norm
NO	SDS-NO2	Enabled	Norm	Norm	Norm	Norm
NO	SDS-QS	Enabled	Norm	Norm	Norm	Norm
SO	SDS-SO2	Enabled	Norm	Norm	Norm	Norm
SO	SDS-SO1	Enabled	Norm	Norm	Norm	Norm
SO	SDS-DP1	Disabled	Warn	Norm	Norm	Man

Procedure 8.4 Restarting the Database Processor Application (DP)

27. ☐

Active SDS VIP:

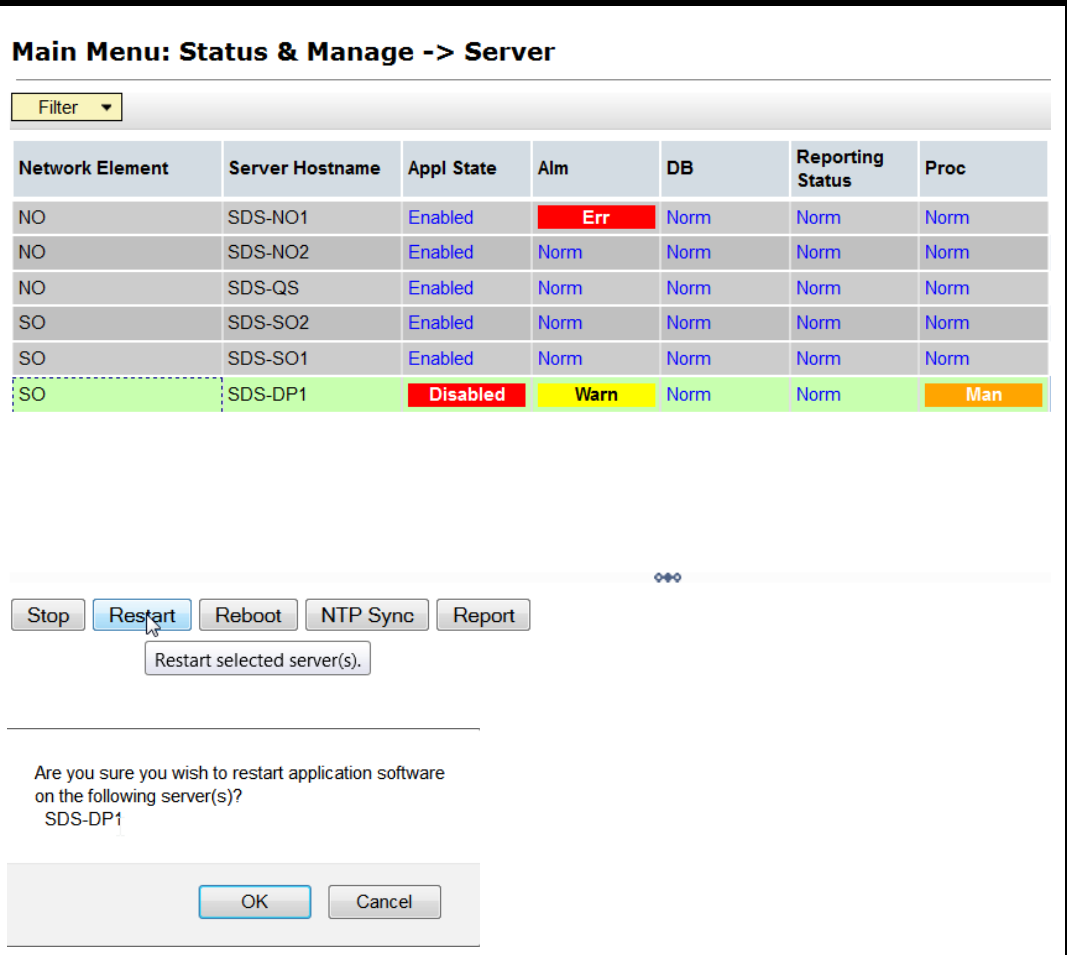
1) Using the mouse, select the **"DP"** hostname. The line entry should now be highlighted in **GREEN**.

2) Select the **"Restart"** dialogue button from the bottom left corner of the screen.

3) Click the **"OK"** button on the confirmation dialogue box.

4) The user should be presented with a confirmation message (in the banner area) for the **"DP"** stating: **"Successfully restarted application"**.

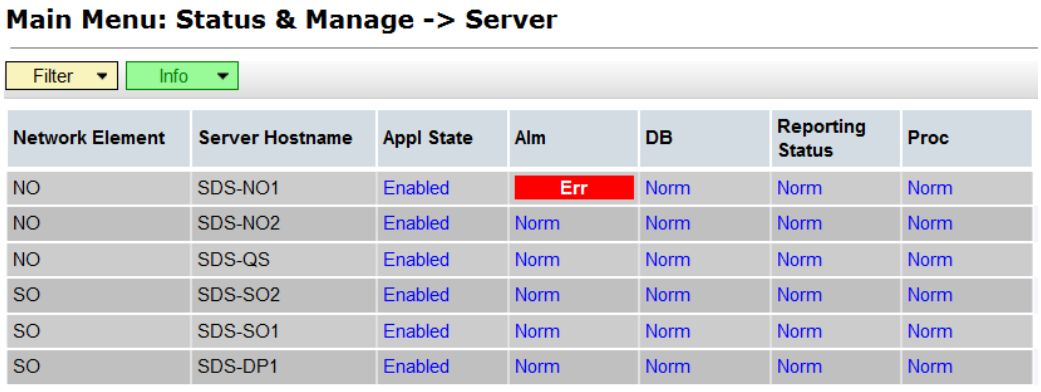
NOTE: *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*



28. ☐

Active SDS VIP:

Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for the **"DP"**.



29. ☐

- Repeat **Steps 25 - 28** of this procedure for each additional **DP** server installed.

Procedure 8.4 Restarting the Database Processor Application (DP)

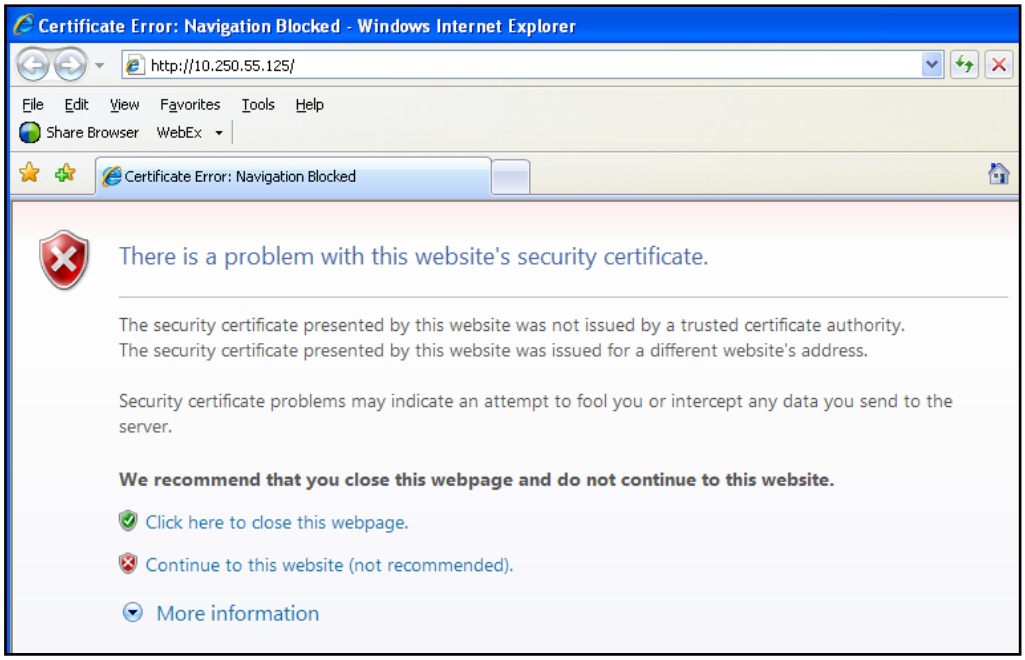
THIS PROCEDURE HAS BEEN COMPLETED

Note: After all DP servers have been installed, the user can configure the ComAgent by following steps in Section 5.7.

5.7 Configuring ComAgent

This procedure configures the ComAgent that allows the SDS Data Processor servers and the DSR Message Processor servers to communicate with each other. These steps cannot be executed until all SDS DP servers are configured.

Procedure 9: Configuring comAgent (All DP-SOAM sites)

Step	Procedure	Result
1. ☐	**Active SDS VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active SDS site** using "https://"	
2. ☐	**Active SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

3. ☐

Active SDS VIP:

Select…

Main Menu

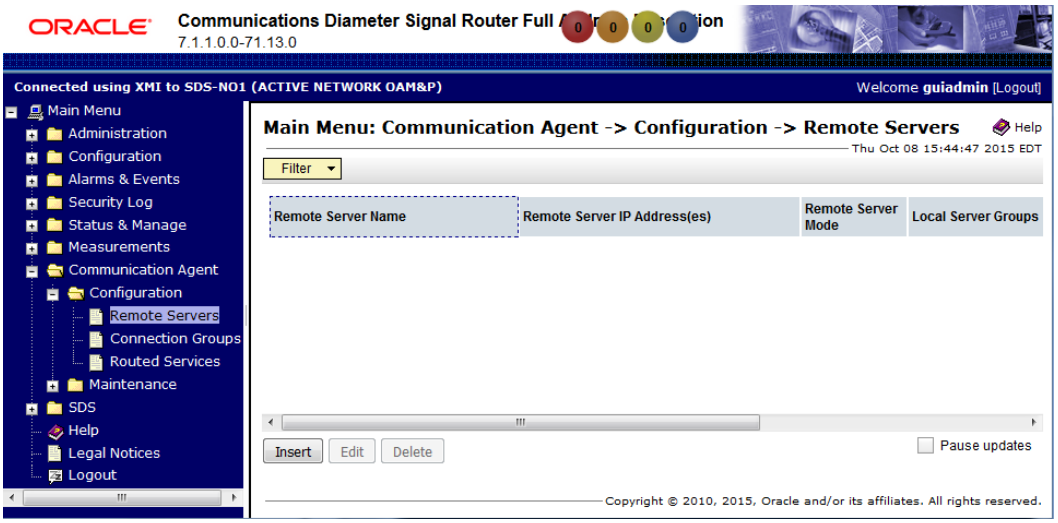
→Communication Agent

→Configuration

→Remote Servers

…as shown on the right.

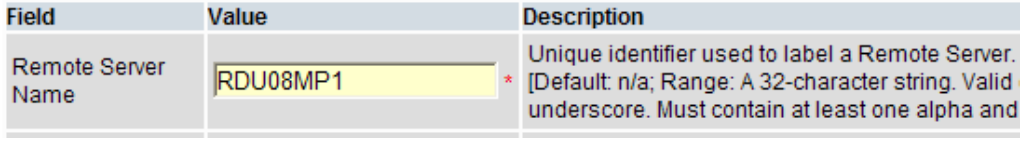
Select the "**Insert**" dialogue button



4. ☐

Active SDS VIP:

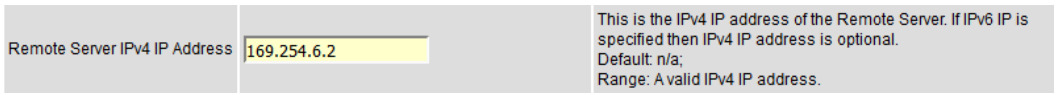
Enter the "**Remote Server Name**" for the DSR Message Processer server



5. ☐

Active SDS VIP:

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



NOTE: *This should be the IMI IP address of the MP.*

6. ☐

Active SDS VIP:

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

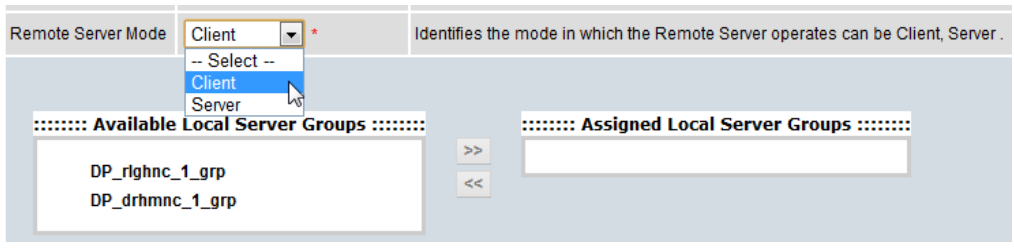
7. ☐

Set preferred IP address.

8. ☐

Active SDS VIP:

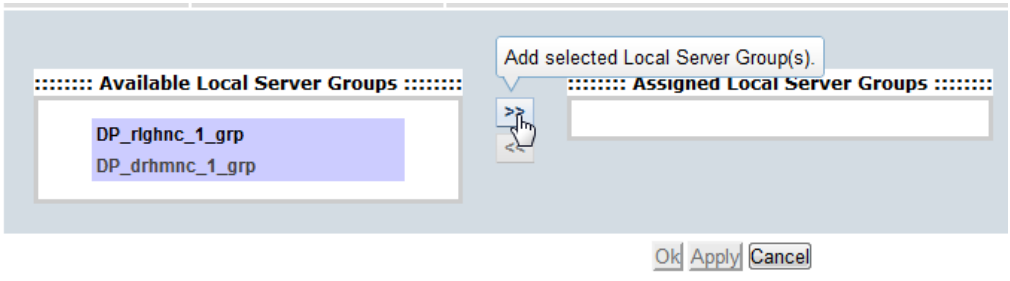
Select "**Client**" for the **Remote Server Mode** from the pull-down menu.

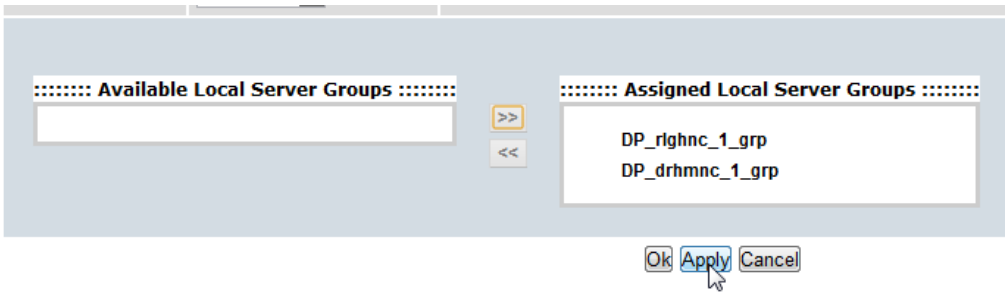
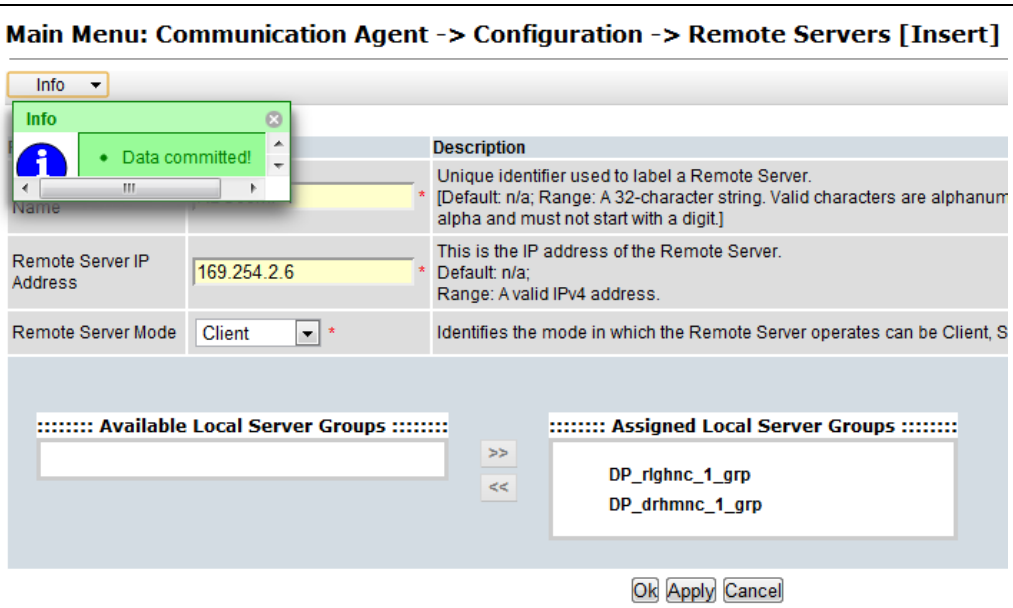


9. ☐

Active SDS VIP:

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



10. ☐	**Active SDS VIP:** Click the "**Apply**" dialogue button	
11. ☐	**Active SDS VIP:** Under the "Info" banner option, the user should be presented with a message stating **"Data committed"**	
12. ☐	• **Repeat steps 3 - 11 of this procedure for each remote MP in the same SOAM NE.**	
THIS PROCEDURE HAS BEEN COMPLETED		

5.8 Backups and Disaster Prevention

Procedure 1: Backups and Disaster Prevention

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

ORACLE Communications
5200 Paramount Parkway
Morrisville, NC 27560 USA
888-FOR-TKLC

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

SDS Network Elements can be created 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 are 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 3 - SDS XML SDS Network Element Configuration File (IPv4)

XML File Text	Description
<?xml version="1.0"?>	
<networkelement>	
<name>**sds_mrsvnc**</name>	Unique identifier used to label a Network Element. [Range = 1-32 character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]
<ntpservers>	
<ntpserver>**10.250.32.10**</ntpserver>	IP Address of the first NTP server. There must be at least one NTP server IP address defined.
<ntpserver>**10.250.32.51**</ntpserver>	IP Address of second NTP server, if it exists; otherwise, this line must be deleted.
</ntpservers>	
<networks>	
<network>	
<name>XMI</name>	Name of customer external network. **Note**: Do NOT change this name.
<vlanId>**3**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**10.250.55.0**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**10.250.55.1**</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. [Range = true/false]
</network>	
<network>	
<name>IMI</name>	Name of customer internal network. **Note**: Do NOT change this name.
<vlanId>**4**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**169.254.100.0**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**169.254.100.3**</gateway>	The gateway router interface address associated with this network

	[Range = A valid IP address]
</network>	
</networks>	
</networkelement>	

.

Table 4 - SDS XML SDS Network Element Configuration File (IPv6)

XML File Text	Description
<?xml version="1.0"?>	
<networkelement>	
<name>**sds_mrsvnc**</name>	Unique identifier used to label a Network Element. [Range = 1-32 character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]
<ntpservers>	
<ntpserver>**10.250.32.10**</ntpserver>	IP Address of the first NTP server. There must be at least one NTP server IP address defined.
<ntpserver>**10.250.32.51**</ntpserver>	IP Address of second NTP server, if it exists; otherwise, this line must be deleted.
</ntpservers>	
<networks>	
<network>	
<name>XMI</name>	Name of customer external network. **Note**: Do NOT change this name.
<vlanId>**3**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>2606:b400:605:b804::</ip>	The network address of this VLAN [Range = 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 [Range = A valid IP address]
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. [Range = true/false]
</network>	
<network>	
<name>IMI</name>	Name of customer internal network. **Note**: Do NOT change this name.
<vlanId>**4**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>FDBD:AAEC:587C:6EFB::</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**/64**</mask>	Subnetting to apply to servers within this VLAN
<gateway>FDBD:AAEC:587C:6EFB:D27E:28FF:FEB3:4FE2</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
</network>	
</networks>	
</networkelement>	

Appendix B. List of Frequently Used Time Zones

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

Table 5 - List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
Etc/UTC	Coordinated Universal Time	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time - Arizona	UTC-07
America/Los_Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico_City	Central Time - most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01

Asia/Hong_Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time - west British Columbia	UTC-08
America/Edmonton	Mountain Time - Alberta, east British Columbia & westSaskatchewan	UTC-07
America/Toronto	Eastern Time - Ontario - most locations	UTC-05
America/Montreal	Eastern Time - Quebec - most locations	UTC-05
America/Sao_Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia - most locations	UTC+08

Australia/Sydney	New South Wales - most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto_Rico		UTC-04
Europe/Moscow	Moscow+00 - west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

Appendix C. Resource Profile

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

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

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

Appendix D. Common KVM/Openstack Tasks

D.1 Import an OVA File

1 ☐	**Create VM flavors.**	Use the Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the "Admin" section, or with the "nova flavor-create" command line tool. Make the flavor names as informative as possible. As flavors describe resource sizing, a common convention is to use a name like "0406060" where the first two figures (04) represent the number of virtual CPUs, the next two figures (06) might represent the RAM allocation in GB and the final three figures (060) might represent the disk space in GB.
2 ☐	**Unpack and import an image file using the glance utility.**	8. Copy the OVA file to the OpenStack control node. i. "$ scp SDS-7.2.x.x.x.ova admusr@node:~" 9. Login to the OpenStack control node. i. "$ ssh admusr@node" 10. In an empty directory unpack the OVA file using "tar" i. "$ tar xvf SDS-7.2.x.x.x.ova" 11. One of the unpacked files will have a ".vmdk" suffix. This is the VM image file that must be imported. i. SDS-7.2.x.x.x-disk1.vmdk 12. Source the OpenStack "admin" user credentials. i. "$. keystonerc_admin" 13. Select an informative name for the new image. i. "sds-7.2.x.x.x-original" 14. Import the image using the "glance" utility from the command line. i. `$ glance image-create --name sds-7.2.x.x.x-original --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file SDS-7.2.x.x.x-disk1.vmdk` This process will take about 5 minutes, depending on the underlying infrastructure

D.2 Create a Network Port

1 ☐	**Create the network ports for the NO network interfaces.**	1. Each network interface on an instance must have an associated network port. a. An instance will usually have at least eth0 and eth1 for a public and private network respectively.

		b. Some configurations will require more interfaces and corresponding network ports. 2. Determine the IP address for the interface. a. For eth0, the IP might be 10.x.x.157. b. For eth1, the IP might be 192.168.x.157 3. Identify the neutron network ID associated with each IP/interface using the "neutron" command line tool. a. "$ neutron net-list" 4. Identify the neutron subnet ID associated with each IP/interface using the "neutron" command line tool. a. "$ neutron subnet-list" 5. Create the network port using the "neutron" command line tool, being sure to choose an informative name. Note the use of the subnet ID and the network ID (final argument). a. Port names are usually a combination of instance name and network name. i. "NO1-xmi" ii. "SO2-imi" iii. "MP5-xsi2" b. 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. i. "$. keystonerc_dsr_user" ii. "$ keystone user-list" c. `$ neutron port-create --name=NO1-xmi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>` d. `$ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>` e. `View your newly created ports using the neutron tool.` i. "$ neutron port-list"

D.3 Create and Boot OpenStack Instance

1 ☐	**Create a VM instance from a glance image.**	3. Get the following configuration values. a. The image ID. i. "$ glance image-list" b. The flavor ID. i. "$ nova flavor-list" c. The port ID(s) i. "$ neutron port-list" d. An informative name for the instance. i. "NO1" ii. "SO2" iii. "MP5" 4. Create and boot the VM instance. a. The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. b. `$ nova boot --image <image ID> --flavor <flavor id> --nic port-id=<first port id> --nic port-id=<second port id> InstanceName` c. View the newly created instance using the nova tool. i. "$ nova list --all-tenants" The VM will take approximately 5 minutes to boot. At this point, the VM has no configured network interfaces, and can only be accessed by the "Horizon" console tool.

D.4 Configure Networking for OpenStack Instance

1 ☐	**Configure the network interfaces and hostname.**	10. Log in to the "Horizon" GUI as the DSR tenant user. 11. Go to the Compute/Instances section. 12. Click on the "Name" field of the newly created instance. 13. Select the "Console" tab. 14. Login as the admusr. 15. Select an informative hostname for the new VM instance. a. "NO1". b. "SO2". c. "MP5". 16. Use sudo to change the machine hostname from the default value.

a. Edit /etc/hosts.
    i. Append the hostname to the IPv4 line.
        1. "127.0.0.1 localhost localhost4 NO1"
    ii. Append the hostname to the IPv6 line.
        1. "::1 localhost localhost6 NO1"
b. Edit /etc/syconfig/hostname.
    i. Change the "HOSTNAME=XXXX" line to the new hostname.
    ii. "HOSTNAME=NO1"
c. Set the hostname on the command line.
    i. "$ sudo hostname NO1"

17. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C.
    a. "$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi port ip> --netmask=<xmi net mask>"
    b. "$ sudo netAdm add --onboot=yes --device=eth1 --address=<imi port ip> --netmask=<imi net mask>"
    c. "$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>"
    d. Under some circumstances, it may be necessary to configure more interfaces.
    e. If netAdm fails to create the new interface (ethX) because it already exists in a partially configured state, perform the following actions.
        i. $ cd /etc/sysconfig/network-scripts
        ii. $ sudo mv ifcfg-ethX /tmp
            1. Keep ifcfg-ethX in /tmp until ethX is working correctly.
        iii. Re-run the netAdm command. It will create and configure the interface in one action.
18. Reboot the VM. It will take approximately 5 minutes for the VM to complete rebooting.
    a. "$ sudo init 6"

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

Appendix E. Application VIP Failover Options (OpenStack)

E.1 Application VIP Failover Options

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

- Allowed address pairs
- Disable port security

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

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

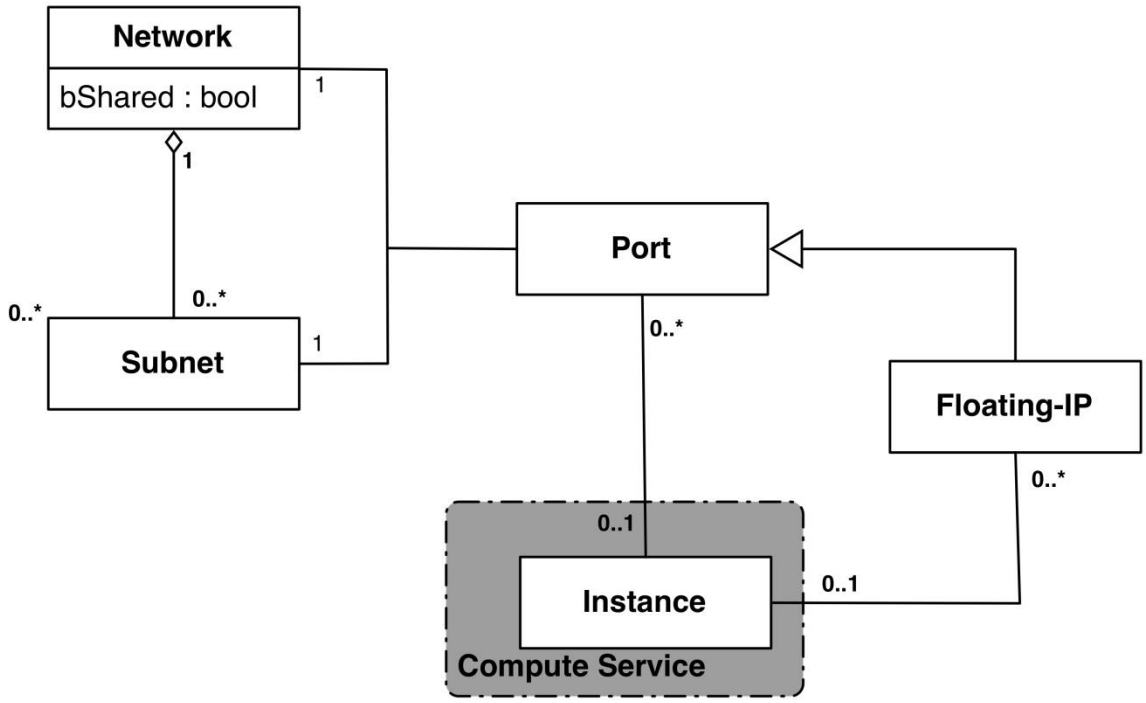


Figure 1 - Neutron High-Level Data Model

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

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

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

The anti-spoofing rules are enforced at the Neutron port level by ensuring that the source IP address of outgoing packets matches the IP address Neutron has associated with the corresponding port assigned to the VM instance. By default if the

source IP address in the outgoing packet does not match the IP address associated with the corresponding Neutron port then the packet is dropped.

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

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

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

E.2 Allowed Address Pairs

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

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

E.3 OpenStack Configuration Requirements

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

```
# neutron ext-list
+-----------------------+-----------------------------------------------+
| alias                 | name                                          |
+-----------------------+-----------------------------------------------+
| security-group        | security-group                                |
| l3_agent_scheduler    | L3 Agent Scheduler                            |
| net-mtu               | Network MTU                                   |
| ext-gw-mode           | Neutron L3 Configurable external gateway mode |
| binding               | Port Binding                                  |
| provider              | Provider Network                              |
| agent                 | agent                                         |
| quotas                | Quota management support                      |
| subnet_allocation     | Subnet Allocation                             |
| dhcp_agent_scheduler  | DHCP Agent Scheduler                          |
| l3-ha                 | HA Router extension                           |
```

```
| multi-provider        | Multi Provider Network                          |
| external-net          | Neutron external network                        |
| router                | Neutron L3 Router                               |
| allowed-address-pairs | Allowed Address Pairs                           |
| extraroute            | Neutron Extra Route                             |
| extra_dhcp_opt        | Neutron Extra DHCP opts                         |
| dvr                   | Distributed Virtual Router                      |
+-----------------------+-------------------------------------------------+
```

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

E.4 After a VM instance has been booted: Allowed Address Pairs

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

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

where the bolded items have the following meaning:

- <Port ID>

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

- <VIP address to be added>

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

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

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

E.5 Before a VM instance has been booted: Allowed Address Pairs

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

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

where the bolded items have the following meaning:

- <Port Name>

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

- <Subnet name>

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

- <Target IP address>

  The unique IP address to be associated with the port.

- <Network Name>

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

- <VIP address to be added>

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

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

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

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

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

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

E.6 Disable Port Security

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

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

OpenStack Configuration Requirements

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

ML2 Port Security Extension Wiki page

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

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

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

E.7 After a VM instance has been booted: Port Security

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

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

where the bolded item has the following meaning:

- <VM instance name>

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

- <Security group name>

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

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

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

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

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

where the bolded item has the following meaning:

- <Port ID>

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

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

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

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

E.8 Before a VM instance has been booted: Port Security

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

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

where the bolded items have the following meaning:

- <Port Name>

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

- <Subnet name>

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

- <Target IP address>

  The unique IP address to be associated with the port.

- <Network Name>

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

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

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

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

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

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

E.9 Managing Application Virtual IP Addresses within VM instances

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

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

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

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