Oracle® Communications

Diameter Signal Router Full Address Resolution

SDS Initial Installation and Configuration Guide

Release 8.1

E88531-01

July 2017

ORACLE

Oracle® Communications Diameter Signal Router Full Address Resolution, SDS Initial Installation and Configuration Guide , Release 8.1.

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

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

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

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

Table of Contents

1. Introduction 8
1.1 Purpose and Scope 8
1.2 References 8
1.3 Acronyms 8
1.4 Assumptions 9
1.5 XML Files 9
1.6 How to Use this Document 9

2. Pre-Installation Setup 10
2.1 Installation Prerequisites 10
2.2 Physical Connections 10
2.3 Access Alternatives for Application Install 11
2.4 Activity Logging 12
2.5 Firmware and BIOS Settings 12
2.6 Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware 13

3. Installation Matrix 15
3.1 Installing SDS on the Customer Network 15

4. Application Installation 16
4.1 Installing the SDS Application (All SDS NOAM Sites) 16

5. Configuration Procedures 24
5.1 Configuring SDS Servers A and B (1st SDS NOAM Site Only) 24
5.2 OAM Pairing (1st SDS NOAM Site Only) 46
5.3 Query Server Installation (All SDS NOAM Sites) 64
5.4 OAM Installation for the DR SDS NOAM Site 83
5.5 OAM Pairing for DR SDS NOAM Site 100
5.6 Add SDS Software Images to PMAC Servers (All SOAM Sites) 114
5.7 OAM Installation for SOAM Sites (All SOAM Sites) 118
5.8 OAM Pairing for SDS SOAM Sites (All SOAM Sites) 145
5.9 DP Installation (All SOAM Sites) 159
5.10 Configuring ComAgent 191

Appendix A. Accessing the iLO VGA Redirection Window 194

Appendix B. Creating Temporary External IP Address for Accessing SDS GUI 196

Appendix C. Establish a Local Connection for Accessing the SDS GUI 197

Appendix D. Configure Cisco 4948E-F Aggregation Switches 200

D-1. Verifying Cisco Switch Wiring (All SDS NOAM Sites) 201

D-2. Configure Cisco 4948E-F Aggregation Switches 206

D-3. Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites) 229

D-4. Cisco 4948E-F Configuration Backup (All SDS NOAM sites) 238

Appendix E. Creating an XML File for Installing Network Elements 240

Appendix F. NetBackup Client Installation 243

Appendix G. List of Frequently Used Time Zones 244

Appendix H. Accepting Installation Through SDS NOAM GUI 245

Appendix I. Disable Hyperthreading for Gen8 and Gen9 (DP Only) 248

Appendix J. Configure the HP DL380 (Gen8 and Gen9) Server CMOS Clock/BIOS Settings 266

J-1. Gen8: Configure the ILO for Rack Mount Server 266

J-2. Gen9: RMS Configure iLO 282

Appendix K. Accessing My Oracle Support (MOS) 303

List of Tables

Table 1 – Acronyms 8
Table 2 – SDS Installation Matrix 15
Table 3 – SDS Installation – List of Procedures 15
Table 4 – SDS Network Element Configuration File (IPv4) 241
Table 5 – SDS Network Element Configuration File (IPv6) 242
Table 6 – List of Selected Time Zone Values 244

List of Figures

Figure 1 – HP DL380 Gen8: DC (Rear Panel) 10
Figure 2 – HP DL380 Gen9: DC (Rear Panel) 11
Figure 3 – HP DL380 Gen8: Front Panel (USB Port) 18
Figure 4 – HP DL380 Gen9: Front Panel (USB Port) 18
Figure 5 – HP DL380 Gen8: Rear Panel (Ethernet) 44
Figure 6 – HP DL380 Gen9: DC (Rear Panel) 44
Figure 7 – Cisco 4948E-F Switch (Maintenance Access Port) 45
Figure 8 – HP DL380 Gen8: Front Panel (USB Port) 73

Figure 9 – HP DL380 Gen9: Front Panel (USB Port) 73
Figure 10 – HP DL380 Gen8: Front Panel (USB Port) 74
Figure 11 – HP DL380 Gen9: Front Panel (USB Port) 74
Figure 12 – HP DL380 Gen8: Front Panel (USB Port) 94
Figure 13 – HP DL380 Gen9: Front Panel (USB Port) 94
Figure 14 – HP DL380 Gen8: Front Panel (USB Port) 96
Figure 15 – HP DL380 Gen9: Front Panel (USB Port) 96
Figure 16 – HP DL380 Gen9: DC (Rear Panel) 198
Figure 17 – SDS Frame Layout 200
Figure 18 – Cisco 4948E-F Switch ISL Connections 201
Figure 19 – Cisco 4948E-F Switch (Console Port) 201
Figure 20 – HP DL380 Gen8: Rear Panel (Quad-Serial Ports) 202
Figure 21 – HP DL380 Gen8: Rear Panel (Ethernet) 203
Figure 22 – Cisco 4948E-F Switch (Console Port) 204
Figure 23 – HP DL380 Gen9: DC (Rear Panel) 204
Figure 24 – HP DL380 Gen9: DC (Rear Panel) 205
Figure 25 – HP DL380 Gen8: Front Panel (USB Port) 230
Figure 26 – HP DL380 Gen9: Front Panel (USB Port) 230
Figure 27 – iLO Configuration – Gen8: Press [F8] to configure 266
Figure 28 – iLO Configuration – Initial iLO Configuration Screen 267
Figure 29 – iLO Configuration – Select Network->DNS/DHCP 267
Figure 30 – iLO Configuration – press [SPACE BAR] to turn DHCP OFF 268
Figure 31 – iLO Configuration – Select NIC and TCP/IP 268
Figure 32 – iLO Configuration – Select NIC and TCP/IP and configure Network 269
Figure 33 – iLO Configuration – Select User – Add 269
Figure 34 – RBSU – Enter RBSU – F9 Pressed indicated in HP Splash Screen 271
Figure 35 – iLO Configuration – Initial iLO Configuration Screen 271
Figure 36 – ROM-Based Setup Utility – Initial Screen 272
Figure 37 – ROM-Based Setup Utility – Serial Port Options 272
Figure 38 – Verify Embedded Serial Port Setting 273
Figure 39 – RBSU – Select Power Management Options 274
Figure 40 – RBSU – Select HP Power Profile and Maximum 275
Figure 41 – Select Standard Boot Order 276
Figure 42 – Select Set the IP Device Boot Order to 1 276
Figure 43 – IPL:1 is Now USB DriveKey (C:) 276
Figure 44 – Select Date and Time 277
Figure 45 – Set Date and Time (UTC) 277
Figure 46 – RBSU – Select Server Availability 278
Figure 47 – RBSU – Verify ASR Status is Set to Enabled 279
Figure 48 – RBSU – Verify Automatic Power-On is Set to Enabled 279
Figure 49 – RBSU – Verify Power-On Delay is Set to No Delay 280
Figure 50 – RBSU – Exit ROM-Based Setup Utility 281
Figure 51 – Gen9: iLO Configuration – Gen9: Press [F9] to configure 282
Figure 52 – Gen9: iLO4 Select System Configuration 283
Figure 53 – Gen9: iLO: Select iLO4 Configuration Utility 283
Figure 54 – Gen9: iLO Configuration – User Management 283
Figure 55 – Gen9: iLO Configuration – Add User 284
Figure 56 – Gen9: iLO Configuration – Add New User Name: tekelec 284

Figure 57 – Gen9: iLO Configuration – Select Network Options 285
Figure 58 – Gen9: iLO Configuration – DHCP Enable to OFF 285
Figure 59 – Gen9: iLO Configuration – Network Configuration IP, Subnet, Gateway 286
Figure 60 – Gen9: iLO Configuration – F10 Save Changes 287
Figure 61 – Gen9: iLO Configuration – Change Reboot Message 287
Figure 62 – Gen9 RBSU – Enter RBSU – F9 Pressed indicated in HP Splash Screen 288
Figure 63 – Gen9: Select System Configuration 289
Figure 64 – Gen9: Select BIOS/Platform Configuration (RBSU) 289
Figure 65 – Gen9: ROM-Based Setup Utility – System Options 290
Figure 66 – Gen9: ROM-Based Setup Utility – Serial Port Options 290
Figure 67 – Gen9: Verify Embedded Serial Port Setting 291
Figure 68 – Gen9: Verify Virtual Serial Port Setting 291
Figure 69 – Gen9: RBSU – Select Power Management 292
Figure 70 – Gen9: RBSU – Select HP Power Profile and Maximum Performance 293
Figure 71 – Gen9: Select Boot Options 294
Figure 72 – Gen9: Select Legacy BIOS Boot Order 294
Figure 73 – Select Set the IP Device Boot Order USB DriveKey 295
Figure 74 – Select Set the IP Device Boot Order Embedded LOM 1 Port 1 295
Figure 75 – Gen9: Select Date and Time 296
Figure 76 – Gen9: Set Date and Time (UTC) 296
Figure 77 – Gen9: RBSU – Select Server Availability 297
Figure 78 – Gen9: RBSU – Verify ASR Status is Set to Enabled 297
Figure 79 – Gen9: RBSU – Verify Automatic Power-On is Set to Restore Last Power State 298
Figure 80 – Gen9: RBSU – Verify Power-On Delay is Set to No Delay 298
Figure 81 – Gen9: RBSU – Verify Post F1 Prompt is Set to Delayed 20 Seconds 299
Figure 82 – Gen9: RBSU – Verify Advanced Options 300
Figure 83 – Gen9: RBSU – Verify Fan and Thermal Options 300
Figure 84 – Gen9: RBSU – Save Changes and Confirm 301
Figure 85 – Gen9: RBSU – Changes Saved 301
Figure 86 – Gen9: Exit System Utilities 302

List of Procedures

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware 13
Procedure 2. Installing the SDS Application (All SDS NOAM Sites) 16
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only) 24
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only) 46
Procedure 5. Configuring the Query Server (All SDS NOAM Sites) 64
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only) 83
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only) 100
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites 114
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites) 119
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites) 145
Procedure 11. Installing the Data Processor Blade (All SOAM Sites) 159
Procedure 12. Configuring ComAgent (All SOAM Sites) 191
Procedure 13. Accessing the iLO VGA Redirection Window 194
Procedure 14. Creating Temporary External IP Address for Accessing SDS GUI 196

Procedure 15. Establish a Local Connection for Accessing SDS GUI 197
Procedure 16. Verifying Cisco Switch Wiring (SDS Sites) 201
Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites) 207
Procedure 18. Configure Cisco 4948E-F Aggregation Switches (All SDS NOAM Sites) 218
Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites) 229
Procedure 20. Cisco 4948E-F Backup (SDS Sites) 239
Procedure 21. NetBackup Client Installation 243
Procedure 22. Accepting Installation Through SDS NOAM GUI 245
Procedure 23. Gen8: Disable Hyerthreading (DP Only) 248
Procedure 24. Gen9: Disable Hyperthreading (DP Only) 256
Procedure 25. Gen8: Configure the iLO for Rack Mount Server 266
Procedure 26. Enter the ROM-Based Setup Utility (RBSU) 271
Procedure 27. Verify/Configure Serial Port Options 272
Procedure 28. Verify/Set Power Management 274
Procedure 29. Verify/Set Standard Boot Order (IPL) 276
Procedure 30. Verify/Set System Date and Time 277
Procedure 31. Verify/Set Server Availability 278
Procedure 32. Exit the RBSU 281
Procedure 33. Gen8: Configure the iLO for Rack Mount Server 282
Procedure 34. Gen9: Enter the ROM-Based Setup Utility (RBSU) 288
Procedure 35. Gen9: Verify/Configure Serial Port Options 289
Procedure 36. Gen9: Verify/Set Power Management 292
Procedure 37. Gen9: Verify/Set Standard Boot Order (IPL) 294
Procedure 38. Gen9: Verify/Set System Date and Time 296
Procedure 39. Gen9: Verify/Set Server Availability 297
Procedure 40. Gen9: Verify Advanced Options 300
Procedure 41. Gen9: Save and Exit the RBSU 301

1. Introduction

1.1 Purpose and Scope

This document describes how to install the Oracle® Communications Diameter Signal Router Full Address Resolution product also known as “Eagle XG Subscriber Data Server (SDS)” within a customer network. It makes use of the Platform 7.3 network installation and is intended to cover the initial network configuration steps for a SDS/Query Server NE and a SOAM/DP (Blade) NE for production use as part of the DSR 8.1 solution. This document includes switch configuration (Cisco 4948E-F) and validation of the initial SDS configuration. This document only describes the SDS product installation on the HP DL380 Gen8 and Gen9 deployed using Cisco 4948E-F switches. 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 cabinet. Users needing familiarity with these areas of interest should refer sources cited in Section 1.2 References.

1.2 References

External (Customer Facing)

[1] TEKELEC Acronym Guide, MS005077, Latest Revision

[2] DSR 8.1 C-Class Hardware and Software Installation Part 1/2, Latest Revision

[3] DSR 8.1 Software Installation & Configuration Procedure Part 2/2, Latest Revision

Internal (ORACLE Communications Personnel Only)

[4] HP Solutions Firmware Upgrade Pack Release Notes, 795-000-4xx, Latest version (2.2.9 or higher)

[5] Platform 7.2 Configuration Guide, Revision 5

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

[7] TPD Initial Product Manufacture, Software Installation Procedure, Release 8.0+, Latest Revision

1.3 Acronyms

Table 1 – Acronyms

Acronym	Description
DP	Data Processor blade
DR	Disaster Recovery
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAM	Network Operations, Administration & Maintenance
iLO	HP Integrated Lights-Out
IPM	Initial Product Manufacture
SDS	Subscriber Data Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)

Acronym	Description
VIP	Virtual IP
XMI	External Management Interface
XML	Extensible Markup Language

1.4 Assumptions

This procedure assumes the following;

- The user has reviewed the latest Network Architecture Planning Document (NAPD) [6]and has received assigned values for all requested information related to SDS, Query Server, SOAM and DP installation.
- The user has taken assigned values from the latest Customer specific DSR Network Planning document [6] and used them to compile XML files (See Appendix E) for each SDS and 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 [6].
- The user has at least an intermediate skill set with command prompt activities on an Open Systems computing environment such as Linux or TPD.
- All SDS servers were IPM'ed with TPD Platform 7.4 of correct version as described in [7].

1.5 XML Files

The XML files compiled for installation of the each of the SDS NOAM and SOAM site Network Elements must be maintained and accessible for use in Disaster Recovery procedures.

If engaged by the customer, the ORACLE Consulting Services Engineer 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 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 Customer Service for assistance before attempting to continue. See Appendix K – Accessing My Oracle Support (MOS) for information on contacting Oracle Customer Support.

2. Pre-Installation Setup

2.1 Installation Prerequisites

The following items/settings are required in order to perform installation for HP DL380 based SDS HW:

- A laptop or desktop computer equipped as follows;
  - 10/100 Base-TX Ethernet Interface.
  - Administrative privileges for the OS.
  - An approved web browser (currently Internet Explorer 10.x or 11.x)
- An IEEE compliant 10/100 Base-TX Ethernet Cable, RJ-45, Straight-Through.
- USB flash drive with at least 1GB of available space.
- TPD “root” user password.
- TPD “admusr” user password.

Note: When using the iLO for SSH connectivity, supported terminal Emulations are **VT100 or higher** (i.e., VT-102, VT-220, VT-320).

2.2 Physical Connections

A connection to the VGA/Keyboard ports on the HP DL Server rear panel or a connection to the iLO is required to initiate and monitor the progress of SDS installation procedures.

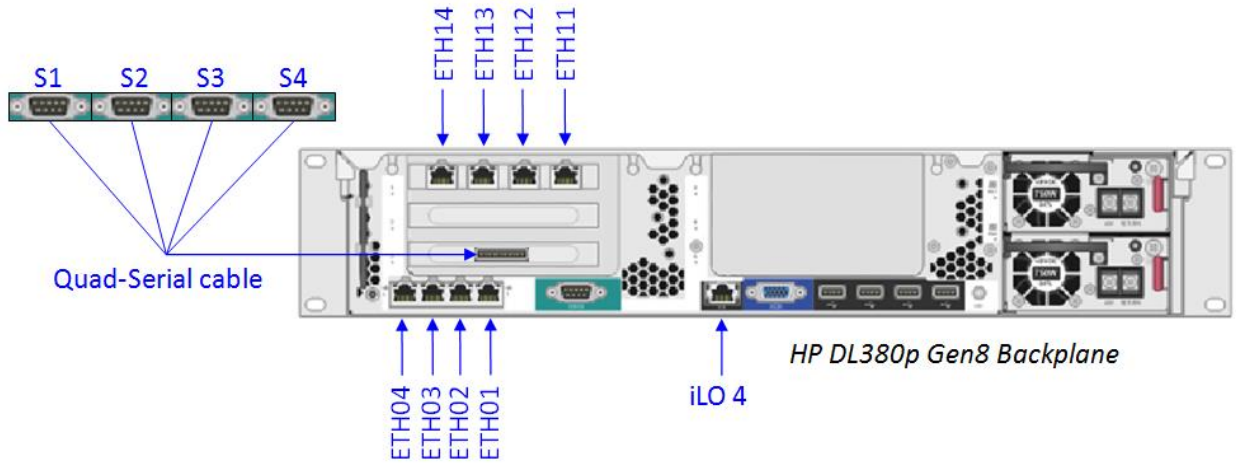


Figure 1 – HP DL380 Gen8: DC (Rear Panel)

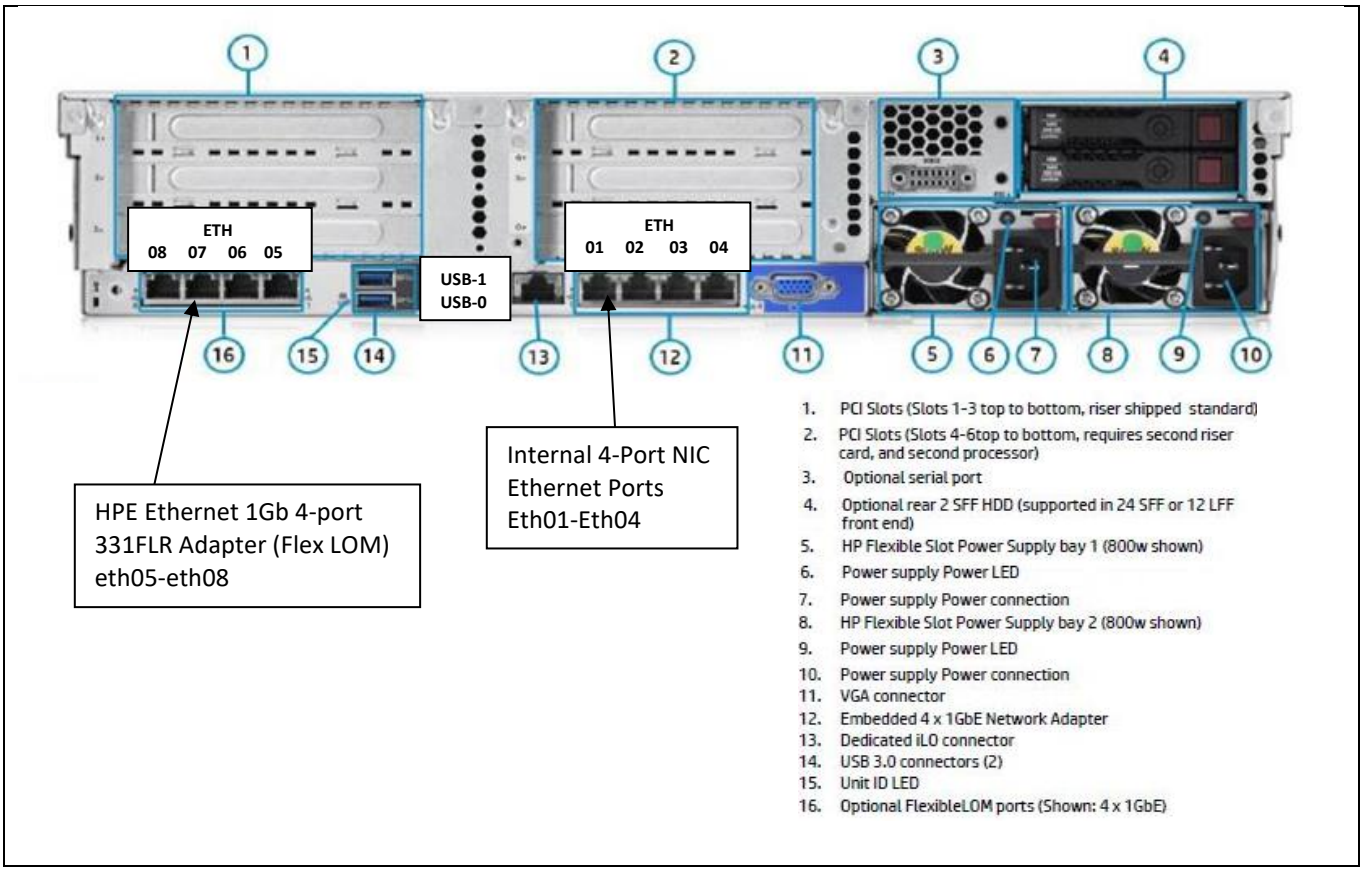


Figure 2 – HP DL380 Gen9: DC (Rear Panel)

2.3 Access Alternatives for Application Install

This procedure may also be executed using one of the access methods described below:

One of the **Access Methods** shown to the right may be used to initiate and monitor SDS installation. ***Note***: *Methods 3 & 4 may only be used on an DL380 with an iLO that has been previously configured with a statically assigned IP address. It is not intended for use with a new, out-of-the-box server.*	☐	**Method 1)** VGA Monitor and PS2 Keyboard.
	☐	**Method 2)** Laptop + epiphan SYSTEMS INC. KVM2USB switch. http://www.epiphan.com/products/frame-grabbers/kvm2usb/
	☐	**Method 3)** iLO VGA Redirection Window, IE8 (or IE9 with Document Mode "IE8 Standards"), Ethernet cable. (See Appendix A).
	☐	**Method 4)** iLO access via SSH, terminal program, Ethernet cable.

2.4 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.

Note: Parts of this procedure will utilize a VGA Monitor (or equivalent) as the active terminal. It is understood that logging is not possible during these times. The user is only expected to provide logs for those parts of the procedures where direct terminal capture is possible (i.e., SSH, serial, etc.).

2.5 Firmware and BIOS Settings

Prior to upgrading the Firmware of the DL380 (Gen8 & Gen9) servers the CMOS Clock, BIOS Settings, and iLO IP Address needed to be configured. These configuration procedures are defined in Appendix J of this document.

Several procedures in this document pertain to the upgrading of firmware on DL380 servers and Cisco 4948 E-F switches that are part of the Platform 7.3.x configuration.

The required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP *Solutions Firmware Upgrade Pack.* The minimum firmware release required for Platform 7.3.x is *HP Solutions Firmware Upgrade Pack 2.2.9 or higher*. If a firmware upgrade is needed, the current GA release of the *HP Solutions Firmware Upgrade Pack* should be used.

Each version of the *HP Solutions Firmware Upgrade Pack* contains multiple items including media and documentation. If an HP FUP 2.x.x version newer than the Platform 7.0.x minimum of HP FUP 2.2.9 is used, then the *HP Solutions Firmware Upgrade Guide* should be used to upgrade the firmware. Otherwise, the HP Solutions Firmware Upgrade Guide, Release 2.x.x should be used.

The three pieces of required firmware media provided in the *HP Solutions Firmware Upgrade Pack* releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP Service Pack for ProLiant (SPP) firmware USB image
- HP MISC Firmware ISO image

Refer to the Release Notes of the *[4] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x, (Min 2.2.9)* to determine specific firmware versions needed.

Contact Accessing My Oracle Support (MOS) for more information on obtaining the HP Firmware Upgrade Packs.

2.6 Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

The following procedure explains the steps needed to configure the CMOS Clock, BIOS Settings, and iLO IP address of the DL80 RMS servers and upgrade the firmware (if needed).

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

S T E P #	The following procedure explains the steps needed to configure the CMOS Clock, BIOS Settings, and iLO IP Address of the DL380 RMS servers and upgrade the firmware. (If needed). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K My Oracle Support and ask for assistance.	
1 ☐	**Configure RMS Server.**	Connect to the RMS Server using a VGA Display and USB Keyboard. **For HP DL 380 (G8) Servers execute:** Appendix J.1.1 RMS: Configure ILO Appendix J.1.2 Gen8: RMS BIOS Configuration, Verify Processor and Memory **For HP DL 380 (G9) Servers execute:** Appendix J.2.1 RMS: Configure iLO Appendix J.2.2 Gen9: RMS BIOS Configuration, verify processor & memory
2 ☐	**RMS Server:** Verify/Upgrade Firmware	Follow the appropriate procedure for the ProLiant DL380(G8/G9) hardware type to verify and upgrade the HP server firmware using the procedures in [7] HP Solutions Firmware Upgrade Pack Upgrade Guide, Release 2.x.x, (Min 2.2.9) Check-off the associated Check Box in step 3 as the RMS server's CMOS Clock, BIOS Settings, and iLO IP Address has been configured and firmware is updated:

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

3 ☐	**RMS Server:** CMOS Clock, BIOS Settings, and iLO IP Address have been configured and firmware updated	Check-off the associated **Check Box** as the RMS server's CMOS Clock, BIOS Settings, and iLO IP Address has been configured and firmware is updated: **Primary Site:** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recover Site: (Optional)** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____
4 ☐	**Optional: Repeat on the Disaster Recovery RMS servers.**	

3. Installation Matrix

3.1 Installing SDS on the Customer Network

Installing the SDS product is a task which requires multiple installations of varying types. The matrix below provides a guide to the user as to which procedures are to be performed on which server 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 Accessing My Oracle Support (MOS) for assistance with post installation configuration options.

***Note*:** Although the SDS sites are fully redundant by function, we must distinguish between them during installation due to procedural changes based on the installation sequence. The user should be aware that any reference to the "SDS" site refers to the 1st installation of a SDS pair on the customer network while references to the "DR SDS" site refers to the 2nd SDS pair to be installed.

Table 2 – SDS Installation Matrix

Server Type		Procedures to perform												
		1	2	3	4	5	6	7	8	9	10	11	E.*	J
☐	SDS NOAM	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
☐	DR SDS NOAM	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗
☐	Query Server	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
☐	SDS SOAM	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
☐	DP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗

Table 3 – SDS Installation – List of Procedures

Procedure No.	Title	Page No.
Procedure 2	Installing the SDS Application (All SDS NOAM Sites)	16
Procedure 3	Configuring SDS Servers A and B (1st SDS NOAM Site Only)	24
Procedure 4	Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)	46
Procedure 5	Configuring the Query Server (All SDS NOAM Sites)	64
Procedure 6	Configuring the DR NOAM Servers (DR SDS NOAM Site Only)	83
Procedure 7	Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)	100
Procedure 8	Add SDS Software Images to PMAC Servers for DSR Signaling Sites	114

Procedure No.	Title	Page No.
Procedure 9	Configuring the SDS SOAM Servers (All SOAM Sites)	119
Procedure 10	Pairing the SDS SOAM Servers (All SOAM Sites)	145
Procedure 11	Installing the Data Processor Blade (All SOAM Sites)	159
Procedure 12	Configuring ComAgent (All SOAM Sites)	191
D-1	Verifying Cisco Switch Wiring (All SDS NOAM Sites)	201
D-2	Configure Cisco 4948E-F Aggregation Switches	218
D-3	Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)	229
D-4	Cisco 4948E-F Configuration Backup (All SDS NOAM sites)	238
Appendix J	Configure the HP DL380 (Gen8 and Gen9) Server CMOS Clock/BIOS Settings	266

4. Application Installation

4.1 Installing the SDS Application (All SDS NOAM Sites)

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
1. ☐	Access the HP server's console.	Connect to the HP DL 380 server's console using one of the access methods described in **Section 2.3.**

2. ☐	**1)** Access the command prompt.
	2) Log into the HP server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

3. ☐	Verify that Date & Time are displayed in **GMT** (+/- 4 min.).	`$ date -u`
		`Wed Oct 22 14:07:12 UTC 2014`
		`$`

IF THE CORRECT DATE & TIME (IN GMT) ARE NOT SHOWN IN THE PREVIOUS STEP, THEN STOP THIS PROCEDURE AND PERFORM THE FOLLOWING STEPS:

1. Execute Appendix J- CONFIGURE THE HP DL380 (GEN8 AND GEN9) SERVER CMOS CLOCK/BIOS SETTINGS
2. Restart Procedure 1 beginning with Step 1.

IF THE CORRECT DATE & TIME (IN GMT) ARE SHOWN IN THE PREVIOUS STEP, THEN CONTINUE ON TO STEP 4 OF THIS PROCEDURE.

4. ☐	Verify that the TPD release is **7.4**	`$ getPlatRev` `7.4.0.0.0-88.30.0`

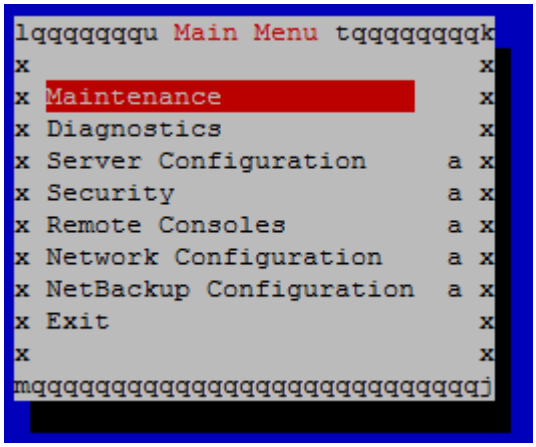
Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
5. ☐	Execute **alarmMgr** command to verify any alarms of the server before the application install.	**$ alarmMgr --alarmStatus** ***NOTE**: This command should return no output on a healthy system. If any alarms are reported as SNMP traps, please stop and contact* Accessing My Oracle Support (MOS) *for the assistance.*
6. ☐	Execute **"syscheck"** to verify the state of the server before Application install.	$ **sudo syscheck** Running modules in class hardware... OK Running modules in class disk... OK Running modules in class net... OK Running modules in class system... OK Running modules in class proc... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log ***NOTE**: The user should stop and resolve any errors returned from "syscheck" before continuing on to the next step.*
7. ☐	Execute **verifyUpgrade** command to verify health of the server before the application install.	**$ sudo verifyUpgrade** ***NOTE**: This command should return no output on a healthy system. If any error are reported, please stop and contact* Accessing My Oracle Support (MOS) *for the assistance.*
8. ☐	Verify Hardware ID is ProLiant DL380 Gen8 or Gen9.	$ **hardwareInfo | grep Hardware** Hardware ID: ProLiantDL380pGen8 – Or – Hardware ID: ProLiantDL380Gen9

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
9. ☐	Place the **USB drive** containing the **SDS Application software** into the server's USB port.	 **Figure 3 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 4 – HP DL380 Gen9: Front Panel (USB Port)**
10. ☐	Very that the USB drive has been mounted under the **/media** directory.	`$ df |grep sdb` `/dev/sdb1  2003076  8  2003068  1% /media/sdb1`
11. ☐	Verify that the **target release** is present on the USB drive.	`$ ls /media/sdb1/` `SDS-8.1.0.0.0_80.16.0-x86_64.iso`
12. ☐	Copy the target release to the server's hard disk under the **/var/TKLC/upgrade** directory.	`$ cp -p /media/sdb1/SDS-8.1.0.0.0_80.16.0-x86_64.iso /var/TKLC/upgrade/`
13. ☐	Unmount the USB drive partition.	`$ sudo umount /media/sdb1` `$`

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
14. ☐	Remove the **USB drive** from the server's front panel.	 **Figure 3 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 4 – HP DL380 Gen9: Front Panel (USB Port)**
15. ☐	Login to the **"platcfg"** utility.	`$ sudo su - platcfg`
16. ☐	From the **"platcfg"** Main Menu… Select **Maintenance** then press the **<ENTER>** key	

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result

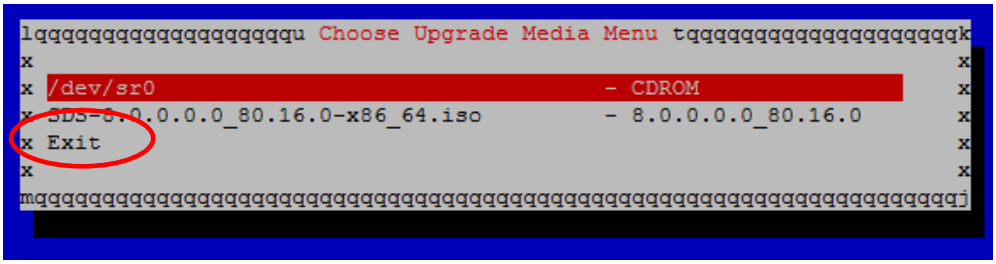
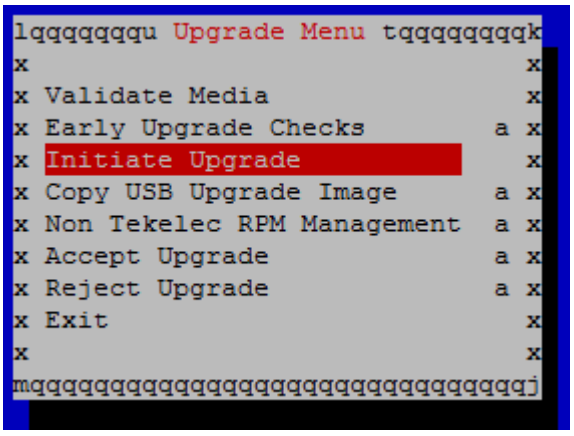
17. ☐	From the **"platcfg"** Main Menu…
	
	Select **Upgrade** then press the **<ENTER>** key
		`lqqqqu Maintenance Menu tqqqqqk`
		`x x`
		`x Upgrade x`
		`x Patching x`
		`x Halt Server a x`
		`x Backup and Restore a x`
		`x Restart Server a x`
		`x Eject CDROM a x`
		`x Save Platform Debug Logs a x`
		`x Platform Data Collector a x`
		`x Exit x`
		`x x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`

☐	Select **Validate** then press the **<ENTER>** key	`lqqqqqqqu Upgrade Menu tqqqqqqqqk`
		`x x`
		`x Validate Media x`
		`x Early Upgrade Checks x`
		`x Initiate Upgrade a x`
		`x Copy USB Upgrade Image a x`
		`x Non Tekelec RPM Management a x`
		`x Accept Upgrade a x`
		`x Reject Upgrade a x`
		`x Exit x`
		`x x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`

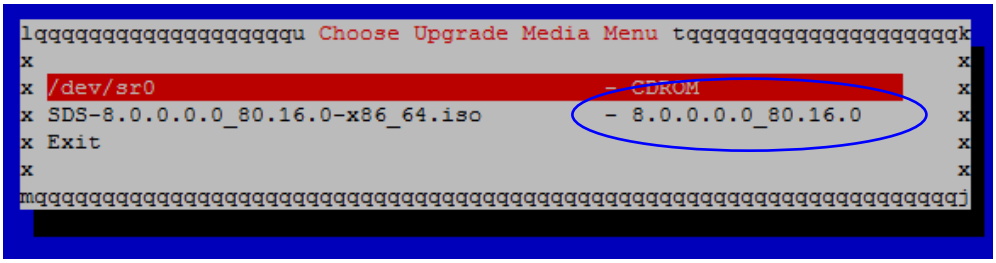
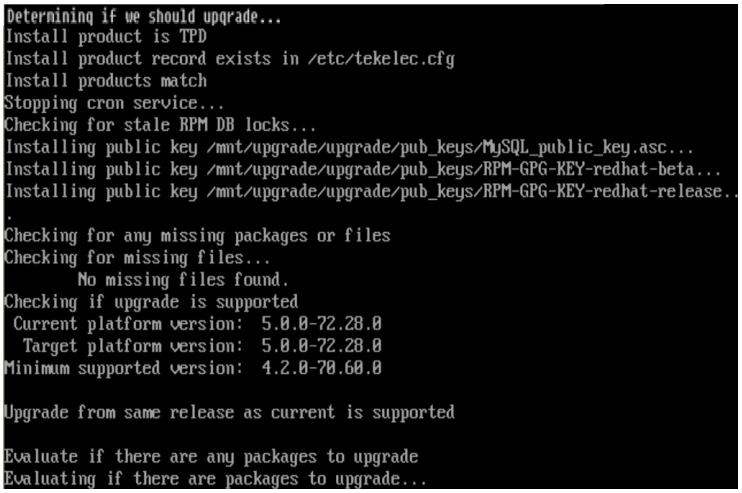
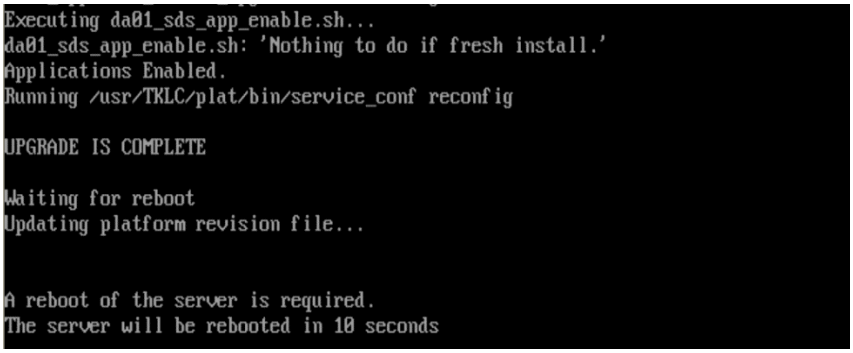
☐	Select **ISO** then press the **<ENTER>** key	`lqqqqqqqqqqqqqqqqqqqqu Choose Upgrade Media Menu tqqqqqqqqqqqqqqqqqqqqqk`
		`x x`
		`x /dev/sr0 - CDROM x`
		`x SDS-8.0.0.0.0_80.16.0-x86_64.iso - 8.0.0.0.0_80.16.0 x`
		`x Exit x`
		`x x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`

☐	Screen will show ISO is **Validated** then press the **ANY** key.	**Validating cdrom...** `############################################################` `############################################################` `############################################################` `############################################################` `############################################################` `############################################################` `############################################################`

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
	Select **Exit** then press the **<ENTER>** key	## ## ## ## ## ## ## UMVT Validate Utility v2.3.4, (c)Tekelec, May 2014 Validating /var/TKLC/upgrade/SDS-8.1.0.0.0_80.16.0-x86_64.iso Date&Time: 2016-08-09 08:20:01 Volume ID: 8.1.0.0.0_80.16.0 Part Number: N/A Version: 8.1.0.0.0_80.16.0 Disc Label: DSR Disc description: DSR The media validation is complete, the result is: PASS CDROM is Valid PRESS ANY KEY TO RETURN TO THE PLATCFG MENU. 
18.	From the **"platcfg"** Main Menu… Select **Initiate Upgrade** then press the **<ENTER>** key	

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
19. ☐	Verify that SDS application release shown matches the target release. Press the **<ENTER>** key to start the SDS application install	
20. ☐	Output similar to that shown on the right may be observed as the SDS application install progresses.	
21. ☐	Output similar to that shown on the right may be observed at the completion of the Application install.	

22. ☐	After the server has completed reboot, log into the HP server as the "**admusr**" user.	`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

23. ☐	Verify that the output contains the line shown to the right indicating a successful installation of SDS application software.	`$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log` `1321462900::  UPGRADE IS COMPLETE`

Procedure 2. Installing the SDS Application (All SDS NOAM Sites)

Step	Procedure	Result
24. ☐	Execute **verifyUpgrade** command to verify status of upgrade. Verify that SDS application release shown matches the target release	**$ sudo verifyUpgrade** ***NOTE**: This command should return no output on a healthy system. If any error are reported, please stop and contact* Accessing My Oracle Support (MOS) *for the assistance* $ **rpm -qa |grep sds** TKLCSDS-8.1.0.0.0_80.16.0.x86_64
25. ☐	Accept upgrade to the Application Software.	$ **sudo /var/TKLC/backout/accept** Called with options: --accept Loading Upgrade::Backout::RPM Accepting Upgrade Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info. Cleaning backout directory. Clearing Upgrade Accept/Reject alarm. Cleaning message from MOTD. Cleaning up RPM config backup files... Checking / Checking /boot Checking /tmp Checking /usr Checking /var Checking /var/TKLC/rundb Starting cleanup of RCS repository. INFO: Removing '/var/lib/prelink/force' from RCS repository INFO: Removing '/etc/my.cnf' from RCS repository
26. ☐	Put the server in trusted time mode	$ **tw.setdate –trusted** Current time: 10/22/2014 16:25:07.869
27. ☐	Exit from the command line to return the server console to the login prompt.	$ **exit**
28. ☐	**Repeat this procedure for each RMS server installed in the cabinet before continuing on to the next procedure (e.g., SDS NOAM A, SDS NOAM B, Query Server).**	
THIS PROCEDURE HAS BEEN COMPLETED		

5. Configuration Procedures

5.1 Configuring SDS Servers A and B (1st SDS NOAM Site Only)

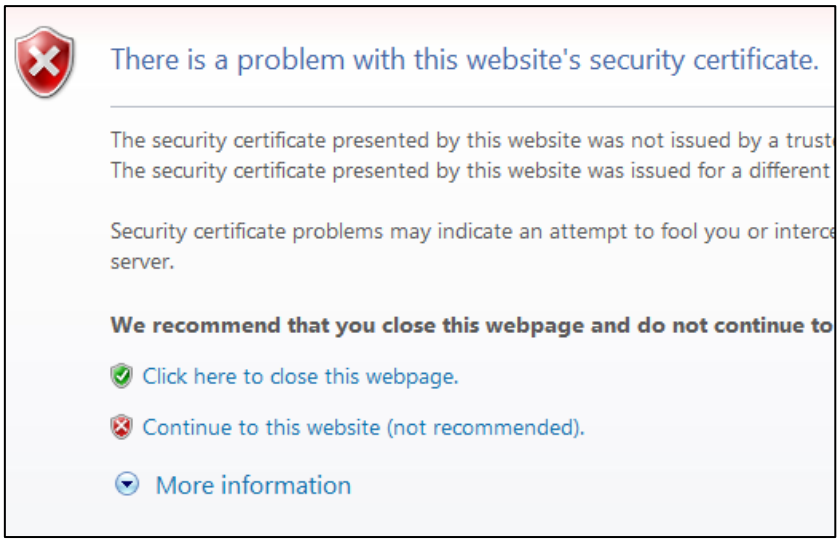
Assumptions:

- This procedure assumes that the SDS Network Element XML file for the Primary Provisioning SDS site has previously been created, as described in Appendix E.
- This procedure assumes that the Network Element XML files are either on a USB flash drive or the laptop's hard drive. The steps are written as if the XML files are on a USB flash drive, but the files can exist on any accessible drive.

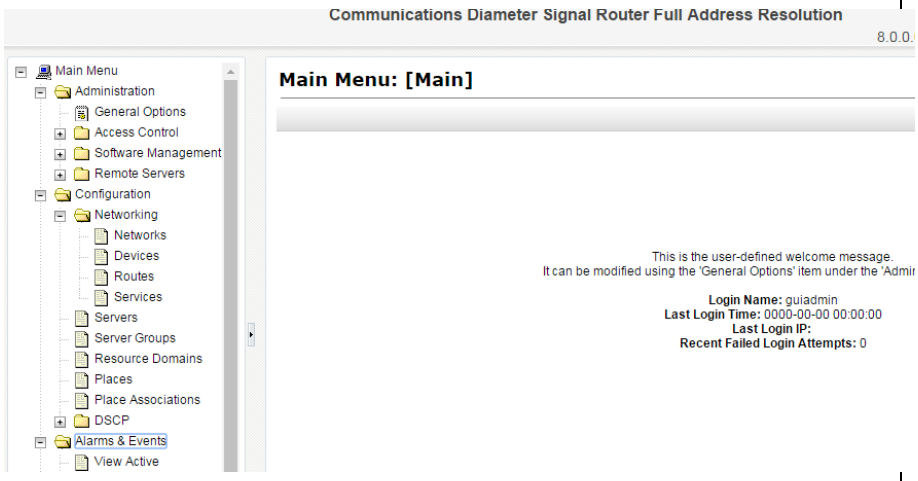
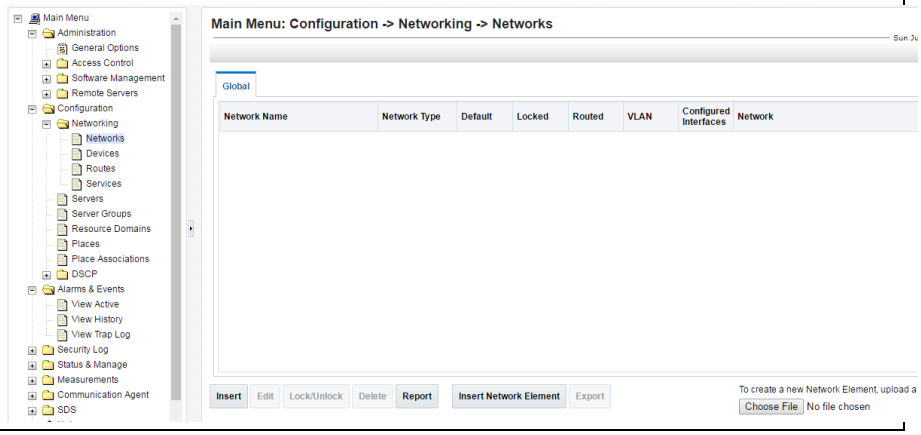
This procedure requires that the user connects to the SDS GUI prior to configuring the first SDS server. This can be done either by one of two procedures:

1. Configuring a temporary external IP address, as described in Appendix B
2. Plugging a laptop into an unused, unconfigured port on the SDS NOAM-A server using a direct-connect Ethernet cable, as described in Appendix C.

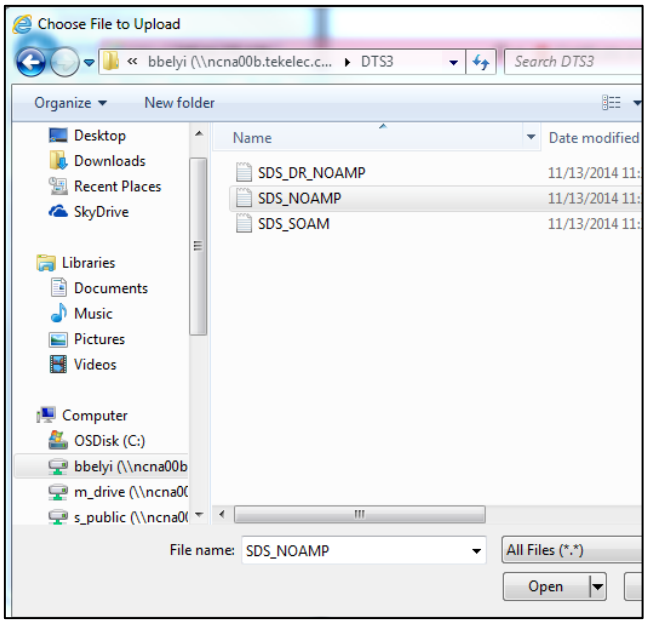
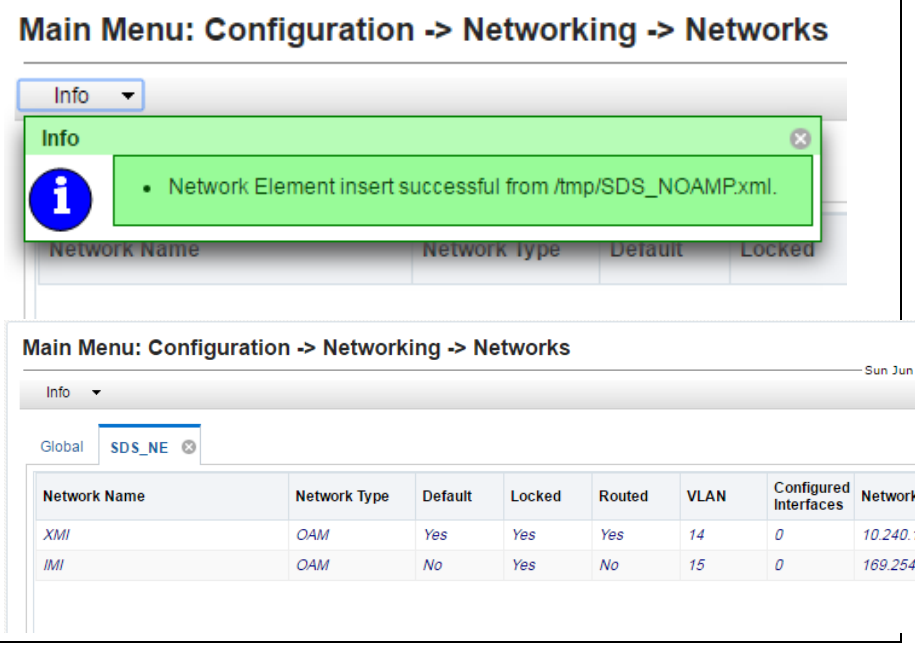
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
1. ☐	**SDS NOAM A:** Connect to the SDS GUI.	Execute Appendix C. *Establishing a Local Connection for Accessing the SDS GUI*
2. ☐	**SDS NOAM A:** Launch an approved web browser and connect to the SDS NOAM A IP address using https://192.168.100.11 **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* *"Continue to this website (not recommended)".*	

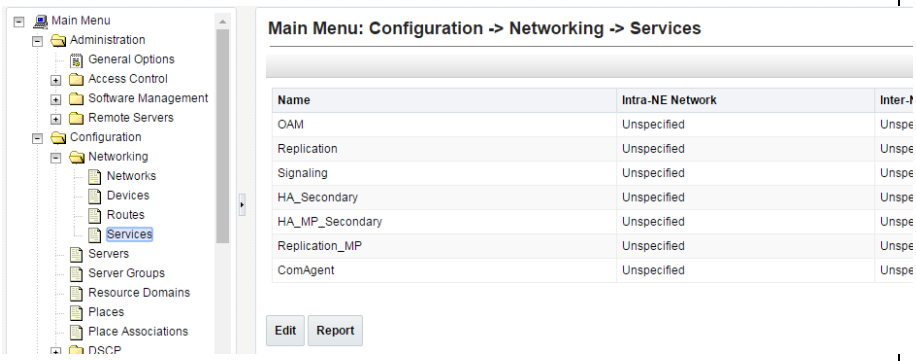
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
3. ☐	**SDS NOAM A:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
4. ☐	**SDS NOAM A:** The user should be presented the SDS Main Menu as shown on the right.	
5. ☐	**SDS NOAM A:** 1) Select… **Main Menu** → **Configuration** → **Networking** → **Networks** …as shown on the right. 2) Select the **"Browse"** dialogue button (scroll to bottom left corner of screen).	

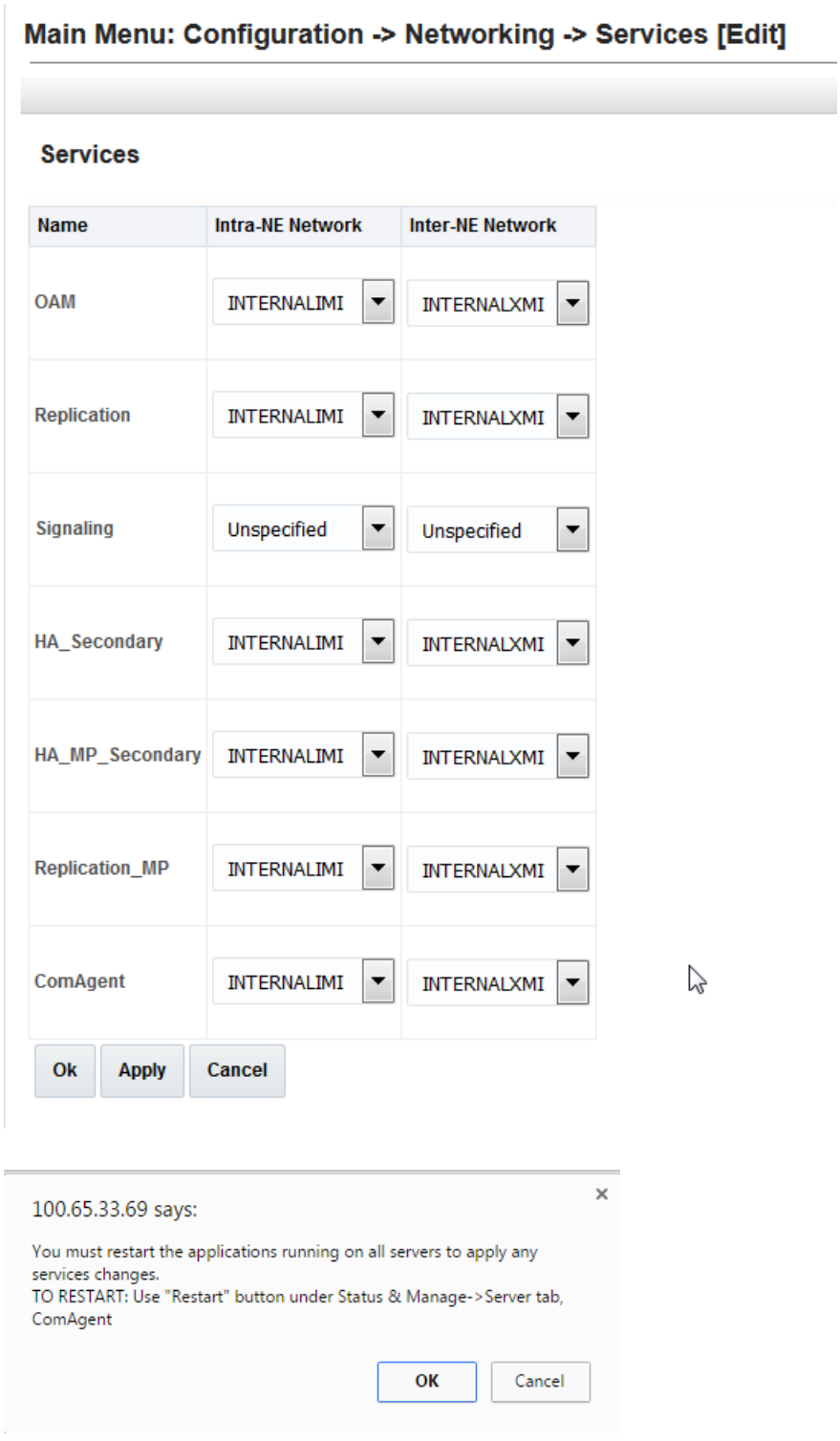
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
6. ☐	**SDS NOAM A:** **Note**: This step assumes that the **xml** files were previously prepared, as described in **Appendix E**. **1)** Select the location containing the site **.xml** file. **2)** Select the **.xml** file and click the **"Open"** dialogue button.	
7. ☐	**SDS NOAM A:** Select the **"Upload File"** dialogue button (bottom left corner of screen).	
8. ☐	**SDS NOAM A:** If the values in the **.xml** file pass validation rules, the user must select the Info box to 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.*	

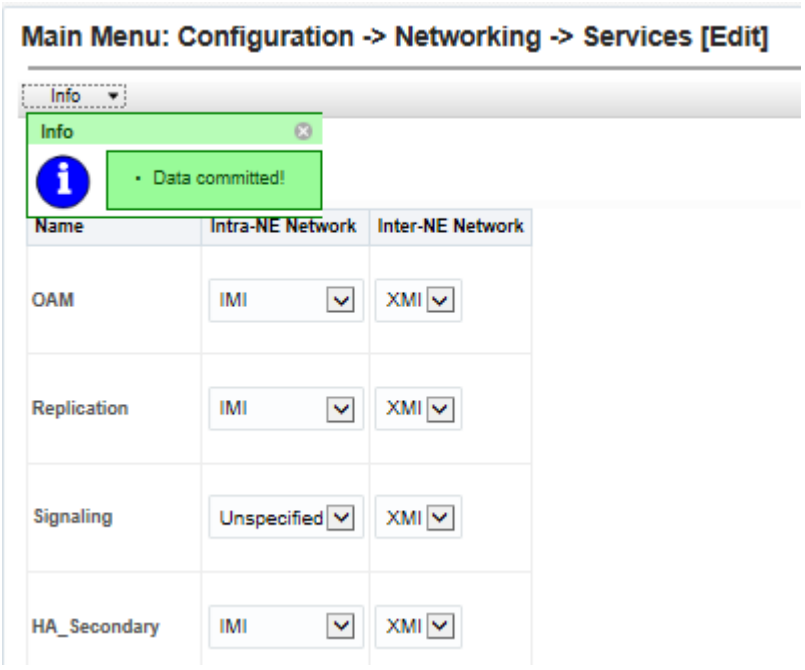
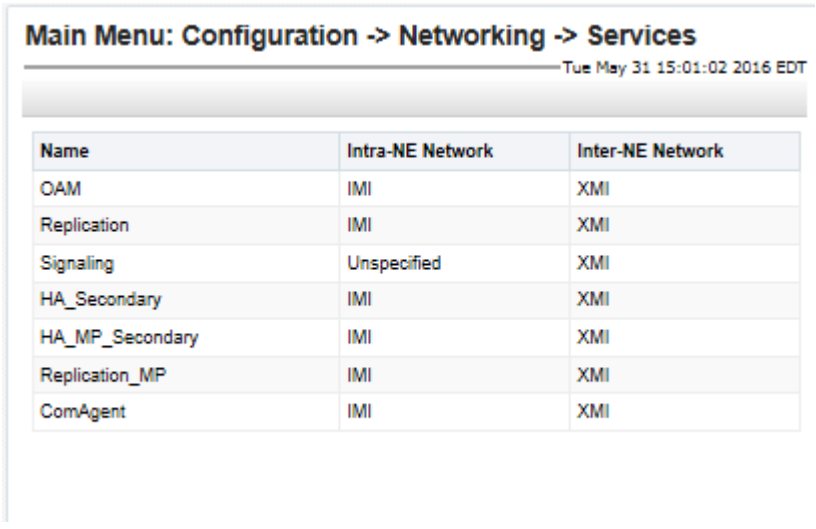
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
9. ☐	**SDS NOAM A:** 1) Select… **Main Menu** → **Configuration** **->Networking** → ***Services*** …as shown on the right. 2) The user will be presented with the "**Services**" configuration screen as shown on the right. 3) Click **Edit**.	

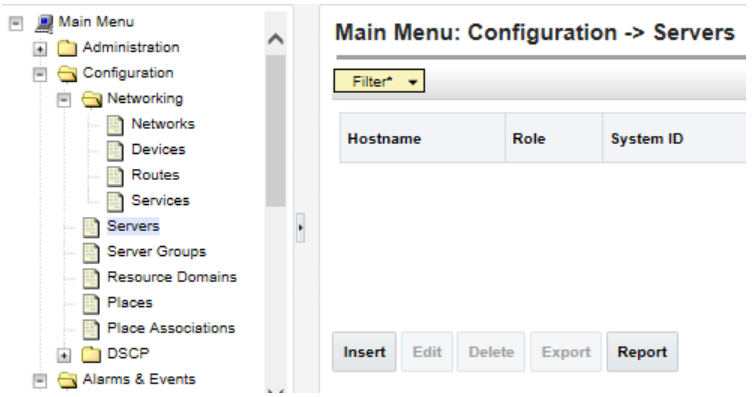
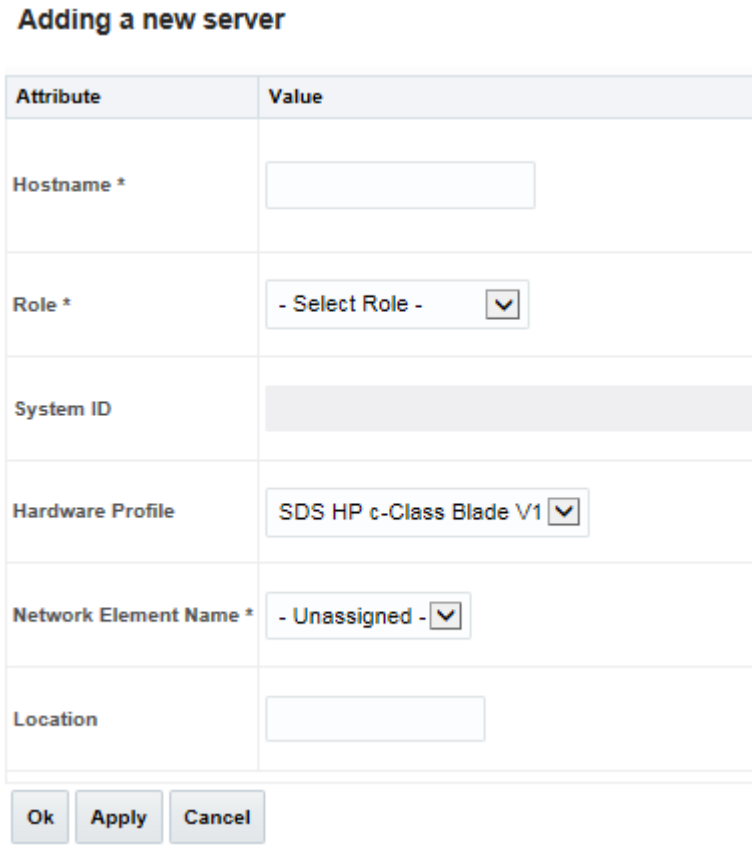
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
10. ☐	**SDS NOAM 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 **"Apply"** dialogue button. 3) Click **OK** in new pop up GUI to change the effect.	

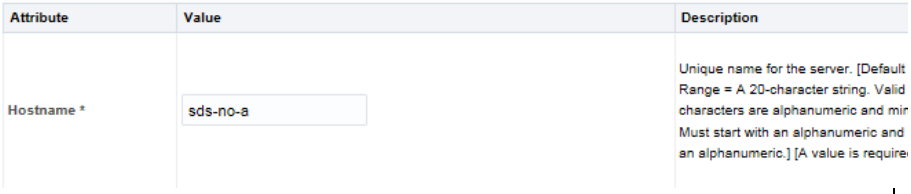
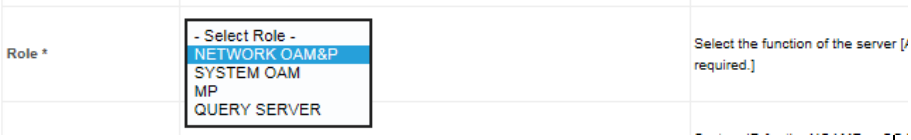
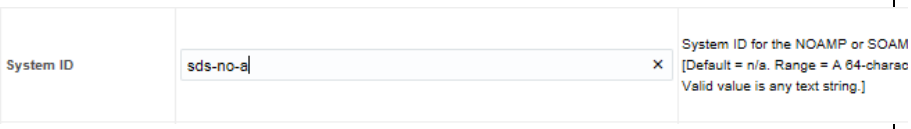
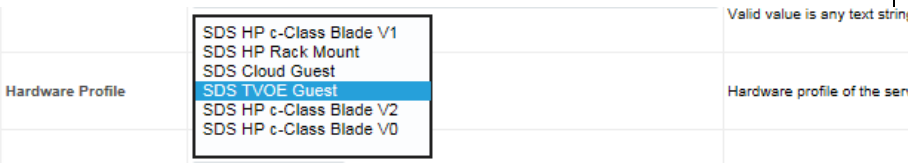
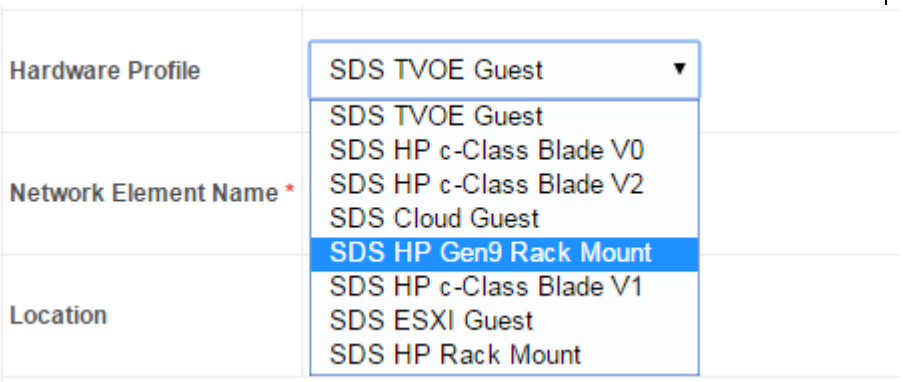
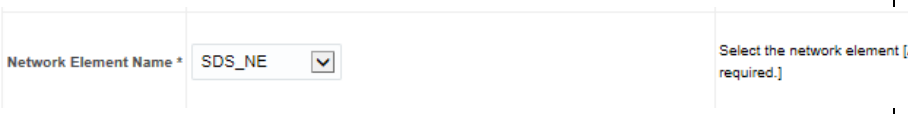
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
11. ☐	**SDS NOAM A:** **1)** The user should now click the **"Info"** tab to be presented with a banner information message stating **"Data committed"** **2)** Click **OK**.	
12. ☐	**SDS NOAM A:** The user will be presented with the "**Services**" configuration screen as shown on the right	

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
13. ☐	**SDS NOAM A:** 1) Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right. 2) Select the **"Insert"** dialogue button.	 **Note:** This step thru the last step of this procedure need to be done for both servers SDS NOAM A and SDS NOAM B.
14. ☐	**SDS NOAM A:** The user is now presented with the **"Adding a new server"** configuration screen.	

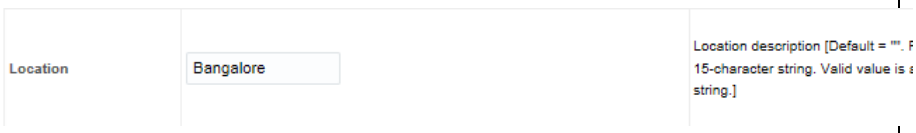
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
15. ☐	**SDS NOAM A:** Input the assigned "**hostname"** for the SDS NOAM (A or B).	
16. ☐	**SDS NOAM A:** Select **"NETWORK OAM&P"** for the server **"Role"** from the pull-down menu.	
17. ☐	**SDS NOAM A:** Input the assigned hostname again as the "**System ID**" for the SDS NOAM (A or B).	
18. ☐	**SDS NOAM A:** For Gen8: Select "**SDS HP Rack Mount**" for the **Hardware Profile** for the SDS from the pull-down menu. For Gen9: Select "**SDS HP Gen9 Rack Mount**" for the **Hardware Profile** for the SDS from the pull-down menu.	For Gen8 select "**SDS HP Rack Mount"** from the **Hardware Profile** pull-down menu.  For Gen9 Select "**SDS HP Gen9 Rack Mount**" from the **Hardware Profile** pull-down menu. 
19. ☐	**SDS NOAM A:** Select the **Network Element Name** for the SDS from the pull-down menu.	

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>20. ☐</td><td>SDS NOAM A:

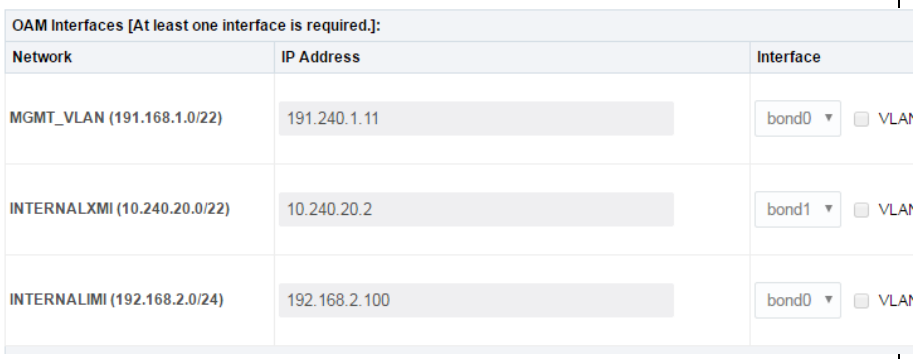
Enter the site location.

NOTE: Location is an optional field.</td><td> 
</td></tr>
<tr><td>21. ☐</td><td>SDS NOAM A:

1) Enter the MGMNT_VLAN IP address for the SDS Server.

2) Set the MGMNT_VLAN Interface to “bond0” and “check” the VLAN checkbox.

3) Enter the IMI IP address for the SDS Server.

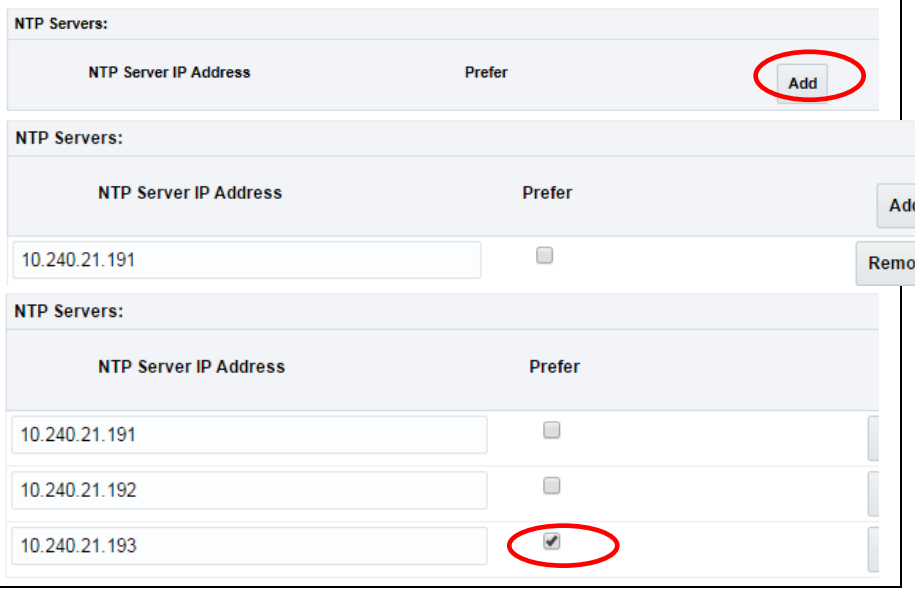
4) Set the IMI Interface to “bond0” and “check” the VLAN checkbox.</td><td> 

<table>
<tr><th>SDS Server
(Primary NOAM)</th><th>Network</th><th>IP Address</th><th>Interface</th><th>VLA
Check</th></tr>
<tr><td rowspan="2">SDS-A</td><td>MGMNT_VLAN</td><td>169.254.1.11</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.11</td></tr>
<tr><td rowspan="2">SDS-B</td><td>MGMNT_VLAN</td><td>169.254.1.12</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.12</td></tr>
</table>
NOTE_1: These IP addresses are based on the info in the NAPD and the Network Element Config file

NOTE_2: The MGMT_VLAN should only be present when 4948E-F AggregationSwitches are deployed with SDS NOAM / Query Server RMS. If the MGMT_VLAN is not present, the IMI network values shown above still apply.</td></tr>
</table>

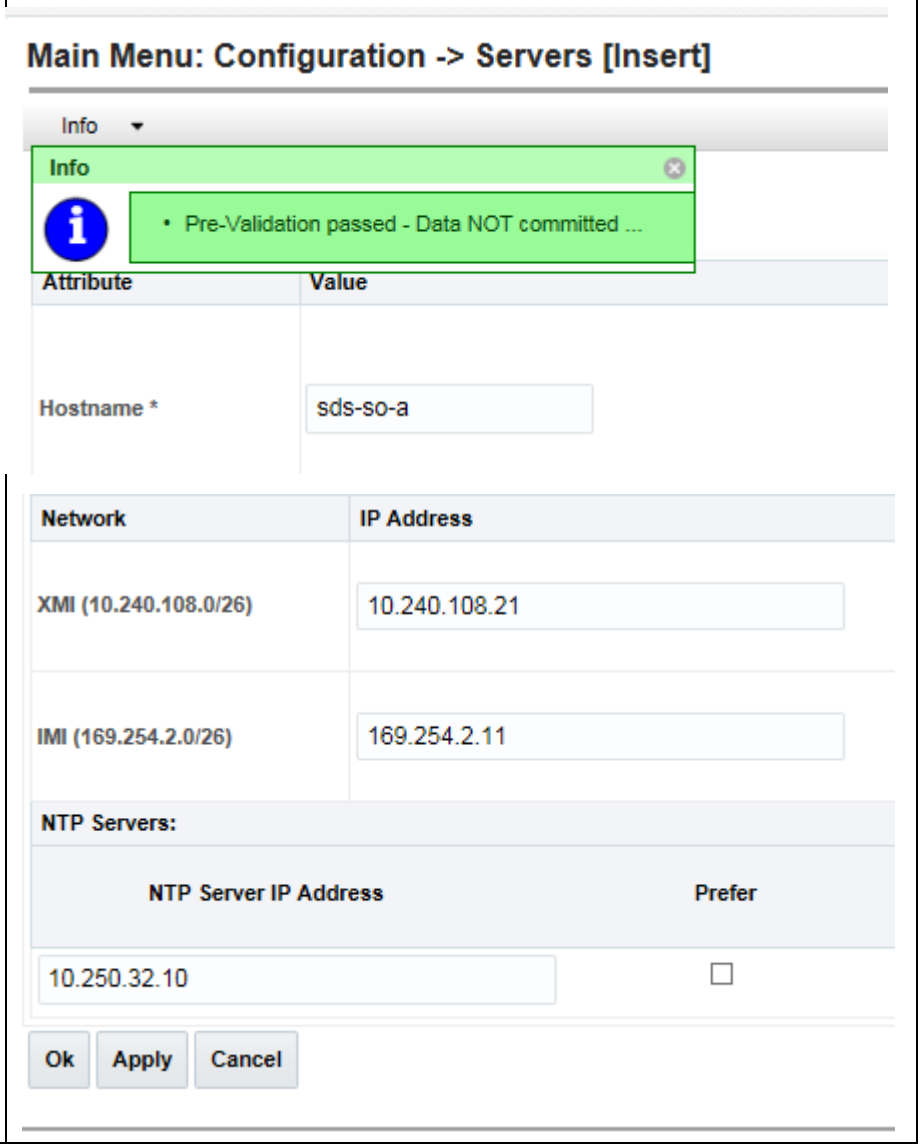
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>22.
☐</td><td>1) Enter the customer assigned XMI IP address for the SDS Server.
Layer 3
(No VLAN tagging used for XMI)
2) Set the XMI Interface to “bond1” and “DO NOT check” the VLAN checkbox.
- OR -
Layer 2
(VLAN tagging used for XMI)
2) Set the XMI Interface to “bond0” and “check” the VLAN checkbox.</td><td>

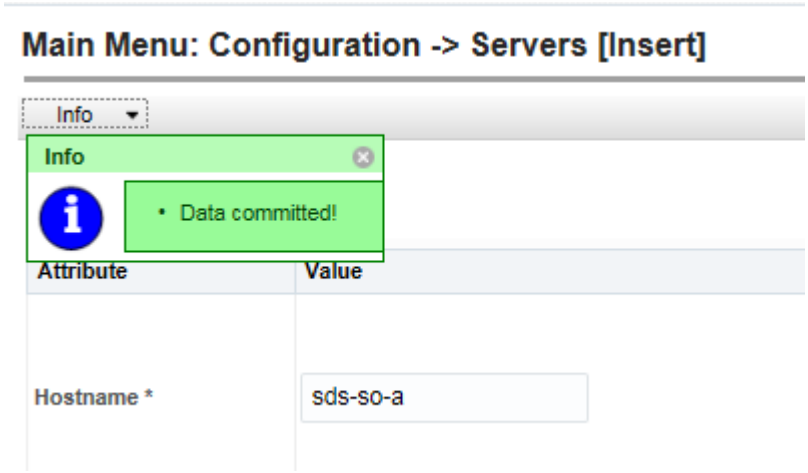
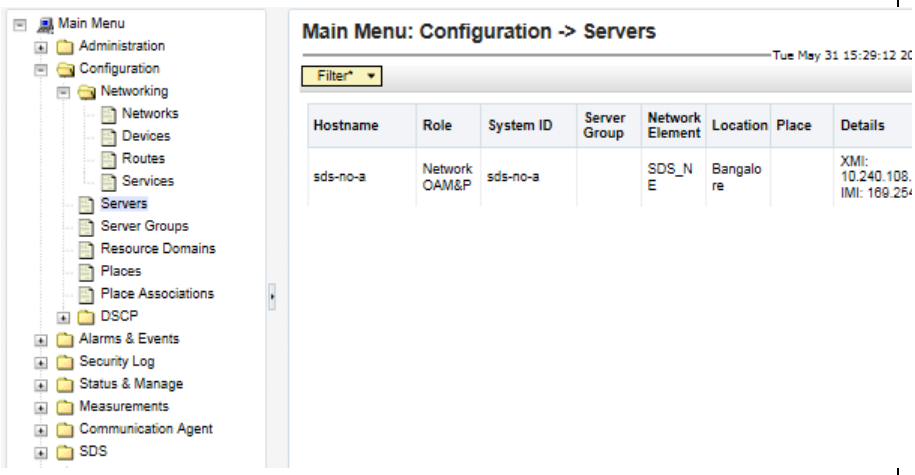
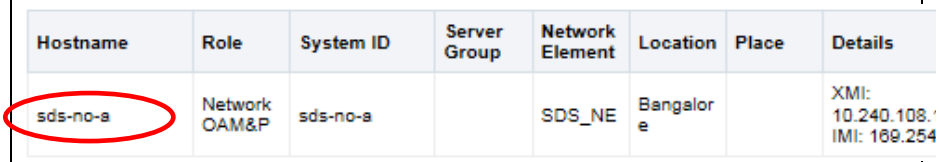

<table>
<tr><th>SDS Server
(Primary NOAM)</th><th>Network</th><th>VLAN tagging
(on XMI network)</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">SDS NOAM Server
(A or B)</td><td rowspan="2">XMI</td><td>No</td><td>bond1</td><td>✖</td></tr>
<tr><td>Yes</td><td>bond0</td><td>✓</td></tr>
</table>
!!! CAUTION !!!
It is crucial that the correct network configuration be selected in Steps 21 & 22 of this procedure. Choosing an incorrect configuration will result in the need to re-install the OS and restart SDS instalation procedures over from the beginning.
</td></tr>
<tr><td>23.
☐</td><td>SDS NOAM A:
1) Click the “NTP Servers:” “Add” dialogue button.
2) Enter the NTP Server IP Address for an NTP Server.
3) Enter 3 NTP Server IP address, repeat (1) and (2) to enter it.
4) Optionally, click the “Prefer” checkbox to prefer one NTP Server over the other.</td><td>


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

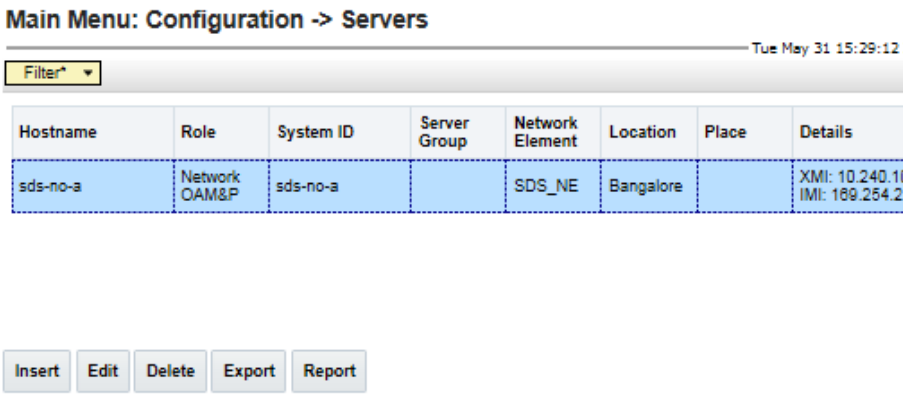
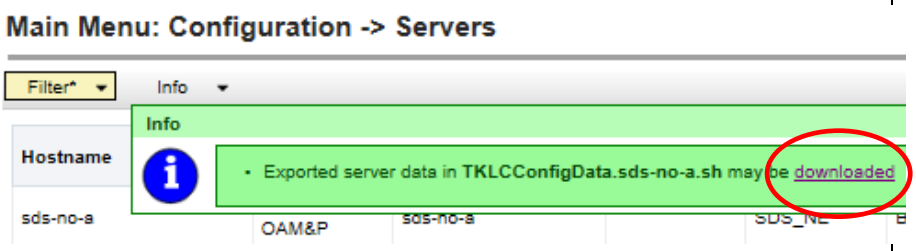
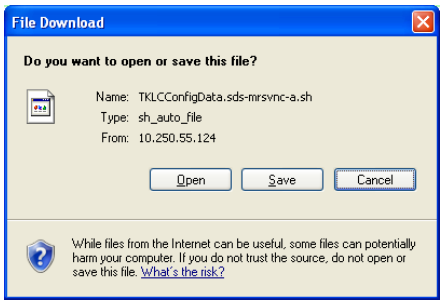
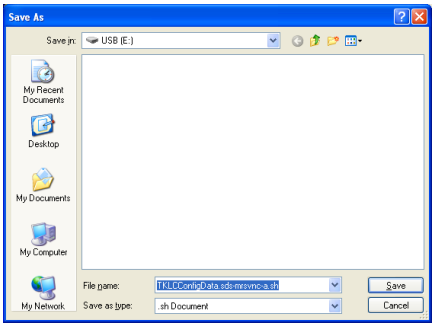
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
24. ☐	**SDS NOAM A:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"Apply"** dialogue button.	

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
25. ☐	**SDS NOAM A:** If the values provided match the network ranges assigned to the SDS NE, the user must select the Info box to receive a banner information message showing that the data has been validated and committed to the DB.	
26. ☐	**SDS NOAM A:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right.	
27. ☐	**SDS NOAM A:** The **"Configuration →Servers" screen** should now show the newly added **SDS Server** in the list.	

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
28. ☐	**SDS NOAM A:** **1)** Use the cursor to select the **SDS Server** entry added in **Steps 13 – 25**. The row containing the desired **SDS Server** should now be highlighted. **2)** Select the **"Export"** dialogue button.	
29. ☐	**SDS NOAM A:** The user must select the Info box to receive a banner information message showing a download link for the **SDS Server** configuration data. Click on the word **"downloaded"** to download and save the configuration file.	 ***Note***: You may be required to click the **Info** tab to display the Info banner shown here.
30. ☐	**SDS NOAM A:** **1)** Click the "**Save**" dialogue button. **2)** Save the **SDS Server** configuration file to a USB flash drive.	 
31. ☐	**SDS Server NOAM A or B:** Access the server console.	Connect to the **SDS NOAM-A and SDS NOAM-B** console using one of the access methods described in Section 2.3.

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result

32. ☐	**SDS Server NOAM A or B:**
	
	1) Access the command prompt.
	
	2) Log into the server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

33. ☐	**SDS Server NOAM A or B:** Insert the USB flash drive containing the server configuration file into the USB port on the front panel of **SDS Server**.	 **Figure 3 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 4 – HP DL380 Gen9: Front Panel (USB Port)**

34. ☐	**SDS Server NOAM A or B:**
	
	Output similar to that shown on the right will appear as the USB flash drive is inserted into the **SDS Server** front USB port.
		`$ sd 3:0:0:0: [sdb] Assuming drive cache: write through`
		`sd 3:0:0:0: [sdb] Assuming drive cache: write through`
		<ENTER>
		
		***NOTE**: Press the **<ENTER>** key to return to the command prompt.*

35. ☐	**SDS Server NOAM A or B:**
	
	Verify that the USB flash drive's partition has been mounted by the OS: Search **df** for the device named in the previous step's output.
		`$ df |grep sdb`
		`/dev/sdb1  2003076  8  2003068  1%`
		`/media/sdb1`

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
36. ☐	**SDS Server NOAM A or B:** Copy the configuration file to the SDS server **NOTE:** *This step can be skipped for SDS Server A because the file should already exist.*	`$ sudo cp -p /media/sdb1/TKLCConfigData.sds-mrsvnc-a.sh /var/TKLC/db/filemgmt/.` **NOTE**: *If **Appendix C** was used to create this interface, un-configure the interface before copying this file.*
37. ☐	Unmount the USB drive partition.	`$ sudo umount /media/sdb1` `$`
38. ☐	**SDS Server NOAM A or B:** Copy the **server** configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname from the file name.	***Example:*** TKLCConfigData<.server_hostname>.sh ➔ will translate to ➔TKLCConfigData.sh `$ sudo cp -p /var/TKLC/db/filemgmt/TKLCConfigData.sds-mrsvnc-a.sh /var/tmp/TKLCConfigData.sh` **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

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

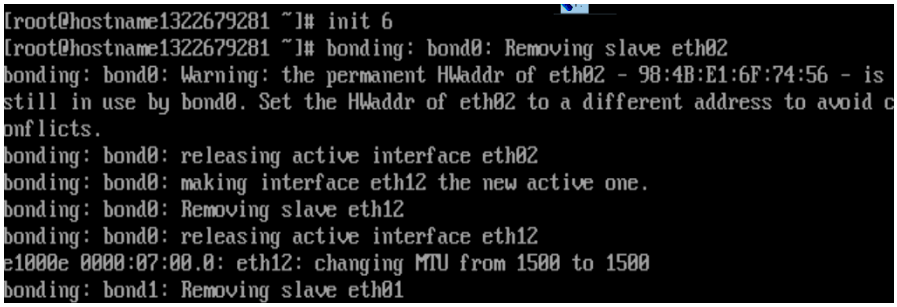
Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
40. ☐	**SDS Server NOAM A or B:** Remove the USB flash drive from the USB port on the front panel of the server. **CAUTION:** *It is important that the USB flash drive be **REMOVED** from the server before continuing on to the next step.*	 **Figure 3 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 4 – HP DL380 Gen9: Front Panel (USB Port)**

41. ☐	**SDS Server NOAM A or B:**
	
	Ignore the output shown and press the **<ENTER>** key to return to the command prompt.
		`Broadcast message from admusr (Thu Dec 1 09:41:24 2011):`
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		`Please remove the USB flash drive if connected and reboot the server.`
		<ENTER>

42.	**SDS Server NOAM A or B:** Verify that the desired Time Zone is currently in use.	`$ date` `Mon Aug 10 19:34:51 UTC 2015`
43. ☐	**SDS Server NOAM A or B:** If the desired Time Zone was not presented in the previous step… **Configure the Time Zone.** Otherwise, skip to the next step.	***Example:*** `$ sudo set_ini_tz.pl <time_zone>` ***Note***: The following command example sets the time to the "UTC" (aka GMT) time zone which is recommneded for all sites. The user may replace, as appropriate, with the customer requested time zone for this site installation. See Appendix G for a list of valid time zones. `$ sudo set_ini_tz.pl "Etc/UTC"`
44. ☐	**SDS Server NOAM A or B:** Initiate a reboot of the **SDS Server**.	`$ sudo init 6`

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
45. ☐	**SDS Server NOAM A or B:** Wait ~9 minutes Output similar to that shown on the right may be observed as the server initiates a reboot.	
46. ☐	**SDS Server NOAM A or B:** After the server has completed reboot, log into the server as the "**admusr**" user.	login: **admusr** Using keyboard-interactive authentication. Password: ***<admusr_password>***
47.	Run Accepting script.	[admusr@nassau-sds-so-b ~]$ sudo /var/TKLC/backout/accept Called with options: --accept Loading Backout::BackoutType::RPM Accepting Upgrade Executing common accept tasks Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info. Cleaning backout directory. Clearing Upgrade Accept/Reject alarm. Cleaning message from MOTD. No patch pending alarm on server so no MOTD update. Cleaning up RPM config backup files... Checking / Checking /boot Checking /tmp Checking /usr Checking /var Checking /var/TKLC Checking /tmp/appworks_temp Checking /usr/openv Checking /var/TKLC/appw/logs/Process Checking /var/TKLC/appw/logs/Security Checking /var/TKLC/db/filemgmt Checking /var/TKLC/rundb Starting cleanup of RCS repository. INFO: Removing '/etc/my.cnf' from RCS repository INFO: Removing '/etc/pam.d/password-auth' from RCS repository INFO: Removing '/etc/pam.d/system-auth' from RCS repository INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0' from RCS repository INFO: Removing '/etc/php.d/zip.ini' from RCS repository INFO: Removing '/var/lib/prelink/force' from RCS repository [admusr@nassau-sds-so-b ~]$

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result

48. ☐	**SDS Server NOAM A or B:**
	
	1) Verify that the **IMI IP address** and the **bond** VLAN configuration input in **Step 21** has been correctly applied.
	
	2) Verify that the **XMI IP address** and the **bond** configuration input in **Step 22** has been correctly applied.
	
	NOTE: *The server's **XMI** & **IMI** addresses can also be verified by reviewing the server configuration through the SDS GUI under **[Main Menu → Configuration → Server]** screen.*
		`$ ifconfig |grep in`
		`bond0 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:68`
		`bond0.4 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:68`
		`inet addr:169.254.100.11 Bcast:169.254.100.255 Mask:255.255.255.0`
		`bond1 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:6A`
		`inet addr:10.250.55.124 Bcast:10.250.55.255 Mask:255.255.255.0`
		`eth01 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:68`
		`eth02 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:6A`
		`eth11 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:68`
		`eth12 Link encap:Ethernet HWaddr 98:4B:E1:6F:74:6A`
		`lo Link encap:Local Loopback`
		`inet addr:127.0.0.1 Mask:255.0.0.0`

49. ☐	**SDS Server NOAM A or B:**
	
	Use the **"ntpq"** command to verify that the server has connectivity to the assigned Primary and Secondary NTP server(s).
		`$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`*10.250.32.10 192.5.41.209 2 u 1 64 1 0.176 -0.446 0.053`
		`10.250.32.51 192.5.41.209 2 u 2 64 1 0.174 -0.445 0.002`

IF CONNECTIVITY TO THE NTP SERVER(S) CANNOT BE ESTABLISHED, STOP AND EXECUTE THE FOLLOWING STEPS:

1) **Have the Customer IT group provide a network path from the SDS NOAM Server XMI IP to the assigned NTP Server IP addresses.**
2) **Once network connectivity is established to the configured NTP Servers, then restart this procedure beginning with STEP 49.**

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result

50. ☐	**SDS Server NOAM A or B:**
	Execute a **"syscheck"** to verify the current health of the server.
		`$ 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`

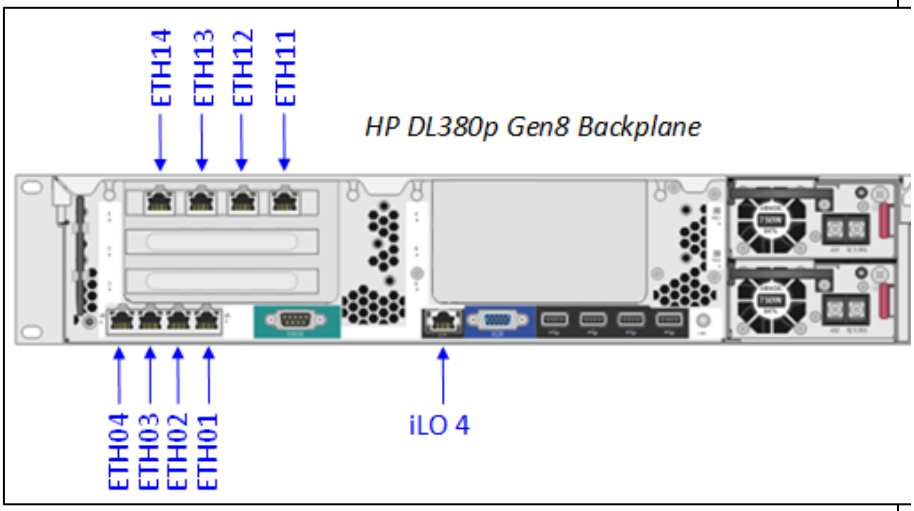
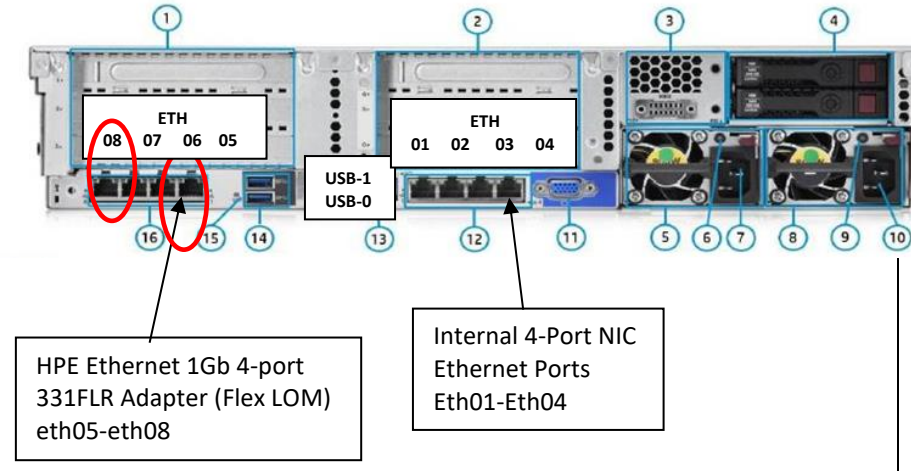
51. ☐	**SDS Server NOAM A or B:** Exit to return to the login prompt.	`$ exit`
52. ☐	• **Configure SDS Server B by repeating steps 13 – 50 of this procedure.**	
	**IF AGGREGATION SWITCHES ARE INSTALLED AND 4948E-F SWITCH CONFIGURATION HAS NOT BEEN COMPLETED PRIOR TO THIS STEP, STOP AND EXECUTE THE FOLLOWING PROCEDURES:** **1) APPENDIX D-1** **2) APPENDIX D-2** *(Appendix **E.2** references Appendix **E.3** where applicable).* **3) APPENDIX D-4**	

53. ☐	**SDS Server NOAM A:**
	From **SDS Server NOAM A, "ping"** the **IMI IP address** configured for on **SDS Server B**.
		`$ ping -c 5 169.254.100.12`
		`PING 169.254.100.12 (169.254.100.12) 56(84) bytes of data.`
		`64 bytes from 169.254.100.12: icmp_seq=1 ttl=64 time=0.020 ms`
		`64 bytes from 169.254.100.12: icmp_seq=2 ttl=64 time=0.026 ms`
		`64 bytes from 169.254.100.12: icmp_seq=3 ttl=64 time=0.025 ms`
		`64 bytes from 169.254.100.12: icmp_seq=4 ttl=64 time=0.025 ms`
		`64 bytes from 169.254.100.12: icmp_seq=5 ttl=64 time=0.026 ms`
		
		`--- 169.254.100.12 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 4000ms`
		`rtt min/avg/max/mdev = 0.020/0.024/0.026/0.005 ms`

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

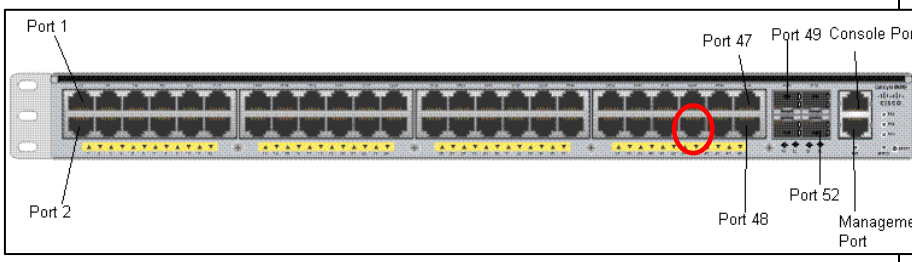
Step	Procedure	Result
54. ☐	**SDS Server NOAM A:** From **SDS Server NOAM A, "ping"** the **XMI IP address** configured for on **SDS Server B**.	$ **ping -c 5 10.250.55.125** PING 10.250.55.125 (10.250.55.125) 56(84) bytes of data. 64 bytes from 10.250.55.125: icmp_seq=1 ttl=64 time=0.166 ms 64 bytes from 10.250.55.125: icmp_seq=2 ttl=64 time=0.139 ms 64 bytes from 10.250.55.125: icmp_seq=3 ttl=64 time=0.176 ms 64 bytes from 10.250.55.125: icmp_seq=4 ttl=64 time=0.209 ms 64 bytes from 10.250.55.125: icmp_seq=5 ttl=64 time=0.179 ms --- 10.250.55.125 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4000ms rtt min/avg/max/mdev = 0.139/0.173/0.209/0.028 ms
55.	**SDS Server NOAM A:** Use **"ping"** to verify that **SDS Server NOAM A** can reach the configured **XMI Gateway address**	$ **ping -c 5 10.250.55.1** PING 10.250.55.1 (10.250.55.1) 56(84) bytes of data. 64 bytes from 10.250.55.1: icmp_seq=1 ttl=64 time=0.166 ms 64 bytes from 10.250.55.1: icmp_seq=2 ttl=64 time=0.139 ms 64 bytes from 10.250.55.1: icmp_seq=3 ttl=64 time=0.176 ms 64 bytes from 10.250.55.1: icmp_seq=4 ttl=64 time=0.209 ms 64 bytes from 10.250.55.1: icmp_seq=5 ttl=64 time=0.179 ms --- 10.250.55.1 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4000ms rtt min/avg/max/mdev = 0.139/0.173/0.209/0.028 ms
56.	**SDS Server B:** Use **"ping"** to verify that **SDS Server B** can reach the configured **XMI Gateway address**	$ **ping -c 5 10.250.55.1** PING 10.250.55.1 (10.250.55.1) 56(84) bytes of data. 64 bytes from 10.250.55.1: icmp_seq=1 ttl=64 time=0.166 ms 64 bytes from 10.250.55.1: icmp_seq=2 ttl=64 time=0.139 ms 64 bytes from 10.250.55.1: icmp_seq=3 ttl=64 time=0.176 ms 64 bytes from 10.250.55.1: icmp_seq=4 ttl=64 time=0.209 ms 64 bytes from 10.250.55.1: icmp_seq=5 ttl=64 time=0.179 ms --- 10.250.55.1 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4000ms rtt min/avg/max/mdev = 0.139/0.173/0.209/0.028 ms

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result
57. ☐	**SDS Server NOAM A:** Disconnect the laptop from the **Server NOAM A, eth14** Ethernet port. For Gen9: Disconnect the laptop from the **Server NOAM A, eth08** Ethernet port.	 **Figure 5 – HP DL380 Gen8: Rear Panel (Ethernet)**  **Figure 6 – HP DL380 Gen9: DC (Rear Panel)**

Procedure 3. Configuring SDS Servers A and B (1st SDS NOAM Site Only)

Step	Procedure	Result

58. ☐	**switch1A:**
	
	Connect the laptop to **Port 44** of **switch1A** (bottom switch).
		
		Figure 7 – Cisco 4948E-F Switch (Maintenance Access Port)
		
		To Configure Port 44
		`$ sudo netConfig --device=<device name> setSwitchport interface=<interface name> type=trunk`
		
		`$sudo netConfig --device=<device name> setSwitchport interface=<interface name> type=access`
		
		`<device name>:` The device name should be the name of switch.
		`<interface name>: GE44`

59. ☐	**Laptop:** Set a static IP address and netmask within the Management VLAN for the laptop's network interface card (***169.254.1.100*** *is suggested*).	Reference Appendix C. Steps 6-7 *if assistance is needed in modifying the laptop's network configuration.*

60. ☐	**SDS Server NOAM A:**
	
	Using **SSH**, login to **Server NOAM A** using its Management VLAN IP address ***169.254.1.11***
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

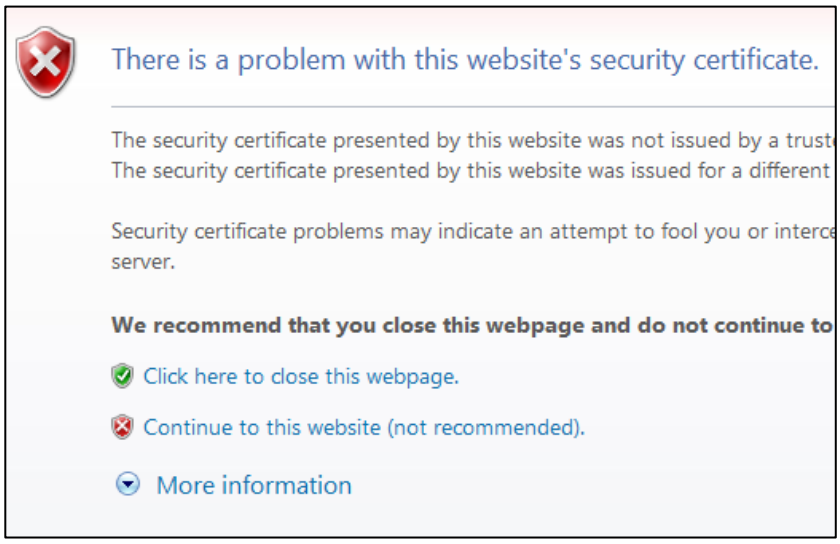
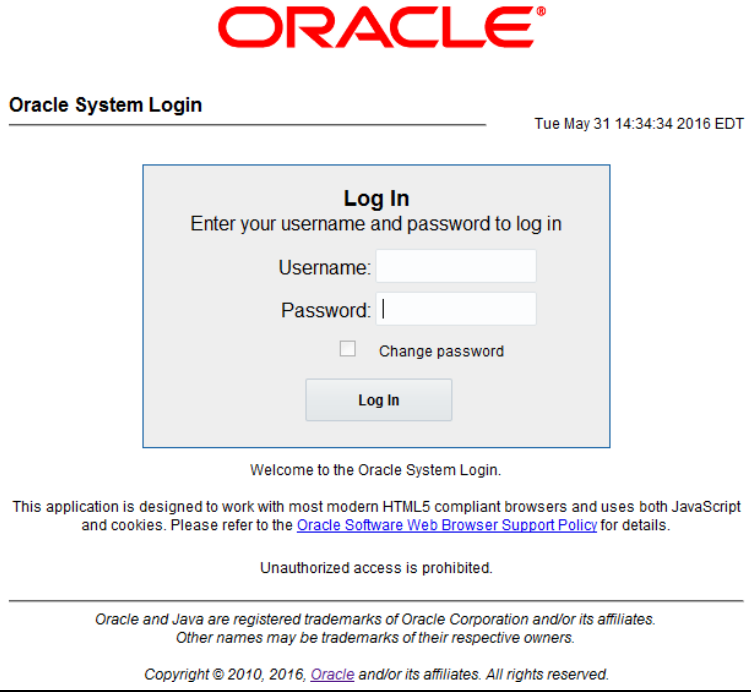
61. ☐	**SDS Server NOAM A:**
	
	For Gen8: Delete eth14
	
	For Gen9:
	Delete eth08
		`For Gen8`
		
		`$ sudo netAdm delete --device=eth14`
		`Interface eth14 removed`
		
		`For Gen9`
		
		`$ sudo netAdm delete --device=eth08`
		`Interface eth08 removed`

THIS PROCEDURE HAS BEEN COMPLETED		

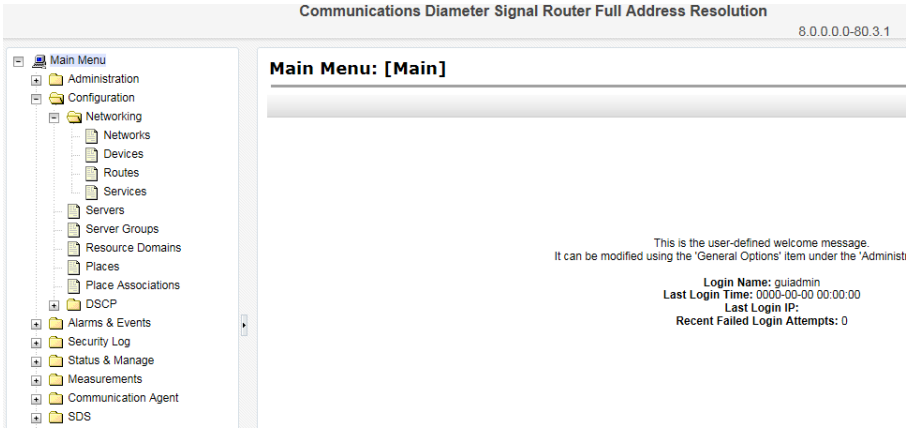
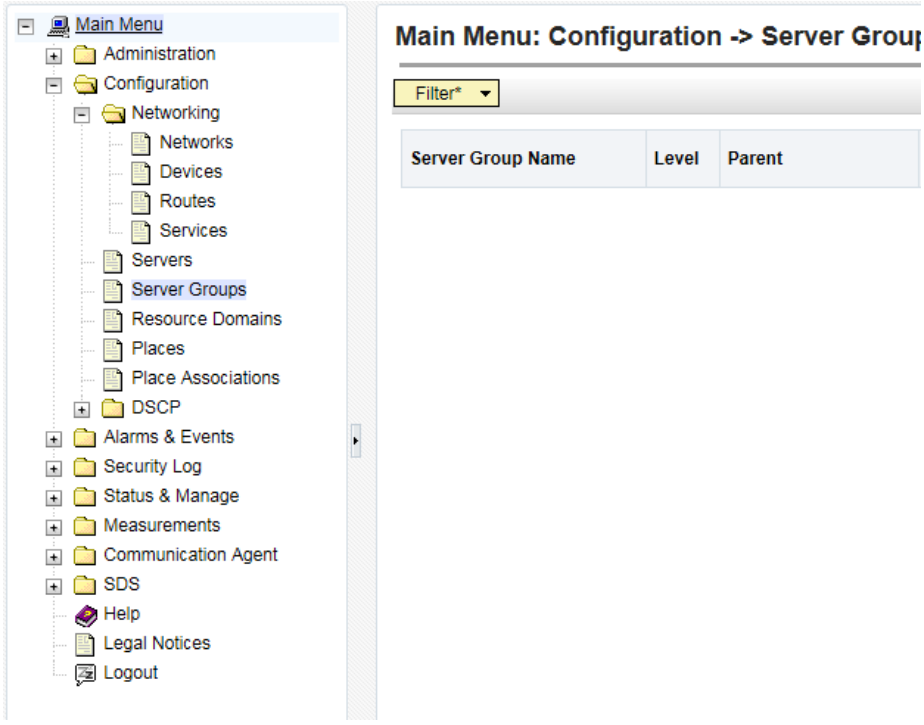
5.2 OAM Pairing (1st SDS NOAM Site Only)

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.

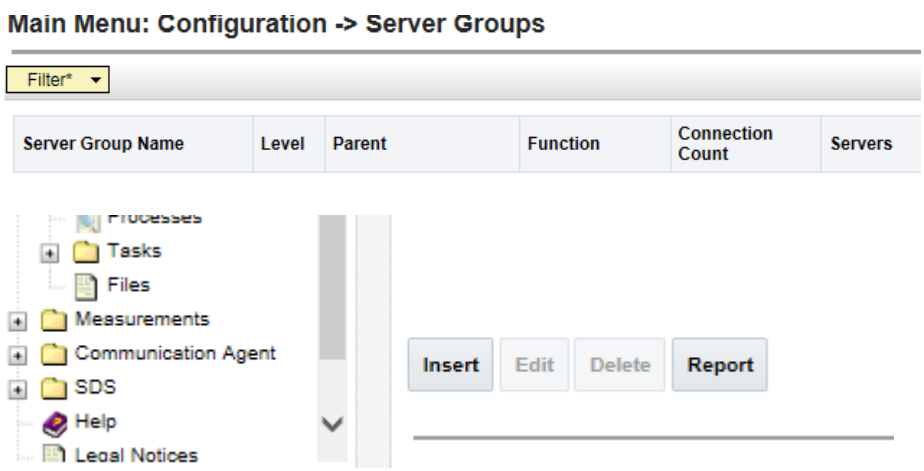
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
1. ☐	**SDS Server NOAM A:** Launch an approved web browser and connect to the SDS Server NOAM A IP XMI address **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**SDS Server NOAM A:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

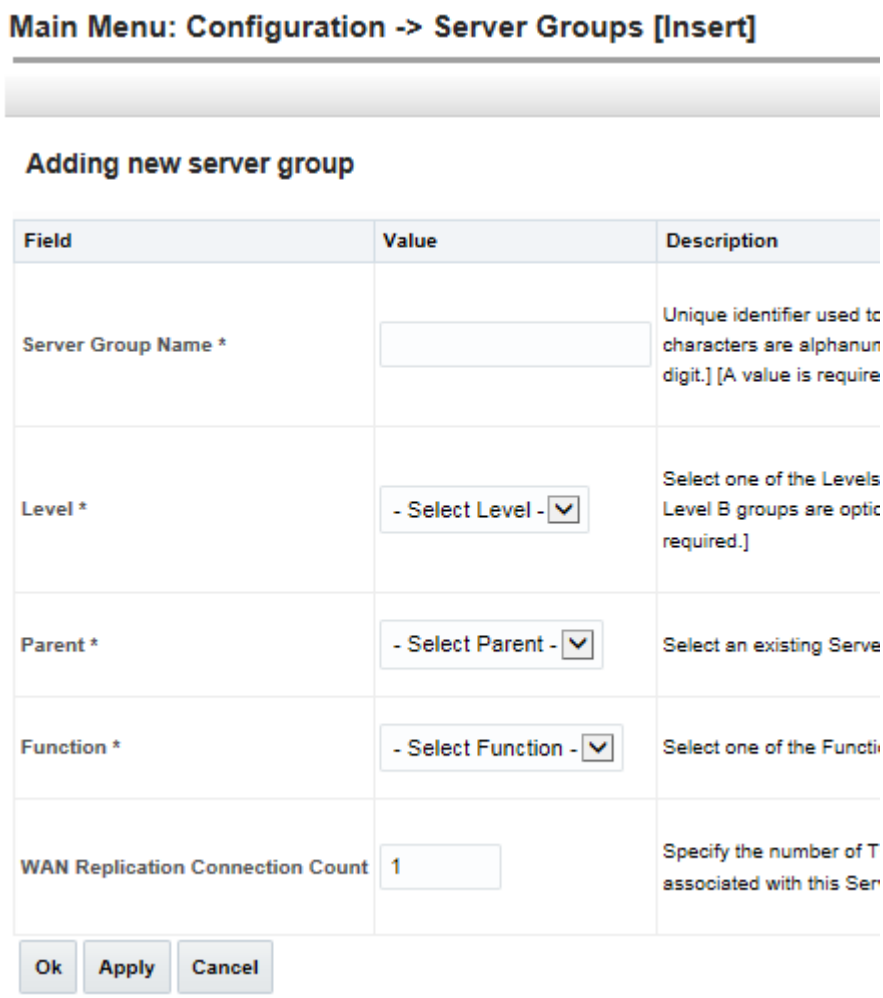
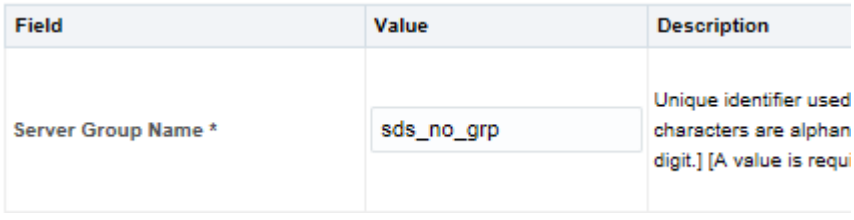
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
3. ☐	**SDS Server NOAM A:** The user should be presented the SDS Main Menu as shown on the right.	
4. ☐	**SDS Server NOAM A:** Select… **<u>Main Menu</u>** **→ Configuration** **→ *Server Groups*** …as shown on the right.	

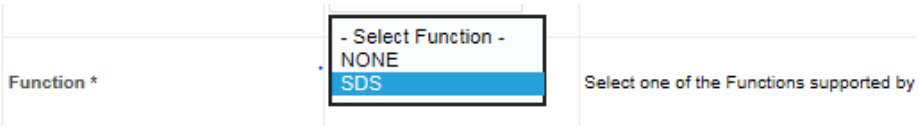
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
5. ☐	**SDS Server NOAM 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

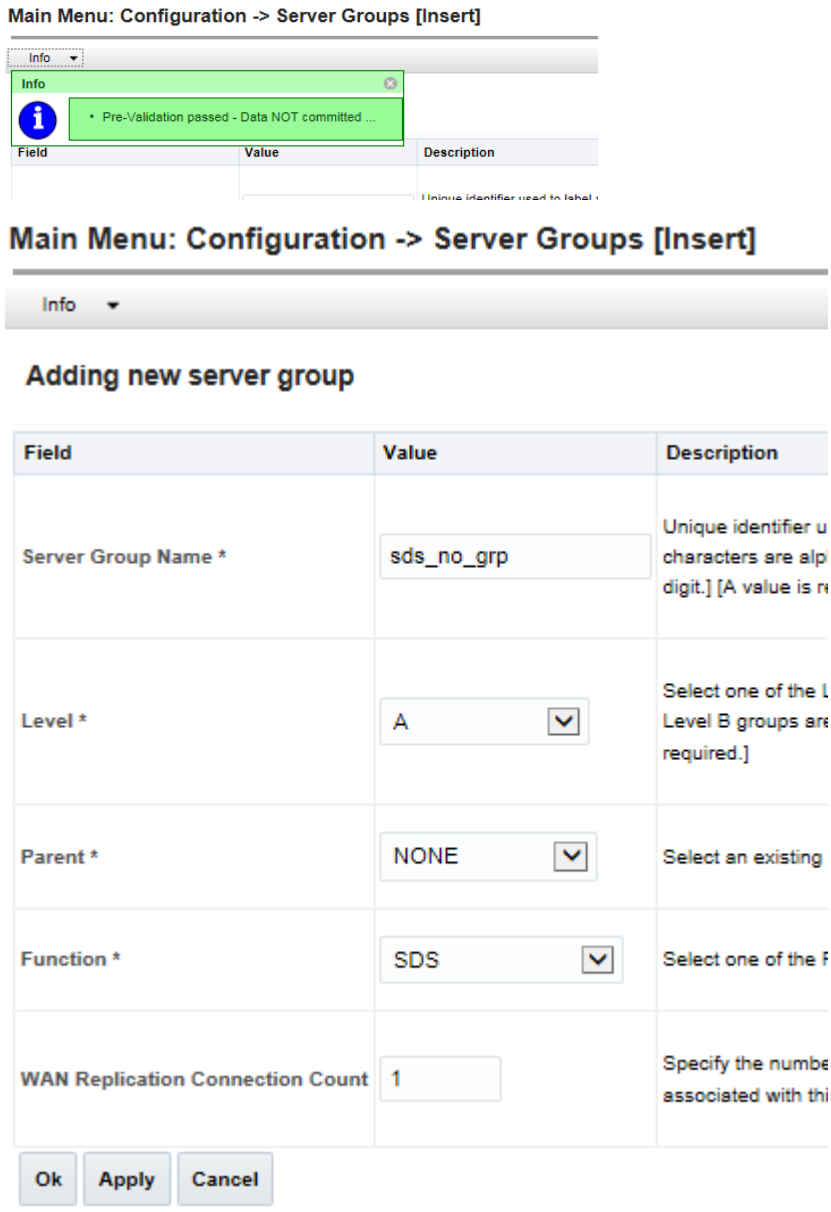
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
6. ☐	**SDS Server NOAM 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).*	
7. ☐	**SDS Server NOAM A:** Input the **Server Group Name**.	
8. ☐	**SDS Server NOAM A:** Select **"A"** on the **"Level"** pull-down menu.	

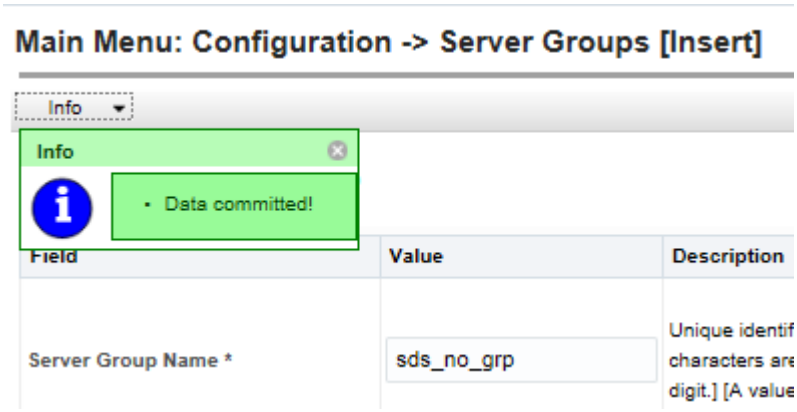
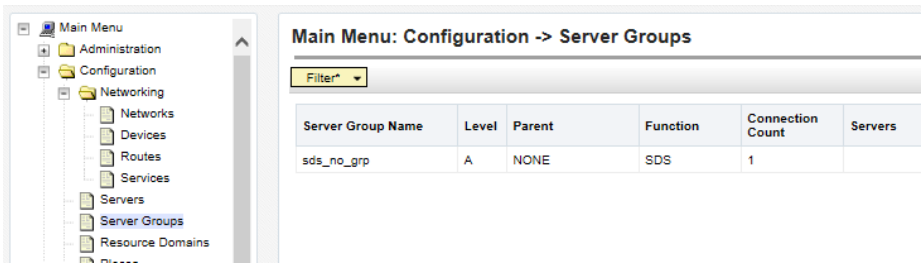
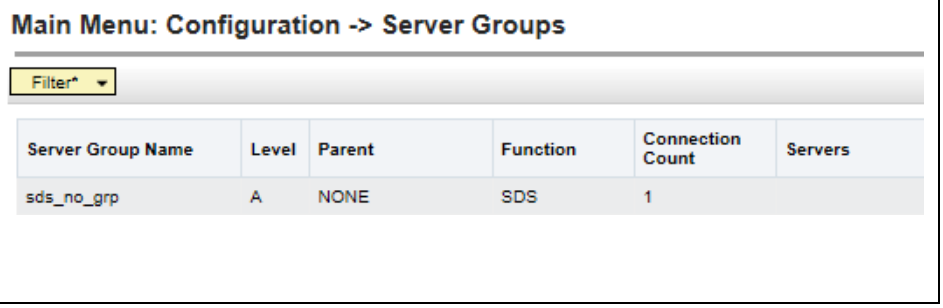
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
9. ☐	**SDS Server NOAM A:** Select **"None"** on the **"Parent"** pull-down menu.	
10. ☐	**SDS Server NOAM A:** Select **"SDS"** on the **"Function"** pull-down menu.	

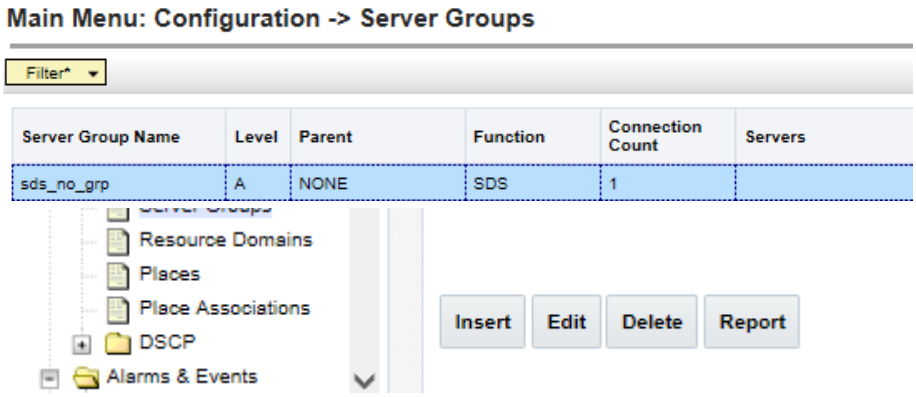
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
11. ☐	**SDS Server NOAM A:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	

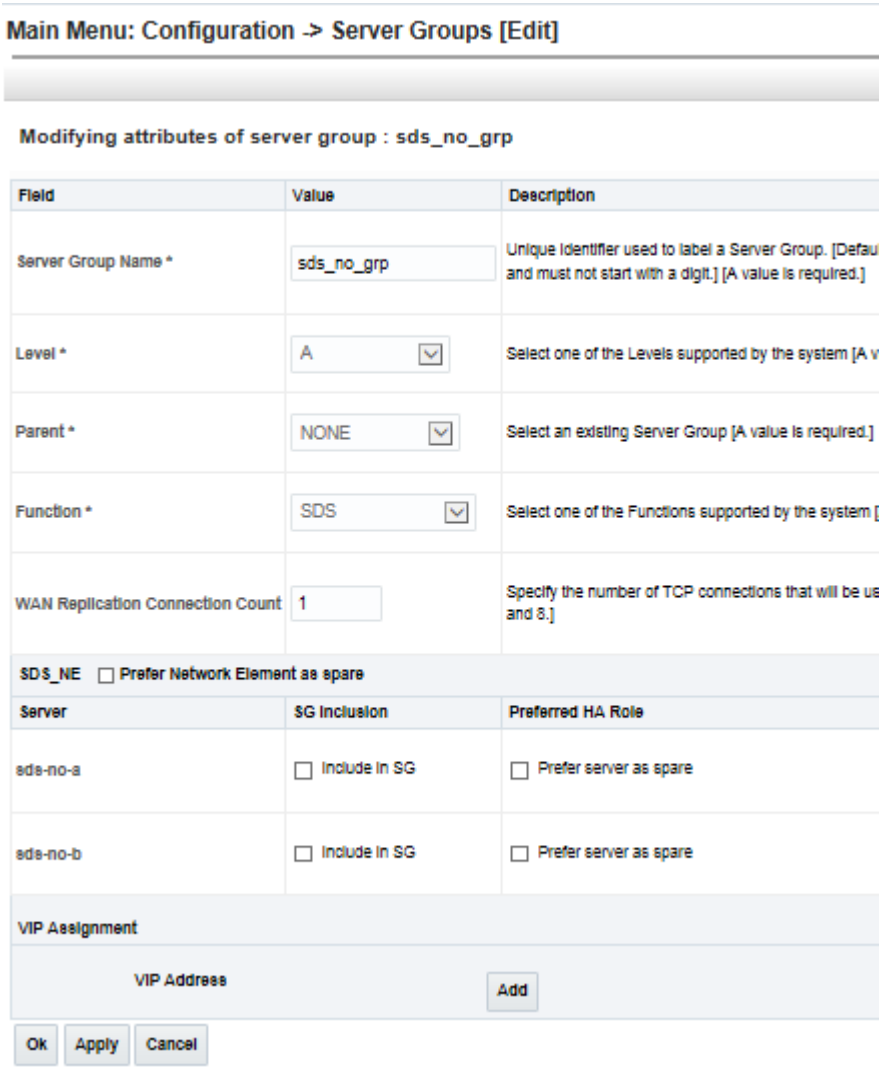
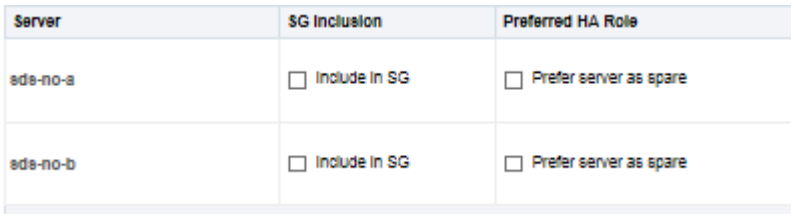
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
12. ☐	**SDS Server NOAM A:** The user should be presented with a banner information message stating **"Data committed"**.	
13. ☐	**SDS Server NOAM A:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	
14. ☐	**SDS Server NOAM A:** The **Server Group** entry added in **Steps 6 – 12** should now appear on the **"Server Groups"** configuration screen as shown on the right.	

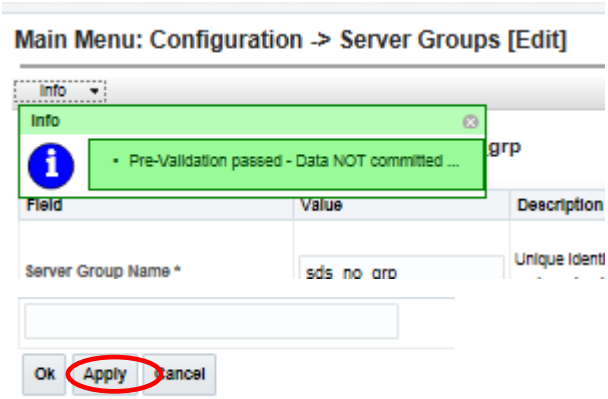
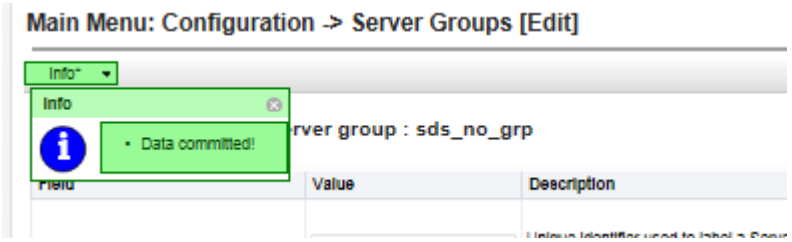
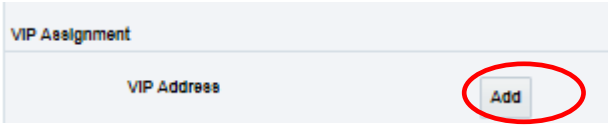
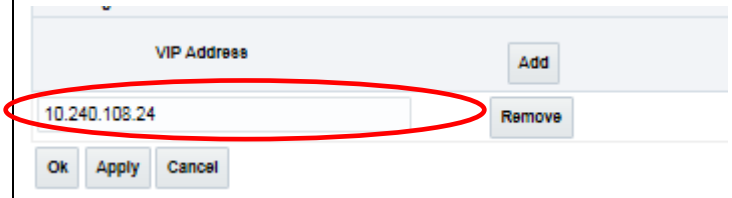
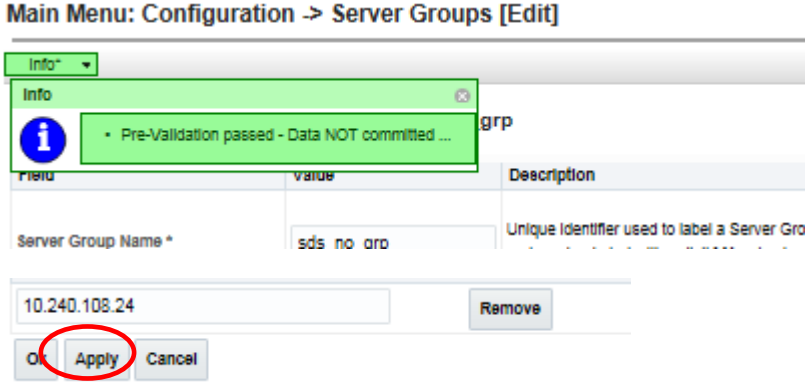
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
15. ☐	**SDS Server NOAM A:** **1)** Select the **Server Group** entry added in **Steps 6 – 12**. The line entry should now be highlighted. **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.*

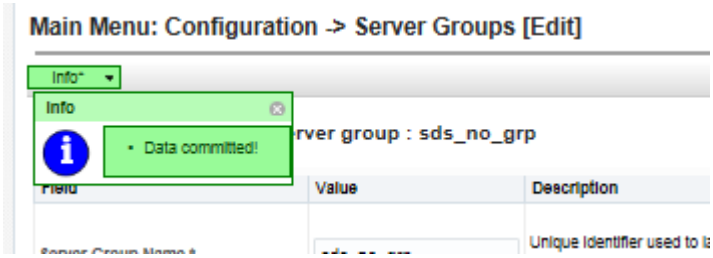
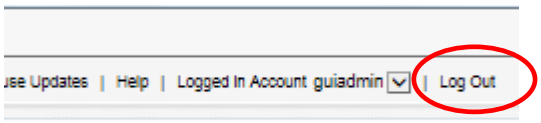
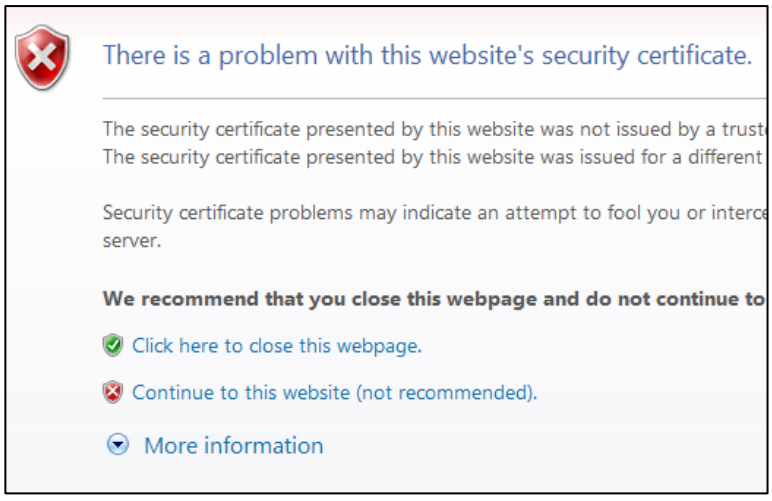
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
16. ☐	**SDS Server NOAM A:** The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	
17. ☐	**SDS Server NOAM A:** Select the **"A"** server and the **"B"** server from the list of **"Servers"** by clicking the check box next to their names.	

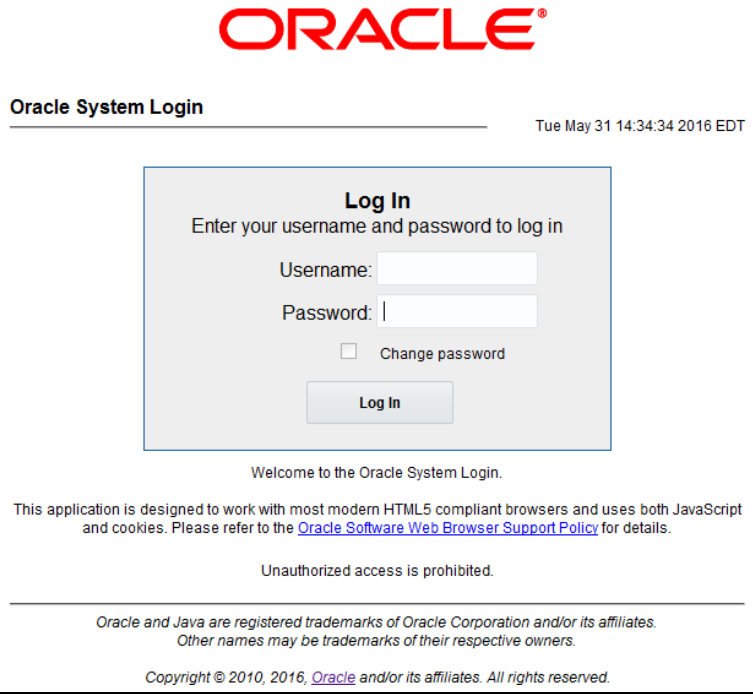
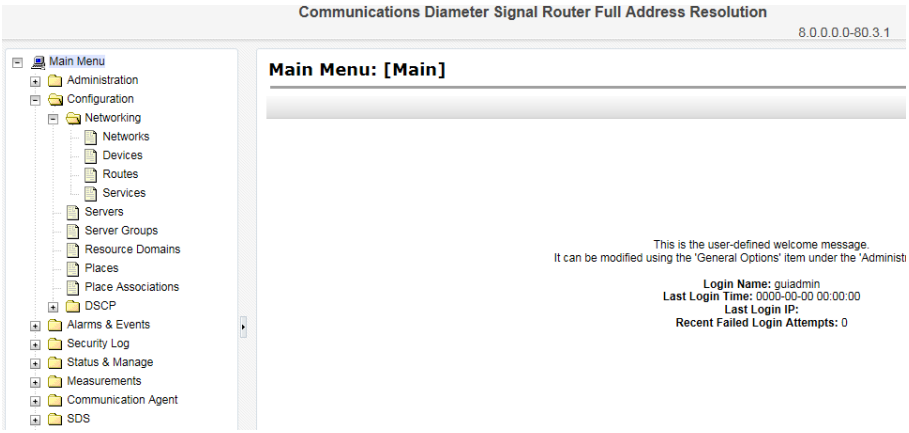
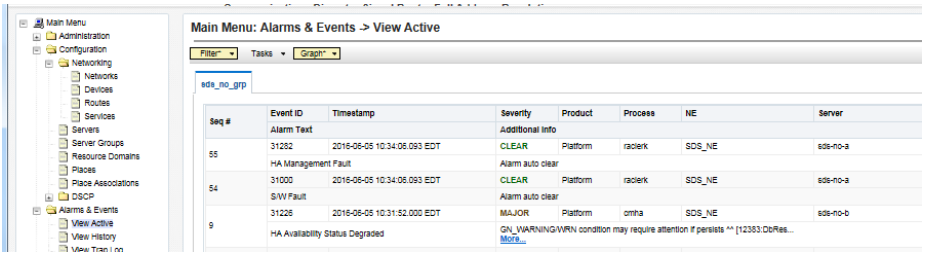
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
18. ☐	**SDS Server NOAM A:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
19. ☐	**SDS Server NOAM A:** The user should be presented with a banner information message stating **"Data committed"**.	
20. ☐	**SDS Server NOAM A:** Click the **"Add"** dialogue button for the **VIP Address**.	
21. ☐	**SDS Server NOAM A:** Input the **VIP Address**	
22. ☐	**SDS Server NOAM A:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	

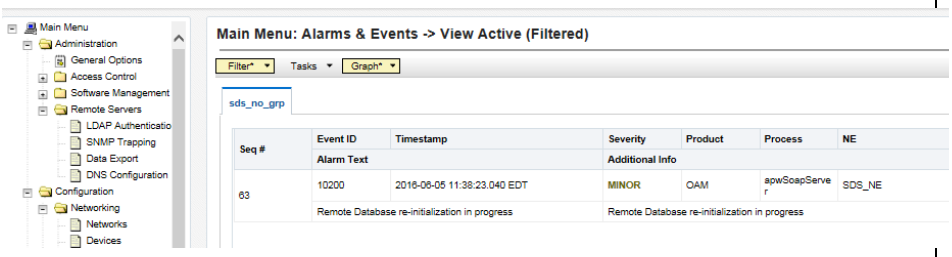
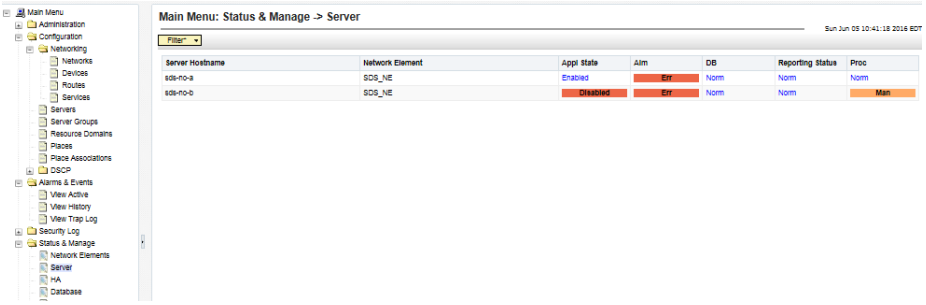
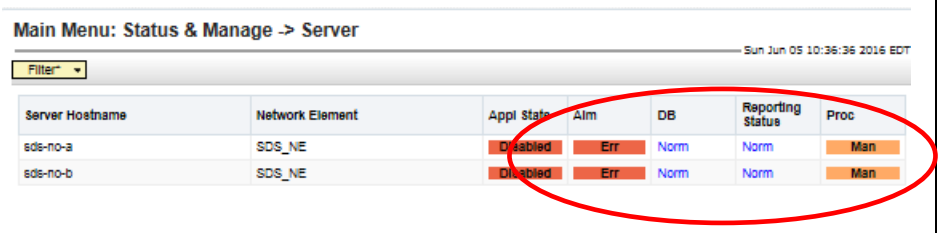
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
23. ☐	**SDS Server NOAM A:** The user should be presented with a banner information message stating **"Data committed"**.	
24. ☐	**SDS Server NOAM A:** Click the **"Logout"** link on the OAM A server GUI.	
25. ☐	**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.
26. ☐	**SDS VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** assigned in **STEP 21** to the SDS Server Group.	

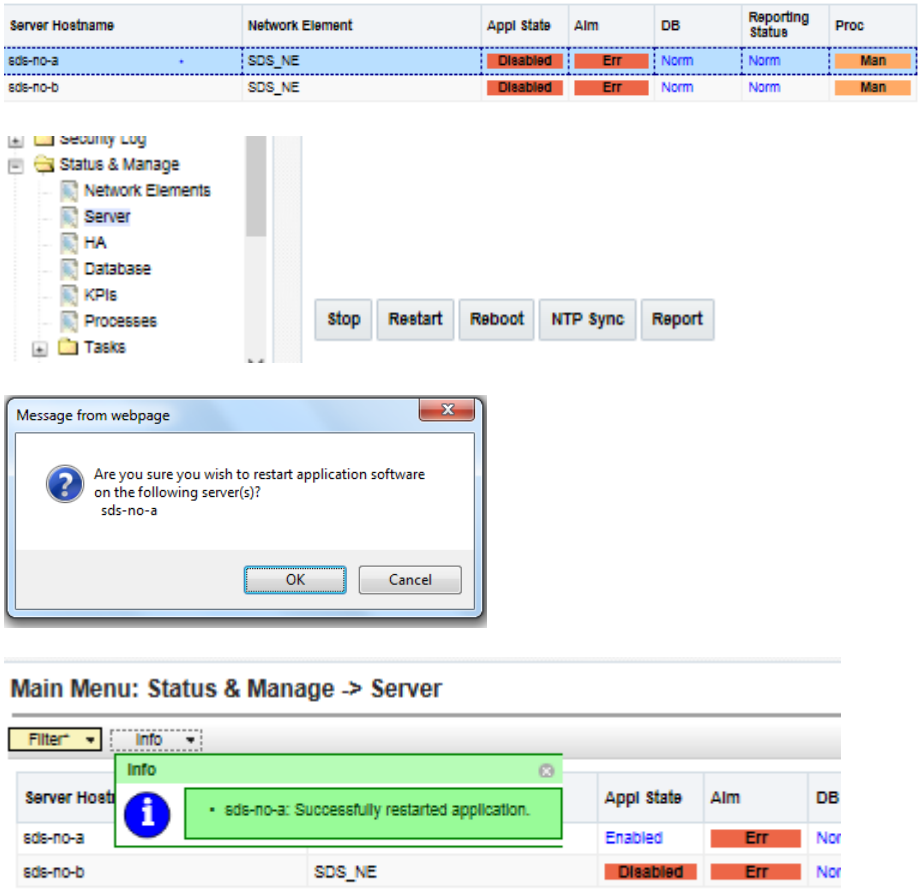
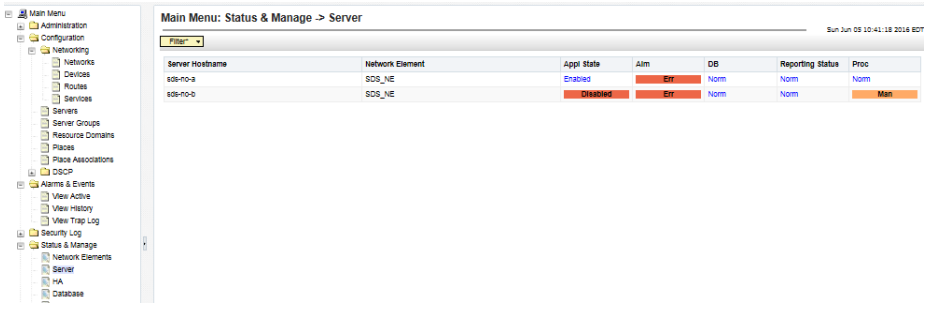
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
27. ☐	**SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
28.	**SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	
29.	**SDS VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	

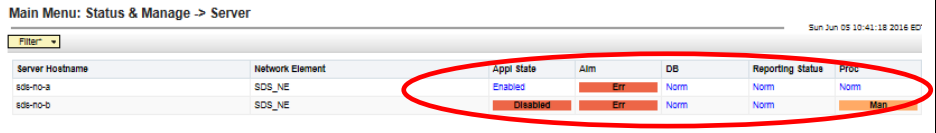
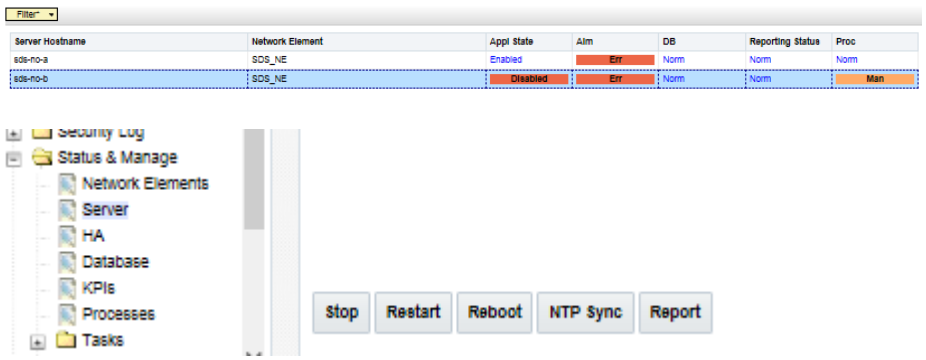
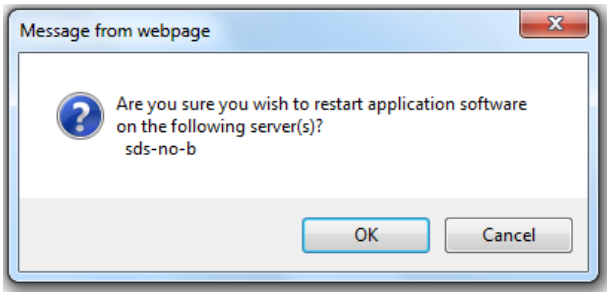
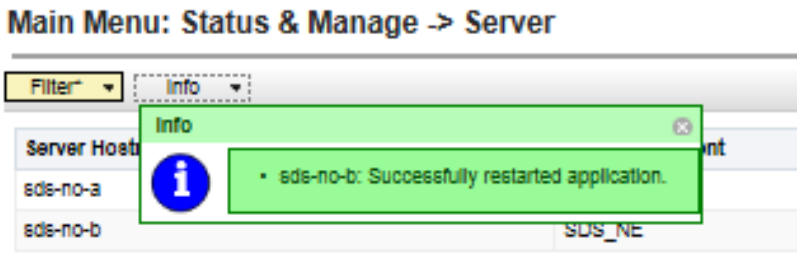
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
30. ☐	**SDS VIP:** Verify whether or not **Event ID 10200** (*Remote Database re-initialization in progress)* is present.	
	**IF EVENT ID 10200 (*Remote Database re-initialization in progress)* IS PRESENT, DO NOT PROCEED TO THE NEXT STEP UNTIL THE ALARM CLEAR IS RECEIVED.**	
31. ☐	**SDS VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	
32. ☐	**SDS VIP:** **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.	

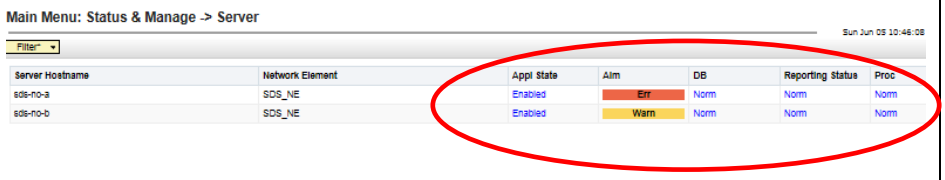
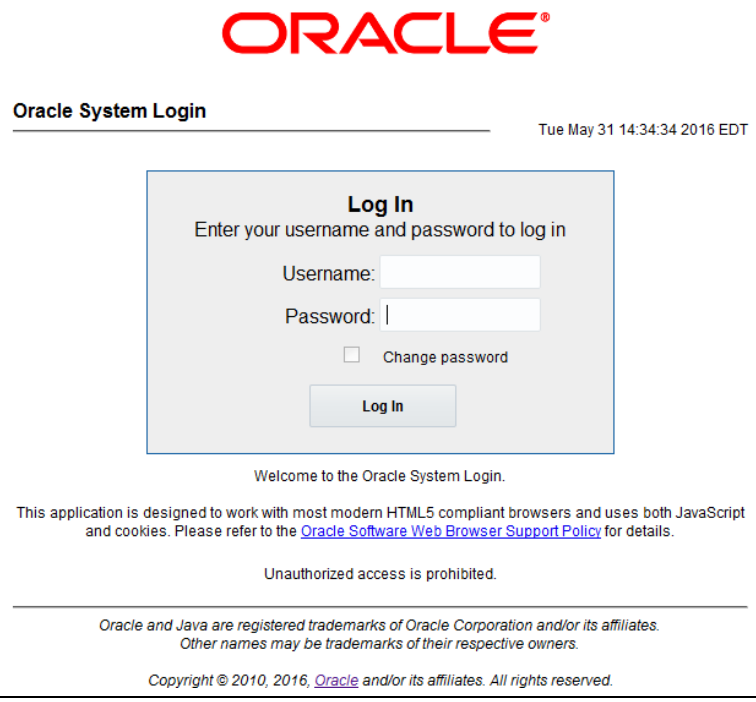
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
33. ☐	**SDS VIP:** **1)** Using the mouse, select **SDS Server NOAM A**. The line entry should now be highlighted. **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 NOAM A** stating: **"Successfully restarted application"**.	
34. ☐	**SDS VIP:** Select… **<u>Main Menu</u>** **→ Status & Manage** **→ *Server*** …as shown on the right.	

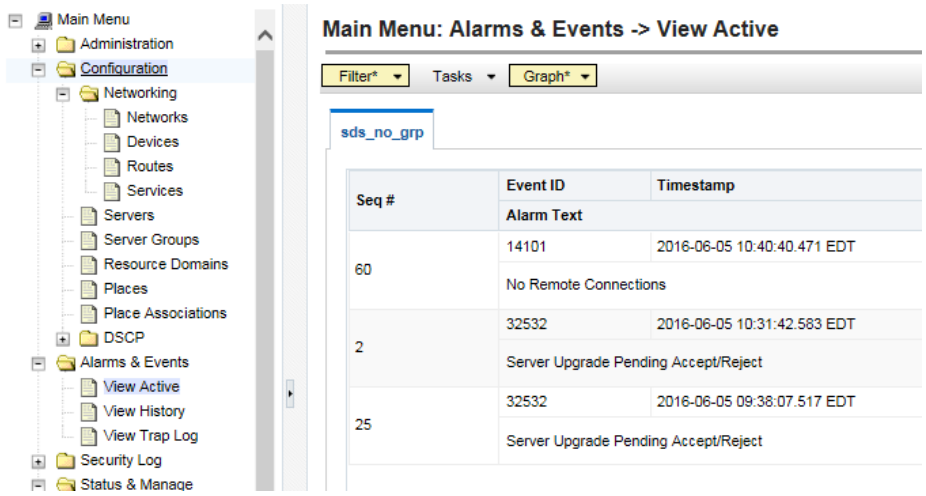
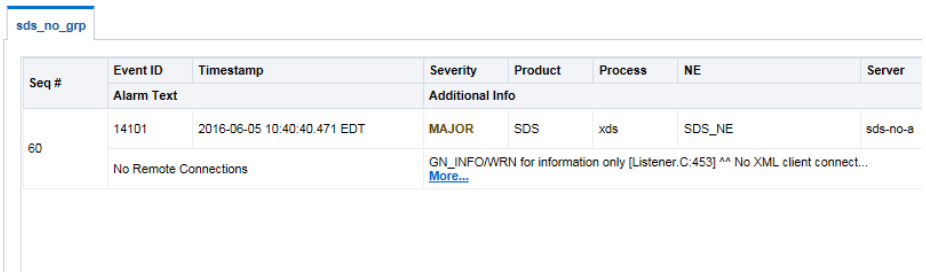
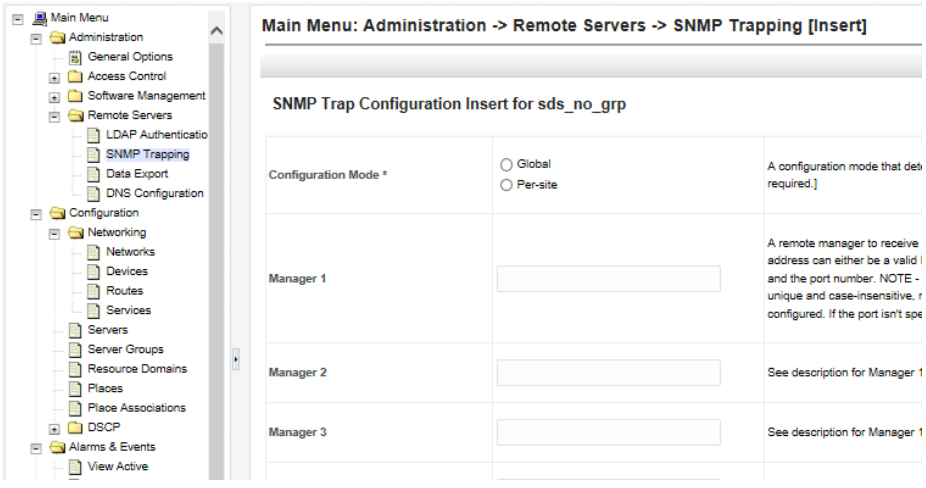
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
35. ☐	**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 NOAM A** before proceeding to the next Step.	
36. ☐	**SDS VIP:** **1)** Using the mouse, select **SDS Server B**. The line entry should now be highlighted. **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 B** stating: **"Successfully restarted application"**. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*	  

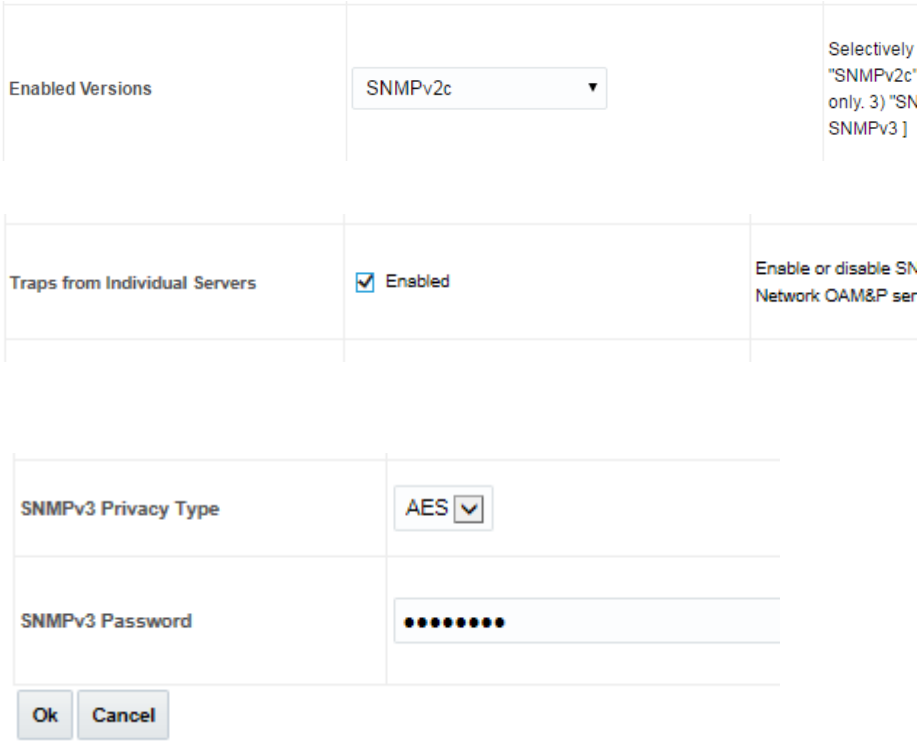
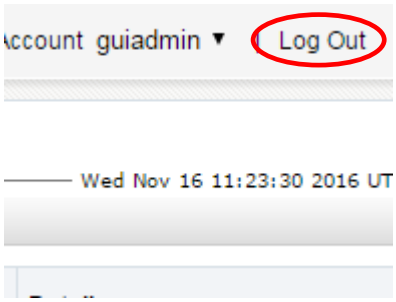
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
37. ☐	**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 NOAM A** and **SDS Server NOAM B** before proceeding to the next Step.	
38. ☐	**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.
39. ☐	**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.	

Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
40. ☐	**SDS VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	
41. ☐	**SDS VIP:** Verify that **Event ID 14101** (“*No remote provisioning clients are connected”)* is the only alarm present on the system at this time.	
42. ☐	**SDS VIP:** Select… **Main Menu** → **Administration** → **Remote Servers** → **SNMP Trapping** …as shown on the right.	

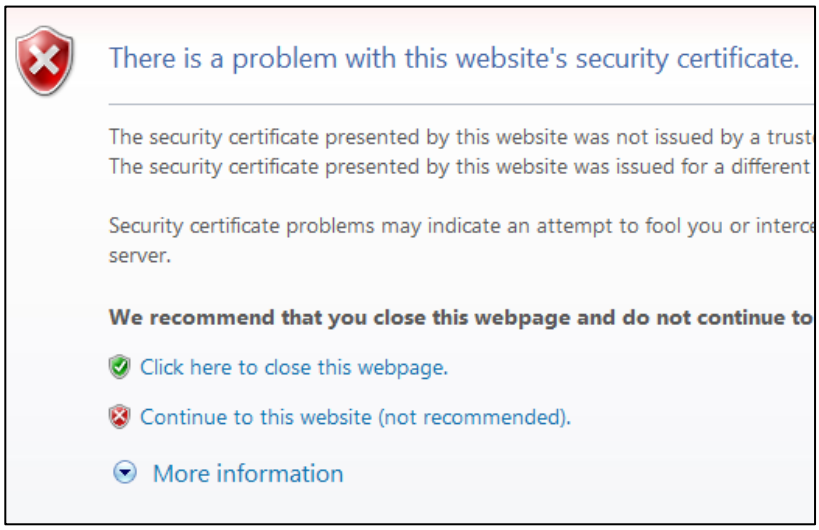
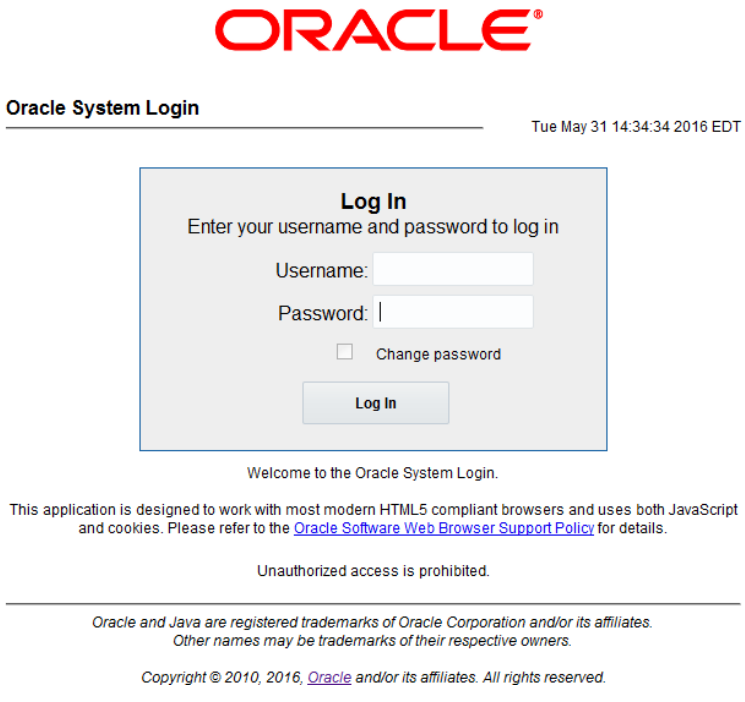
Procedure 4. Pairing the SDS NOAM Servers (1st SDS NOAM Site Only)

Step	Procedure	Result
43. ☐	**SDS VIP:** **1)**Enable Version field changed to SNMPv2c before you select OK **2)** Using the cursor, place a "check" in the check box for **"Traps from Individual Servers"**. **3)** Click the **"Ok"** dialogue button located at the bottom of the right panel.	
44. ☐	**SDS VIP:** Click the **"Logout"** link on the server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

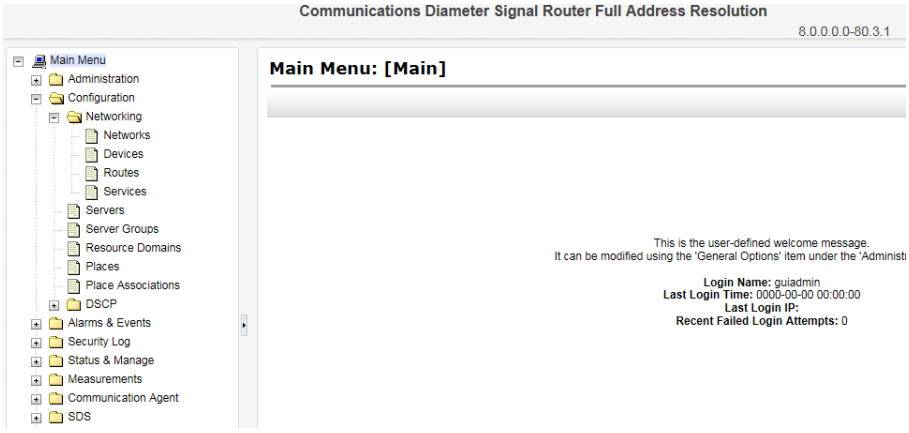
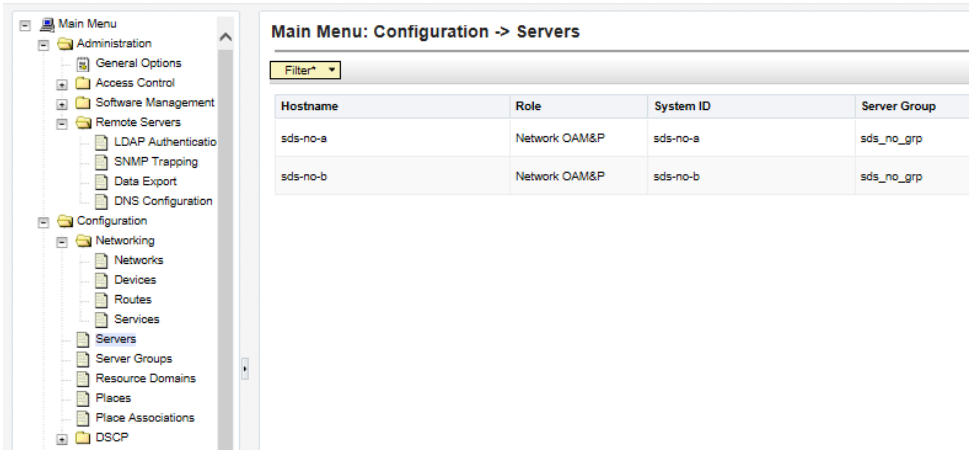
5.3 Query Server Installation (All SDS NOAM Sites)

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.

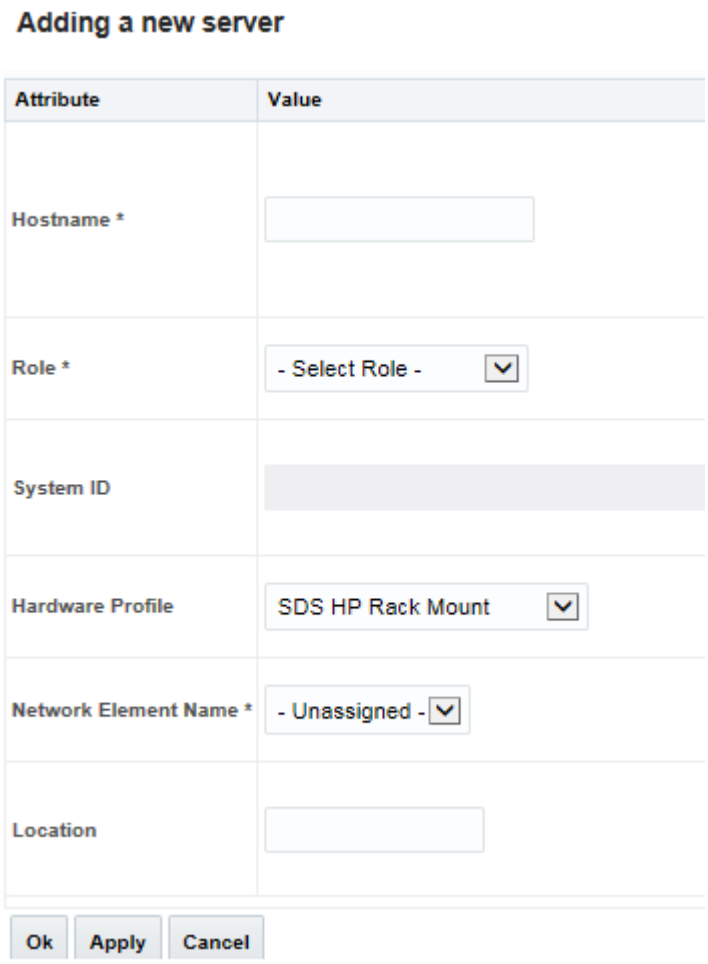
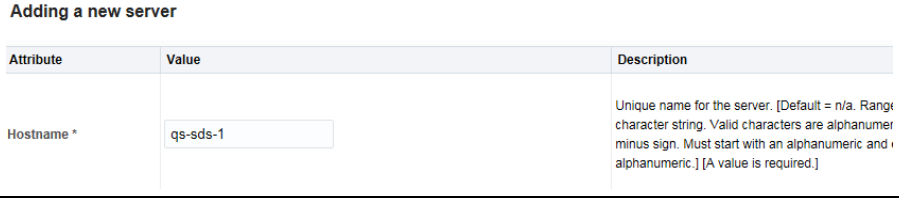
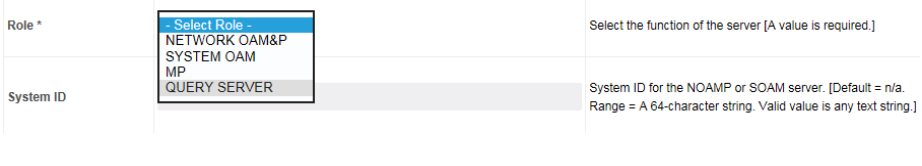
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
1. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**Primary 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. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
3. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	
4. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right.	
5. ☐	**Primary SDS VIP:** Select the **"Insert"** dialogue button.	

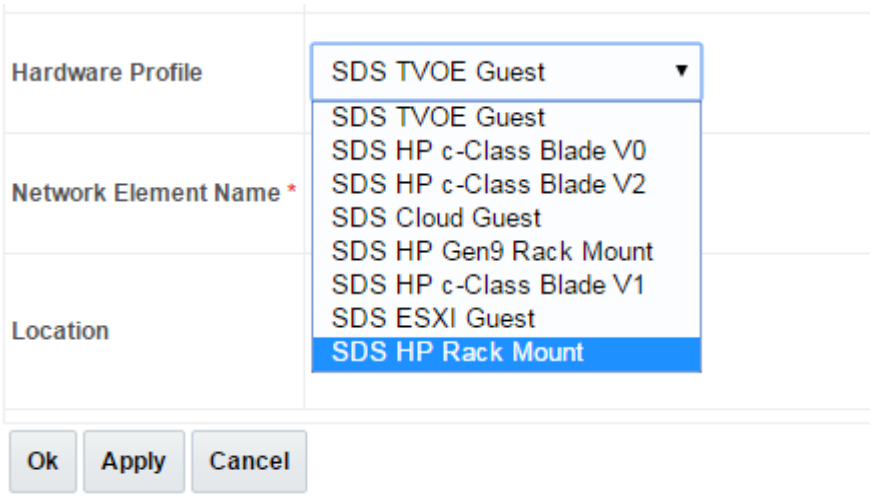
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

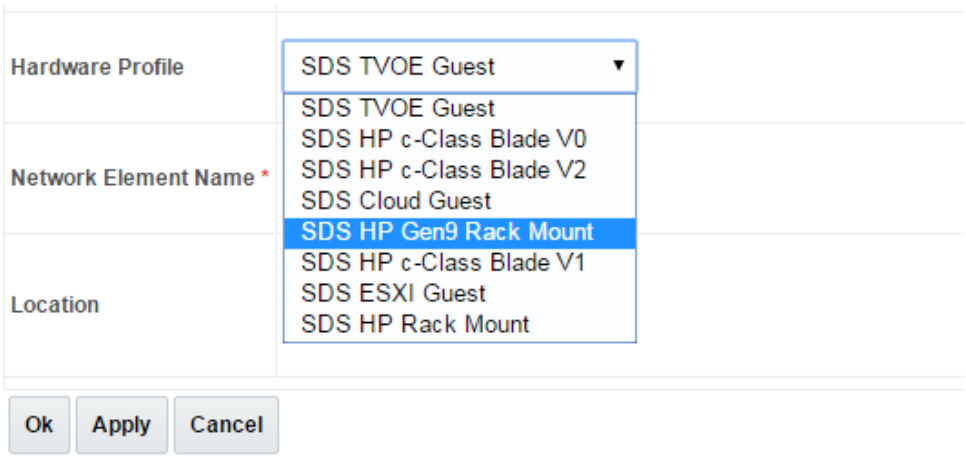
Step	Procedure	Result
6. ☐	**Primary SDS VIP:** The user is now presented with the **"Adding a new server"** configuration screen.	
7. ☐	**Primary SDS VIP:** Input the assigned "**hostname"** for the Query Server.	
8. ☐	**Primary SDS VIP:** Select **"QUERY SERVER"** for the server **"Role"** from the pull-down menu.	

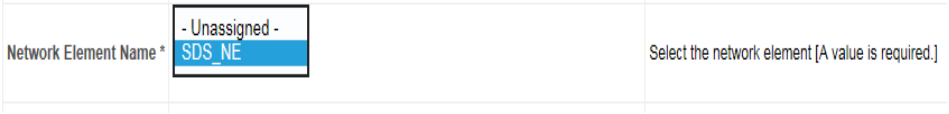
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>9.
☐</td><td>Primary SDS VIP:

For Gen8 Server
Select “SDS HP Rack Mount” for the Hardware Profile for the SDS from the pull-down menu.

For Gen9 Server:
Select “SDS HP Gen9 Rack Mount” for the Hardware Profile for the SDS from the pull-down menu.</td><td>For Gen8 select “SDS HP Rack Mount” from the Hardware Profile pull-down menu.
 

For Gen9 Server, Select “SDS HP Gen9 Rack Mount” from the Hardware Profile pull-down menu.
 
</td></tr>
<tr><td>10.
☐</td><td>Primary SDS VIP:

Select the Network Element Name of the SDS site where the Query Server is physically located.</td><td> 
</td></tr>
<tr><td>11.
☐</td><td>Primary SDS VIP:

Enter the site location.</td><td> 

Note: Location is an optional field.</td></tr>
</table>

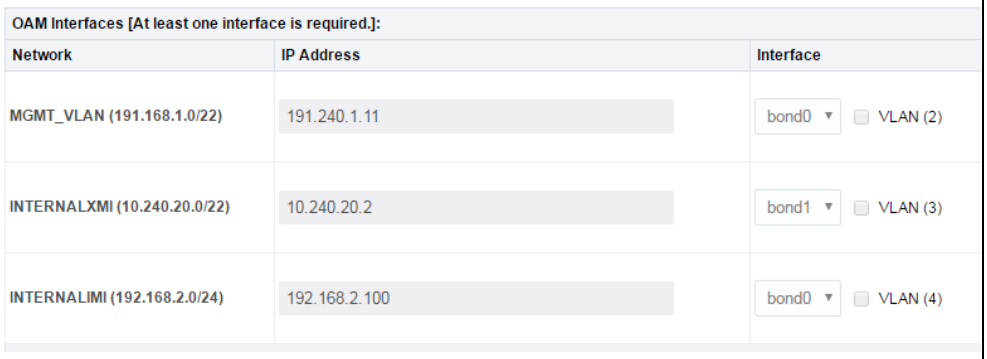
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr>
<td>12. ☐</td>
<td>SDS Server NOAM A:

1) Enter the MGMNT_VLAN IP address for the Query Server.

2) Set the MGMNT_VLAN Interface to “bond0” and “check” the VLAN checkbox.

3) Enter the IMI IP address for the Query Server.

4) Set the IMI Interface to “bond0” and “check” the VLAN checkbox.</td>
<td>


<table>
<tr><th>Query Server</th><th>Network</th><th>IP Address</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">SDS-QS
(Primary NE)</td><td>MGMNT_VLAN</td><td>169.254.1.13</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.13</td></tr>
<tr><td rowspan="2">SDS-QS
(DR NE)</td><td>MGMNT_VLAN</td><td>169.254.1.16</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.16</td></tr>
</table>
Note: These IP addresses are based on the info in the NAPD and the Network Element Config file.

Note: The MGMT_VLAN should only be present when 4948E-F AggregationSwitches are deployed with SDS NOAM / Query Server RMS. If the MGMT_VLAN is not present, the IMI network values shown above still apply.
</td>
</tr>
</table>

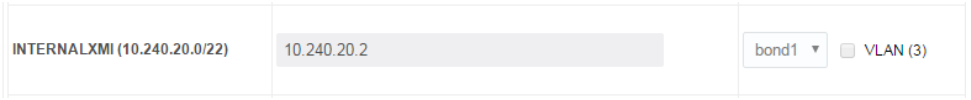
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>13.</td><td>1) Enter the customer assigned XMI IP address for the Query Server.

Layer 3
(No VLAN tagging used for XMI)

2) Set the XMI Interface to “bond1” and “DO NOT check” the VLAN checkbox.
- OR -

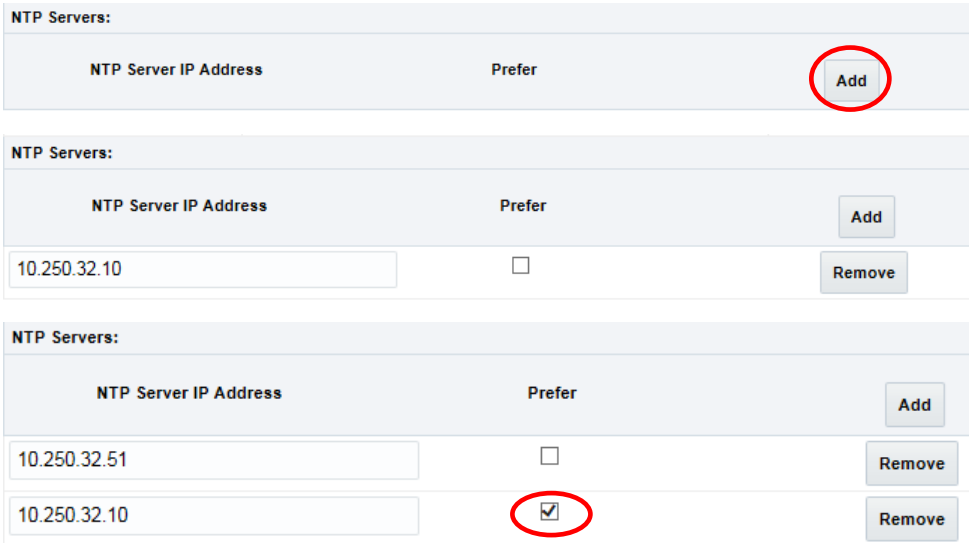
Layer 2
(VLAN tagging used for XMI)

2) Set the XMI Interface to “bond0” and “check” the VLAN checkbox.</td><td> 

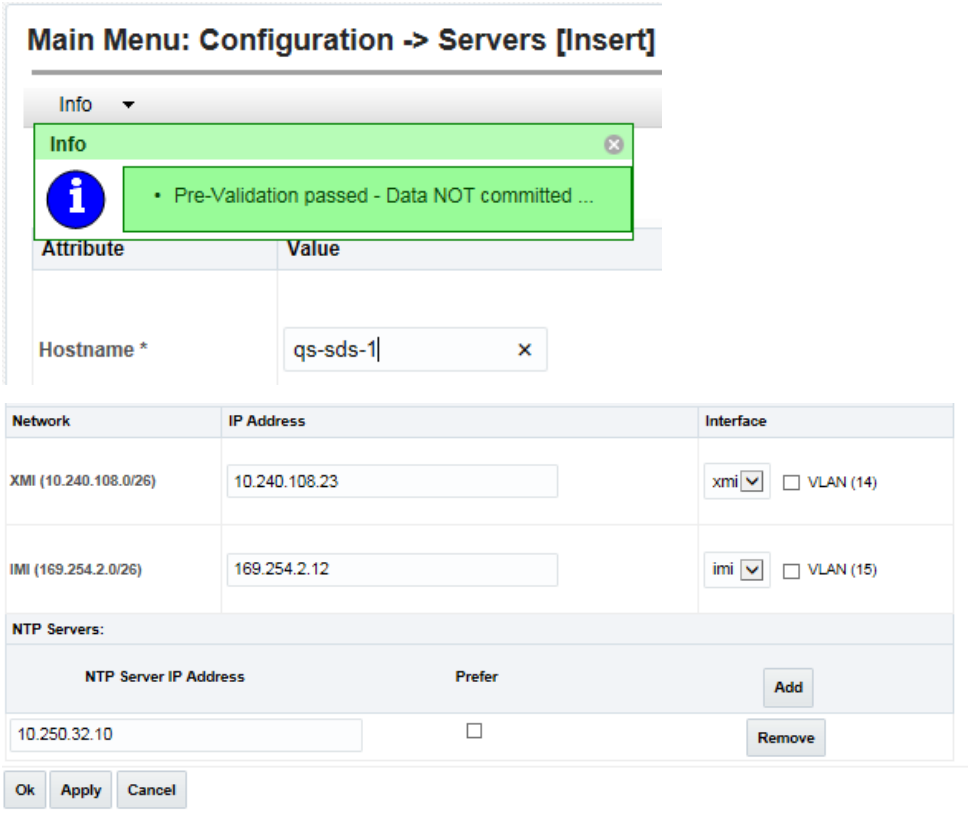
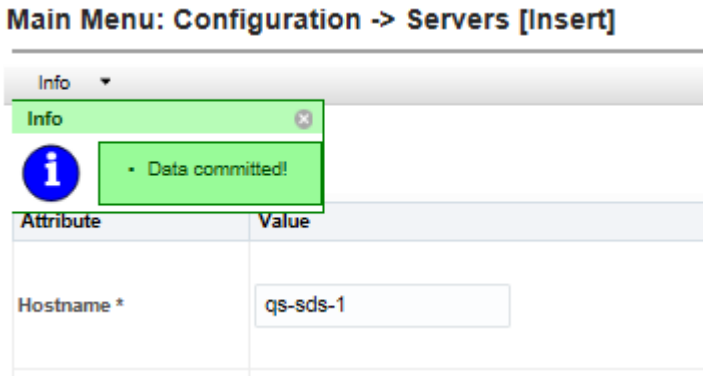
<table>
<tr><th>Query Server</th><th>Network</th><th>VLAN tagging
(on XMI network)</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">SDS-QS
(Primary & DR)</td><td rowspan="2">XMI</td><td>No</td><td>bond1</td><td>✗</td></tr>
<tr><td>Yes</td><td>bond0</td><td>✓</td></tr>
</table>
!!! CAUTION !!!
It is crucial that the correct network configuration be selected in Steps 12 & 13 of this procedure. Choosing an incorrect configuration will result in the need to re-install the OS and restart the Query Server instalation procedure over from the beginning.</td></tr>
<tr><td>14. ☐</td><td>SDS Server NOAM A:

1) Click the “NTP Servers:” “Add” dialogue button.

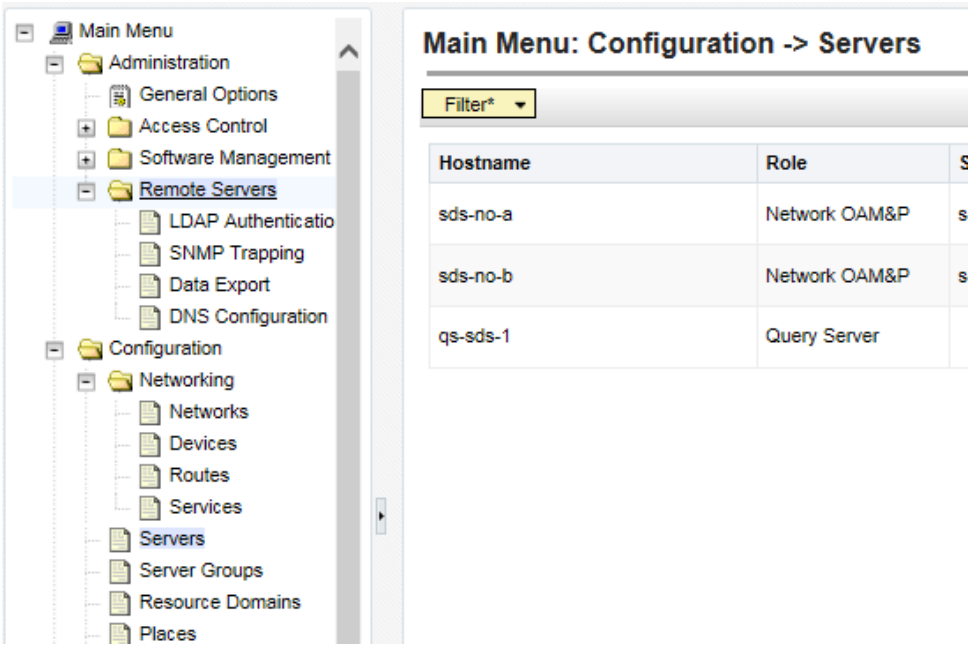
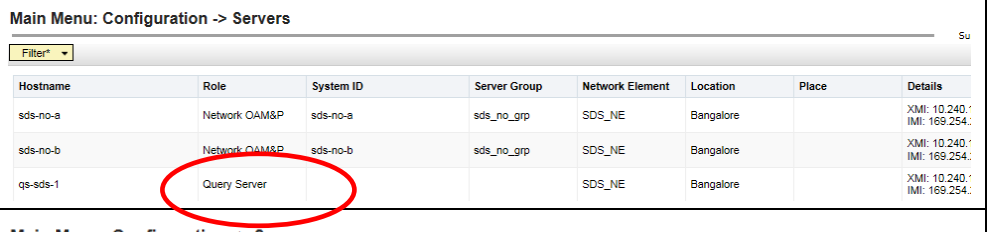
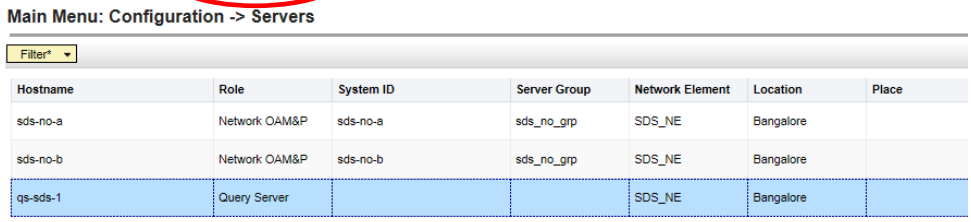
2) Enter the NTP Server IP Address for an NTP Server.

3) Enter 3 NTP Server IP address, repeat (1) and (2) to enter it.
4) Optionally, click the “Prefer” checkbox to prefer one NTP Server over the other.</td><td> 
</td></tr>
</table>

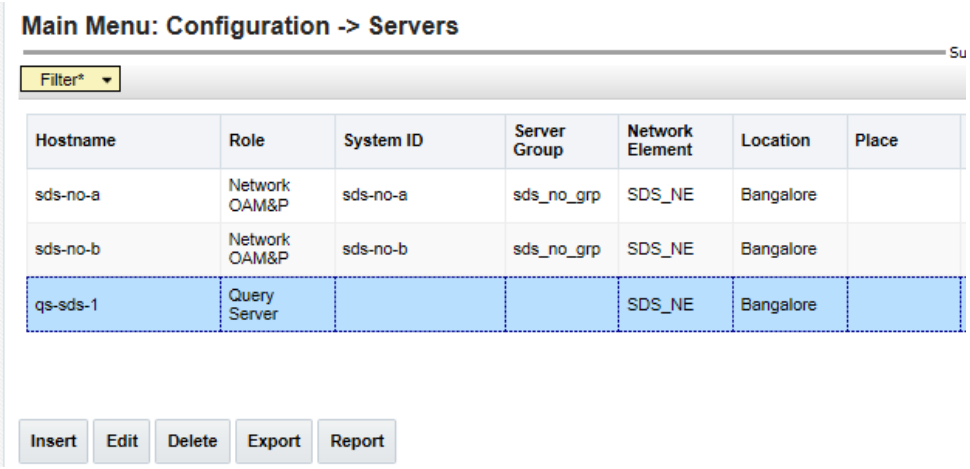
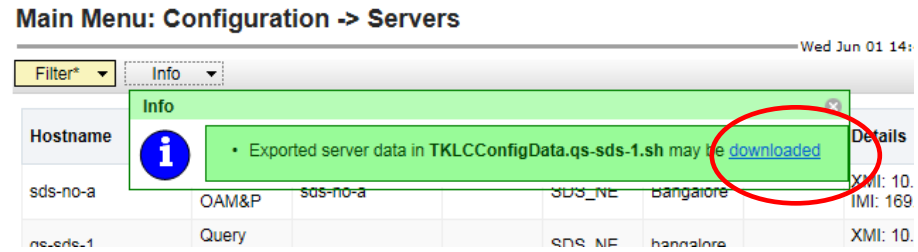
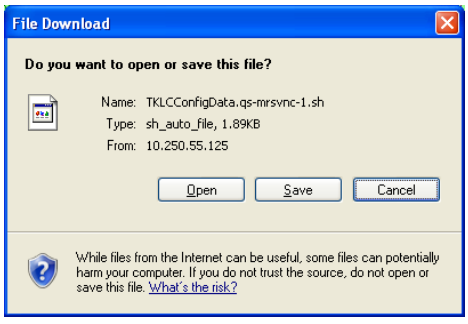
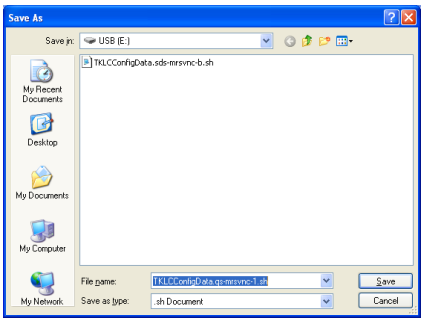
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
15. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"Apply"** dialogue button.	
16. ☐	**Primary SDS VIP:** If the values provided match the network ranges assigned to the NE, the user must select the Info box to receive a banner information message showing that the data has been validated and committed	

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
17. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right.	
18. ☐	**Primary SDS VIP:** The **"Configuration →Servers" screen** now shows the newly added Query Server in the list.	
19. ☐	**Primary SDS VIP:** Using the mouse, select the Query Server. The line entry containing the Query Server should now be highlighted.	

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
20. ☐	**Primary SDS VIP:** Select the **"Export"** dialogue button.	
21. ☐	**Primary SDS VIP:** The user must select the Info box to receive a banner information message showing a download link for the Query Server configuration data. Click on the word **"downloaded"** to download and save the file.	
22. ☐	**Primary SDS VIP:** **1)** Click the "Save" dialogue button. **2)** Save the Query Server configuration file to a USB flash drive.	 
23. ☐	**Query Server:** Access the server console.	Connect to the **Query Server** console using one of the access methods described in Section 2.3.

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result

24. ☐	**Query Server:**
	
	1) Access the command prompt.
	
	2) Log into the server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

25. ☐	**Query Server:** Insert the USB flash drive containing the server configuration file into the USB port on the front panel of the Query Server.	 **Figure 8 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 9 – HP DL380 Gen9: Front Panel (USB Port)**

26. ☐	**Query Server:**
	
	Output similar to that shown on the right will appear as the USB flash drive is inserted into the **SDS Server** front USB port.
		`$ sd 3:0:0:0: [sdb] Assuming drive cache: write through`
		`sd 3:0:0:0: [sdb] Assuming drive cache: write through <ENTER>`
		
		***NOTE**: Press the **<ENTER>** key to return to the command prompt.*

27. ☐	**Query Server:**
	
	Verify that the USB flash drive's partition has been mounted by the OS.
		`$ df |grep sdb`
		`/dev/sdb1  2003076  8  2003068  1% /media/sdb1`
		
		***NOTE**: Search **df** for the device named in the previous step's output.*

28. ☐	**Query Server:** Copy the configuration file.	`$ sudo cp -p /media/sdb1/TKLCConfigData.qs-mrsvnc-1.sh /var/TKLC/db/filemgmt/`

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
29. ☐	**Query Server:** 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.	***Example:*** TKLCConfigData<.server_hostname>.sh ➔ will translate to ➔TKLCConfigData.sh `$ sudo cp -p /var/TLKC/db/filemgmt/TKLCConfigData.qs-mrsvnc-1.sh /var/tmp/TKLCConfigData.sh` **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

30. ☐	**Query Server:**
	
	After the script completes, a broadcast message will be sent to the terminal.
	
	NOTE: *This step varies by server and may take 3…20 minutes to complete.*
		`*** NO OUTPUT FOR ≈ 3-20 MINUTES ***`
		
		`Broadcast message from admusr (Mon Dec 14 16:17:13 2009):`
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		`Please remove the USB flash drive if connected and reboot the server.`

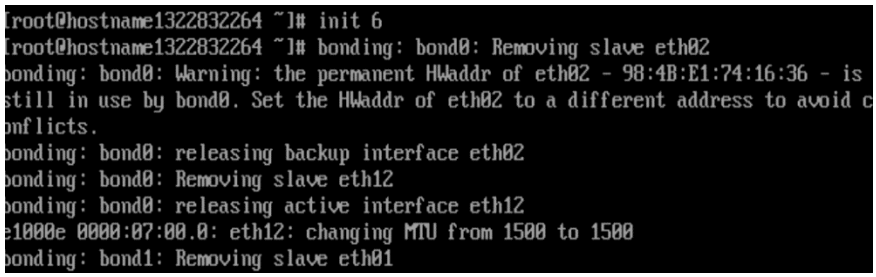
31. ☐	**Query Server:** Remove the USB flash drive from the USB port on the front panel of **Query Server**. **CAUTION:** *It is important that the USB flash drive be removed from the server before continuing on to the next step.*	 **Figure 10 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 11 – HP DL380 Gen9: Front Panel (USB Port)**

32. ☐	**Query Server:**
	
	Ignore the output shown and press the **<ENTER>** key to return to the command prompt.
		`Broadcast message from admusr (Mon Dec 14 16:17:13 2009):`
		
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		
		`Please remove the USB flash drive if connected and reboot the server.` **<ENTER>**

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
33.	**SDS Server NOAM A or B:** Verify that the desired Time Zone is currently in use.	`$ date` `Mon Aug 10 19:34:51 UTC 2015`

34. ☐	**SDS Server NOAM A or B:**
	
	If the desired Time Zone was not presented in the previous step…
	
	Configure the Time Zone.
	
	Verify the timezone was changed.
	Otherwise, skip to the next step.
		Example: `$ sudo set_ini_tz.pl <time_zone>`
		
		NOTE: *The following command example sets the time to the "UTC" (aka GMT) time zone which is recommneded for all sites.*
		The user may replace, as appropriate, with the customer requested time zone for this site installation. See ***Appendix G*** *for a list of valid time zones.*
		
		`$ sudo set_ini_tz.pl "Etc/UTC"`
		
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2015`

35. ☐	**Query Server:** Initiate a reboot of the Query Server.	`$ sudo init 6`
36. ☐	**Query Server:** Output similar to that shown on the right may be observed as the server initiates a reboot.	

37. ☐	**Query Server:**
	
	1) Access the command prompt.
	
	2) Login as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
38.	**Query Server:** Accept upgrade to the Application Software..	[admusr@rlghnc-sds-QS ~]$ sudo /var/TKLC/backout/accept Called with options: --accept Loading Backout::BackoutType::RPM Accepting Upgrade Executing common accept tasks Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info. Cleaning backout directory. Clearing Upgrade Accept/Reject alarm. Cleaning message from MOTD. No patch pending alarm on server so no MOTD update. Cleaning up RPM config backup files... Checking / Checking /boot Checking /tmp Checking /usr Checking /var Checking /var/TKLC Checking /tmp/appworks_temp Checking /usr/openv Checking /var/TKLC/appw/logs/Process Checking /var/TKLC/appw/logs/Security Checking /var/TKLC/db/filemgmt Checking /var/TKLC/rundb Starting cleanup of RCS repository. INFO: Removing '/etc/my.cnf' from RCS repository INFO: Removing '/etc/pam.d/password-auth' from RCS repository INFO: Removing '/etc/pam.d/system-auth' from RCS repository INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0' from RCS repository INFO: Removing '/etc/php.d/zip.ini' from RCS repository INFO: Removing '/var/lib/prelink/force' from RCS repository [admusr@rlghnc-sds-QS ~]$
39. ☐	**Query Server:** **1)** Verify that the **IMI IP address** input in **Step 12** has been applied to **"bond0.4"**. **2)** Verify that the **XMI IP address** input in **Step 13** has been applied to **"bond1"**.	$ **ifconfig |grep in** bond0 Link encap:Ethernet HWaddr 98:4B:E1:74:16:34 bond0.4 Link encap:Ethernet HWaddr 98:4B:E1:74:16:34 inet addr:169.254.100.13 Bcast:169.254.100.255 Mask:255.255.255.0 bond1 Link encap:Ethernet HWaddr 98:4B:E1:74:16:36 inet addr:10.250.55.127 Bcast:10.250.55.255 Mask:255.255.255.0 eth01 Link encap:Ethernet HWaddr 98:4B:E1:74:16:34 eth02 Link encap:Ethernet HWaddr 98:4B:E1:74:16:36 eth11 Link encap:Ethernet HWaddr 98:4B:E1:74:16:34 eth12 Link encap:Ethernet HWaddr 98:4B:E1:74:16:36 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result

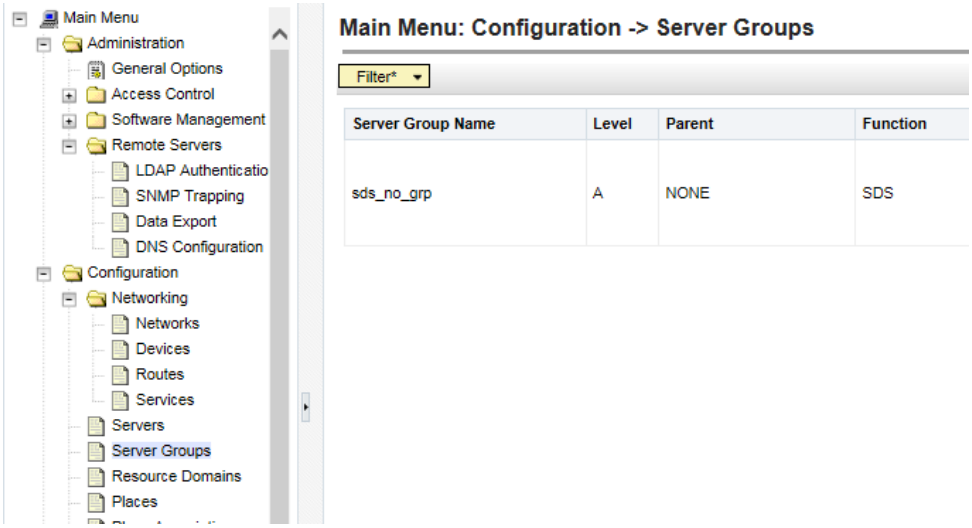
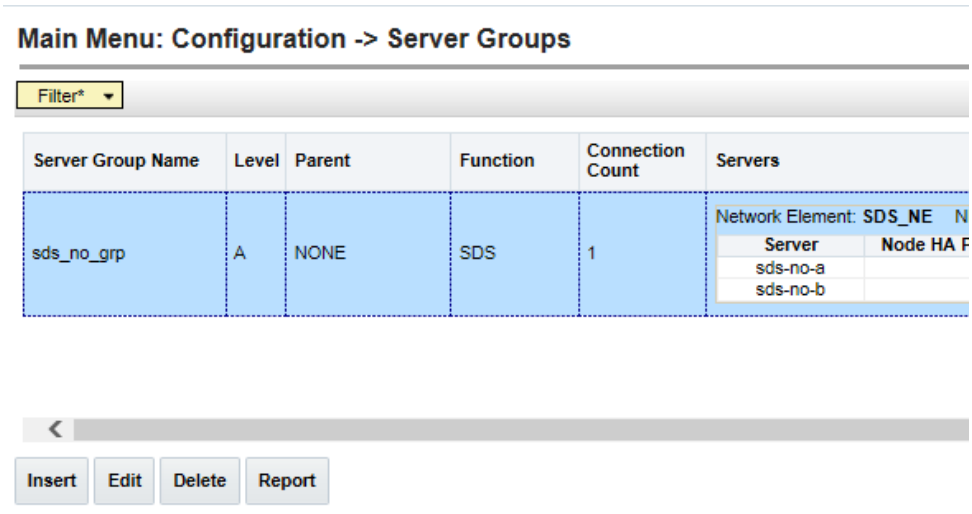
40. ☐	**Query Server:**
	From the **Query Server, "ping"** the **IMI IP address** configured for **SDS Server NOAM A**.
		`$ ping -c 5 169.254.100.11`
		`PING 169.254.100.11 (169.254.100.11) 56(84) bytes of data.`
		`64 bytes from 169.254.100.11: icmp_seq=1 ttl=64 time=0.021 ms`
		`64 bytes from 169.254.100.11: icmp_seq=2 ttl=64 time=0.019 ms`
		`64 bytes from 169.254.100.11: icmp_seq=3 ttl=64 time=0.006 ms`
		`64 bytes from 169.254.100.11: icmp_seq=4 ttl=64 time=0.019 ms`
		`64 bytes from 169.254.100.11: icmp_seq=5 ttl=64 time=0.006 ms`
		
		`--- 169.254.100.11 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 3999ms`
		`rtt min/avg/max/mdev = 0.006/0.014/0.021/0.007 ms`

41. ☐	**Query Server:**
	Use **"ping"** to verify that the **Query Server** can reach the configured **XMI Gateway address**.
		`$ ping -c 5 10.250.55.1`
		`PING 10.250.55.1 (10.250.55.1) 56(84) bytes of data.`
		`64 bytes from 10.250.55.1: icmp_seq=1 ttl=64 time=0.018 ms`
		`64 bytes from 10.250.55.1: icmp_seq=2 ttl=64 time=0.016 ms`
		`64 bytes from 10.250.55.1: icmp_seq=3 ttl=64 time=0.013 ms`
		`64 bytes from 10.250.55.1: icmp_seq=4 ttl=64 time=0.016 ms`
		`64 bytes from 10.250.55.1: icmp_seq=5 ttl=64 time=0.011 ms`
		
		`--- 10.250.55.1 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 3999ms`
		`rtt min/avg/max/mdev = 0.011/0.014/0.018/0.005 ms`

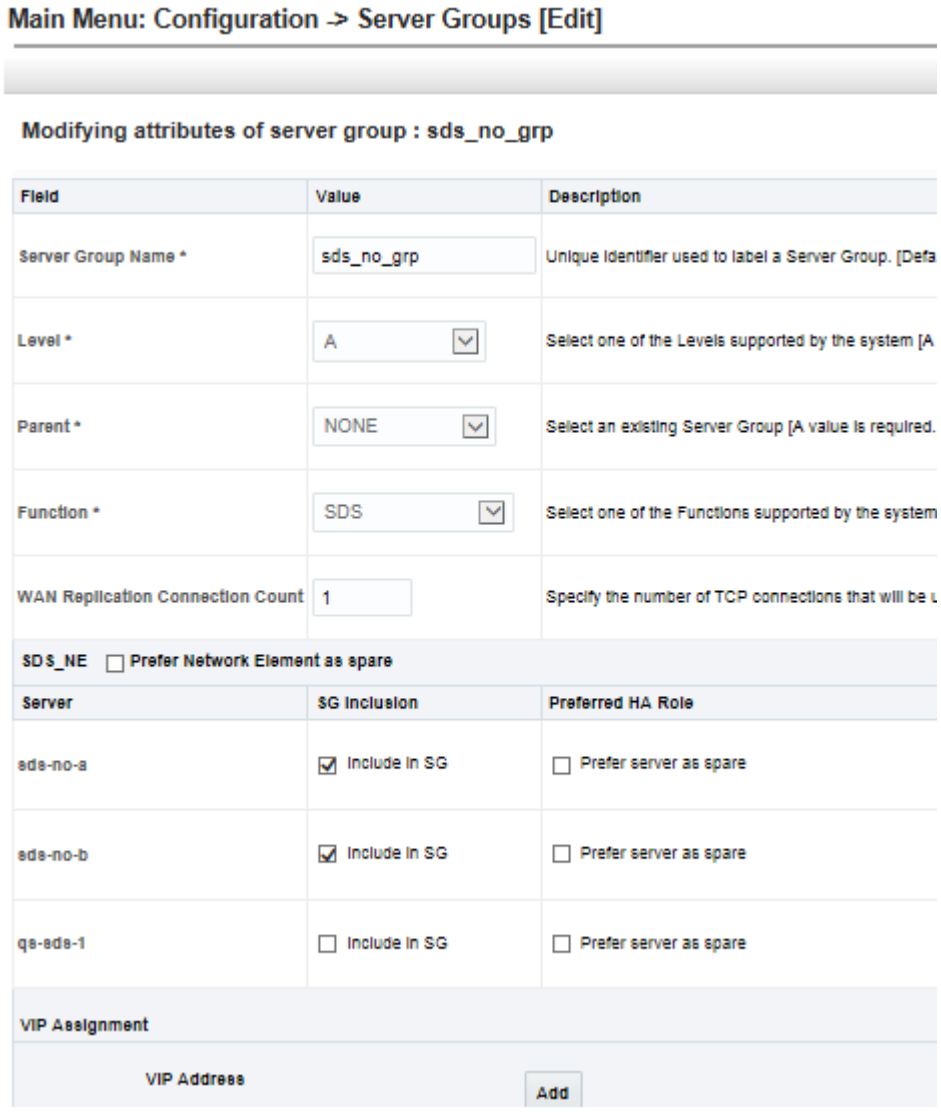
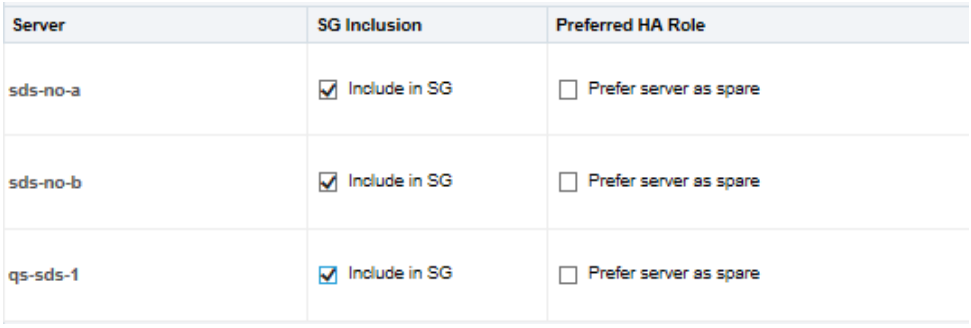
42. ☐	**Query Server:**
	Use the **"ntpq"** command to verify that the server has connectivity to the assigned NTP server(s).
		`$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`+10.250.32.10 192.5.41.209 2 u 184 256 175 0.220 46.852 35.598`
		`*10.250.32.51 192.5.41.209 2 u 181 256 377 0.176 7.130 22.192`

43. ☐	**Query Server:**
	Execute a **"syscheck"** to verify the current health of the server.
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`$`

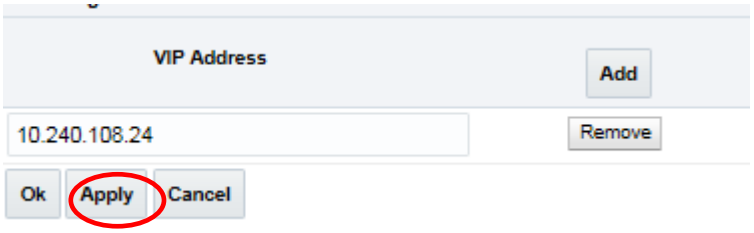
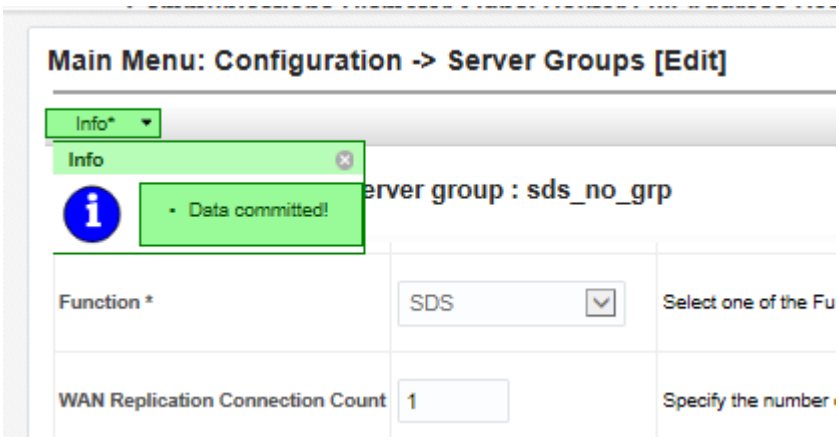
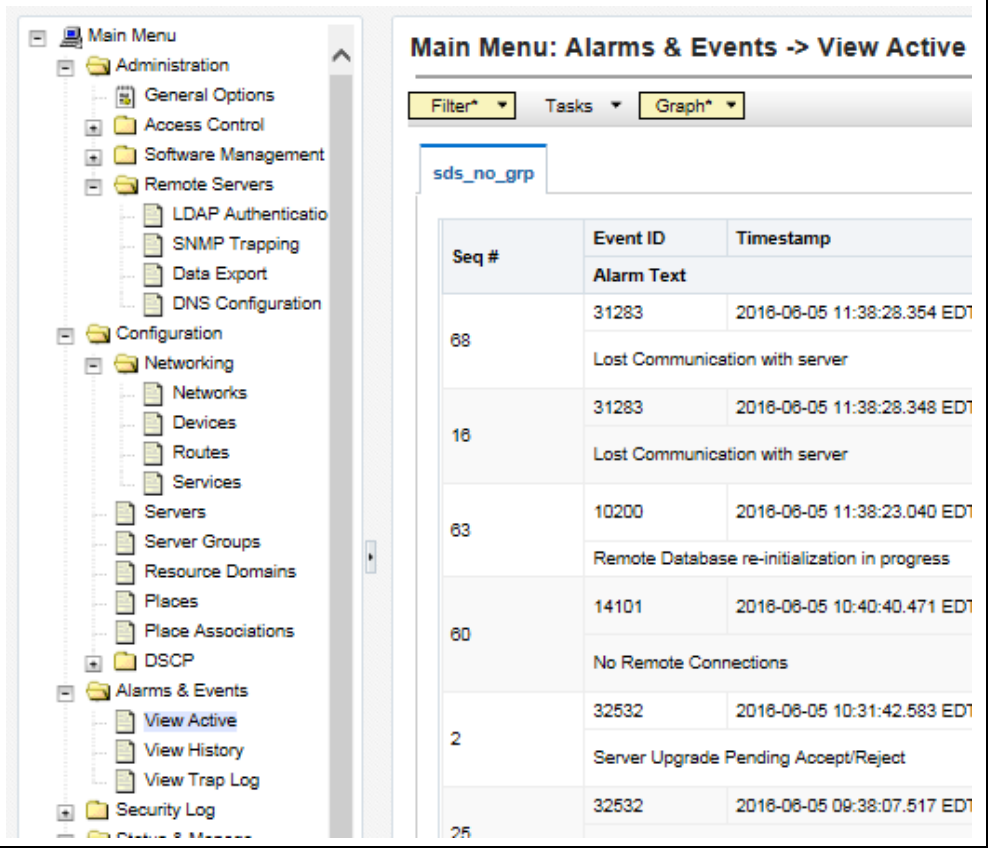
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
44. ☐	**Query Server:** Exit to the login prompt.	`$ exit`
45. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	
46. ☐	**Primary SDS VIP:** The user will be presented with the **"Configuration → Server Groups"** screen as shown on the right	
47. ☐	**Primary 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.	

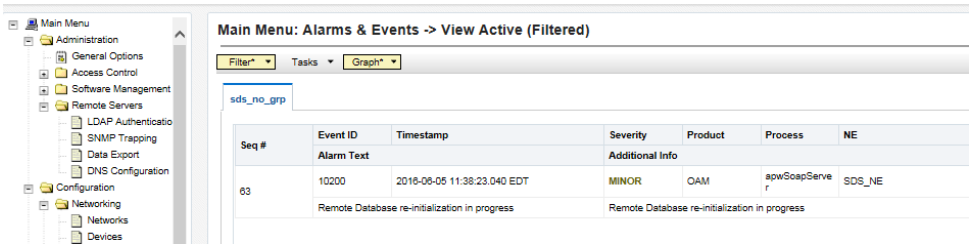
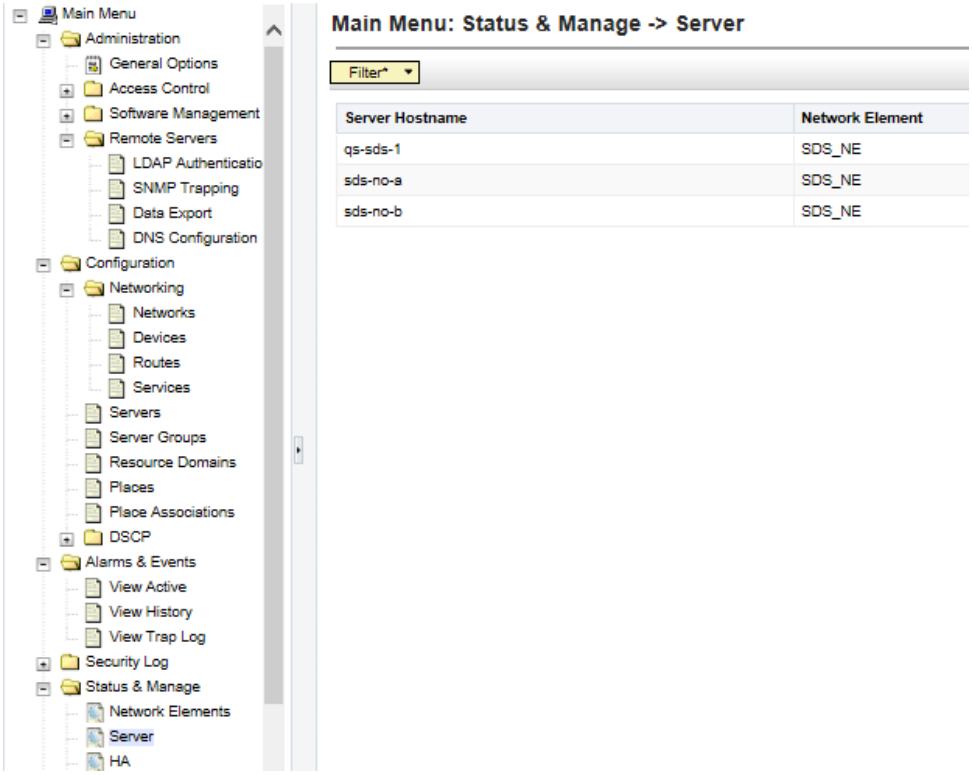
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
48. ☐	**Primary SDS VIP:** The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	
49.	**Primary SDS VIP:** Select the **"Query Server"** from the list of **"Available Servers in Network Element"** by clicking on the check box next to its name.	

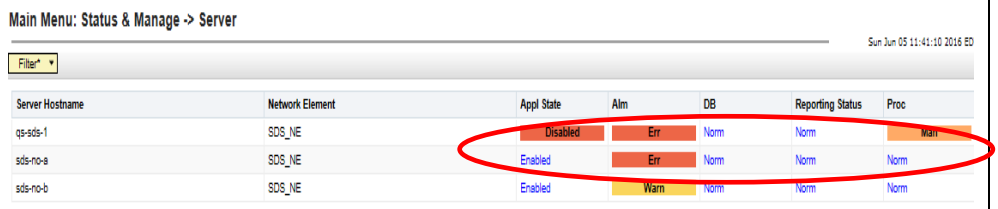
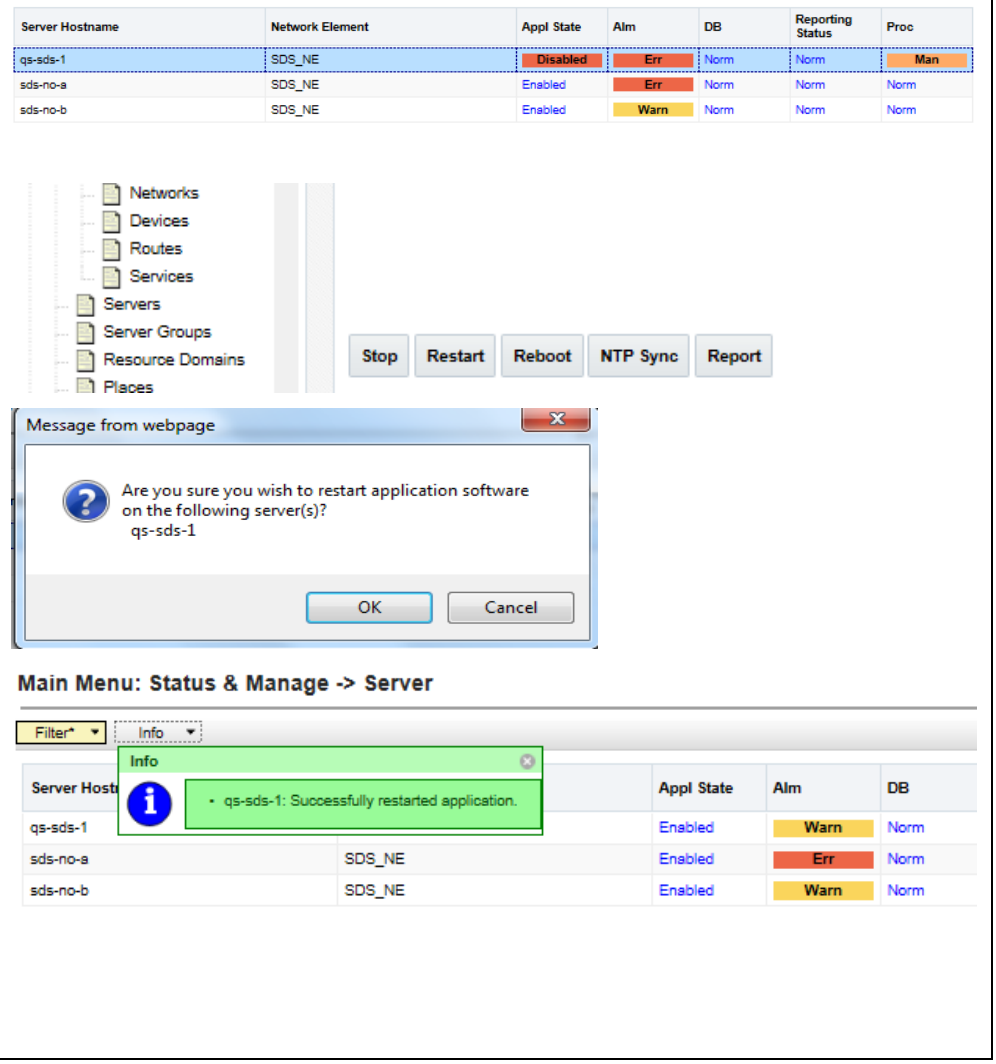
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
50. ☐	**Primary SDS VIP:** Click the **"Apply"** dialogue button from the bottom of the screen.	
51. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
52.	**Primary SDS VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	

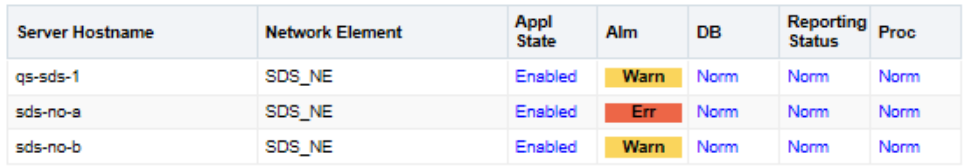
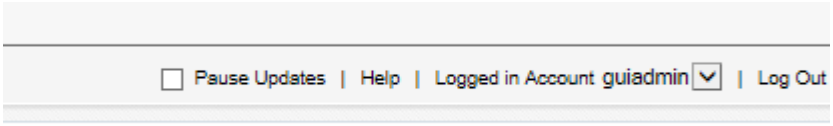
Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
53.	**SDS VIP:** Verify that **Event ID 10200** (*Remote Database re-initialization in progress)* is present with the **Query Server hostname** in the **"Instance"** field..	
	MONITOR EVENT ID 10200 (*Remote Database re-initialization in progress*). **DO NOT PROCEED TO THE NEXT STEP UNTIL THE ALARM CLEAR IS RECEIVED.**	
54. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	

Procedure 5. Configuring the Query Server (All SDS NOAM Sites)

Step	Procedure	Result
55. ☐	**Primary 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"**.	
56. ☐	**Primary SDS VIP:** **1)** Using the mouse, select the **"Query Server"** hostname. The line entry should now be highlighted. **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. Configuring the Query Server (All SDS NOAM Sites)

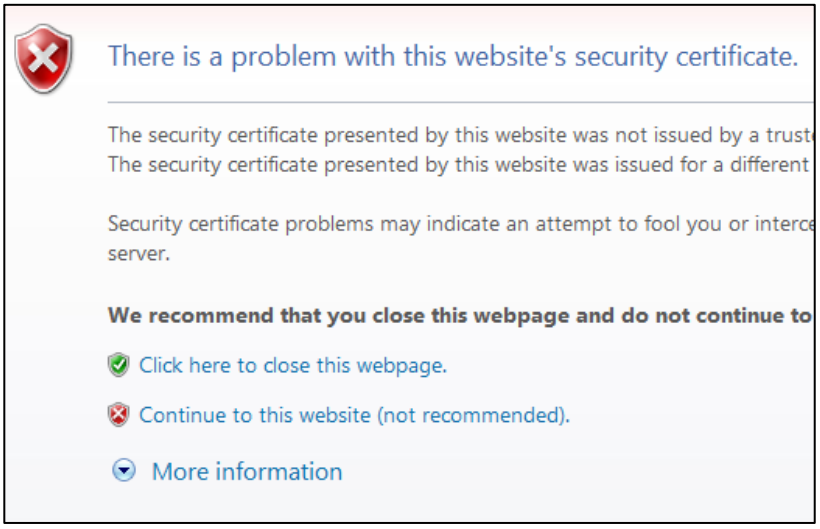
Step	Procedure	Result
57. ☐	**Primary SDS VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for the **"Query Server"**.	
58. ☐	**Primary SDS VIP:** Click the **"Logout"** link on the SDS server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

5.4 OAM Installation for the DR SDS NOAM Site

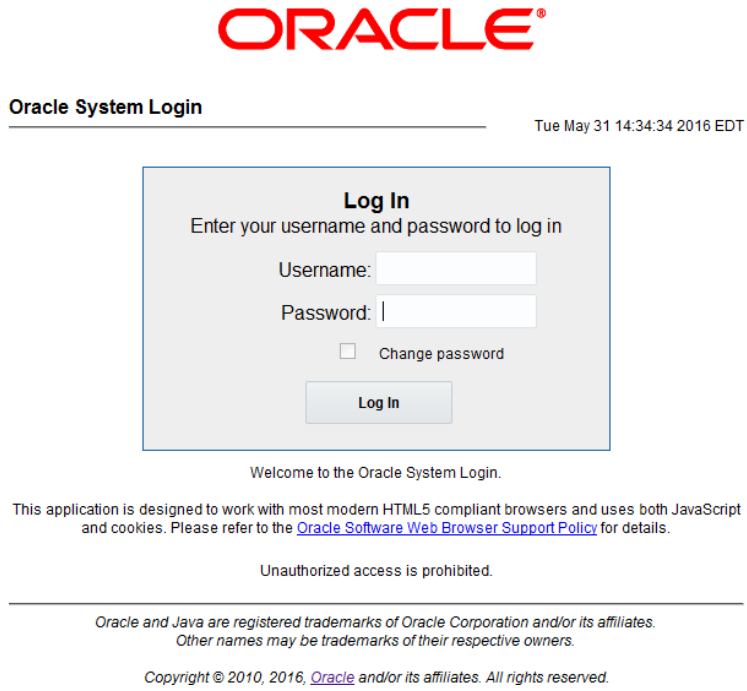
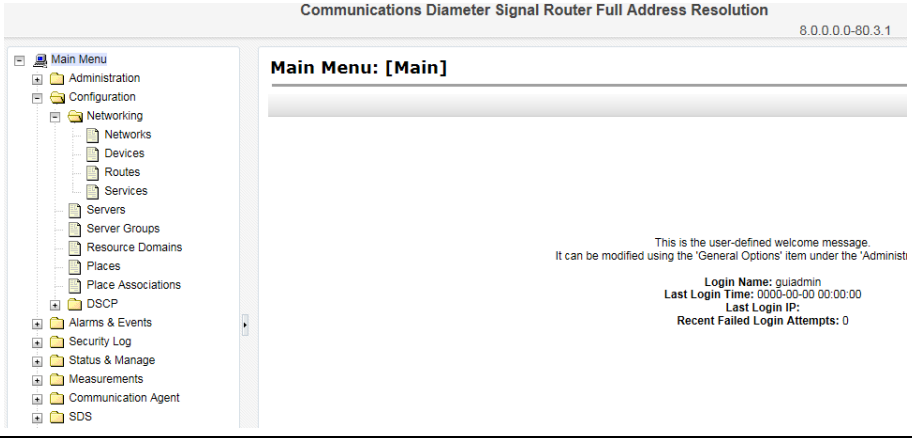
Assumptions:

- This procedure assumes that the SDS Network Element XML file for the Disaster Recovery SDS Provisioning site has previously been created, as described in **Appendix E.**
- This procedure assumes that the Network Element XML files are either on a USB flash drive or the laptop's hard drive. The steps are written as if the XML files are on a USB flash drive, but the files can exist on any accessible drive.

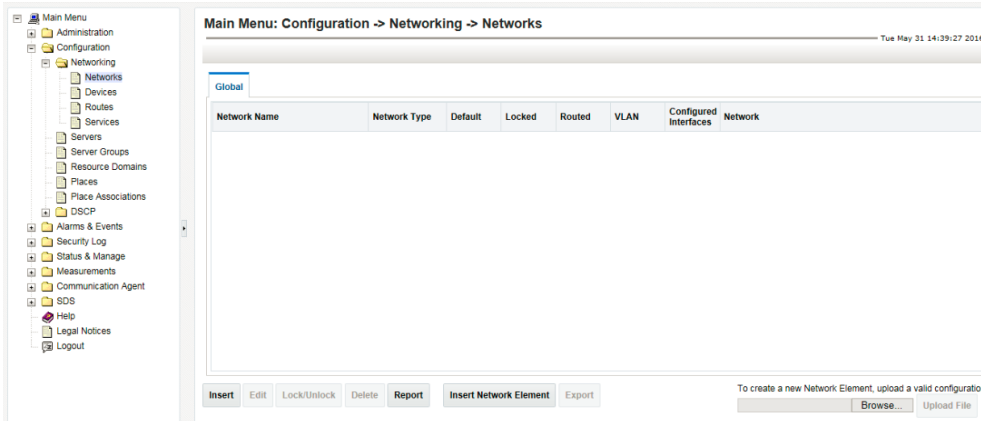
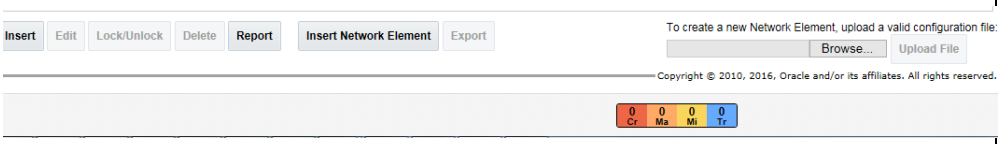
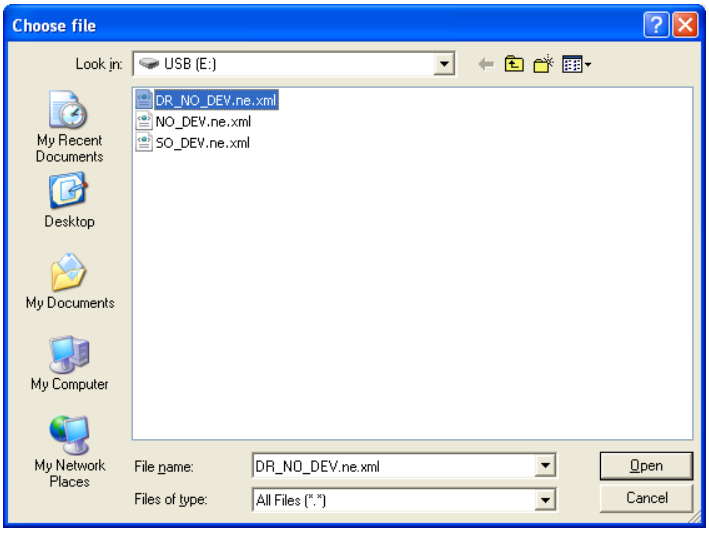
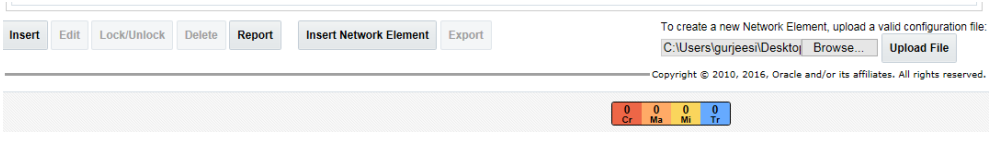
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
1. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP Address (VIP) of the Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	

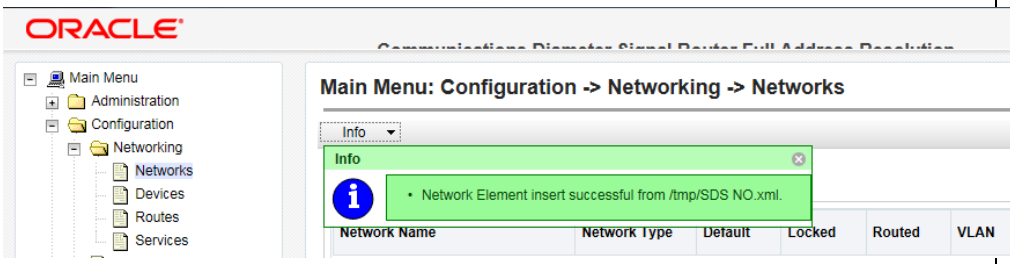
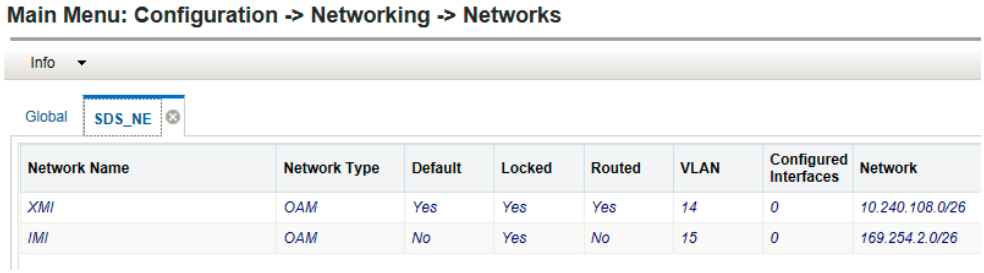
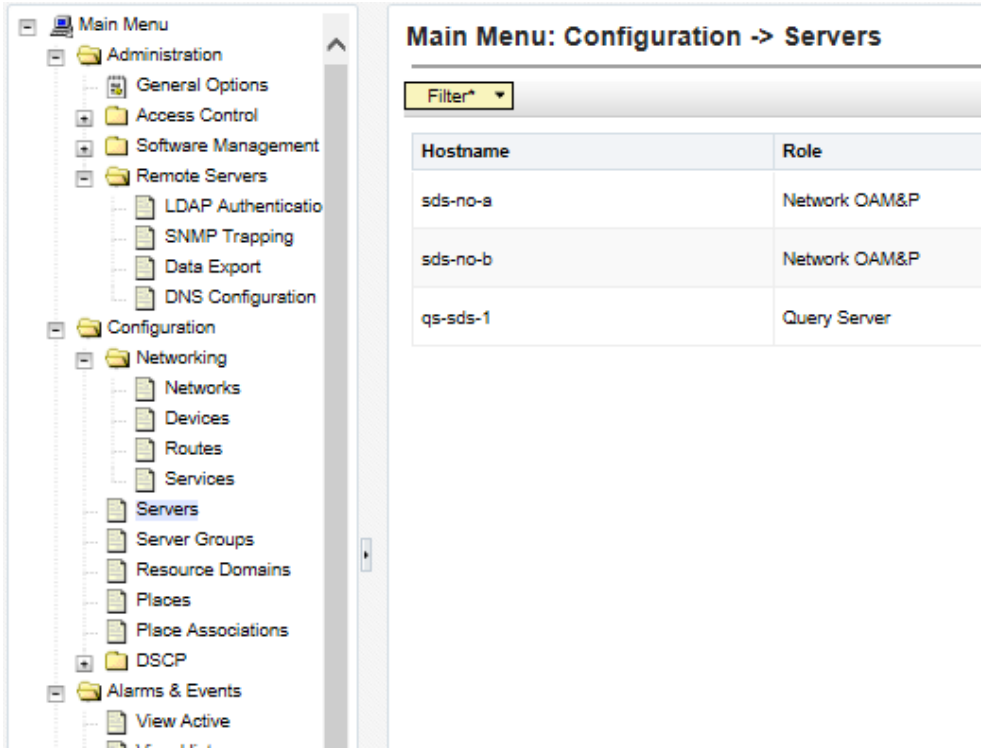
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
2. ☐	**Primary 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. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	

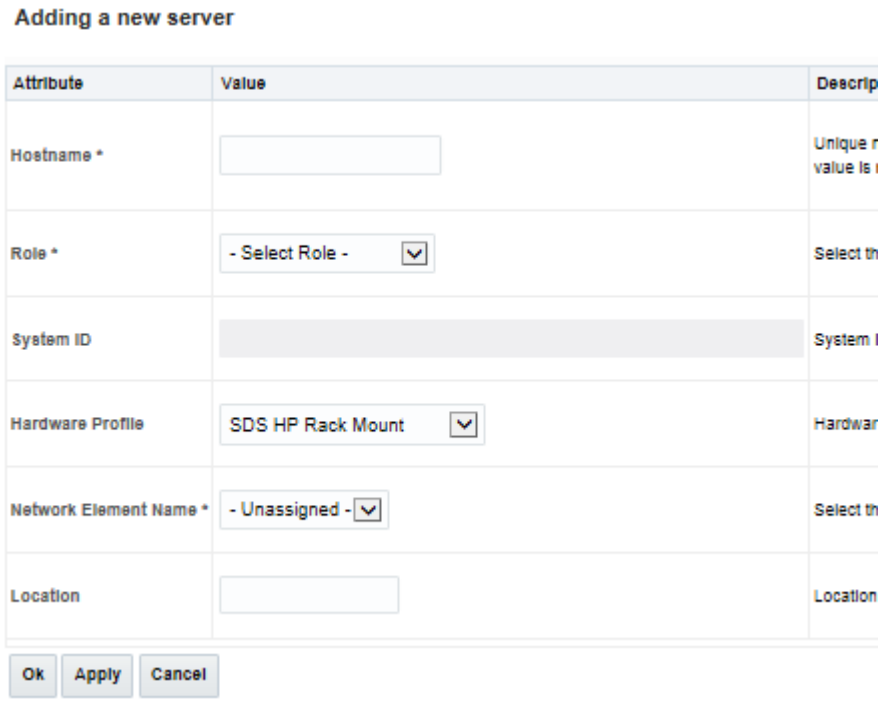
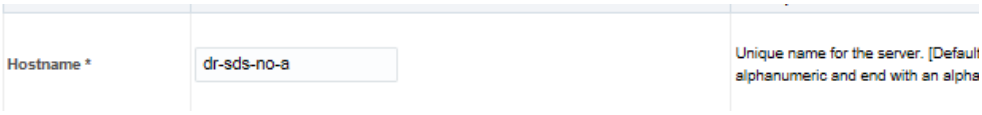
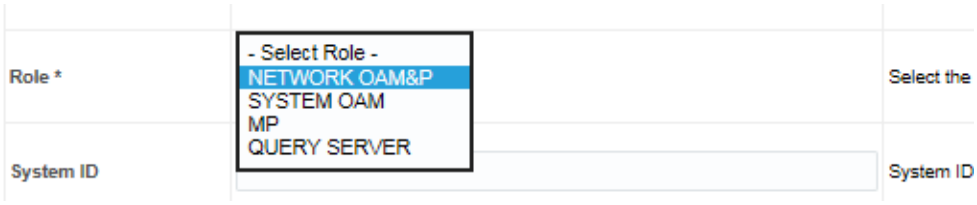
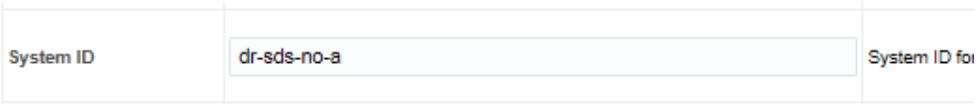
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
4.	**Primary SDS VIP:** Select… **<u>Main Menu</u>** → **Configuration** → ***Network Elements*** …as shown on the right.	
5. ☐	**Primary SDS VIP:** From the **Configuration / Network Elements** screen… Select the **"Browse"** dialogue button (scroll to bottom left corner of screen).	
6. ☐	**Primary SDS VIP:** **Note**: This step assumes that the **xml** files were previously prepared, as described in **Appendix E**. **1)** Select the location containing the site **.xml** file. **2)** Select the **.xml** file and click the **"Open"** dialogue button.	
7. ☐	**Primary SDS VIP:** Select the **"Upload File"** dialogue button (bottom left corner of screen).	

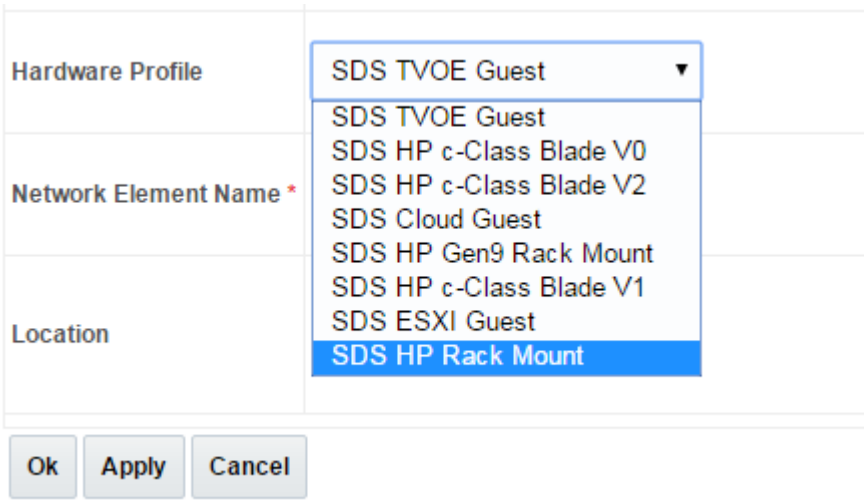
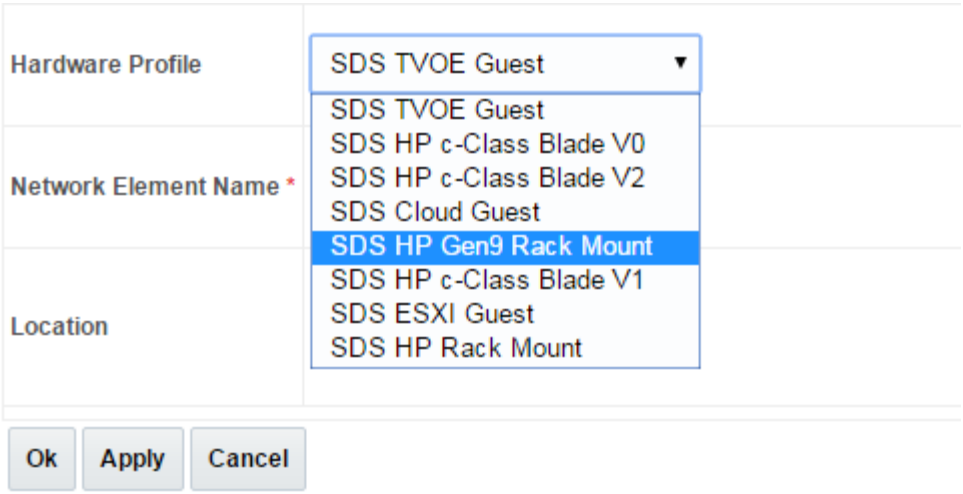
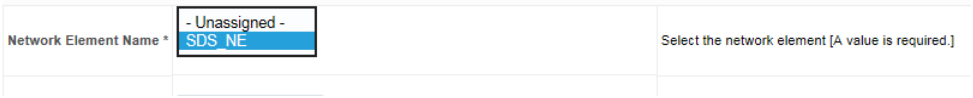
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
8. ☐	**Primary SDS VIP:** If the values in the **.xml** file pass validation rules, the user must select the Info box to receive a banner information message showing that the data has been successfully validated and committed to the DB.	 
9. ☐	**Primary SDS VIP:** **1)** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right. **2)** Select the **"Insert"** dialogue button (bottom left corner of screen).	

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
10. ☐	**Primary SDS VIP:** The user is now presented with the **"Adding a new server"** configuration screen.	
11. ☐	**Primary SDS VIP:** Input the assigned "**hostname"** for DR NOAM Server.	
12. ☐	**Primary SDS VIP:** Select **"NETWORK OAM&P"** for the server **"Role"** from the pull-down menu.	
13. ☐	**Primary SDS VIP:** Input the assigned hostname again as the "**System ID**" for the SDS DR Server (A or B).	

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
14. ☐	**Primary SDS VIP:** For **Gen8 Server:** Select "**SDS HP Rack Mount**" for the **Hardware Profile** for the SDS from the pull-down menu. For **Gen9 Server:** Select "**SDS HP Gen9 Rack Mount**" for the **Hardware Profile** for the SDS from the pull-down menu.	For Gen8 select "**SDS HP Rack Mount"** from the **Hardware Profile** pull-down menu.  For Gen9 select "**SDS HP Gen9 Rack Mount"** from the **Hardware Profile** pull-down menu. 
15. ☐	**Primary SDS VIP:** 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 17****.*
16. ☐	**Primary SDS VIP:** Enter the site location.	 **NOTE:** *Location is an optional field.*

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>17.</td><td>SDS Server NOAM A:

1) Enter the MGMNT_VLAN IP address for the DR SDS Server.

2) Set the MGMNT_VLAN Interface to “bond0” and “check” the VLAN checkbox.

3) Enter the IMI IP address for the DR SDS Server.

4) Set the IMI Interface to “bond0” and “check” the VLAN checkbox.</td><td> 

<table>
<tr><th>SDS Server
(DR NOAM)</th><th>Network</th><th>IP Address</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">DR SDS-A</td><td>MGMNT_VLAN</td><td>169.254.1.14</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.14</td></tr>
<tr><td rowspan="2">DR SDS-B</td><td>MGMNT_VLAN</td><td>169.254.1.15</td><td rowspan="2">bond0</td><td rowspan="2">✓</td></tr>
<tr><td>IMI</td><td>169.254.100.15</td></tr>
</table>
NOTE_1: These IP addresses are based on the info in the NAPD and the Network Element Config file.

NOTE_2: The MGMT_VLAN should only be present when 4948E-F AggregationSwitches are deployed with SDS NOAM / Query Server RMS. If the MGMT_VLAN is not present, the IMI network values shown above still apply.</td></tr>
<tr><td>18.</td><td>1) Enter the customer assigned XMI IP address for the DR SDS Server.

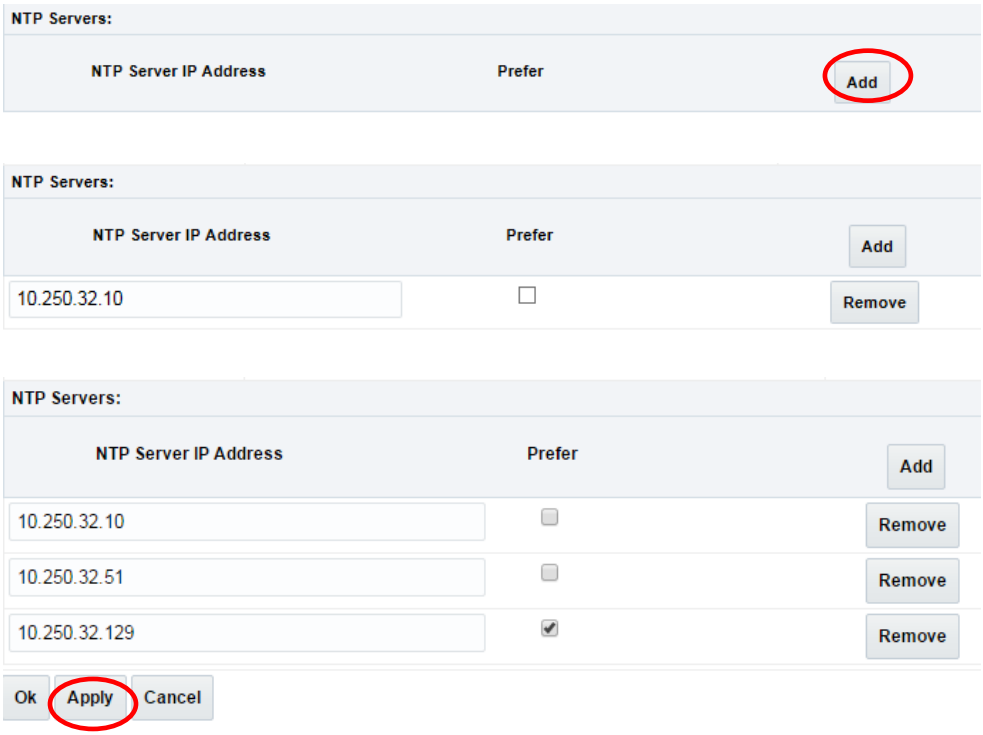
Layer 3
(No VLAN tagging used for XMI)

2) Set the XMI Interface to “bond1” and “DO NOT check” the VLAN checkbox.
- OR -

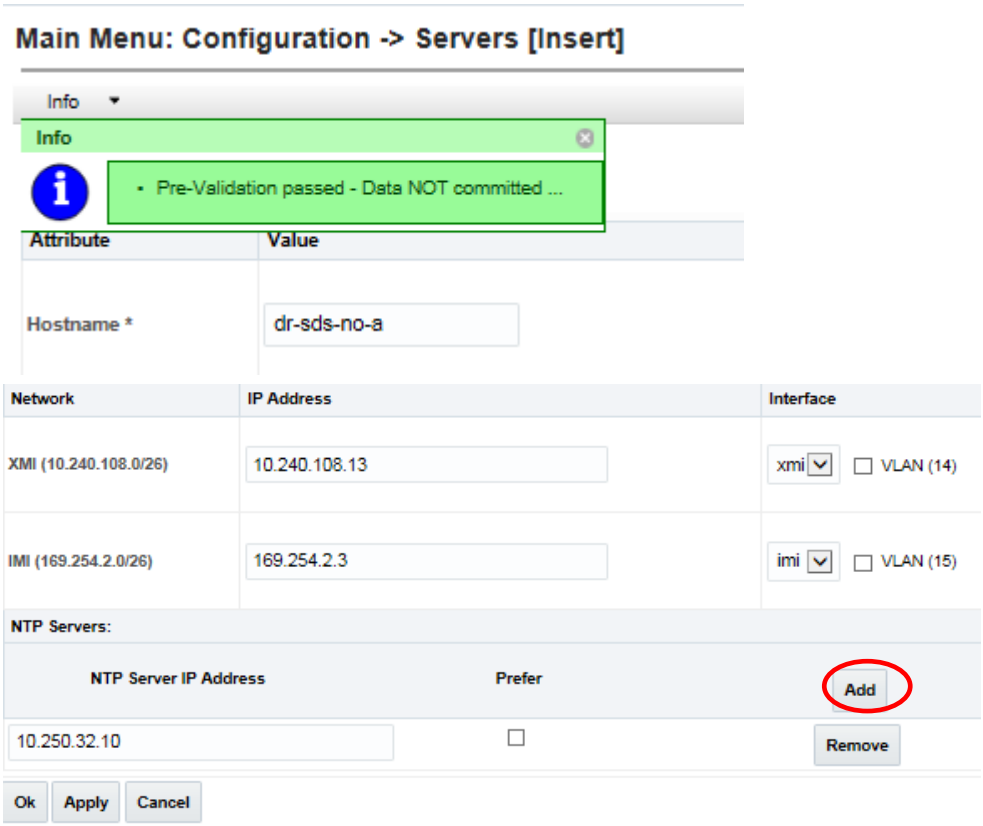
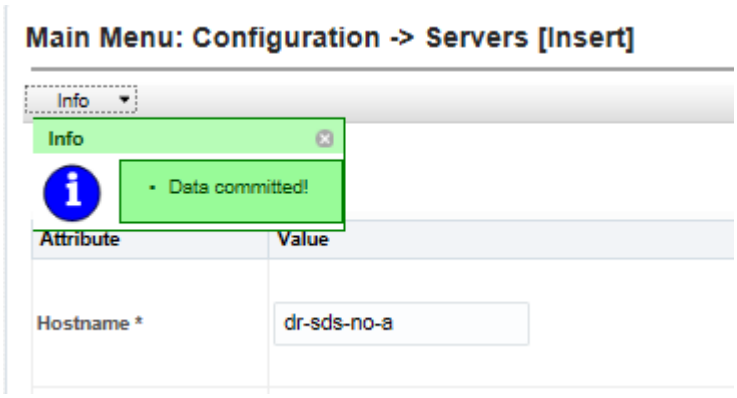
Layer 2
(VLAN tagging used for XMI)

2) Set the XMI Interface to “bond0” and “check” the VLAN checkbox.</td><td>
<table>
<tr><th>SDS Server
(DR NOAM)</th><th>Network</th><th>VLAN tagging
(on XMI network)</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">DR SDS NOAM Server
(A or B)</td><td rowspan="2">XMI</td><td>No</td><td>bond1</td><td>✗</td></tr>
<tr><td>Yes</td><td>bond0</td><td>✓</td></tr>
</table>
!!! CAUTION !!!
It is crucial that the correct network configuration be selected in Steps 17 & 18 of this procedure. Choosing an incorrect configuration will result in the need to re-install the OS and restart the DR SDS instalation procedures over from the beginning.</td></tr>
</table>

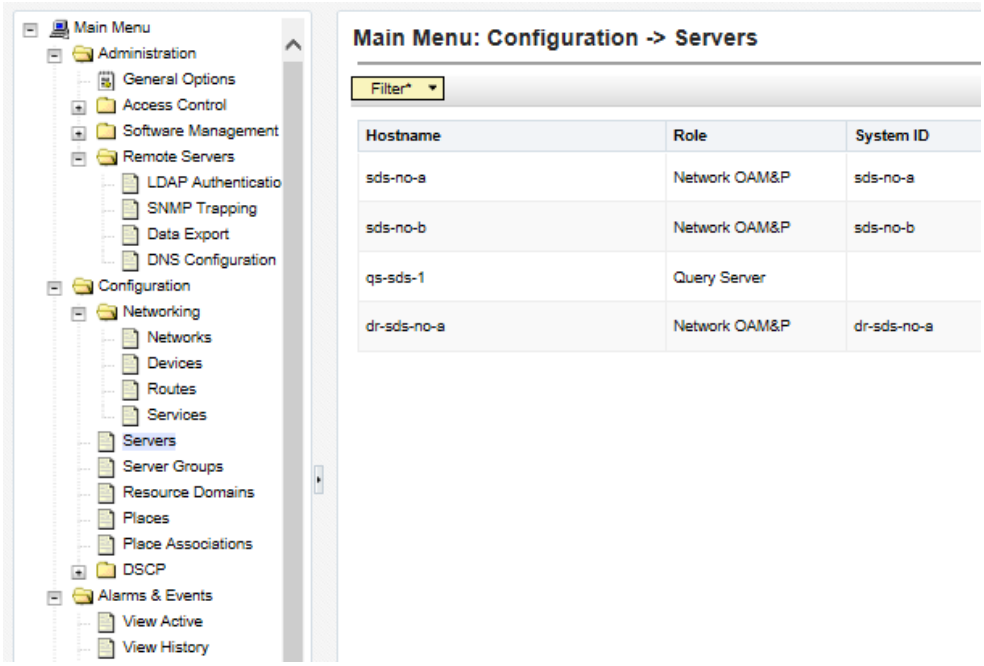
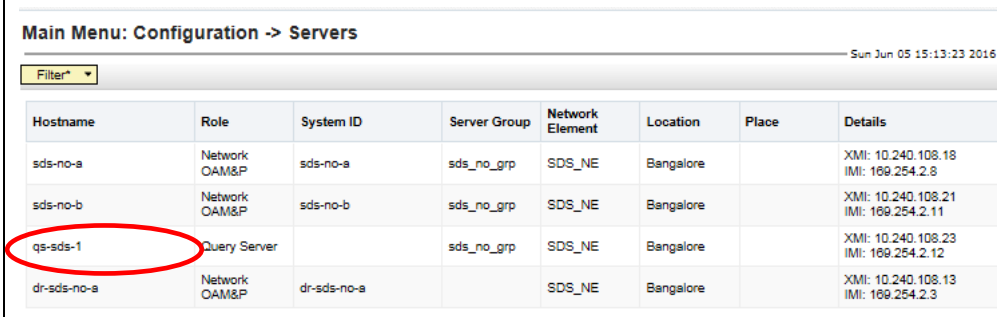
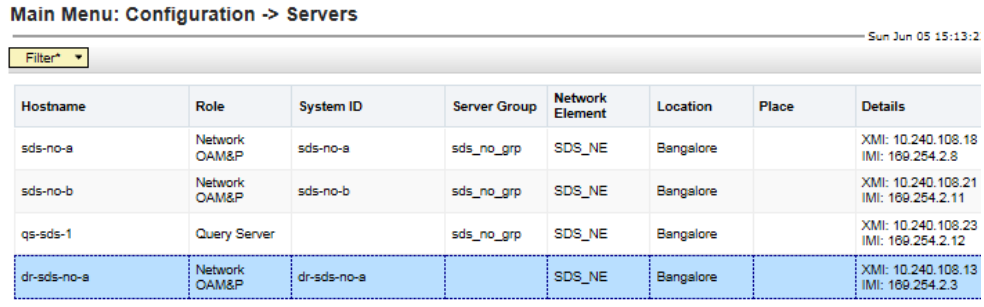
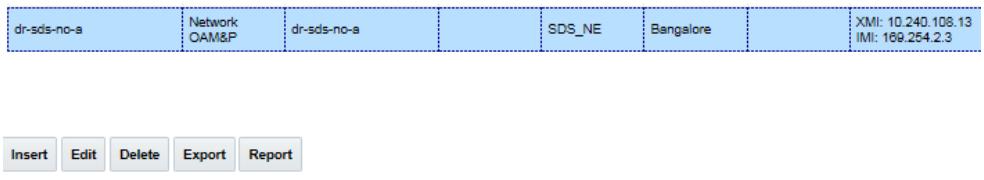
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
19. ☐	**SDS Server NOAM A:** **1)** Click the "**NTP Servers:**" **"Add"** dialogue button. **2)** Enter the **NTP Server IP Address** for an NTP Server. **3)** Enter 3 NTP Server **IP address**, repeat (1) and (2) to enter it. **4)** Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other.	

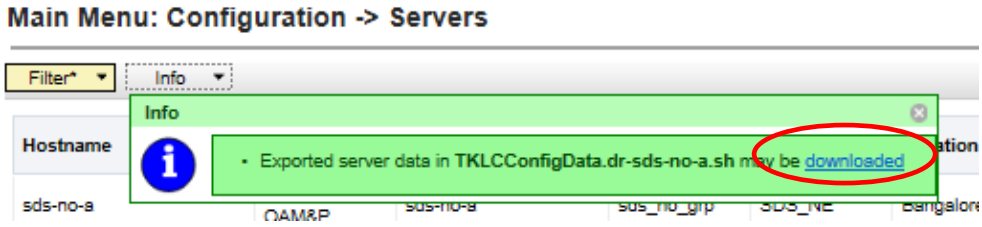
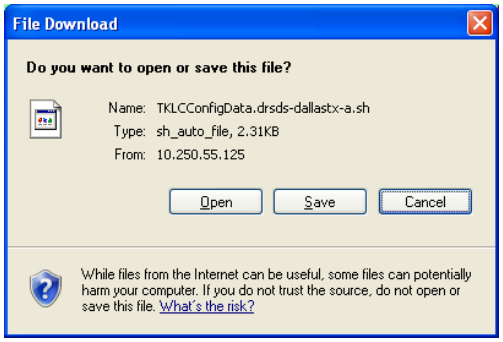
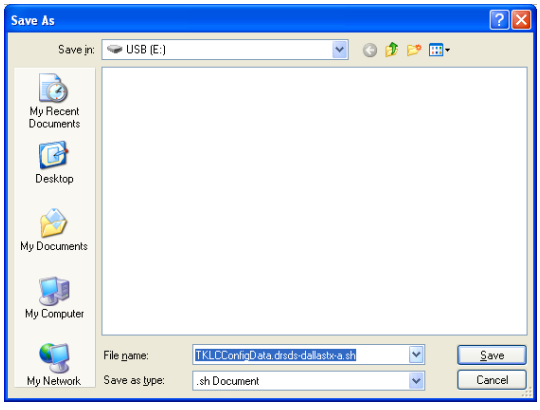
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
20. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"Apply"** dialogue button.	
21. ☐	**Primary SDS VIP:** If the values provided match the network ranges assigned to the NE, the user must select the Info box to receive a banner information message showing that the data has been committed to the DB.	

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
22. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right.	
23. ☐	**Primary SDS VIP:** On the **"Configuration →Servers" screen**, find the newly added DR NOAM server in the list.	
24. ☐	**Primary SDS VIP:** Use the cursor to select the new DR NOAM server entry added in the **Steps10 – 21**. The row containing the server should now be highlighted.	
25. ☐	**Primary SDS VIP:** Select the **"Export"** dialogue button (bottom left corner of screen).	

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
26. ☐	**Primary SDS VIP:** The user must select the Info box to receive a banner information message showing a download link for the Server configuration data. Click on the word **"downloaded"** to download and save the **SDS DR NOAM** server configuration file.	
27. ☐	**Primary SDS VIP:** **1)** Click the "Save" dialogue button. **2)** Save the **SDS DR NOAM** server configuration file to a USB flash drive.	 
28. ☐	**SDS DR NOAM Server:** Access the server console.	Connect to the **SDS DR NOAM Server** console using one of the access methods described in **Section 2.3.**

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result

29. ☐	**SDS DR NOAM Server:**
	
	1) Access the command prompt.
	
	2) Log into the server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

30. ☐	**SDS DR NOAM Server:** Insert the USB flash drive containing the server configuration file into the USB port on the front panel of the server.	 **Figure 12 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 13 – HP DL380 Gen9: Front Panel (USB Port)**

31. ☐	**SDS DR NOAM Server:**
	
	Output similar to that shown on the right will appear as the USB flash drive is inserted into the **SDS Server** front USB port.
		`$ sd 3:0:0:0: [sdb] Assuming drive cache: write through`
		`sd 3:0:0:0: [sdb] Assuming drive cache: write through <ENTER>`
		
		NOTE: *Press the **<ENTER>** key to return to the command prompt.*

32. ☐	**SDS DR NOAM Server:** Verify that the USB flash drive's partition has been mounted by the OS	`$ df |grep sdb` `/dev/sdb1  2003076  8  2003068  1% /media/sdb1`

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
33. ☐	**SDS DR NOAM Server:** Copy the configuration file to the SDS server with the server name as shown in red	`$ sudo cp -p /media/sdb1/TKLCConfigData.dr-sds-no-a.sh /var/TKLC/db/filemgmt/.`
34. ☐	**SDS DR NOAM Server:** 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.	***Example:*** TKLCConfigData<.server_hostname>.sh ➔ will translate to ➔TKLCConfigData.sh `$ sudo cp -p /var/TKLC/db/filemgmt/TKLCConfigData.dr-sds-no-a.sh /var/tmp/TKLCConfigData.sh` **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

35. ☐	**SDS DR NOAM Server:**
	
	After the script completes, a broadcast message will be sent to the terminal.
		***** NO OUTPUT FOR ≈ 3-20 MINUTES *****
		
		`Broadcast message from admusr (Mon Dec 14 15:47:33 2009):`
		
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		
		`Please remove the USB flash drive if connected and reboot the server.`
		<ENTER>
		
		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.*

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
36. ☐	**SDS DR NOAM Server:** Remove the USB flash drive from the USB port on the front panel of **OAM server**. **CAUTION:** *It is important that the USB flash drive be removed from the server before continuing on to the next step.*	 **Figure 14 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 15 – HP DL380 Gen9: Front Panel (USB Port)**
37.	**SDS Server NOAM A or B:** Verify that the desired Time Zone is currently in use.	`$ date` `Mon Aug 10 19:34:51 UTC 2015`
38. ☐	**SDS Server NOAM A or B:** If the desired Time Zone was not presented in the previous step… **Configure the Time Zone.** Otherwise, skip to the next step.	***Example:*** `$ sudo set_ini_tz.pl <time_zone>` **NOTE:** *The following command example sets the time to the "UTC" (aka GMT) time zone which is recommneded for all sites.* *The user may replace, as appropriate, with the customer requested time zone for this site installation. See **Appendix G** for a list of valid time zones.* `$ sudo set_ini_tz.pl "Etc/UTC"`
39. ☐	**Server NOAM A:** Initiate a reboot of the OAM server.	`$ sudo init 6`

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
40. ☐	**SDS DR NOAM Server:** Wait ~9 minutes Output similar to that shown on the right may be observed as the server initiates a reboot.	[root@hostname1322679281 ~]# init 6 [root@hostname1322679281 ~]# bonding: bond0: Removing slave eth02 bonding: bond0: Warning: the permanent HWaddr of eth02 - 98:4B:E1:6F:74:56 - i still in use by bond0. Set the HWaddr of eth02 to a different address to avoid onflicts. bonding: bond0: releasing active interface eth02 bonding: bond0: making interface eth12 the new active one. bonding: bond0: Removing slave eth12 bonding: bond0: releasing active interface eth12 e1000e 0000:07:00.0: eth12: changing MTU from 1500 to 1500 bonding: bond1: Removing slave eth01
41. ☐	**SDS DR NOAM Server:** **1)** After the reboot, access the command prompt. **2)** Log into the server as the "**admusr**" user.	login: **admusr** Using keyboard-interactive authentication. Password: ***<admusr_password>***
42. ☐	**SDS DR NOAM *Server:*** ***1)** Verify that the **IMI IP address** input in **Step 18** has been applied to **"bond0.4"**.* ***2)** Verify that the **XMI IP address** input in **Step 17** has been applied to **"bond1"**.*	$ **ifconfig |grep in** bond0 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2C bond0.4 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2C inet addr:169.254.100.14 Bcast:169.254.100.255 Mask:255.255.255.0 bond1 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2E inet addr:10.250.55.161 Bcast:10.250.55.255 Mask:255.255.255.0 eth01 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2C eth02 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2E eth11 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2C eth12 Link encap:Ethernet HWaddr 98:4B:E1:74:15:2E lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0
43. ☐	**SDS DR NOAM Server B:** Use the **"ntpq"** command to verify that the server has connectivity to the assigned Primary and Secondary NTP server(s).	$ **ntpq -np** remote refid st t when poll reach delay offset jitter ========== +10.250.32.10 192.5.41.209 2 u 59 64 377 0.142 -2468.3 99.875 *10.250.32.51 192.5.41.209 2 u 58 64 377 0.124 -2528.2 128.432

Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
	IF CONNECTIVITY TO THE NTP SERVER(S) CANNOT BE ESTABLISHED, STOP AND EXECUTE THE FOLLOWING STEPS: **1)** Contact the customer to verify that the IP addresses for the NTP server(s) are correct. **2)** Have the customer IT group provide a network path from the OAM server IP to the assigned NTP IP addresses. **ONCE NETWORK CONNECTIVITY IS ESTABLISHED TO THE ASSIGNED NTP IP ADDRESSES, THEN RESTART THIS PROCEDURE BEGINNING WITH STEP 44.**	

44. ☐	**SDS DR NOAM Server:**
	
	Execute a **"syscheck"** to verify the current health of the server.
		`$ sudo syscheck`
		`Running modules in class hardware... OK`
		`Running modules in class disk... OK`
		`Running modules in class net... OK`
		`Running modules in class system... OK`
		`Running modules in class proc... OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

45. ☐	**SDS DR NOAM Server:** Exit from the command line to return the server console	`$ exit` `logout`
46. ☐	• **Configure DR SDS Server B by repeating steps 9 – 45 of this procedure.**	
	IF 4948E-F SWITCH CONFIGURATION HAS NOT BEEN COMPLETED PRIOR TO THIS STEP, STOP AND EXECUTE THE FOLLOWING STEPS: **4) APPENDIX D-1** ***5)*** **APPENDIX D-2** *(Appendix **D.2** references Appendix **D.3** where applicable).* **6) APPENDIX D-4**	

47. ☐	**DR SDS Server NOAM A:**
	
	From **DR SDS Server NOAM A, "ping"** the **IMI** IP address **DR SDS NOAM Server B**.
		`$ ping -c 5 169.254.100.15`
		`PING 169.254.100.14 (169.254.100.15) 56(84) bytes of data.`
		`64 bytes from 169.254.100.15: icmp_seq=1 ttl=64 time=0.021 ms`
		`64 bytes from 169.254.100.15: icmp_seq=2 ttl=64 time=0.011 ms`
		`64 bytes from 169.254.100.15: icmp_seq=3 ttl=64 time=0.020 ms`
		`64 bytes from 169.254.100.15: icmp_seq=4 ttl=64 time=0.011 ms`
		`64 bytes from 169.254.100.15: icmp_seq=5 ttl=64 time=0.023 ms`**<CTRL-C>**
		
		`--- 169.254.100.15 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 3999ms`
		`rtt min/avg/max/mdev = 0.011/0.017/0.023/0.005 ms`

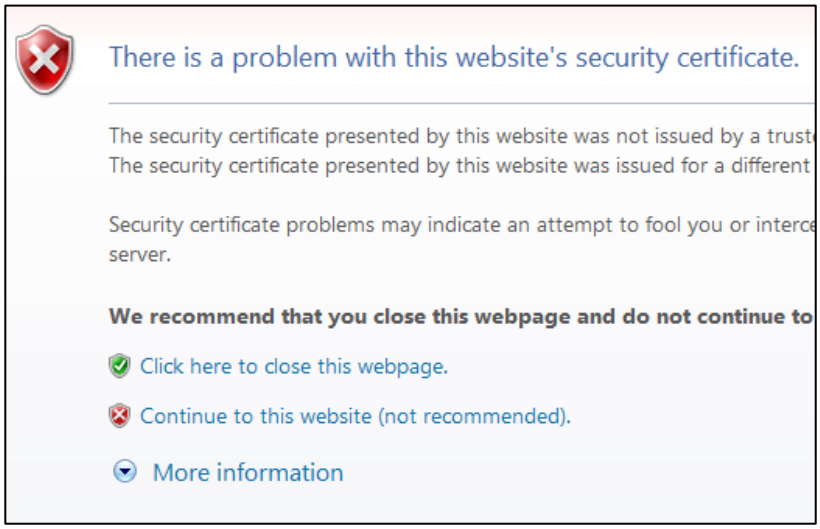
Procedure 6. Configuring the DR NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
48. ☐	**DR SDS NOAM Server(s):** **A & B** Use **"ping"** to verify that the **DR SDS NOAM Server** can now reach the local **XMI Gateway address**.	$ **ping 10.250.55.161** PING 10.250.55.161 (10.250.55.161) 56(84) bytes of data. 64 bytes from 10.250.55.161: icmp_seq=1 ttl=64 time=0.021 ms 64 bytes from 10.250.55.161: icmp_seq=2 ttl=64 time=0.017 ms 64 bytes from 10.250.55.161: icmp_seq=3 ttl=64 time=0.017 ms 64 bytes from 10.250.55.161: icmp_seq=4 ttl=64 time=0.022 ms 64 bytes from 10.250.55.161: icmp_seq=5 ttl=64 time=0.012 ms**<CTRL-C>** --- 10.250.55.161 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 3999ms rtt min/avg/max/mdev = 0.012/0.017/0.022/0.006 ms
49.	**DR SDS Server(s):** **A & B** Use **"ping"** to verify that the **DR SDS Server** can now reach the **Primary SDS VIP address**.	$ **ping -c 5 10.250.55.126** PING 10.250.55.126 (10.250.55.126) 56(84) bytes of data. 64 bytes from 10.250.55.126: icmp_seq=1 ttl=64 time=0.021 ms 64 bytes from 10.250.55.126: icmp_seq=2 ttl=64 time=0.017 ms 64 bytes from 10.250.55.126: icmp_seq=3 ttl=64 time=0.017 ms 64 bytes from 10.250.55.126: icmp_seq=4 ttl=64 time=0.022 ms 64 bytes from 10.250.55.126: icmp_seq=5 ttl=64 time=0.012 ms**<CTRL-C>** --- 10.250.55.126 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 3999ms rtt min/avg/max/mdev = 0.012/0.017/0.022/0.006 ms
THIS PROCEDURE HAS BEEN COMPLETED		

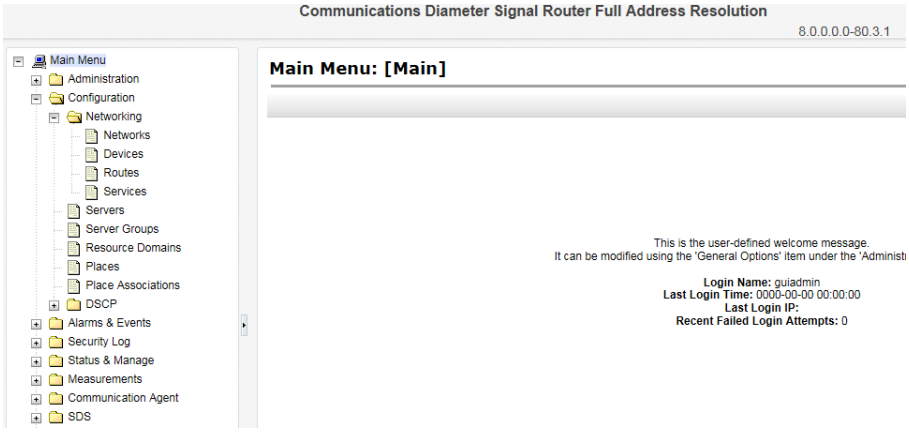
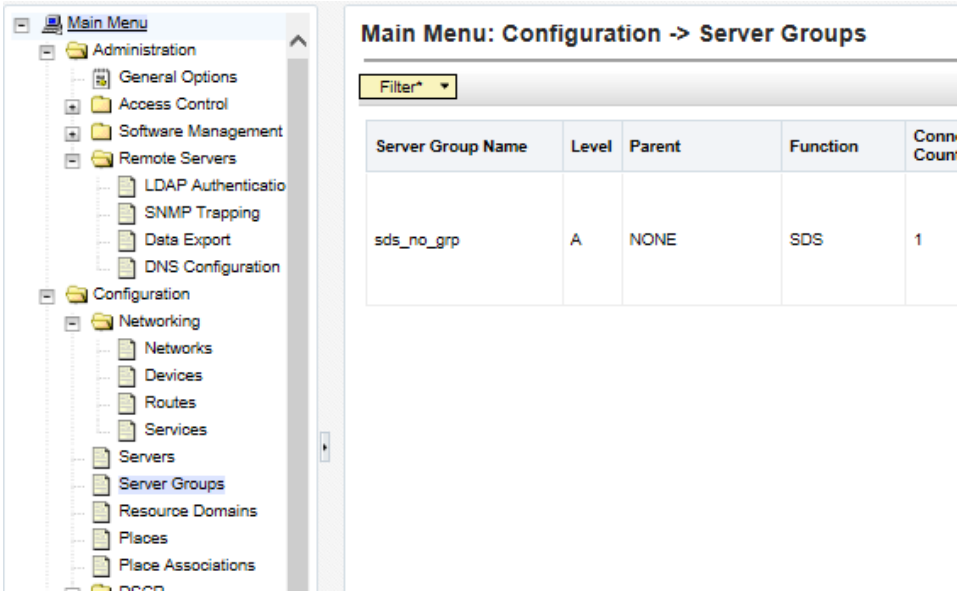
5.5 OAM Pairing for DR SDS NOAM Site

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.

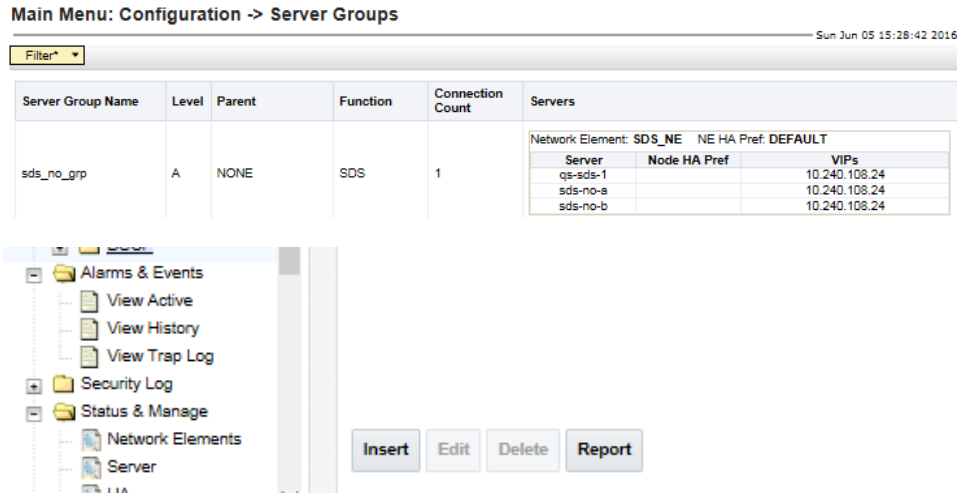
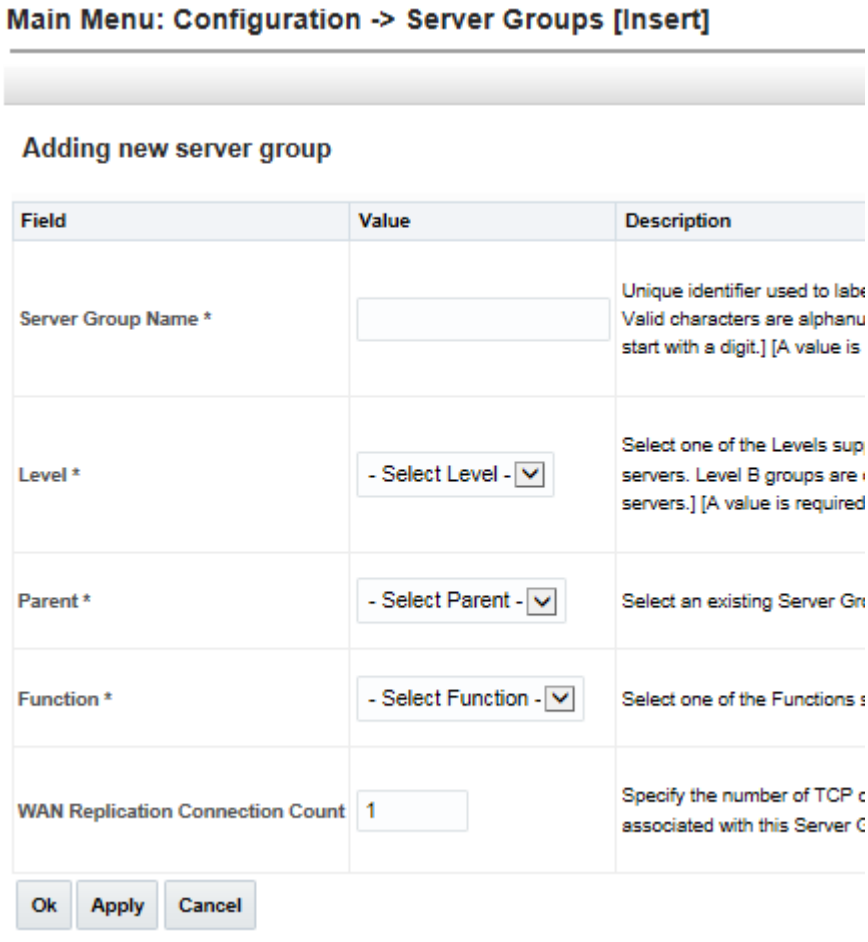
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
1. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP Address (VIP) of the Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**Primary SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

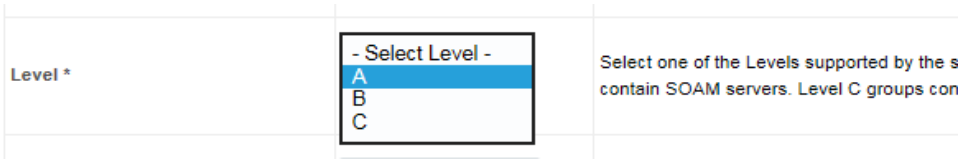
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
3. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	
4. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	

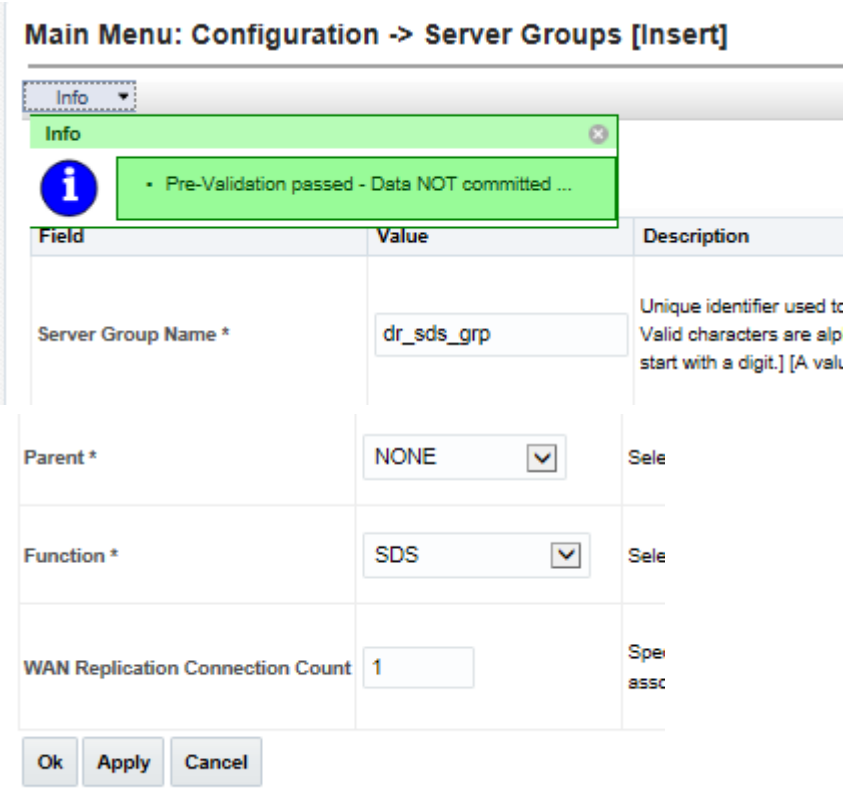
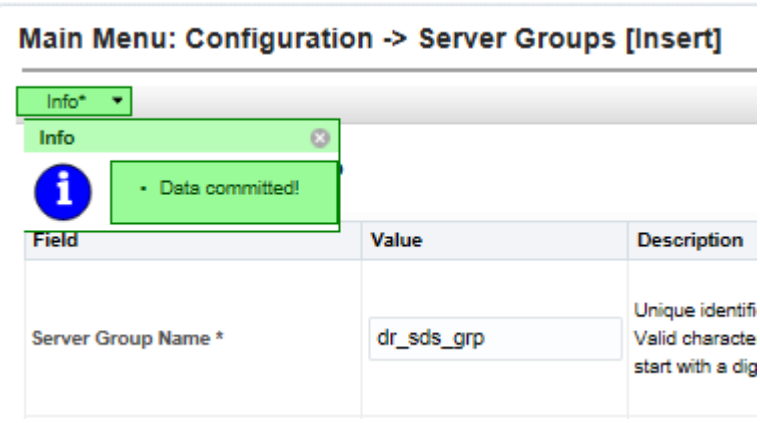
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
5. ☐	**Primary 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.	
6. ☐	**Primary 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).*	

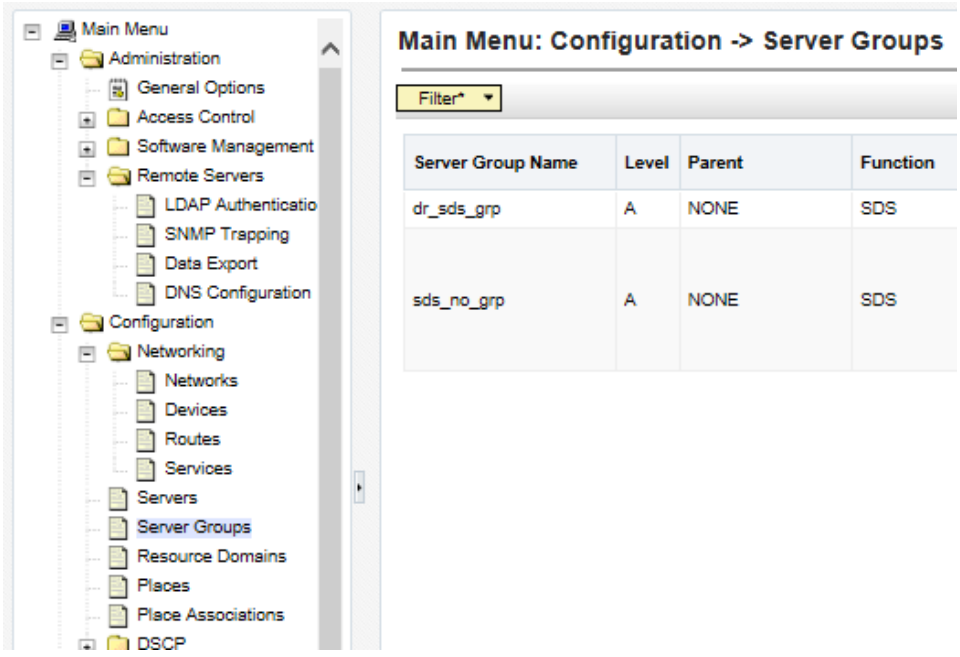
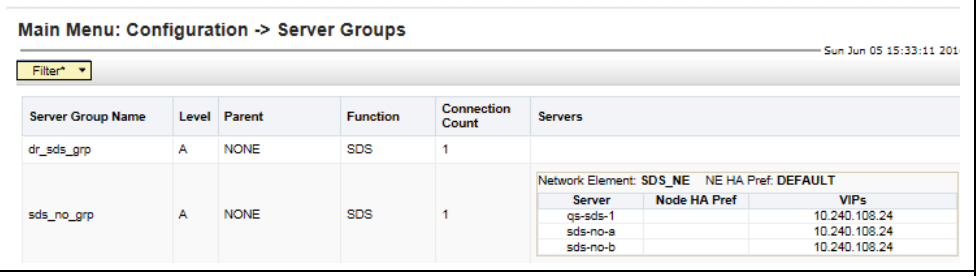
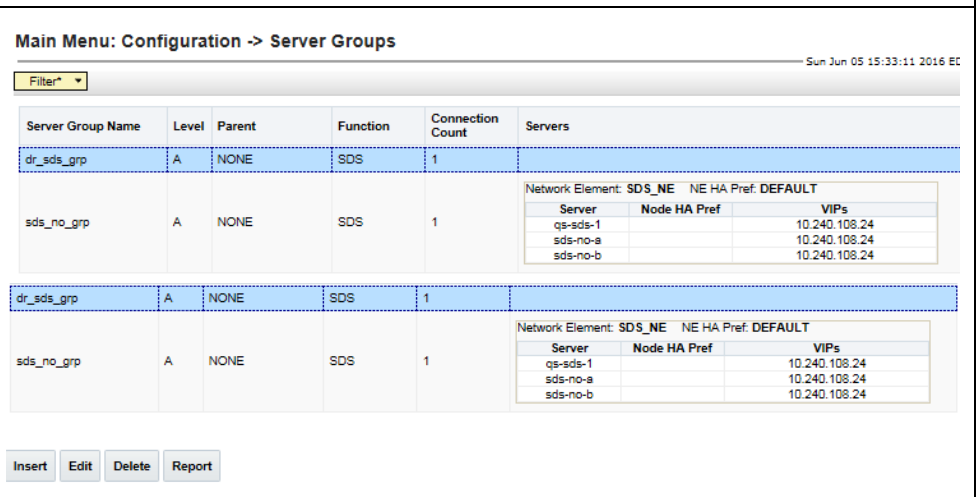
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
7. ☐	**Primary SDS VIP:** Input the **Server Group Name**.	
8. ☐	**Primary SDS VIP:** Select **"A"** on the **"Level"** pull-down menu.	
9. ☐	**Primary SDS VIP:** Select Parent **"NONE"** on the pull-down menu.	
10. ☐	**Primary SDS VIP:** Select **"SDS"** on the **"Function"** pull-down menu.	

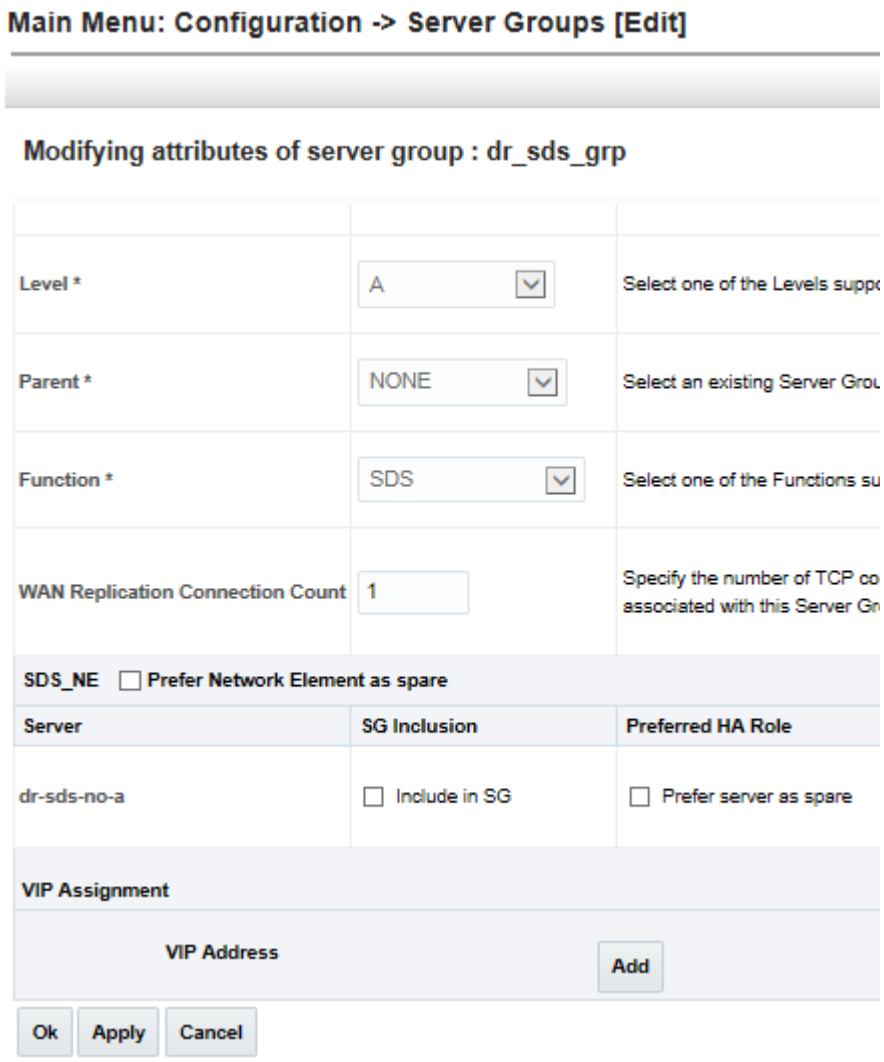
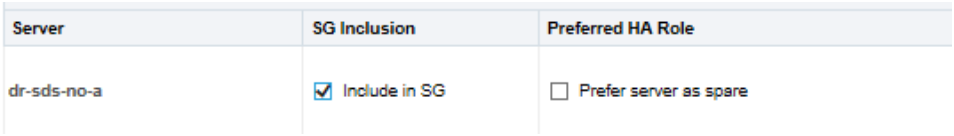
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
11. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
12. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	

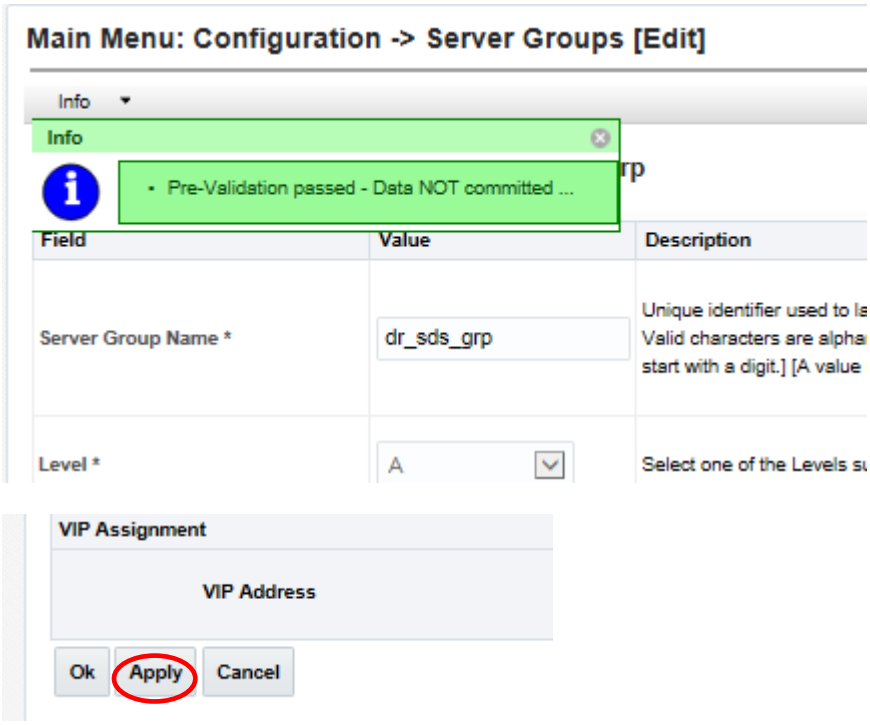
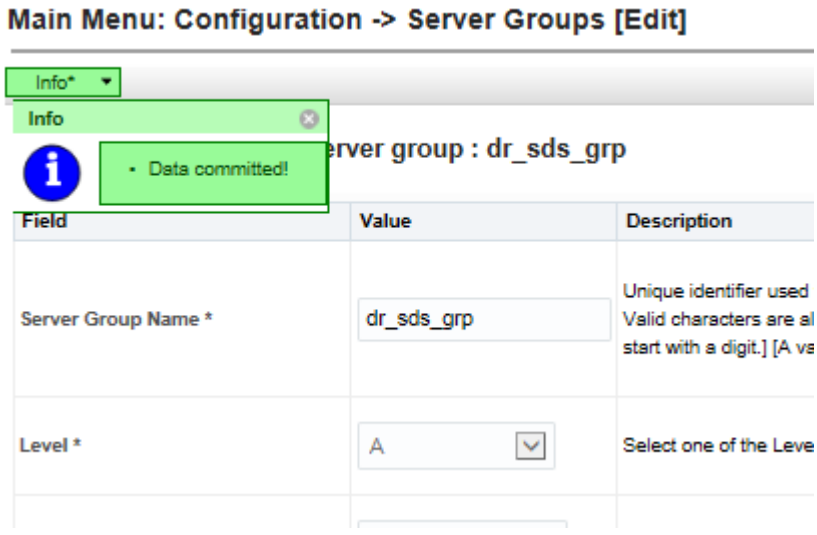
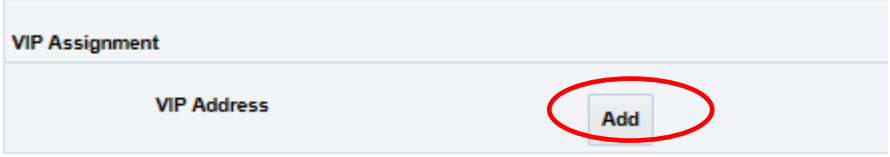
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
13. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	
14. ☐	**Primary SDS VIP:** The **Server Group** entry should be shown on the **"Server Groups"** configuration screen as shown on the right.	
15. ☐	**Primary SDS VIP:** **1)** Select the **Server Group** entry applied in **Step 12**. The line entry should now be highlighted. **2)** Select the **"Edit"** dialogue button from the bottom left corner of the screen.	

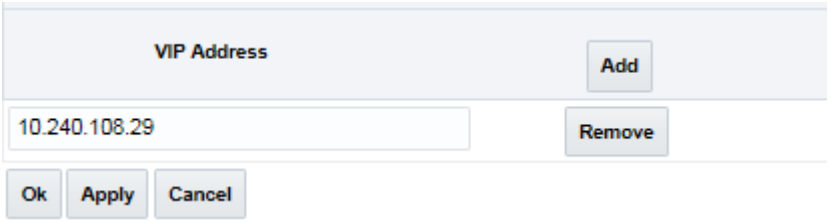
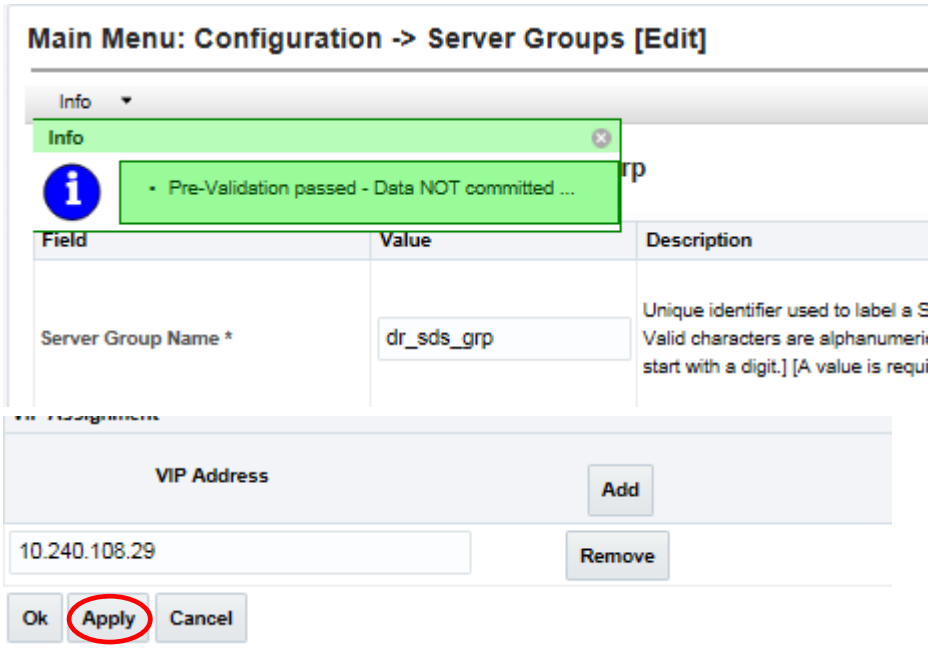
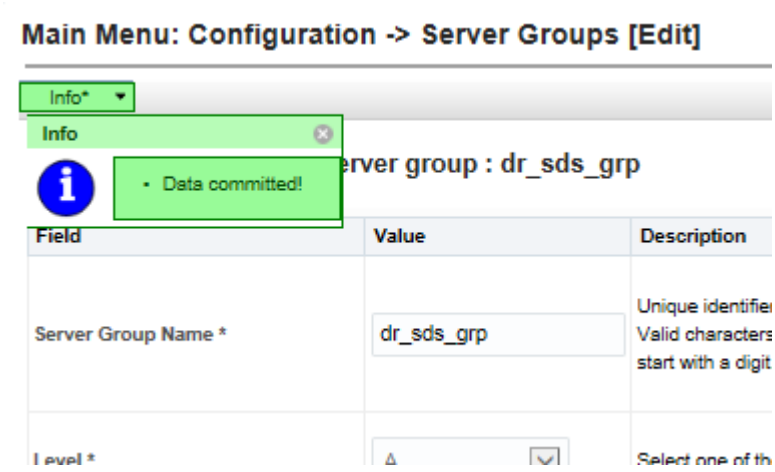
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
16. ☐	**Primary SDS VIP:** The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	
17. ☐	**Primary SDS NOAM VIP:** Select the **"A"** server and the **"B"** server from the list of **"Servers"** by clicking the check box next to their names.	

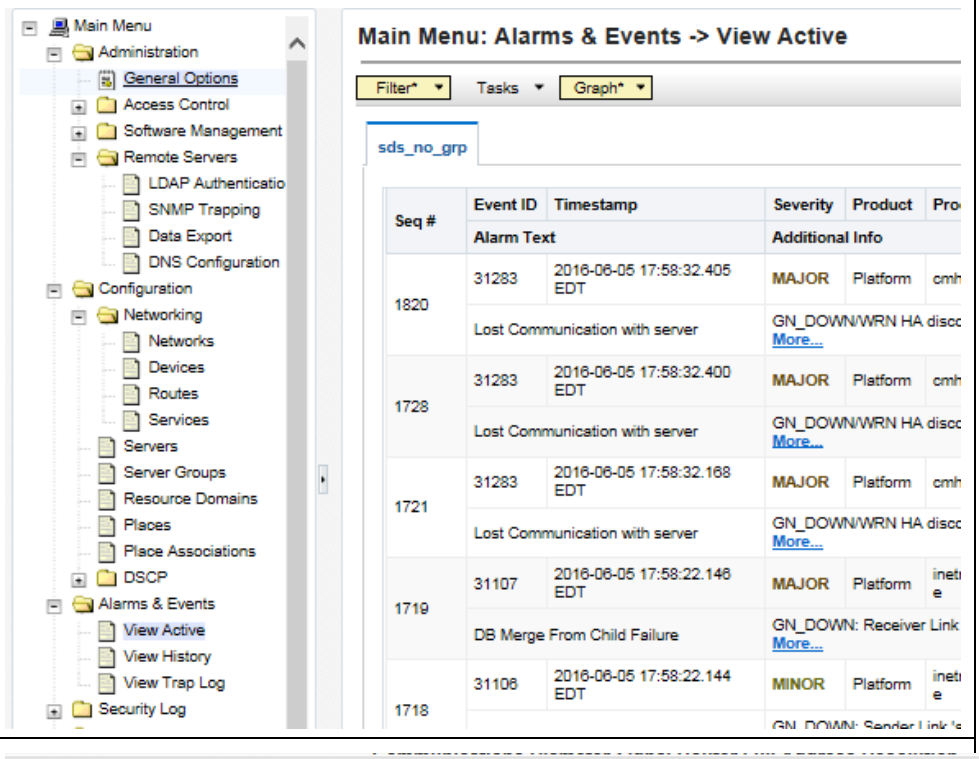
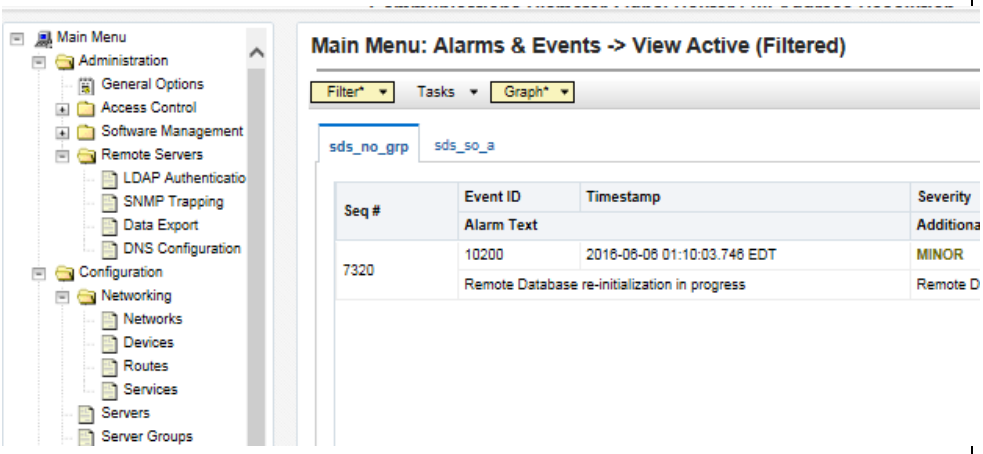
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
18. ☐	**Primary SDS NOAM VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
19. ☐	**Primary SDS NOAM VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
20. ☐	**Primary SDS NOAM VIP:** Click the **"Add"** dialogue button for the **VIP Address**.	

Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
21. ☐	**Primary SDS NOAM VIP:** Input the **VIP Address**	
22. ☐	**Primary SDS NOAM VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
23. ☐	**Primary SDS NOAM VIP:** The user should be presented with a banner information message stating **"Data committed"**.	

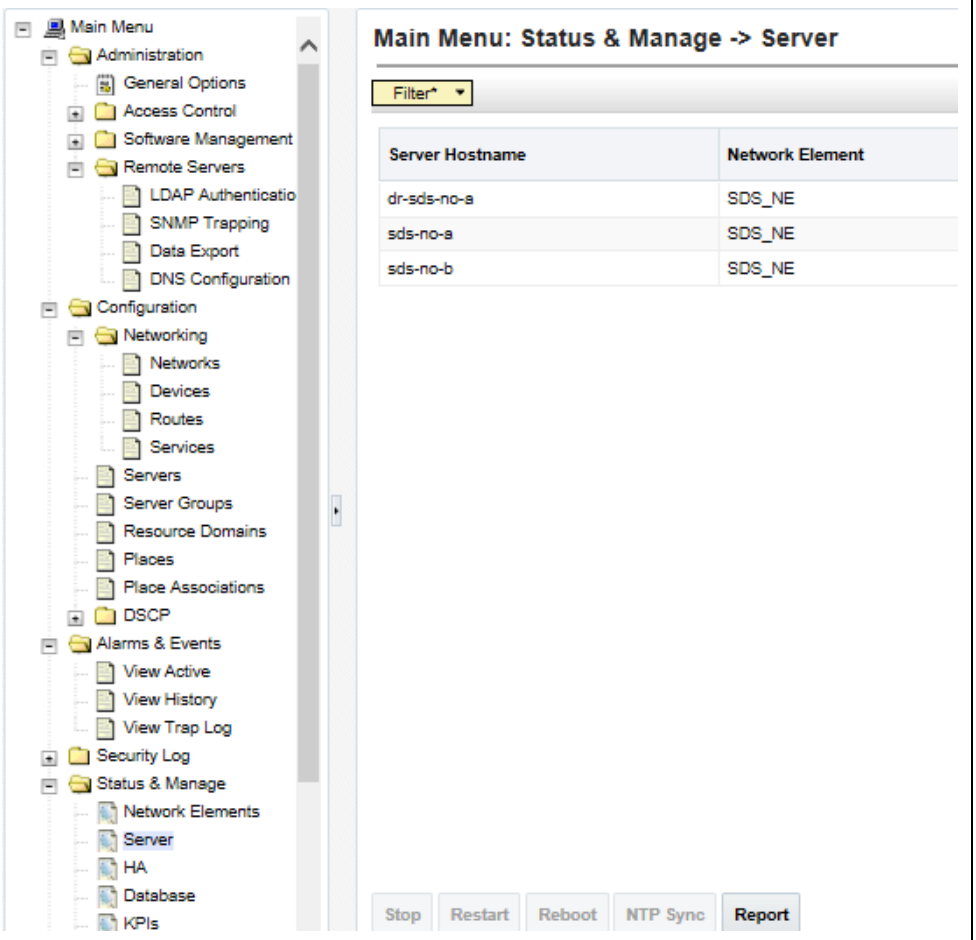
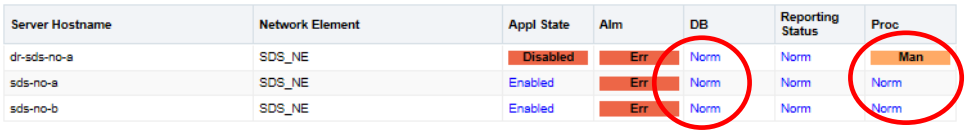
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
24.	**Primary SDS NOAM VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	
25.	**Primary SDS NOAM VIP:** Verify that **Event ID 10200** (*Remote Database re-initialization in progress)* alarms are present with the **DR SDS NOAM Server hostnames** in the **"Instance"** field..	

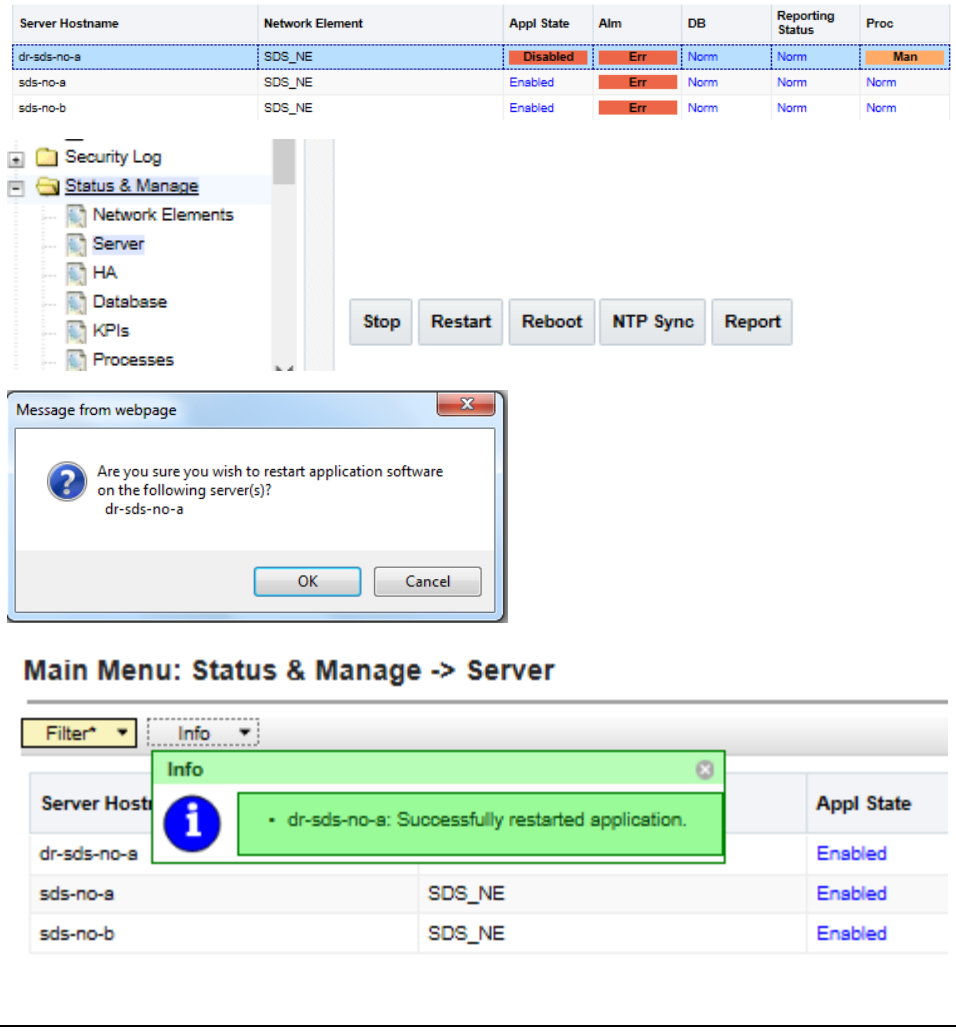
MONITOR THE EVENT ID 10200 (*Remote Database re-initialization in progress)* ALARMS.

DO NOT PROCEED TO THE NEXT STEP UNTIL THE ALARM CLEAR IS RECEIVED FOR BOTH DR SDS NOAM SERVERS.

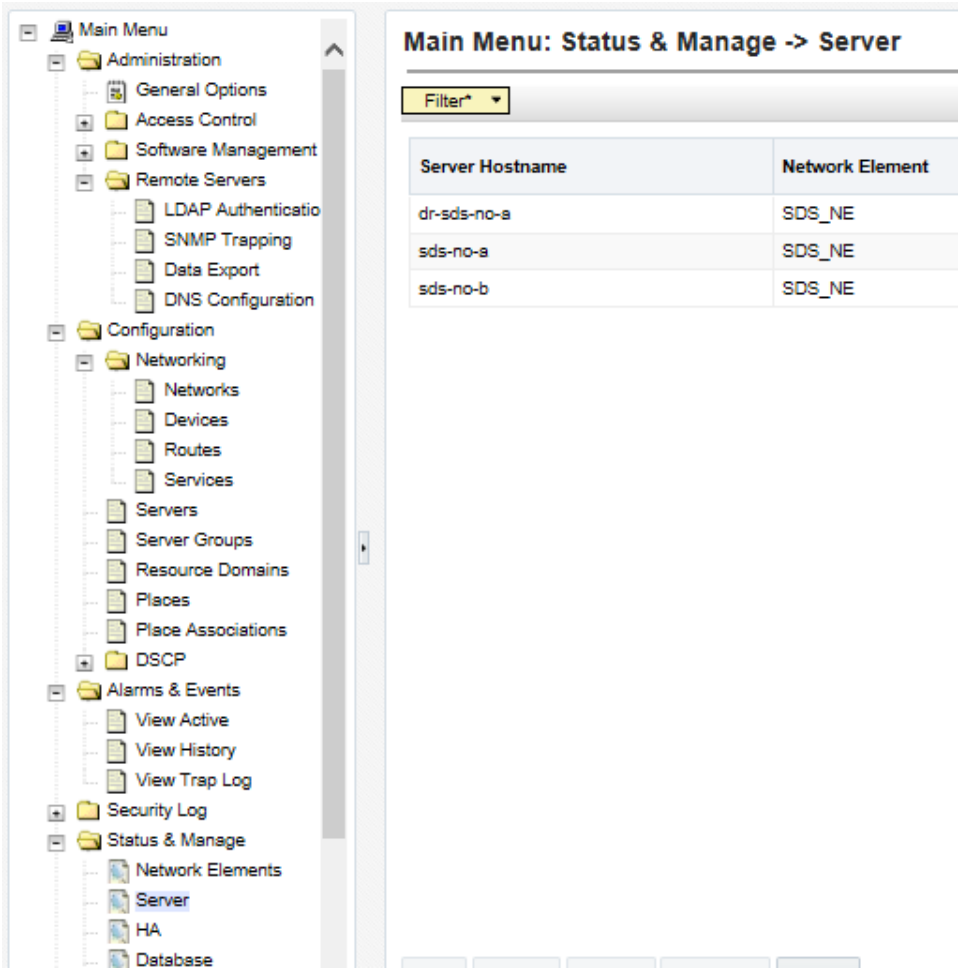
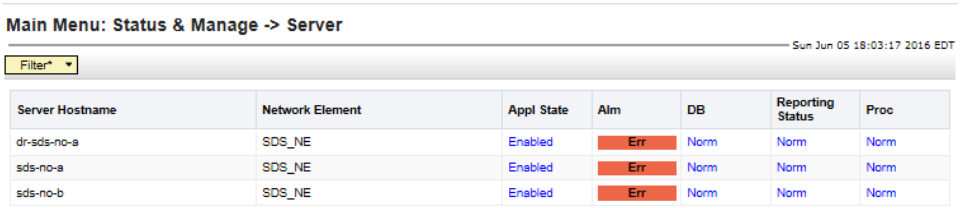
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
26. ☐	**Primary SDS NOAM VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	
27. ☐	**Primary SDS NOAM VIP:** **1)** The **"A"** and **"B"** DR 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.	

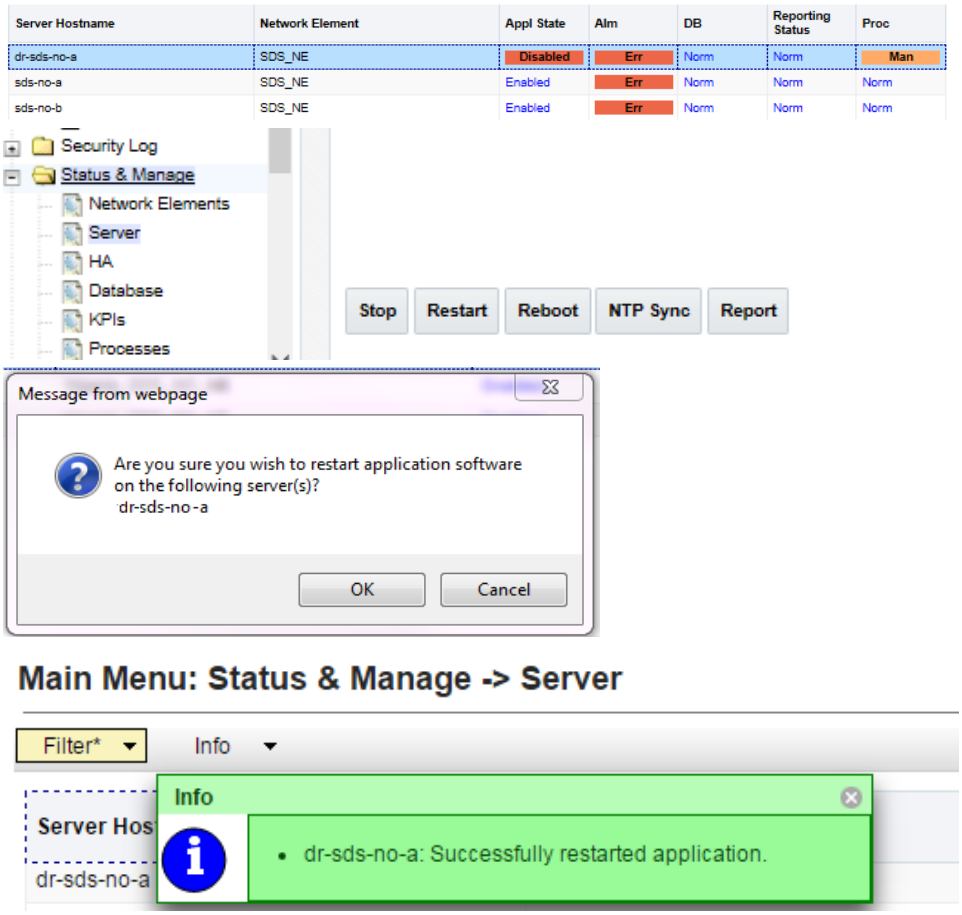
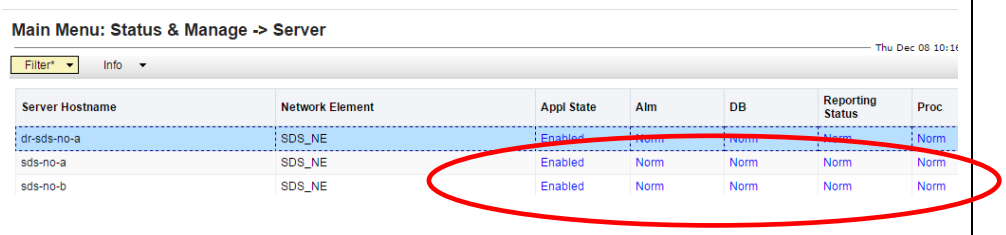
Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
28. ☐	**Primary SDS NOAM VIP:** **1)** Using the mouse, select **DR SDS NOAM Server A**. The line entry should now be highlighted. **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 **DR SDS NOAM Server A** stating: **"Successfully restarted application"**.	

Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
29. ☐	**Primary SDS NOAM VIP:** Select… **Main Menu** **→ Status & Manage** **→ *Server*** …as shown on the right.	
30. ☐	**Primary SDS NOAM VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for N**OAM Server A** before proceeding to the next Step.	

Procedure 7. Pairing the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Step	Procedure	Result
31. ☐	**Primary SDS NOAM VIP:** **1)** Using the mouse, select **DR NOAM Server B**. The line entry should now be highlighted. **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 **DR NOAM Server B** stating: **"Successfully restarted application"**.	
32. ☐	**Primary SDS VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for N**OAM Server A** and N**OAM Server B** before proceeding to the next Step.	
33. ☐	**Primary SDS VIP:** Add the Query Server for the DR SDS Server	• **Repeat all steps listed in Procedure 4 except use the DR SDS NOAM NE and Server Group instead of the Primary SDS NOAM NE (1st SDS NOAM site) and Server Group.**
THIS PROCEDURE HAS BEEN COMPLETED		

5.6 Add SDS Software Images to PMAC Servers (All SOAM Sites)

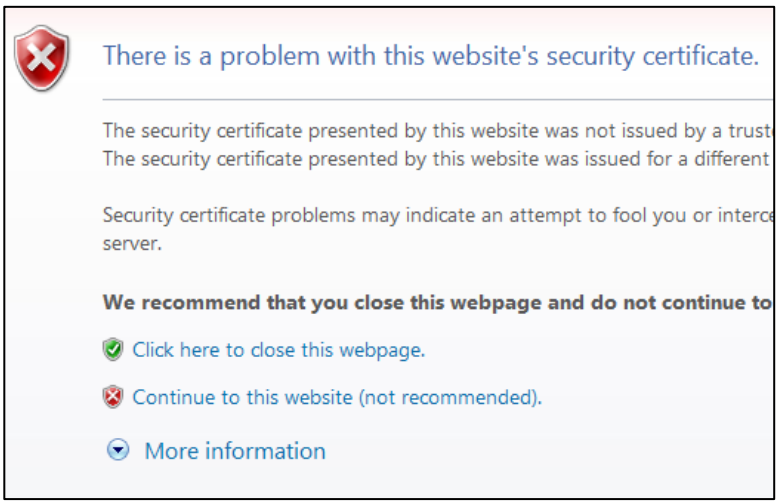
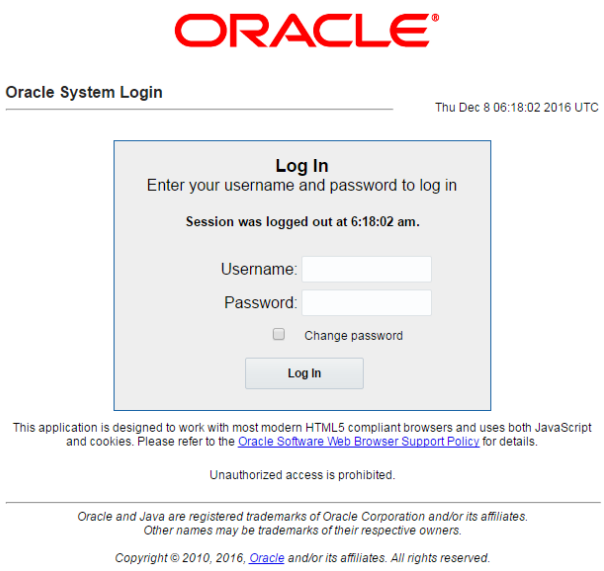
This procedure must be done once for each DSR signaling site, which is also an SDS SOAM site.

This procedure assumes that the PMAC server has already been installed, as described in [4] HP Solutions Firmware Upgrade Pack Release Notes, 795-000-4xx, Latest version (2.2.9 or higher).

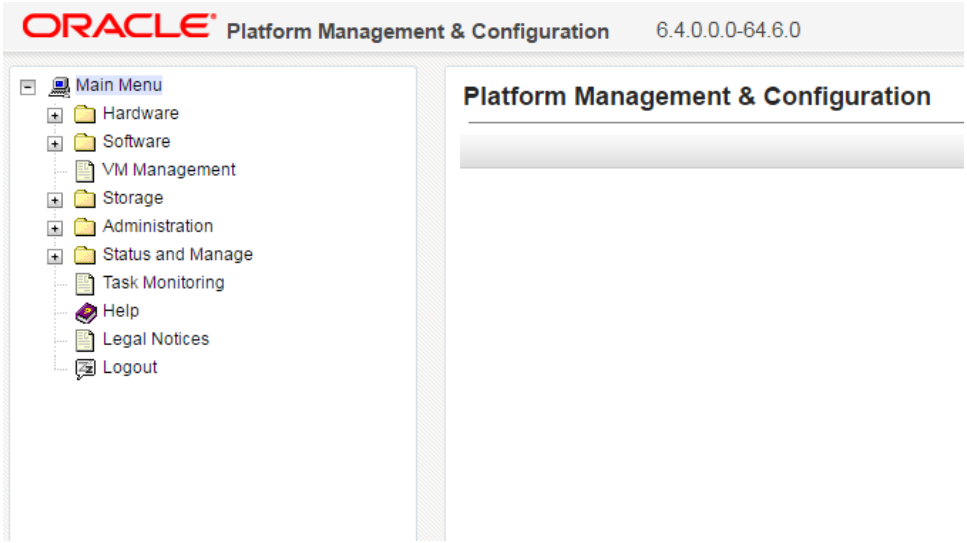
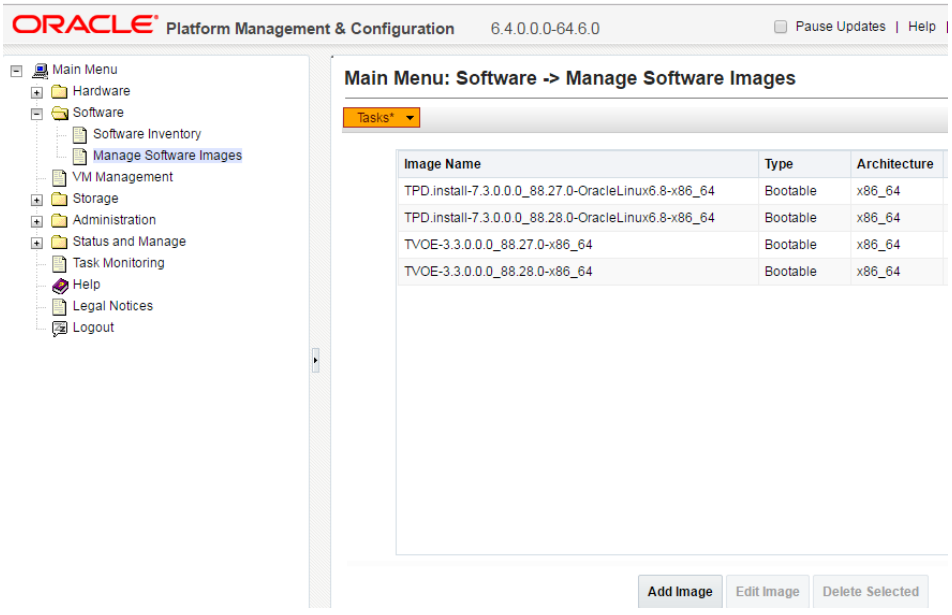
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites

Step	Procedure	Result
1.	**Active SDS VIP (CLI):** **1)** Access the command prompt. **2)** Log into the HP server as the "**admusr**" user.	login: **admusr** Using keyboard-interactive authentication. Password: ***<admusr_password>*** $
2.	**Active SDS VIP (CLI):** **"cd"** into the /var/TKLC/upgrade/ directory.	$ **cd /var/TKLC/upgrade/** **$**
3.	**Active SDS VIP (CLI):** Verify that the **SDS ISO** file is present.	$ **ls** SDS-8.1.0.0.0_80.16.0-x86_64.iso $
4.	**Active SDS VIP (CLI):** **"sftp"** the **SDS ISO** file to the PMAC Server as shown to the right..	$ **sftp pmacftpusr@*<PMAC_Mgmt_IP_address>*:/var/TKLC/upgrade/** Password: ***<admusr_password>*** Changing to: /var/TKLC/upgrade sftp> put SDS-8.1.0.0.0_80.16.0-x86_64.iso Uploading SDS-8.1.0.0.0_81.16.0-x86_64.iso to /var/TKLC/upgrade/SDS-8.1.0.0.0_81.16.0-x86_64.iso SDS-8.1.0.0.0_80.16.0-x86_64.iso 100% 853MB 53.3MB/s 00:16 $SDS-8.1.0.0.0_80.16.0-x86_64.iso 100% 853MB 53.3MB/s 00:16 $

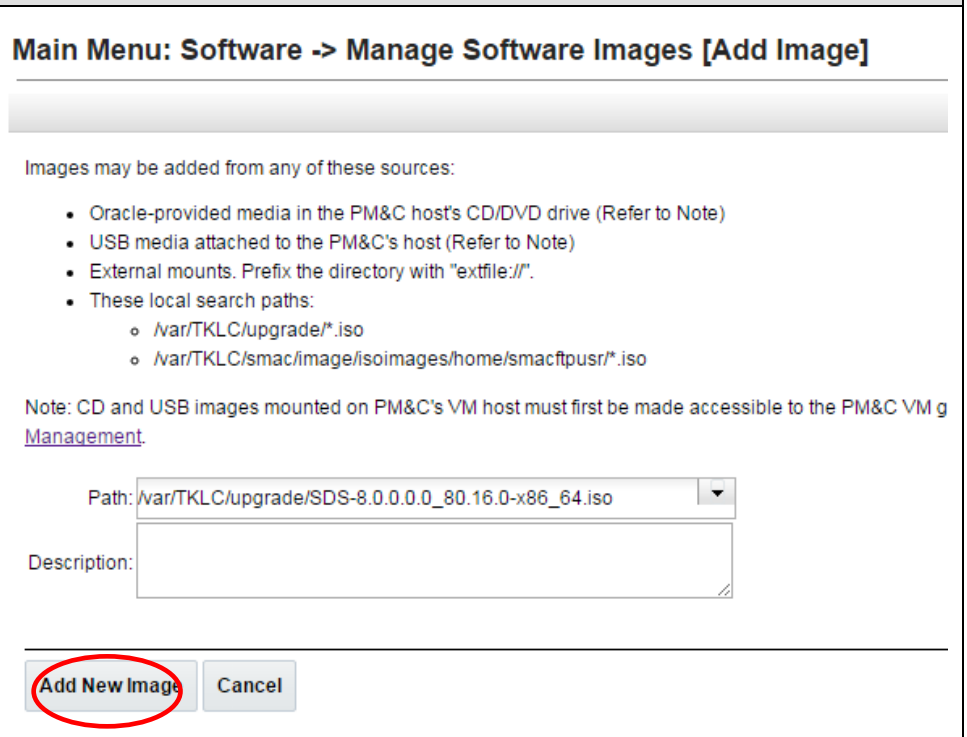
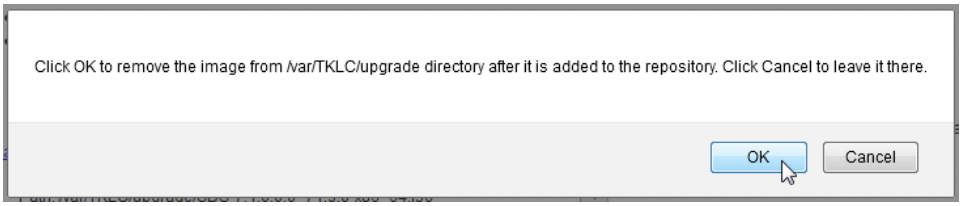
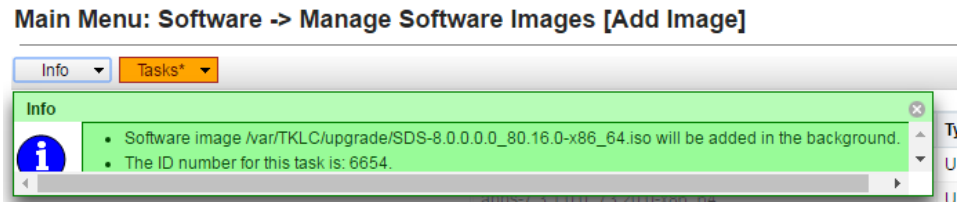
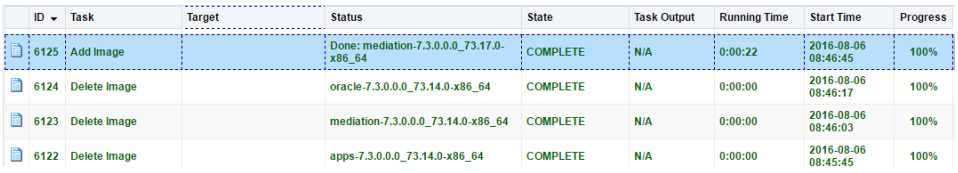
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites

Step	Procedure	Result
5. ☐	**PMAC Server GUI:** Launch an approved web browser and connect to the **Mgmt IP Address** of the PMAC Guest server at the SOAM site. **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
6. ☐	**PMAC Server GUI:** The user should be presented the login screen shown on the right. Login to the PMAC using the default user and password.	

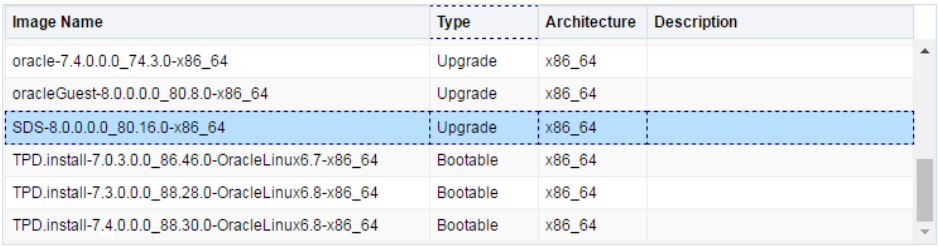
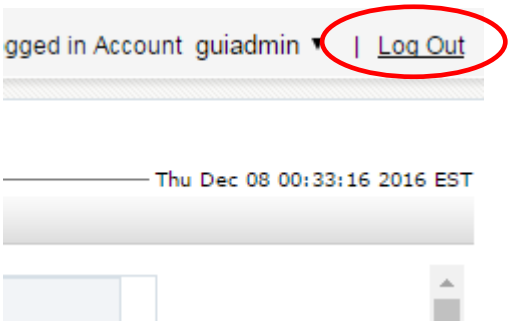
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites

Step	Procedure	Result
7. ☐	**PMAC Server GUI:** The user should be presented with the PMAC Main Menu as shown on the right.	
8. ☐	**PMAC Server GUI:** **1)** Select… **Main Menu** → **Software** → ***Manage Software Images*** …as shown on the right. **2)** Select the **"Add Image"** button	

Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites

Step	Procedure	Result
9. ☐	**PMAC Server GUI:** **1)** Click the **"Path:"** pull-down menu and select the **SDS ISO** file from the /var/TKLC/upgrade directory. **2**) Add a comment if desired in the Description field. **3)** Click the **"Add New Image"** dialogue button.	
10.	**PMAC Server GUI:** Click the **"OK"** button on the confirmation dialogue box to remove the source image after it has been successfully added to the SW Inventory	
11. ☐	**PMAC Server GUI:** An info message will be raised to show a new background task.	
12. ☐	**PMAC Server GUI:** Watch the extraction progress in the lower task list on the same page.	

Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites

Step	Procedure	Result
13. ☐	**PMAC Server GUI:** When the extraction task is complete, a new software image will be displayed.	
14. ☐	**PMAC Server GUI:** Click the **"Logout"** link on the PMAC server GUI.	
15.	**PMACServer GUI:** Load TPD ISO.	If the TPD ISO hasn't been loaded onto the PMAC already, repeat **steps 1 through 14** to load it using the TPD media or ISO.
THIS PROCEDURE HAS BEEN COMPLETED		

5.7 OAM Installation for SOAM Sites (All SOAM Sites)

Assumptions:

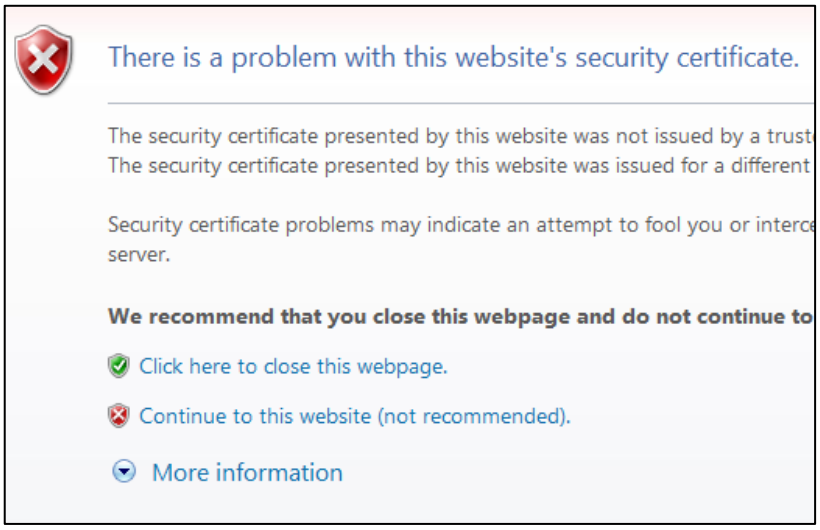
- This procedure assumes that the SOAM Network Element XML file for the SOAM site has previously been created, as described in **Appendix E.**
- This procedure assumes that the Network Element XML files are either on a USB flash drive or the laptop's hard drive. The steps are written as if the XML files are on a USB flash drive, but the files can exist on any accessible drive.

This procedure is for installing the SOAM software on the OAM server blades located at each DSR Signaling Site. The SOAM and DSR OAM servers run in 2 virtual machines on the same HP C-Class blade.

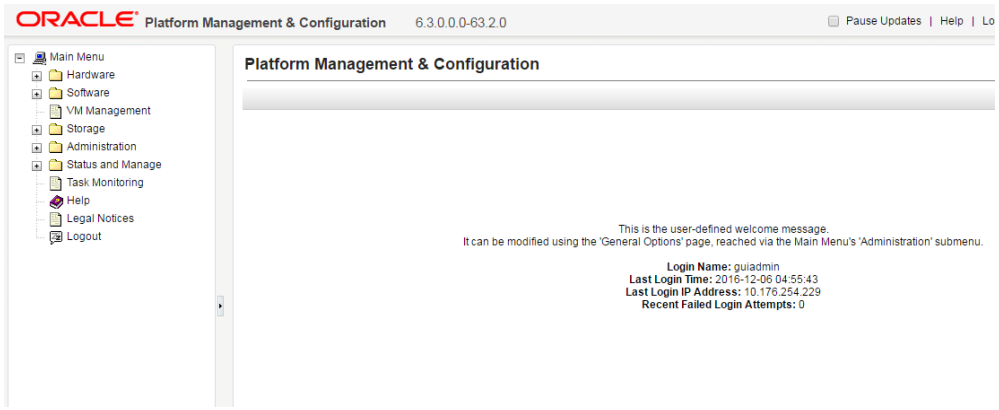
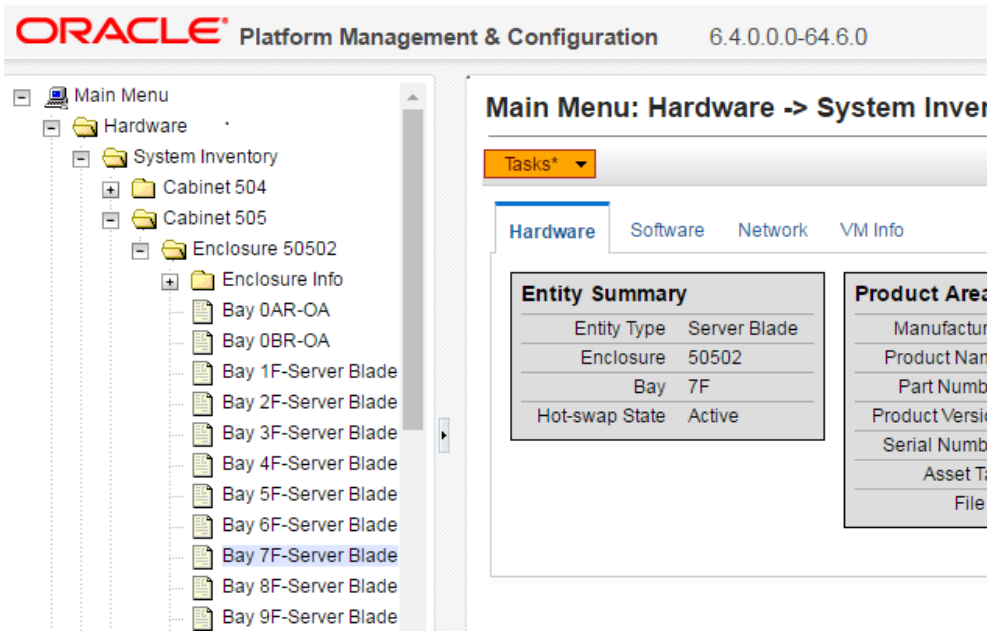
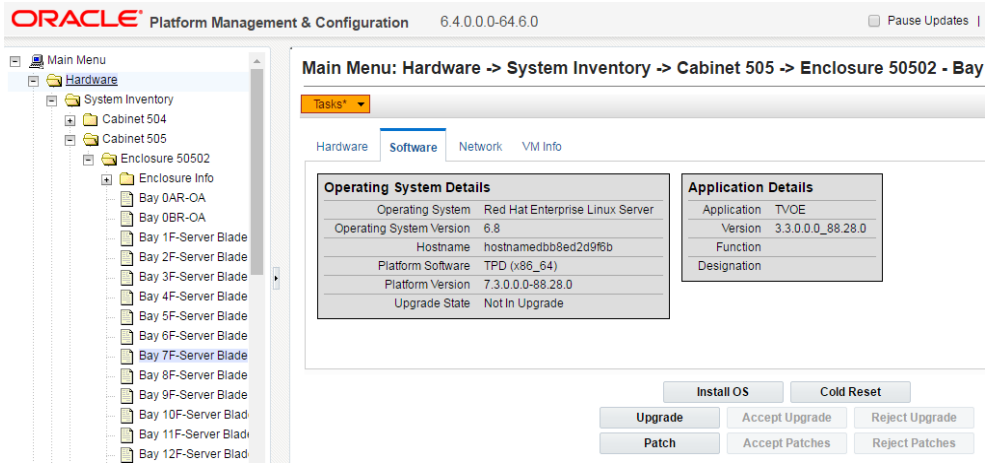
This procedure assumes that the DSR 8.1 or later OAM has already been installed in a virtual environment on the server blade, as described in as described in [4].

This assumption also implies that the PMAC server has been installed and that TVOE has been installed in the OAM server blades. This procedure also assumes that the SDS software image has already been added to the PMAC server, as described in section 5.6.

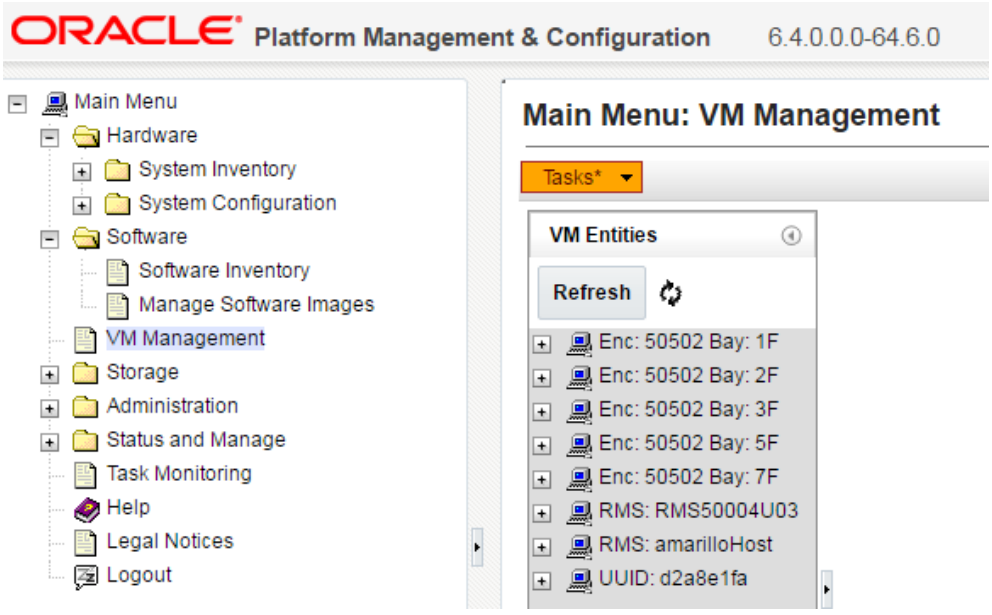
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
1. ☐	**PMAC Server GUI:** Launch an approved web browser and connect to the **Mgmt IP Address** of the PMAC server at the SOAM site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**PMAC Server GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

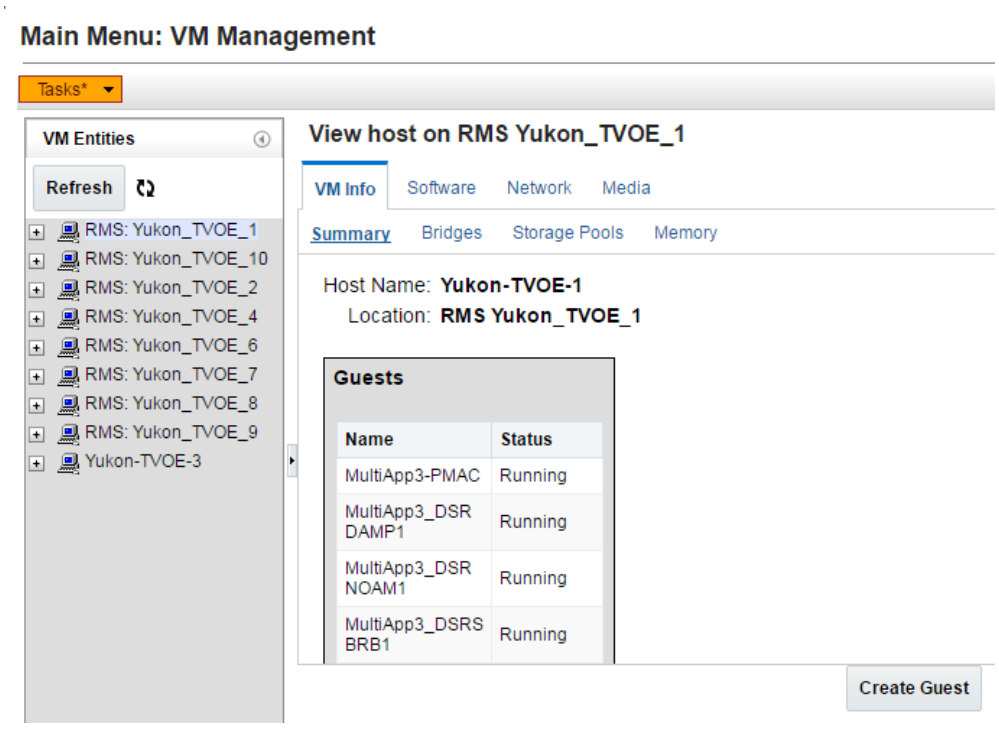
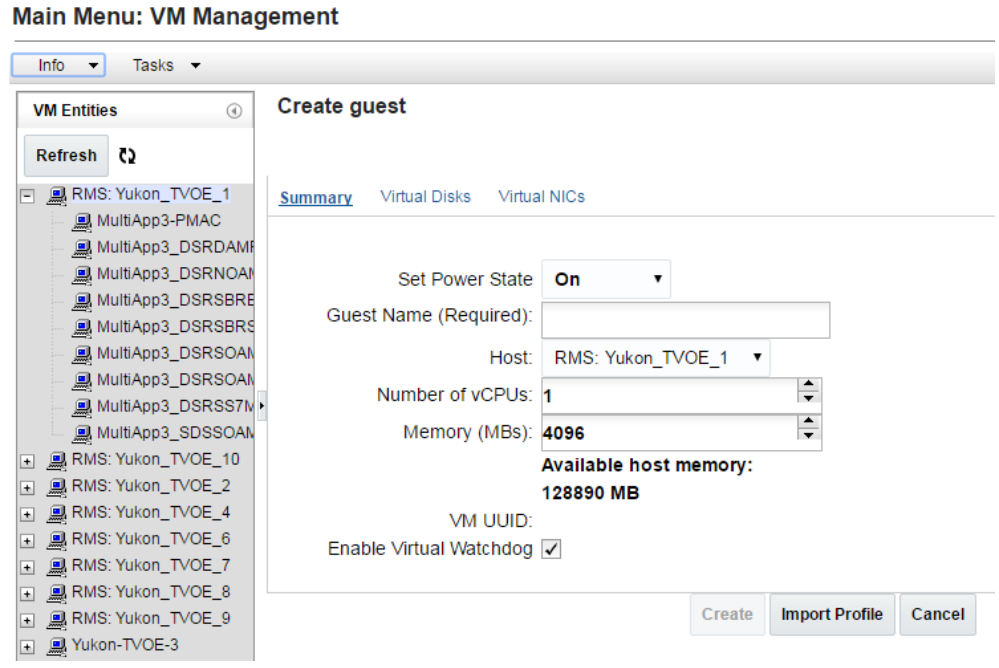
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
3. ☐	**PMAC Server GUI:** The user should be presented the PMAC Main Menu as shown on the right.	
4. ☐	**PMAC Server GUI:** Select desired OAM server blade… **Main Menu** → **Hardware** → **System Inventory** → **<Enclosure>** → **<Server Blade>** …as shown on the right.	
5. ☐	**PMAC Server GUI:** Select the Software tab. …as shown on the right. Verify that TVOE application has been installed.	

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
		IF TVOE WAS NOT INSTALLED OR IS THE INCORRECT VERSION ON THE BLADE SERVER, STOP AND EXECUTE THE FOLLOWING STEPS: **1)** Verify that the enclosure and bay number are correct. **2)** Refer [3] for TVOE Installation or Contact DSR Installation Engineer to confirm location of OAM blade and status of TVOE installation. **3)** Restart this procedure. **IF TVOE WAS NOT INSTALLED OR IS THE INCORRECT VERSION ON THE BLADE SERVER, STOP AND EXECUTE THE FOLLOWING STEPS:** **NOTE:** It is assumed that the TVOE version corresponds with the correct DSR and SDS installation guidelines, this can be checked by executing "appRev".
6. ☐	**PMAC Server GUI:** Select … **Main Menu** → **VM Management** …as shown on the right.	

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
7. ☐	**PMAC Server GUI:** **1)** In the VM Entities box, select the desired server …as shown on the right. **2)** Click the "**Create Guest**" dialogue button	
8. ☐	**PMAC Server GUI:** Click the "**Import Profile**" dialogue button …as shown on the right.	

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>9. ☐</td><td>PMAC Server GUI:

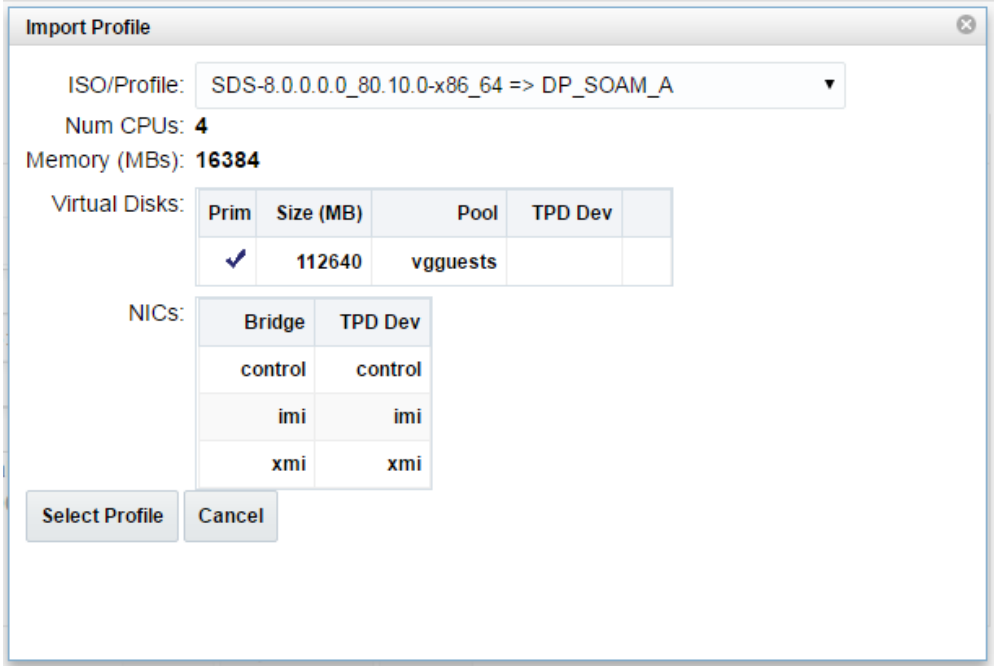
1) Select the desired ISO/Profile value

…as shown on the right.

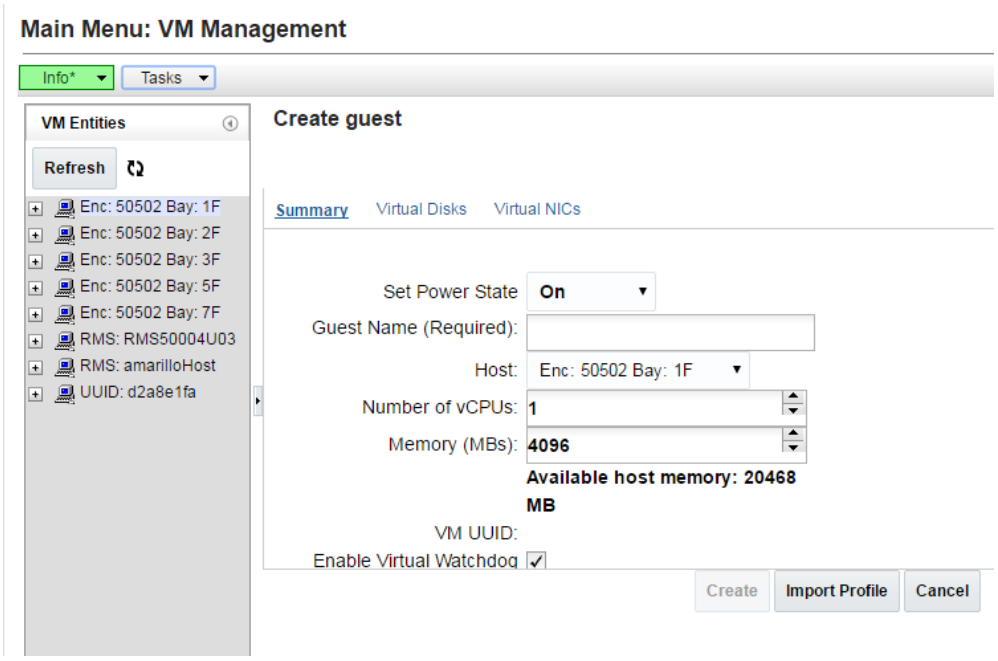
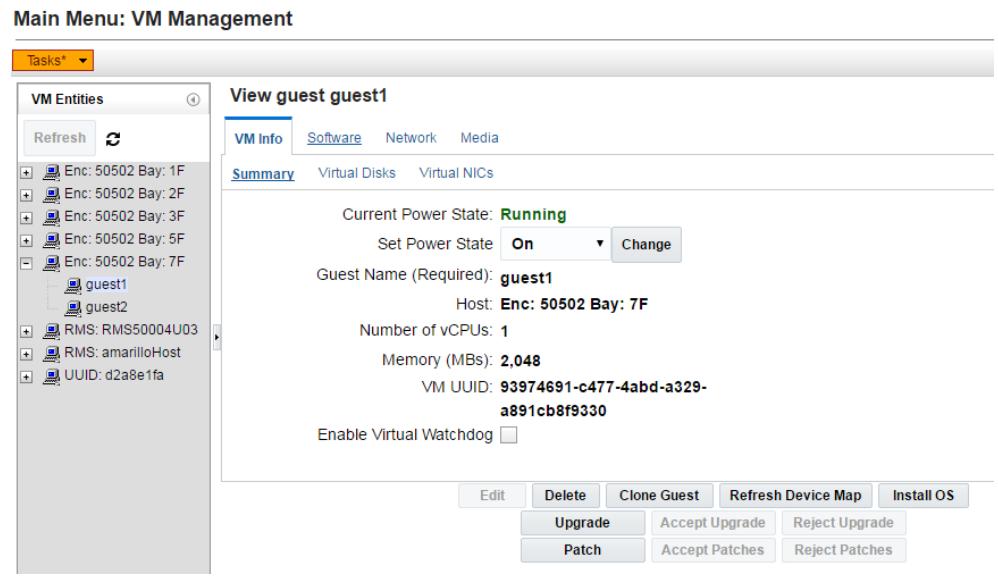
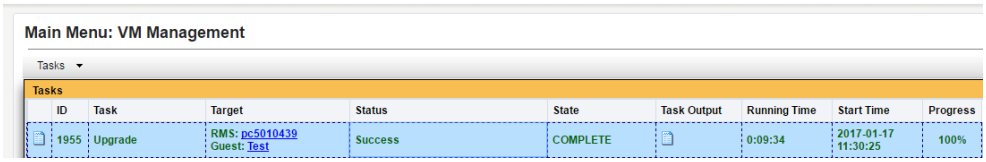
2) Click the “Select Profile” dialogue button</td><td>From the “ISO/Profile” drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running:

<table>
<tr><th>SDS Release</th><th>TVOE HW Type (BL460 Blade Server)</th><th>Role</th><th>Choose Profile (<Application ISO NAME>)➔</th></tr>
<tr><td rowspan="2">8.1</td><td rowspan="2">Gen8 Blade</td><td>SOAM-A</td><td>DP_SOAM_A</td></tr>
<tr><td>SOAM-B</td><td>DP_SOAM_B</td></tr>
<tr><td>8.1</td><td>Gen8/ Gen9 Blade</td><td>SOAM-A
SOAM-B</td><td>DP_SOAM_1B_RE</td></tr>
</table>

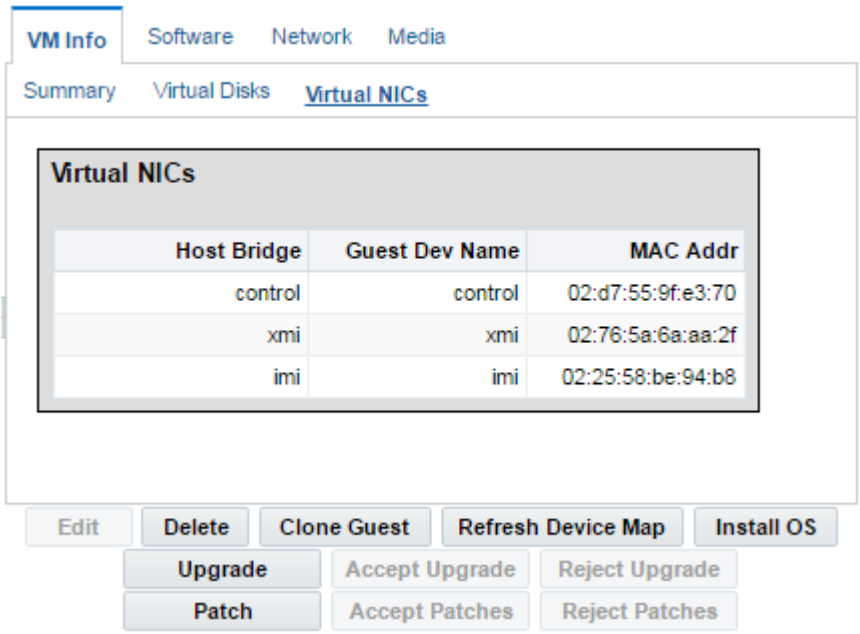
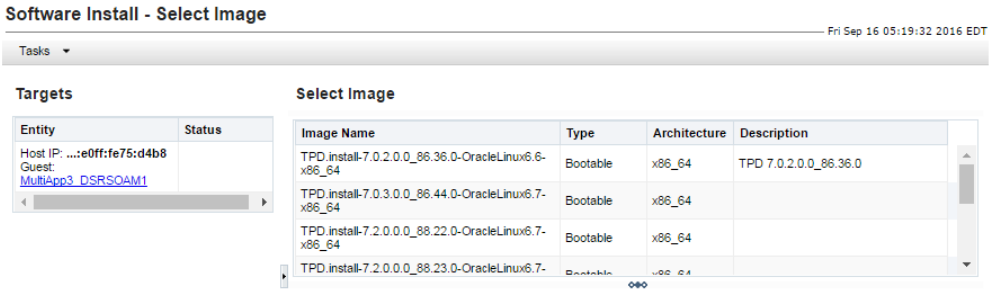
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM

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

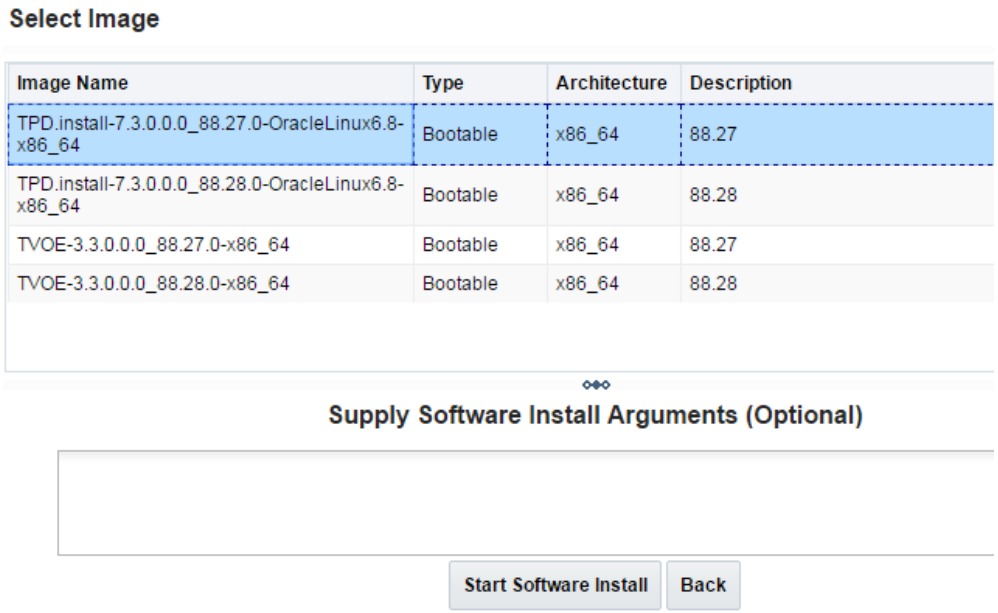
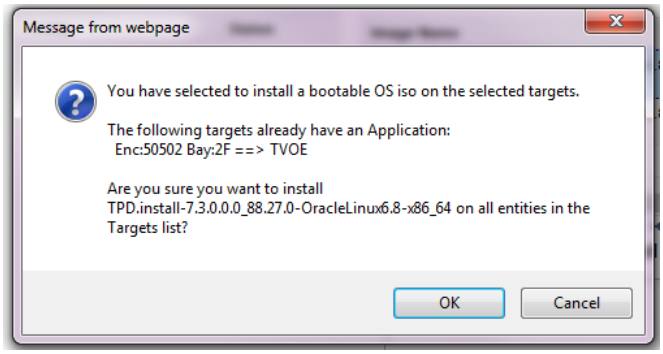
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
10. ☐	**PMAC Server GUI:** **1)** Overwrite the **Name** field with the Server host name (e.g.” so-mrsvnc-a”) **2)** Click the **“Create”** dialogue button	
11. ☐	**PMAC Server GUI:** Verify that task successfully completes. The user should see a screen similar to the one on below with **Progress** value of **100%**. **"Using the "Tasks" tab, verify that the task completes successfully**	 

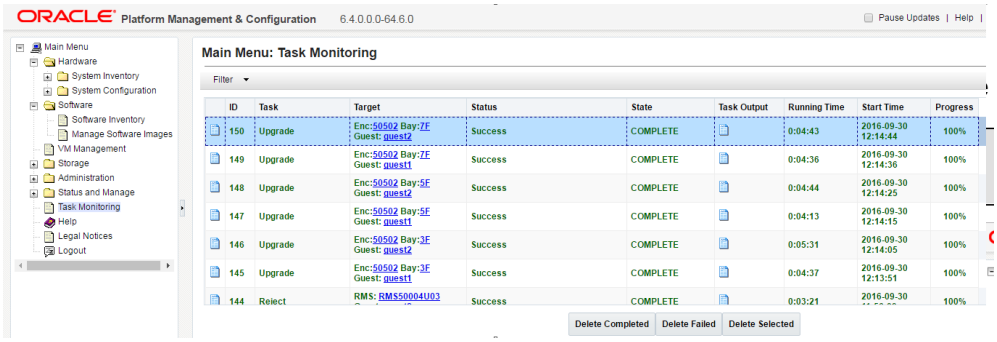
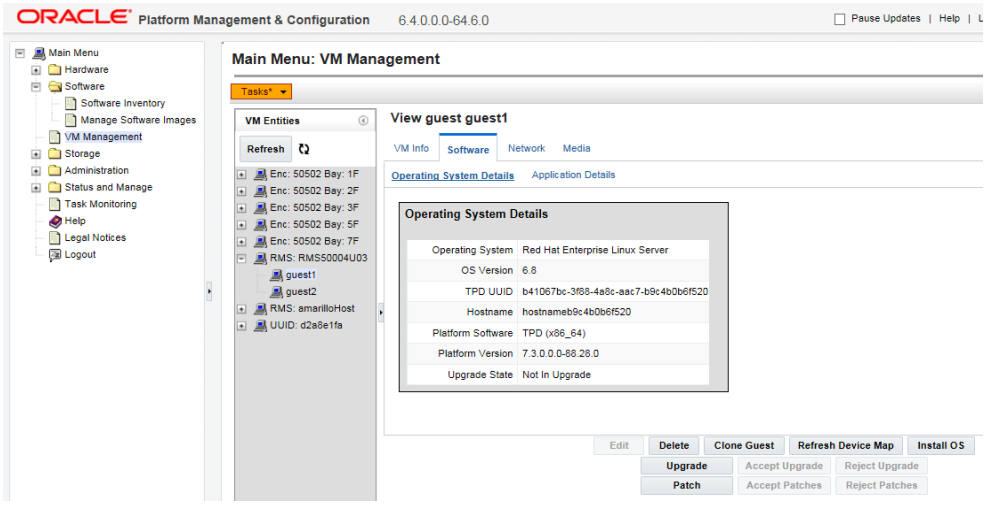
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
12. ☐	**PMAC Server GUI:** Install the operating system by clicking the **"Install OS"** dialogue button	
13. ☐	**PMAC Server GUI:** The user should see a screen similar to the one on the right.	

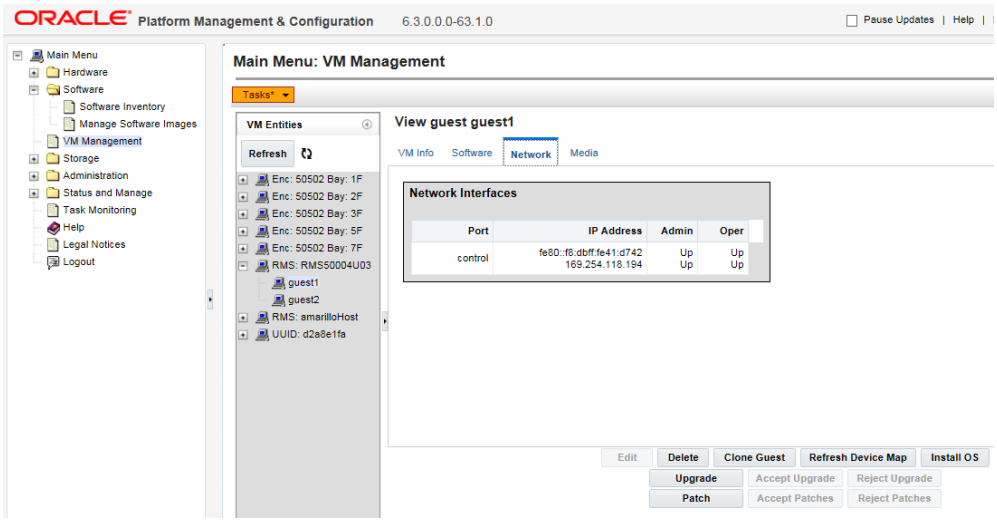
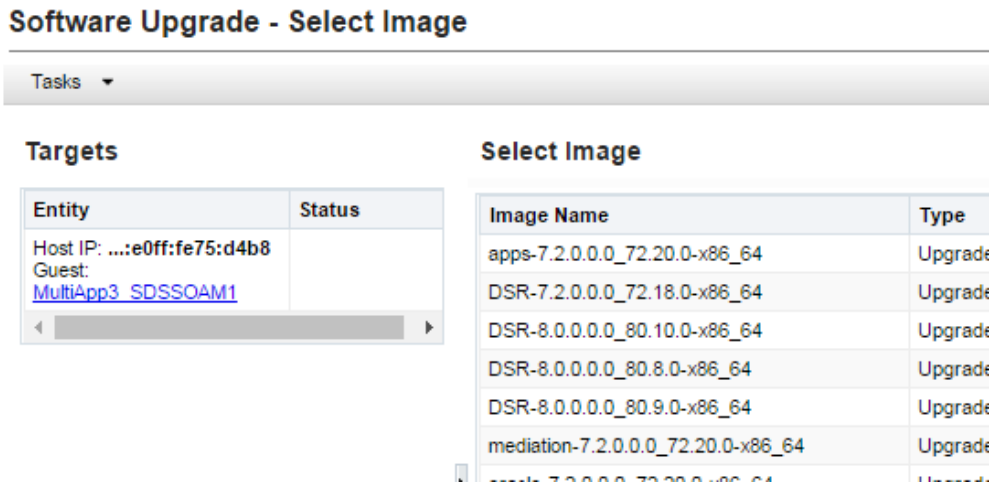
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
14. ☐	**PMAC Server GUI:** **1)** Select the desired **TPD Image** **2)** Click the **"Start Install"** dialogue button.	
15. ☐	**PMAC Server GUI:** The user should be presented with an "**Are you sure you want to install**" message box as shown on the right. Click the "**OK**" dialogue button.	

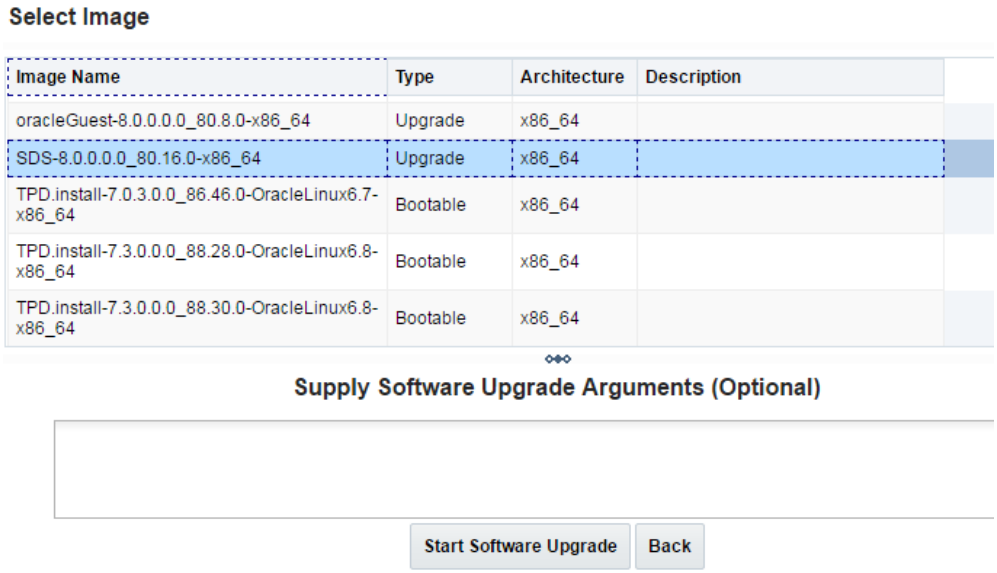
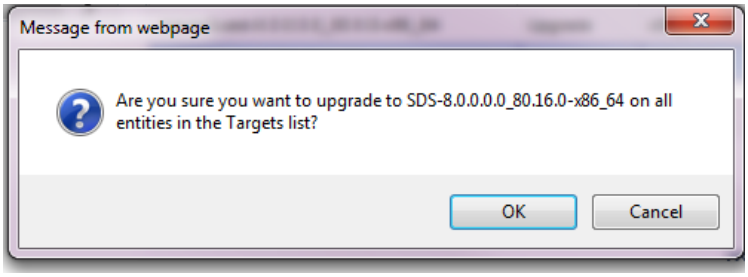
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
16. ☐	**PMAC Server GUI:** An installation task will be started. This task takes ~11 minutes. The user can monitor this task by doing the following: Select… **Main Menu** **→ Task Monitoring** **Wait till Progress is 100% with a Status of Success and a State of Complete.**	
17. ☐	**PMAC Server GUI:** 1. Select [Main Menu: VM Management]. 2. Under VM Etities column, expand (+) plus sign on the Host server containing the newly created VM Guest. 3. Select the VM Guest. 4. Select the "Software" tab. 5. Verify that the OS has been installed. 6. Click on the "Application Details" tab. 7. Verify that the "Application Details" table is blank.	

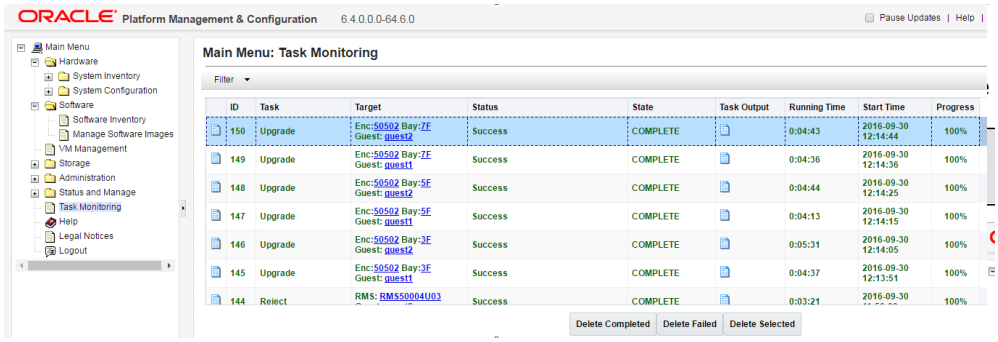
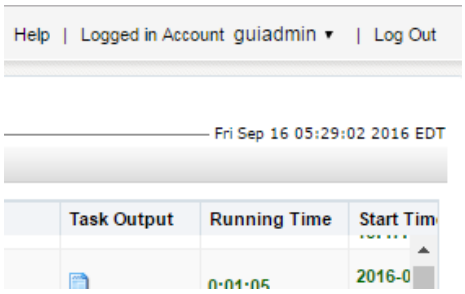
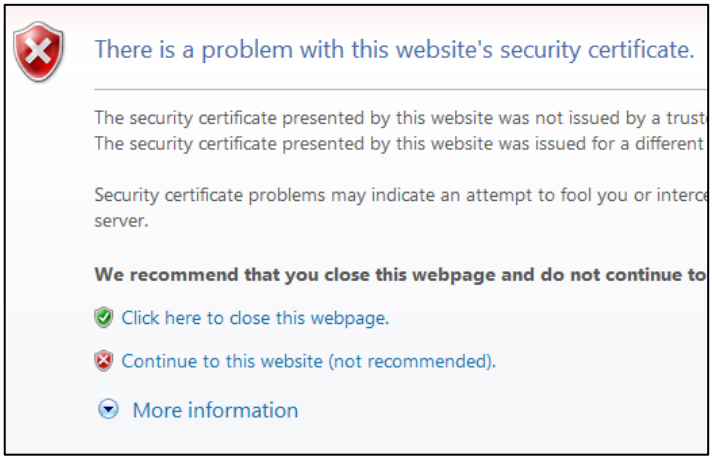
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
18. ☐	**PMAC Server GUI:** **1)** Select the **"Network"** tab **2) Record** the **control IP address** for this SOAM VM; it will be referenced later. **3)** Select the "**Upgrade**" dialogue button	
19. ☐	**PMAC Server GUI:** The user should be presented the Select Image screen as shown on the right	

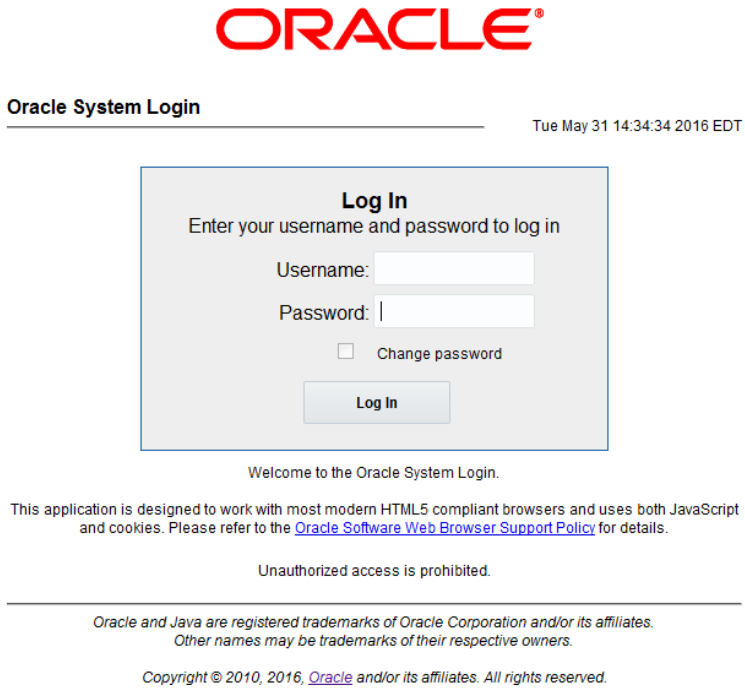
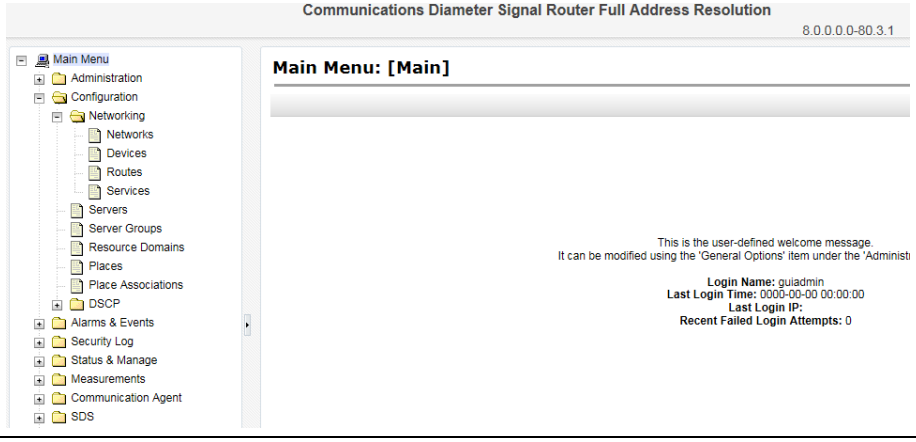
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
20. ☐	**PMAC Server GUI:** **1)** Select the correct **SDS** version from the "**Image Name"** list. The line entry should now be highlighted. **2)** Select the "**Start Upgrade**" dialogue button	
21. ☐	**PMAC Server GUI:** The user should be presented with an "**Are you sure you want to upgrade**" message box ....as shown on the right. Click the "**OK**" dialogue button.	

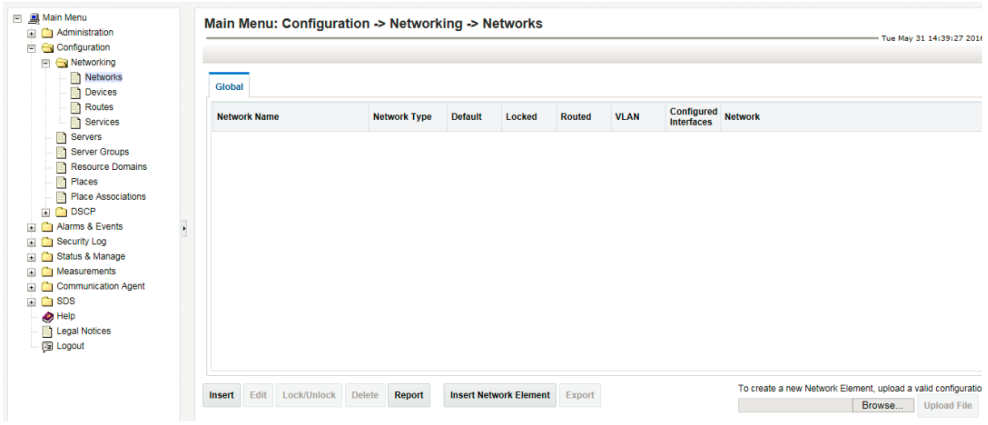
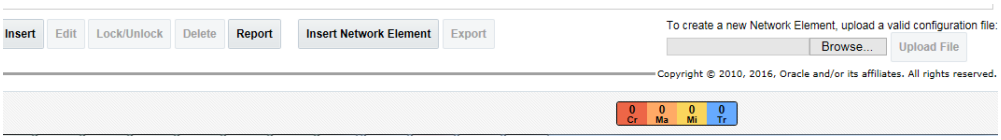
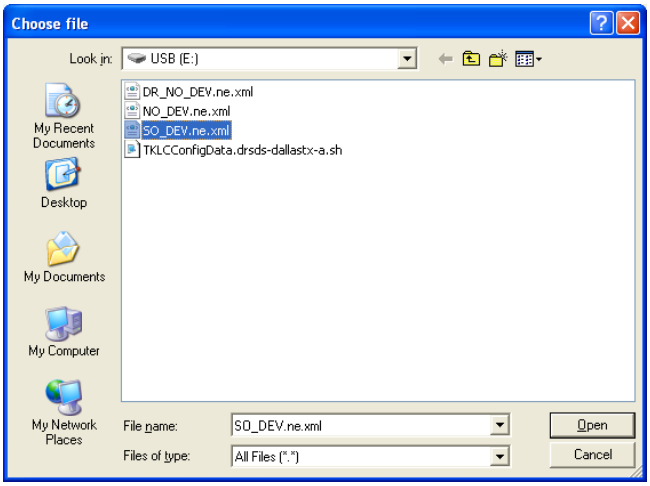
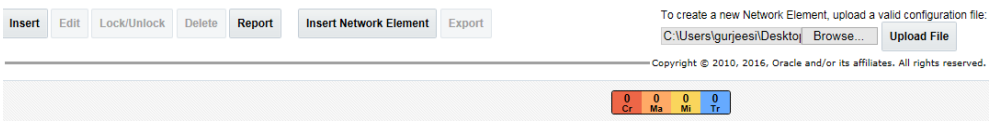
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
22. ☐	**PMAC Server GUI:** An upgrade task will be started. This task takes ~8 minutes. The user can monitor this task by doing the following: Select… **<u>Main Menu</u>** **→ Task Monitoring** Wait till Progress is 100% with a Status of Success and a State of Complete.	
23. ☐	Repeat **Steps 4 – 22** of this procedure for the **SOAM B Server**.	
24. ☐	**PMAC Server GUI:** Click the **"Logout"** link on the PMAC server GUI.	
25. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	

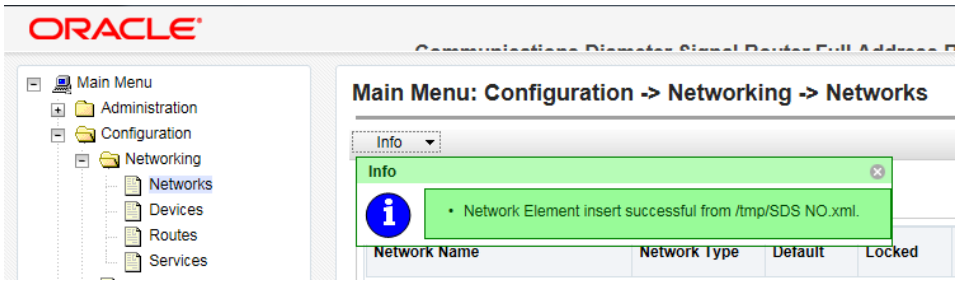
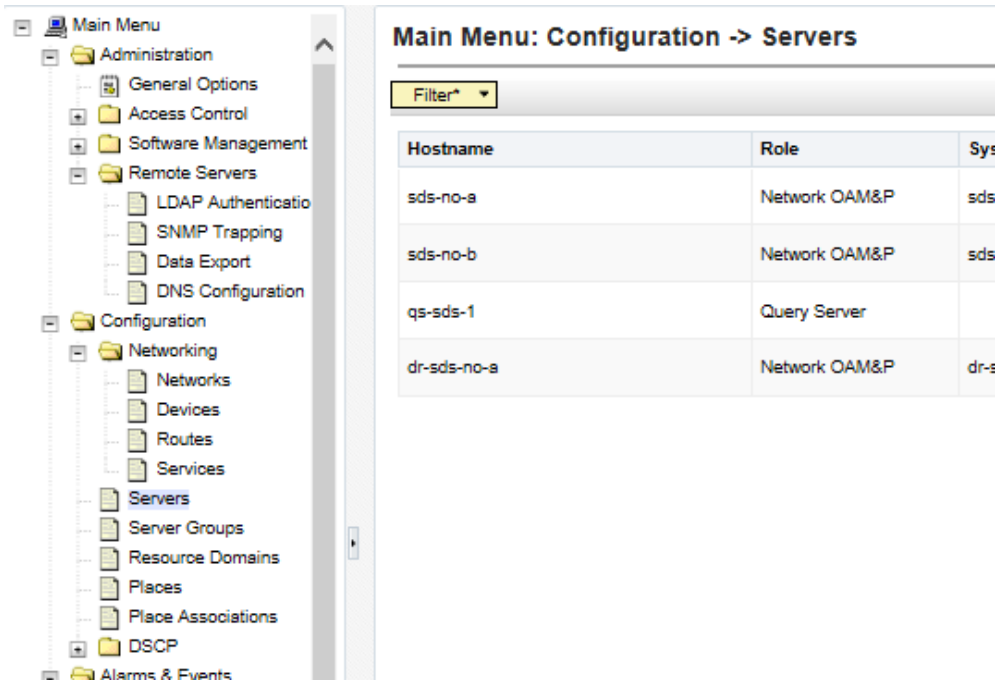
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
26. ☐	**Primary SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
27. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	

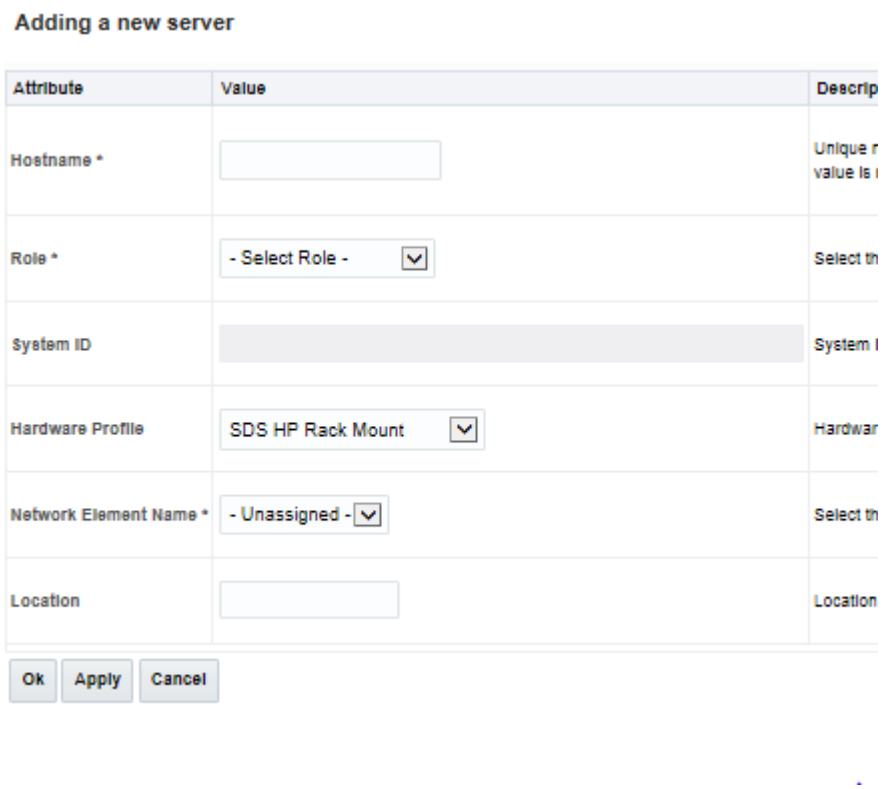
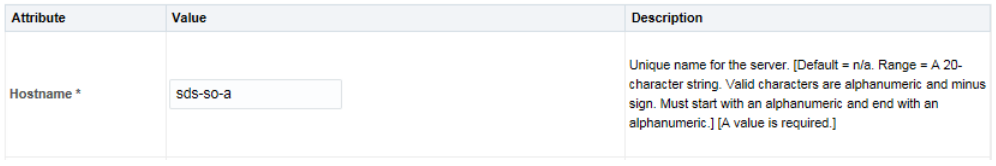
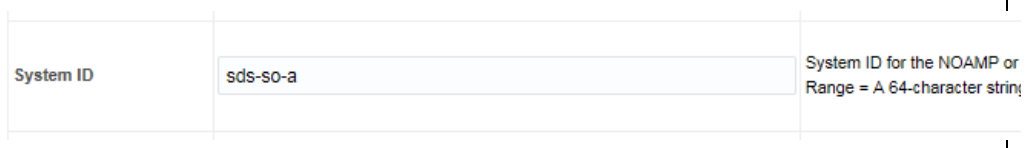
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
28. ☐	**Primary SDS VIP:** Select… **<u>Main Menu</u>** → **Configuration** → ***Network Elements*** …as shown on the right.	
29. ☐	**Primary SDS VIP:** From the **Configuration / Network Elements** screen, select the **"Browse"** dialogue button.	
30. ☐	**Primary SDS VIP:** **Note**: This step assumes that the **xml** files were previously prepared, as described in **Appendix E**. **1)** Select the location containing the site **.xml** file. **2)** Select the **.xml** file and click the **"Open"** dialogue button.	
31. ☐	**Primary SDS VIP:** Select the **"Upload File"** dialogue button (bottom left corner of screen).	

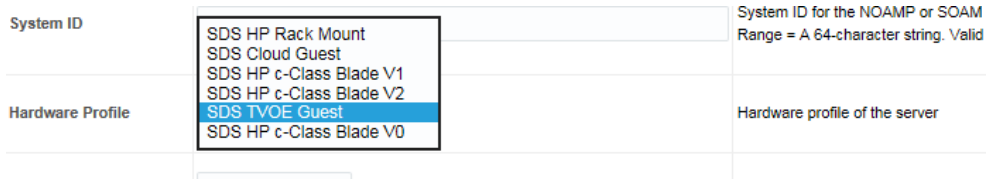
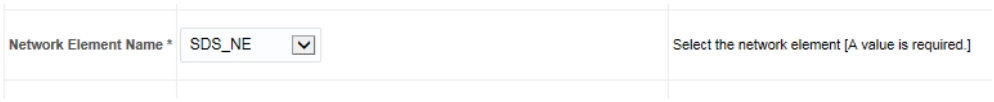
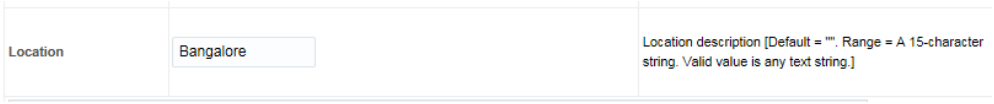
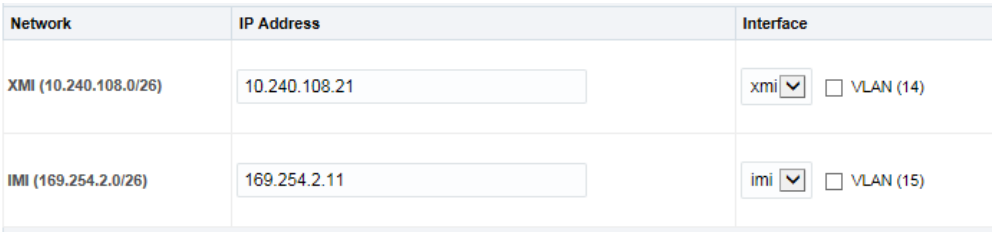
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
32. ☐	**Primary SDS VIP:** If the values in the **.xml** file pass validation rules, the user must select the Info box to receive a banner information message showing that the data has been successfully validated and committed to the DB.	
33. ☐	**Primary SDS VIP:** 1) Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right. 2) Select the **"Insert"** dialogue button	

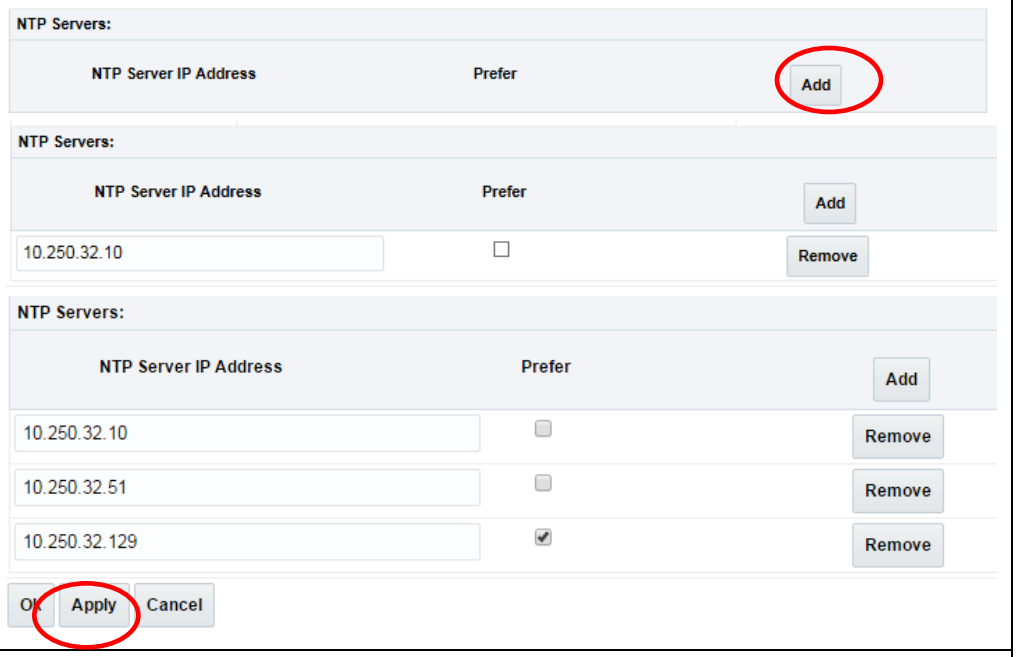
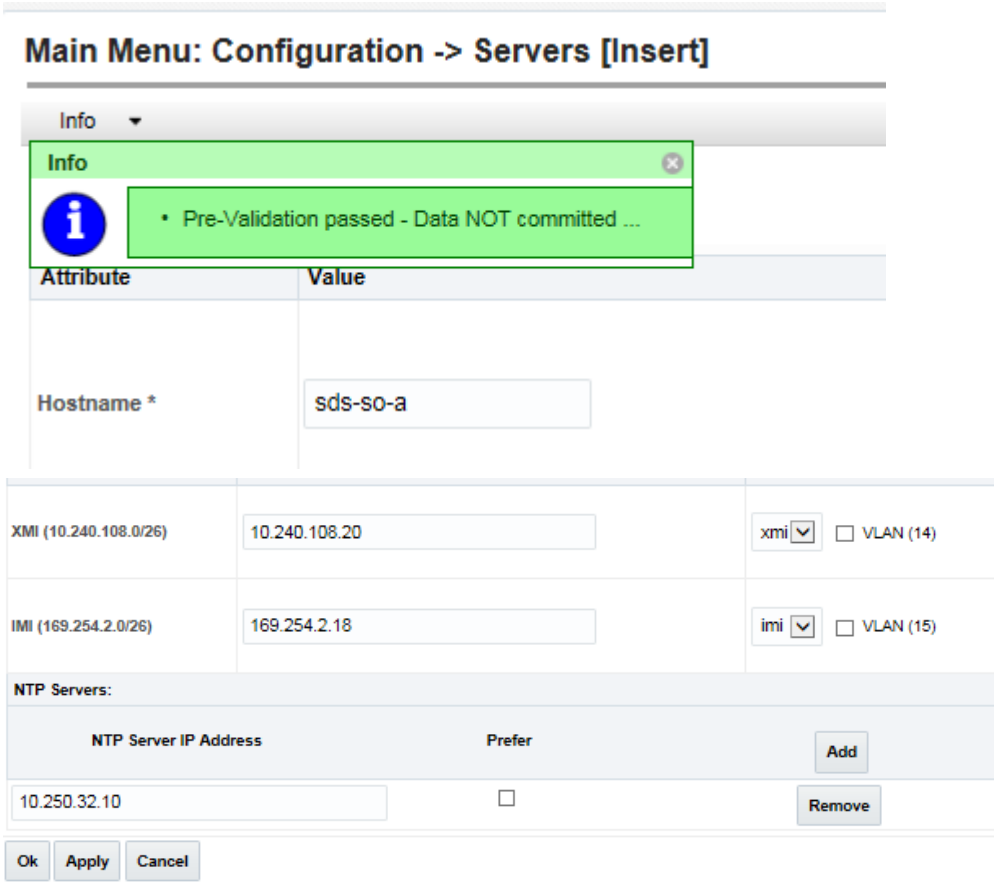
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
34. ☐	**Primary SDS VIP:** The user is now presented with the **"Adding a new server"** configuration screen.	
35. ☐	**Primary SDS VIP:** Input the assigned "**hostname"** for SOAM Server.	
36. ☐	**Primary SDS VIP:** Select ***"SYSTEM OAM"*** for the **Role** from the pull-down menu.	
37. ☐	**Primary SDS VIP:** Input the assigned hostname again as the "**System ID**" for the SO Server (A or B).	

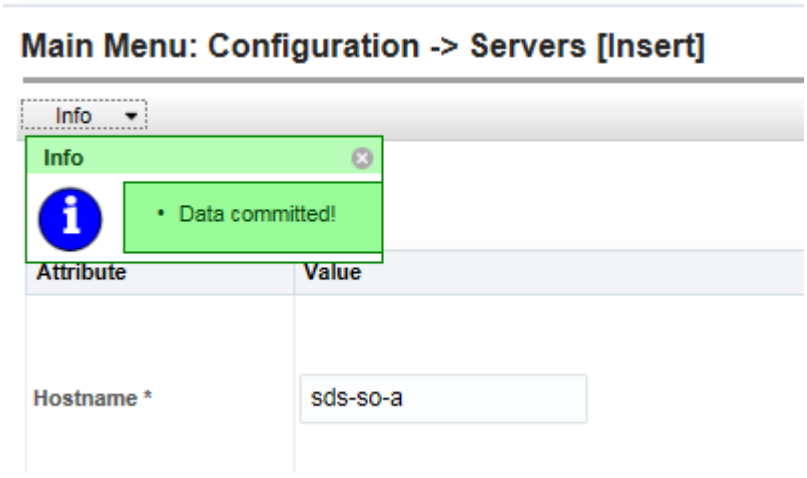
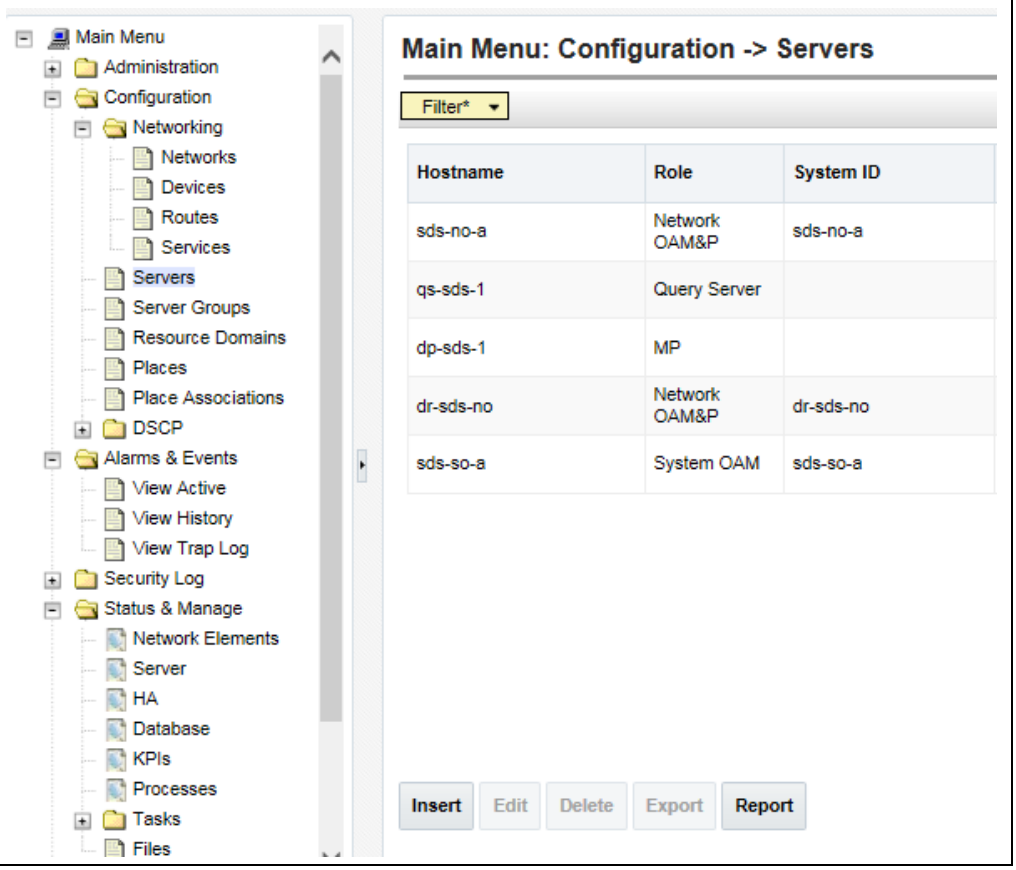
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
38. ☐	**Primary SDS VIP:** Select "**SDS TVOE Guest**" for the **Hardware Profile** for the SOAM from the pull-down menu.	
39. ☐	**Primary SDS VIP:** 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 41**.*	
40. ☐	**Primary SDS VIP:** Enter the site location.	 **NOTE:** *Location is an optional field.*
41. ☐	**Primary SDS VIP:** **1)** Enter the **XMI IP address** and **IMI IP address** for the **SDS SOAM Server**. **2)** Set the **XMI Interface** to "**xmi**" and **DO NOT** check the **VLAN** checkbox. **3)** Set the **IMI Interface** to "**imi**" and **DO NOT** check the **VLAN** checkbox.	

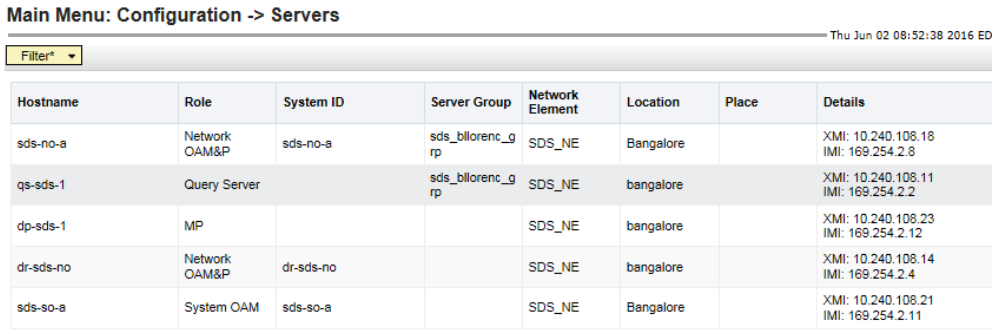
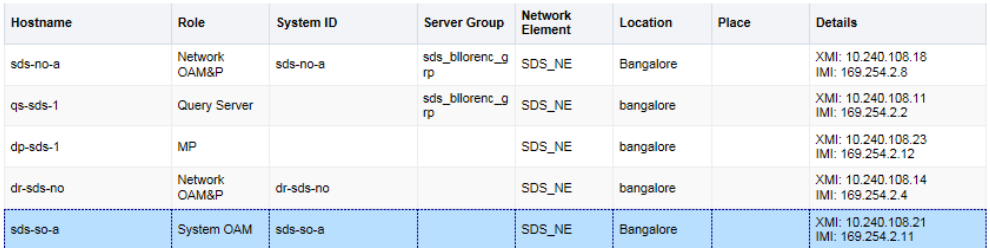
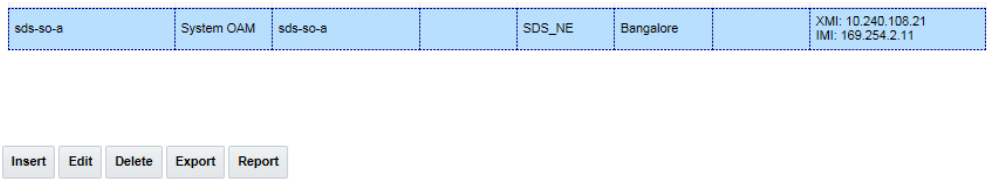
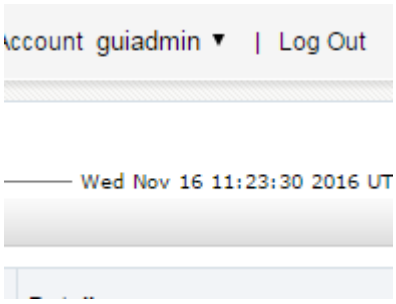
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
42. ☐	**Primary SDS VIP:** **1)** Click the "**NTP Servers:**" **"Add"** dialogue button. **2)** Enter the **NTP Server IP Address** for an NTP Server. **3)** Enter 3 NTP Server **IP address**, repeat (1) and (2) to enter it. **4)** Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other.	
43. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"Apply"** dialogue button.	

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
44. ☐	**Primary SDS VIP:** If the values provided match the network ranges assigned to the NE, the user must select the Info box to receive a banner information message showing that the data has been validated and committed	
45. ☐	**Primary SDS VIP:** Select… **<u>Main Menu</u>** → **Configuration** → ***Servers*** …as shown on the right.	

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
46. ☐	**Primary SDS VIP:** On the **"Configuration →Servers" screen**, find the newly added System SOAM server in the list.	
47. ☐	**Primary SDS VIP:** Use the cursor to select the new SOAM server entry added in the **Step 35**. The row containing the server should now be highlighted.	
48. ☐	**Primary SDS VIP:** Select the **"Export"** dialogue button (bottom left corner of screen).	
49. ☐	Configure the **SDS SOAM B** server.	• Repeat **Steps 33- 48** of this procedure for the **SDS SOAM B Server**.
50. ☐	**Primary SDS VIP:** Click the **"Logout"** link on the SDS server GUI.	
51. ☐	**Primary SDS VIP:** Access the server console.	Connect to the **Active SDS VIP** console using one of the access methods described in **Section 2.3.**

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
52. ☐	**Primary SDS VIP:** Log into the server as the **admusr**	login: **admusr** Password: **<admusr_password>**
53. ☐	**Primary SDS VIP:** Change directory into the file management space.	$ sudo **cd /var/TKLC/db/filemgmt**
54. ☐	**Primary SDS VIP:** Get a directory listing and find the configuration files with the SOAM server A and B name as shown in red. Note: These should appear toward the bottom of the listing.	$ **ls -ltr TKLCConfigData*.sh** ***** TRUNCATED OUTPUT ***** -rw-rw-rw- 1 admusr admusr 2208 Dec 19 16:37 TKLCConfigData.**so-carync-a**.sh -rw-rw-rw- 1 admusr admusr 2208 Dec 19 16:50 TKLCConfigData.**so-carync-b**.sh
55. ☐	**Primary SDS VIP:** Copy the configuration files found in the previous step to the PMAC.	$ sudo **scp -p** *<configuration_file-a> <configuration_file-b>* admusr@*<PMAC_Mgmt_IP>*:/tmp/ **admusr@10.240.39.4's password:** **TKLCConfigData.so-carync-a.sh 100% 1741 1.7KB/s 00:00** **TKLCConfigData.so-carync-b.sh 100% 1741 1.7KB/s 00:00** **[admusr@sds-mrsvnc-a filemgmt]#**
56.	**Primary SDS VIP:** Logout of the Primary SDS CLI.	$ **exit**
57.	**PMAC Server CLI:** Use **SSH** to login to the **PMAC Guest** VM server as the **admusr.**	login: **admusr** Password: **<admusr_password>**

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
58.	**PMAC Guest VM:** **Keyexchange with DP control IP**	**$ keyexchange admusr@<DP_Control_IP>** **Example:** **[admusr@nassau-enc-pmac-1 ~]$ keyexchange admusr@192.168.1.22** **The server does not know of 192.168.1.22.** **Will just exchange host keys for the name given!** **Password of admusr:** **Could not get authorized keys file from remote (192.168.1.22).** **Maybe it does not exist. Continuing...** **The server does not know of 192.168.1.22.** **Will just exchange host keys for the name given!** **ssh is working correctly.** **[admusr@nassau-enc-pmac-1 ~]$**
59. ☐	**PMAC Guest VM:** Copy the server configuration file to the Control IP for the SOAM. **Note:** The Control IP for each OAM is obtained in **Step 18** of this procedure.	$ sudo **scp -p /tmp/**<*configuration_file*> admusr@<*SOAM_Control_IP*>:/var/TKLC/db/filemgmt **admusr@192.168.1.199's password:** **TKLCConfigData.so-carync-a.sh 100% 1741 1.7KB/s 00:00**
60. ☐	**PMAC Guest VM:** Connect to the SOAM server console from the PMAC Server Console	$ sudo **ssh < SOAM_Guest_Control_IP>** admusr@192.168.1.199's password: ***<admusr_password>***
61. ☐	**SOAM Guest VM:** Copy the server configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname (shown in red) from the file name.	***Example:*** TKLCConfigData<.server_hostname>.sh ➔ will translate to ➔TKLCConfigData.sh $ sudo **cp -p /**var/TKLC/db/filemgmt**/**TKLCConfigData.so-carync-a.sh /var/tmp/**TKLCConfigData.sh** **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result

62. ☐	**SOAM Guest VM:**
	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 admusr (Mon Dec 14 15:47:33 2009):`
		
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		
		`Please remove the USB flash drive if connected and reboot the server.`
		<ENTER>

63.	**SOAM Guest VM:** Verify that the desired Time Zone is currently in use.	`$ date` `Mon Aug 10 19:34:51 UTC 2015`
64. ☐	**SOAM Guest VM:** If the desired Time Zone was not presented in the previous step… **Configure the Time Zone.** Otherwise, skip to the next step.	***Example:*** `$` **`sudo set_ini_tz.pl <time_zone>`** **NOTE:** *The following command example sets the time to the "UTC" (aka GMT) time zone which is recommneded for all sites.* *The user may replace, as appropriate, with the customer requested time zone for this site installation. See* ***Appendix G*** *for a list of valid time zones.* `$` **`sudo set_ini_tz.pl "Etc/UTC"`**
65. ☐	**SOAM Guest VM:** Initiate a reboot of the SOAM server.	`$` **`sudo init 6`**
66. ☐	**SOAM Guest VM:** Output similar to that shown on the right may be observed as the server initiates a reboot.	`Connection to 192.168.1.199 closed by remote host.` `Connection to 192.168.1.199 closed.`

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
67. ☐	**PMAC Guest VM:** After the SOAM server has completed reboot, re-connect to the SOAM server console from the PMAC Server Console	`$ sudo ssh <SOAM_Control_IP>` `admusr@192.168.1.199's password: <admusr_password>`

68. ☐	**SOAM Guest VM:**
	
	1) Verify that the I**MI IP address** input in **Step 41** has been applied as specified.
	
	2) Verify that the X**MI IP address** input in **Step 41** has been applied as specified.
		`$ ifconfig |grep in`
		`control  Link encap:Ethernet  HWaddr 52:54:00:23:DC:32`
		`inet addr:192.168.1.199  Bcast:192.168.1.255  Mask:255.255.255.0`
		`imi  Link encap:Ethernet  HWaddr 52:54:00:33:DC:DC`
		`inet addr:10.240.38.78  Bcast:10.240.38.127  Mask:255.255.255.192`
		`lo  Link encap:Local Loopback`
		`inet addr:127.0.0.1  Mask:255.0.0.0`
		`xmi  Link encap:Ethernet  HWaddr 52:54:00:63:63:BD`
		`inet addr:10.240.39.150  Bcast:10.240.39.255  Mask:255.255.255.128`

69.	**SOAM Guest VM:**
	
	Execute a **"syscheck"** to verify the current health of the server.
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
70.	**SOAM Guest VM:** Accept upgrade to the Application Software. - Running the "accept" script from the command line now launches a screen session on blades & VM Guest. - Use the "q" key to exit the screen session	- **[admusr@nassau-sds-so-b ~]$ sudo /var/TKLC/backout/accept** Called with options: --accept Loading Backout::BackoutType::RPM Accepting Upgrade Executing common accept tasks Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info. Cleaning backout directory. Clearing Upgrade Accept/Reject alarm. Cleaning message from MOTD. No patch pending alarm on server so no MOTD update. Cleaning up RPM config backup files... Checking / Checking /boot Checking /tmp Checking /usr Checking /var Checking /var/TKLC Checking /tmp/appworks_temp Checking /usr/openv Checking /var/TKLC/appw/logs/Process Checking /var/TKLC/appw/logs/Security Checking /var/TKLC/db/filemgmt Checking /var/TKLC/rundb Starting cleanup of RCS repository. INFO: Removing '/etc/my.cnf' from RCS repository INFO: Removing '/etc/pam.d/password-auth' from RCS repository INFO: Removing '/etc/pam.d/system-auth' from RCS repository INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0' from RCS repository INFO: Removing '/etc/php.d/zip.ini' from RCS repository INFO: Removing '/var/lib/prelink/force' from RCS repository === Window terminated (Thu Feb 2 20:07:21 2017) === screen session: use 'screen -x upgrade' to reconnect Type the letter "q" on the keyboard to exit the screen session. [screen is terminating] **[admusr@nassau-sds-so-b ~]$**
71.	Apply the **SDS SOAM B** server configuration file.	• Repeat Steps 57 – 70 of this procedure for **SOAM Server B**.

Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result

72. ☐	**SOAM Guest B:**
	From the **SOAM-B** Guest, **"ping"** the **IMI IP address** of the **SOAM-A** Guest
		`$ ping -c 5 10.240.38.78`
		`PING 10.240.38.78 (10.240.38.78) 56(84) bytes of data.`
		`64 bytes from 10.240.38.78: icmp_seq=1 ttl=64 time=0.031 ms`
		`64 bytes from 10.240.38.78: icmp_seq=2 ttl=64 time=0.017 ms`
		`64 bytes from 10.240.38.78: icmp_seq=3 ttl=64 time=0.031 ms`
		`64 bytes from 10.240.38.78: icmp_seq=4 ttl=64 time=0.028 ms`
		`64 bytes from 10.240.38.78: icmp_seq=5 ttl=64 time=0.030 ms`
		`64 bytes from 10.240.38.78: icmp_seq=6 ttl=64 time=0.028 ms`
		
		`--- 10.240.38.78 ping statistics ---`
		`6 packets transmitted, 6 received, 0% packet loss, time 5000ms`
		`rtt min/avg/max/mdev = 0.017/0.027/0.031/0.007 ms`

73.	**SOAM Guest B:**
	From the **SOAM-B** Guest, **"ping"** the **XMI IP address** of the **SOAM-A** Guest
		`$ ping -c 5 10.240.39.150`
		`PING 10.240.39.150 (10.240.39.150) 56(84) bytes of data.`
		`64 bytes from 10.240.39.150: icmp_seq=1 ttl=64 time=0.024 ms`
		`64 bytes from 10.240.39.150: icmp_seq=2 ttl=64 time=0.033 ms`
		`64 bytes from 10.240.39.150: icmp_seq=3 ttl=64 time=0.032 ms`
		`64 bytes from 10.240.39.150: icmp_seq=4 ttl=64 time=0.026 ms`
		`64 bytes from 10.240.39.150: icmp_seq=5 ttl=64 time=0.027 ms`
		`64 bytes from 10.240.39.150: icmp_seq=6 ttl=64 time=0.026 ms`
		
		`--- 10.240.39.150 ping statistics ---`
		`6 packets transmitted, 6 received, 0% packet loss, time 5004ms`
		`rtt min/avg/max/mdev = 0.024/0.028/0.033/0.003 ms`

74. ☐	**SOAM Guest B:**
	From the **SOAM-B** Guest, **"ping"** the local **XMI Gateway address** associated with the SOAM NE.
		`$ ping -c 5 10.240.39.1`
		`PING 10.240.39.1 (10.240.39.1) 56(84) bytes of data.`
		`64 bytes from 10.240.39.1: icmp_seq=1 ttl=64 time=0.024 ms`
		`64 bytes from 10.240.39.1: icmp_seq=2 ttl=64 time=0.033 ms`
		`64 bytes from 10.240.39.1: icmp_seq=3 ttl=64 time=0.032 ms`
		`64 bytes from 10.240.39.1: icmp_seq=4 ttl=64 time=0.026 ms`
		`64 bytes from 10.240.39.1: icmp_seq=5 ttl=64 time=0.027 ms`
		`64 bytes from 10.240.39.1: icmp_seq=6 ttl=64 time=0.026 ms`
		
		`--- 10.240.39.1 ping statistics ---`
		`6 packets transmitted, 6 received, 0% packet loss, time 5004ms`
		`rtt min/avg/max/mdev = 0.024/0.028/0.033/0.003 ms`

75. ☐	**SOAM Guest VM:**
	Use the **"ntpq"** command to verify that the server has connectivity to the assigned Primary and Secondary NTP server(s).
		`$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`+10.250.32.10 192.5.41.209 2 u 139 1024 377 2.008 1.006 1.049`
		`*10.250.32.51 192.5.41.209 2 u 979 1024 377 0.507 1.664 0.702`

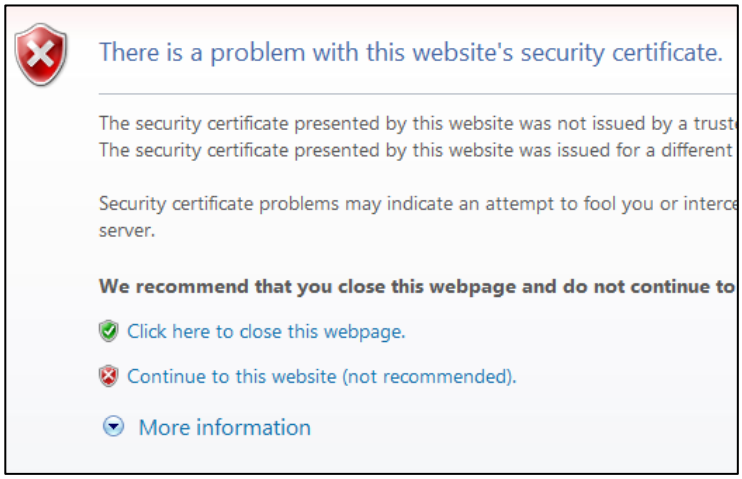
Procedure 9. Configuring the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
	IF CONNECTIVITY TO THE NTP SERVER(S) CANNOT BE ESTABLISHED, STOP AND EXECUTE THE FOLLOWING STEPS: **1)** Contact the customer to verify that the IP addresses for the NTP server(s) are correct. **2)** Have the customer IT group provide a network path from the OAM server IP to the assigned NTP IP addresses. **ONCE NETWORK CONNECTIVITY IS ESTABLISHED TO THE ASSIGNED NTP IP ADDRESSES, THEN RESTART THIS PROCEDURE BEGINNING WITH STEP 75.**	
76. ☐	**SOAM Guest VM:** Exit from the SOAM command line to return the PMAC server console prompt.	`$ exit`
77. ☐	**PMAC Guest VM:** Exit from the PMAC server	`$ exit`
THIS PROCEDURE HAS BEEN COMPLETED		

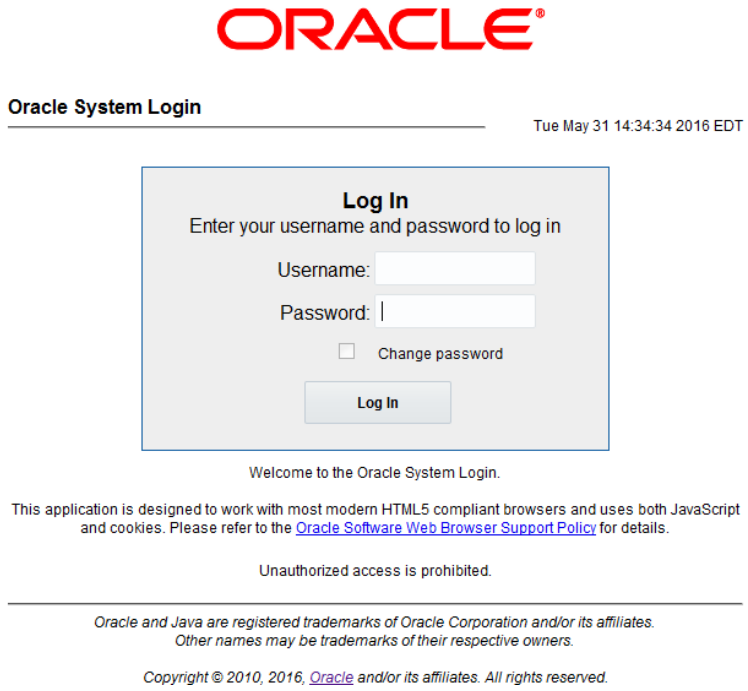
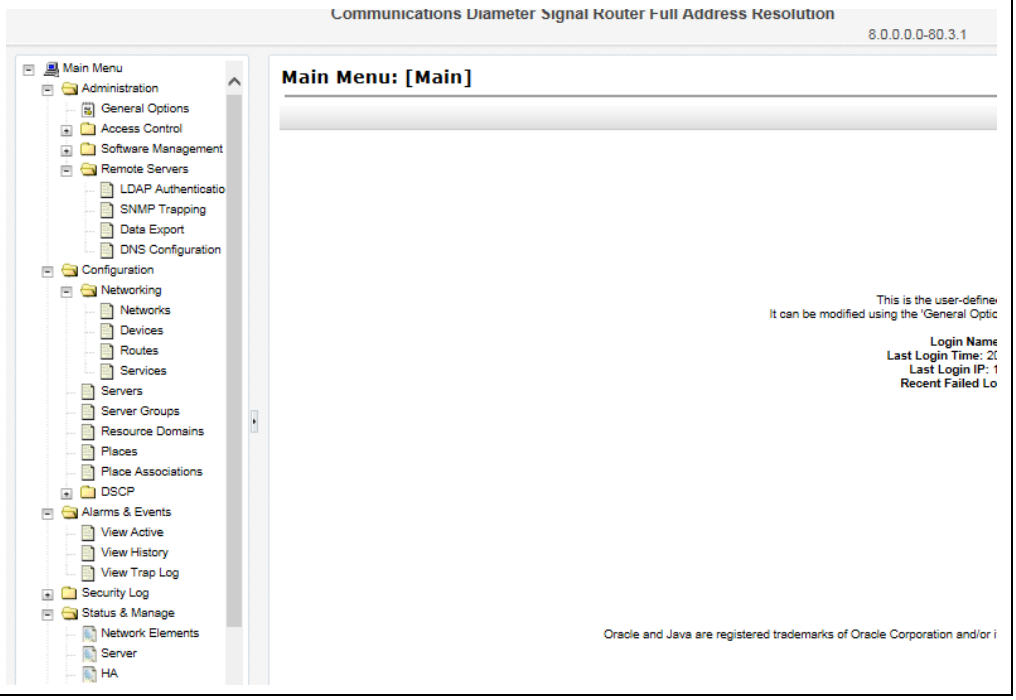
5.8 OAM Pairing for SDS SOAM Sites (All SOAM Sites)

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.

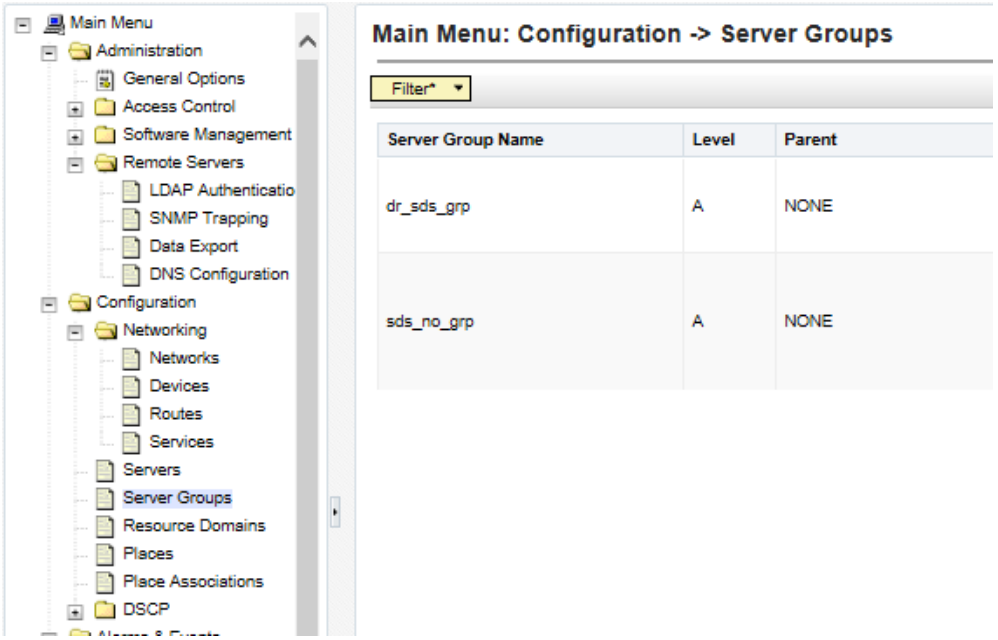
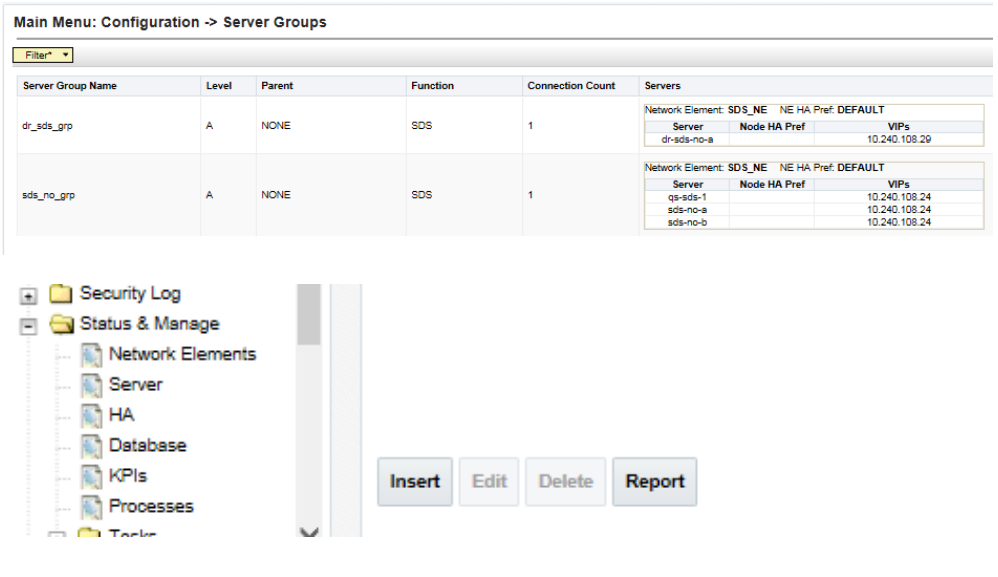
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

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

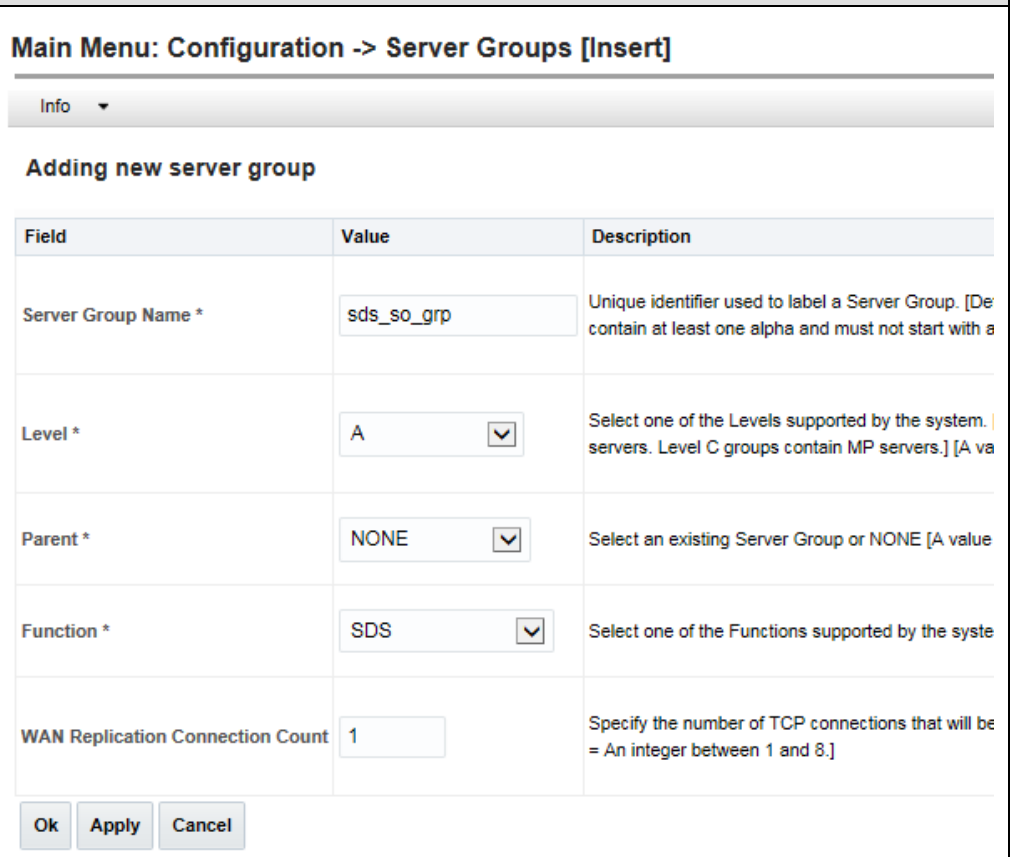
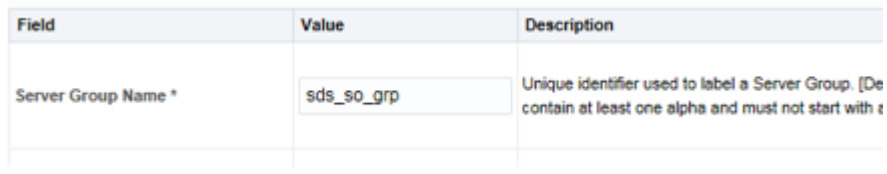
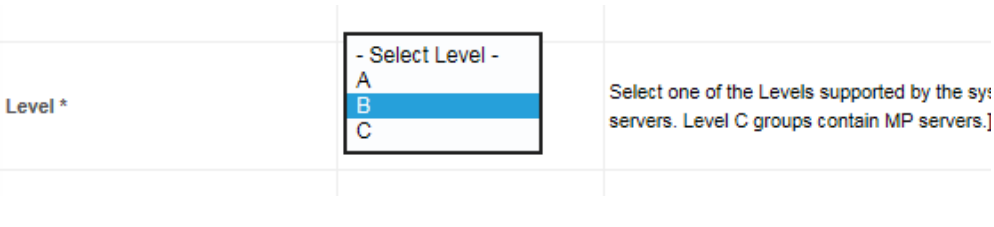
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
2. ☐	**Primary 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. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	

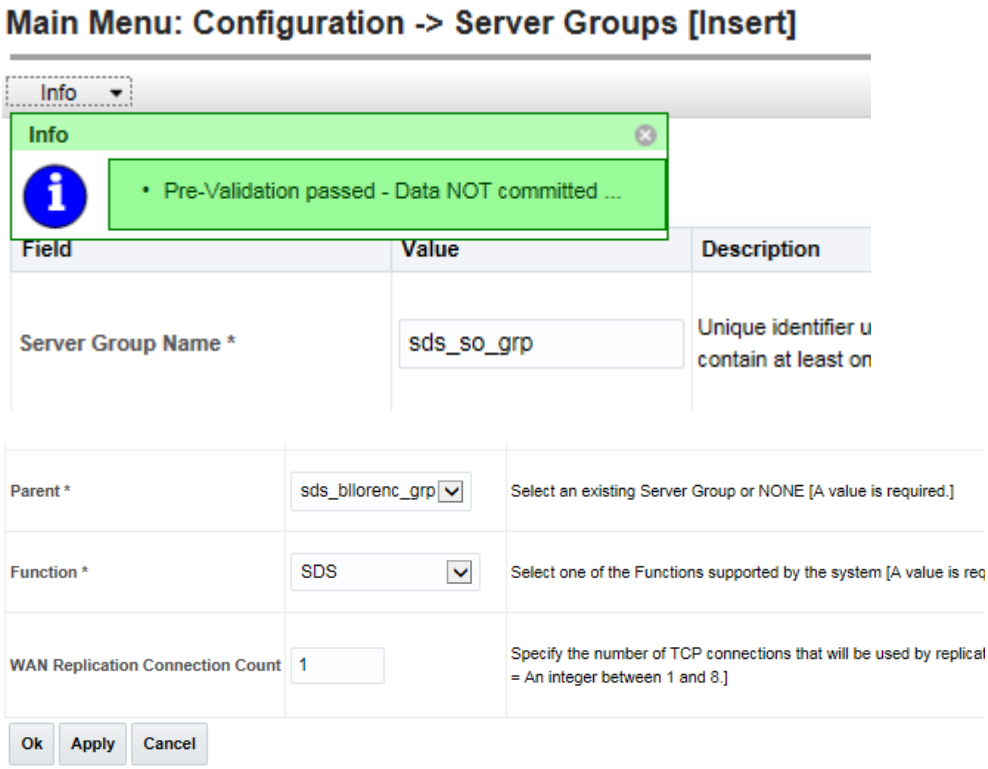
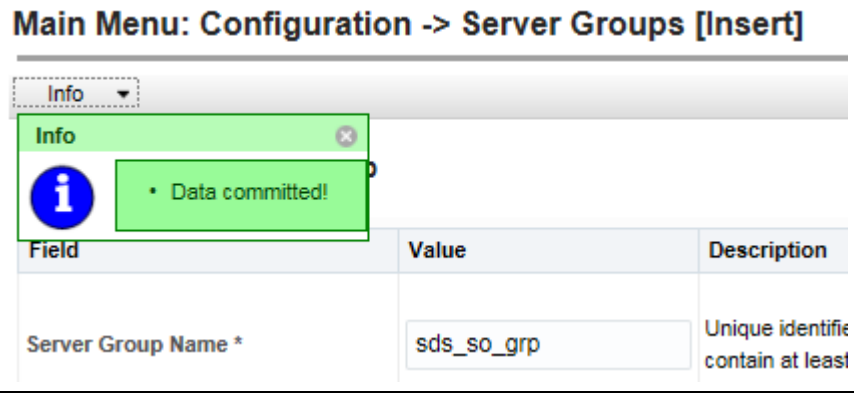
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
4. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	
5. ☐	**Primary 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.*	

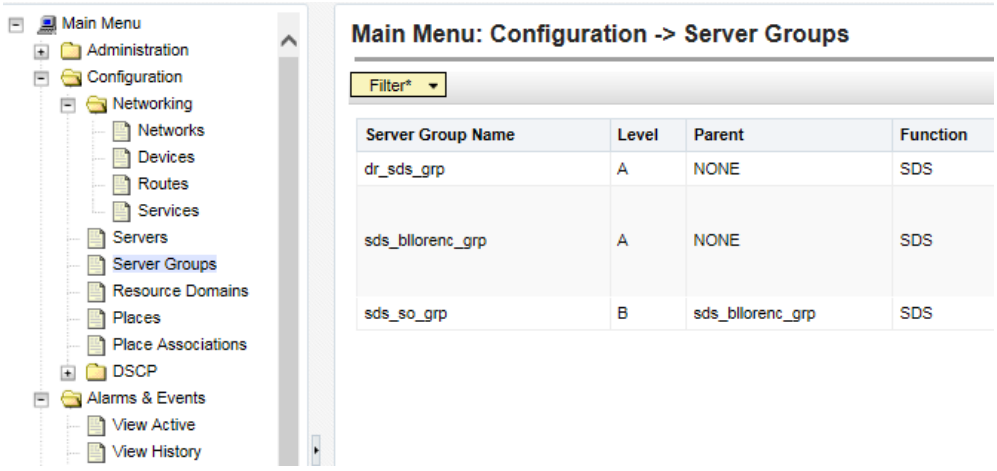
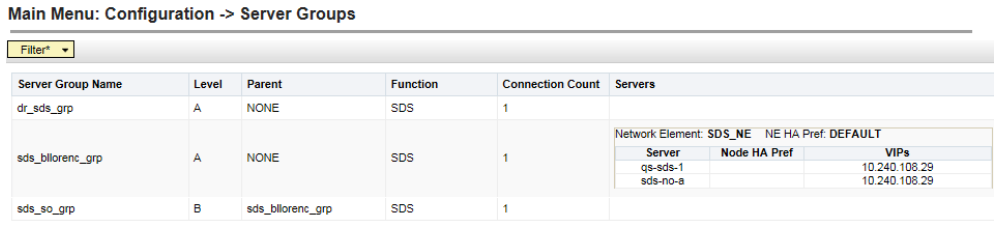
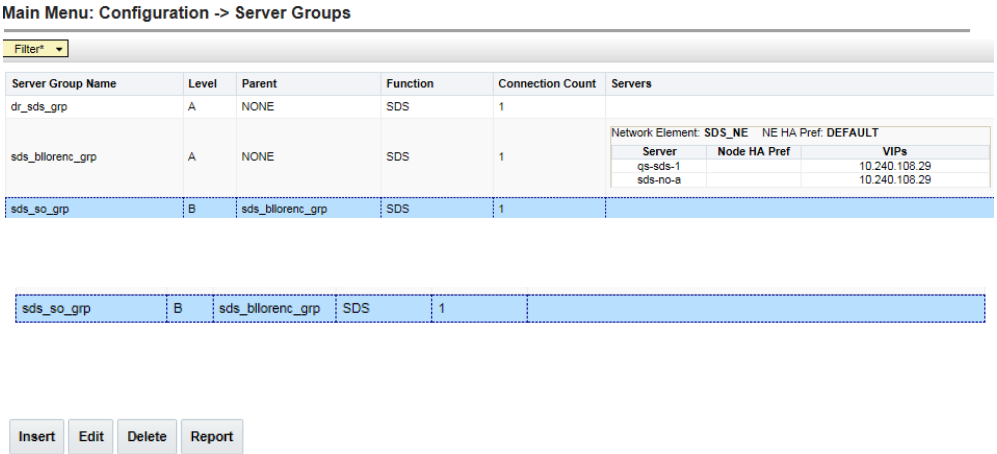
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
6. ☐	**Primary 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).*	
7. ☐	**Primary SDS VIP:** Input the **Server Group Name**.	
8. ☐	**Primary SDS VIP:** Select **"B"** on the **"Level"** pull-down menu...	
9. ☐	**Primary SDS VIP:** Select the 1st SDS Site's server group, as entered in **Procedure 3, Step 7,** on the **"Parent"** pull-down menu...	

Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
10. ☐	**Primary SDS VIP:** Select **"SDS"** on the **"Function"** pull-down menu.	
11. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
12. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	

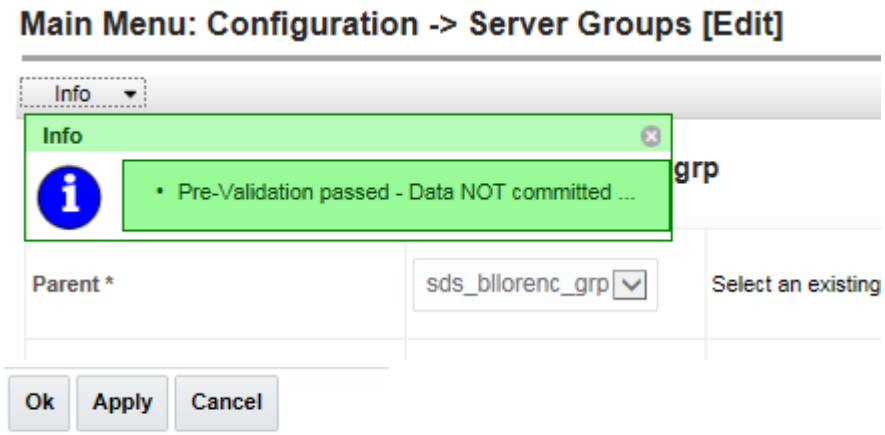
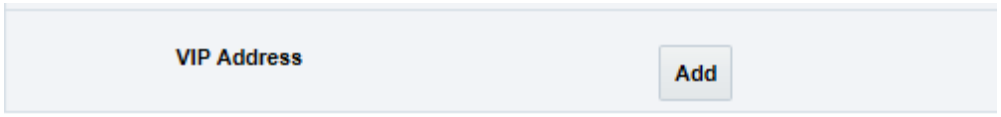
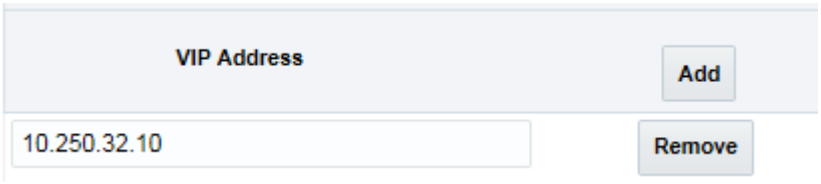
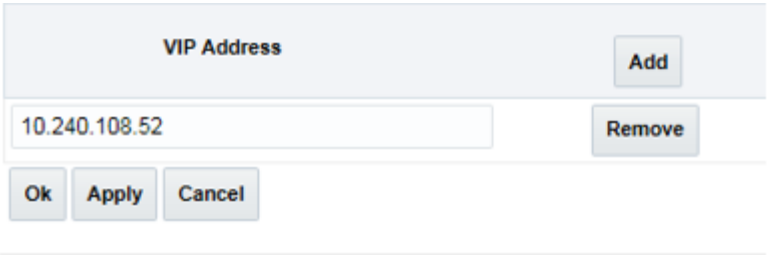
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
14. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	
15. ☐	**Primary SDS VIP:** The **Server Group** entry should be shown on the **"Server Groups"** configuration screen as shown on the right.	
16. ☐	**Primary SDS VIP:** **1)** Select the **Server Group** entry applied in **Step 12**. The line entry should now be highlighted. **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.*	

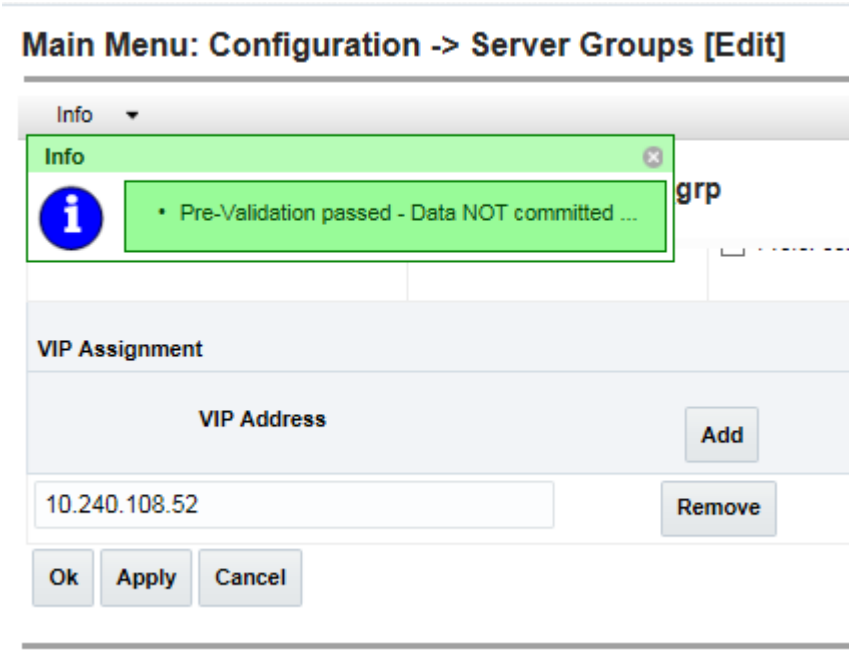
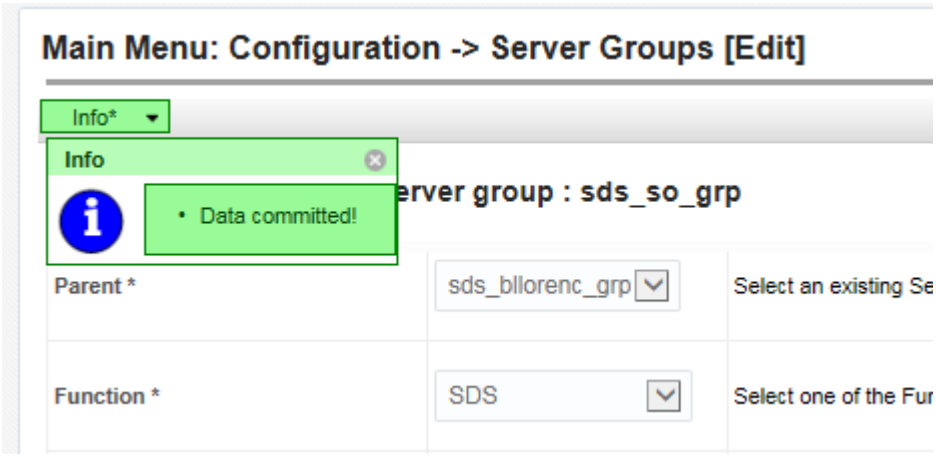
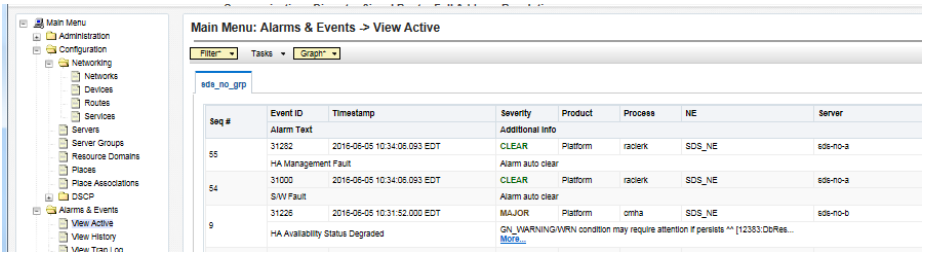
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
17. ☐	**Primary SDS VIP:** The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	
18. ☐	**Primary SDS VIP:** Select the **"A"** server and the **"B"** server from the list of **"Servers"** by clicking the check box next to their names.	

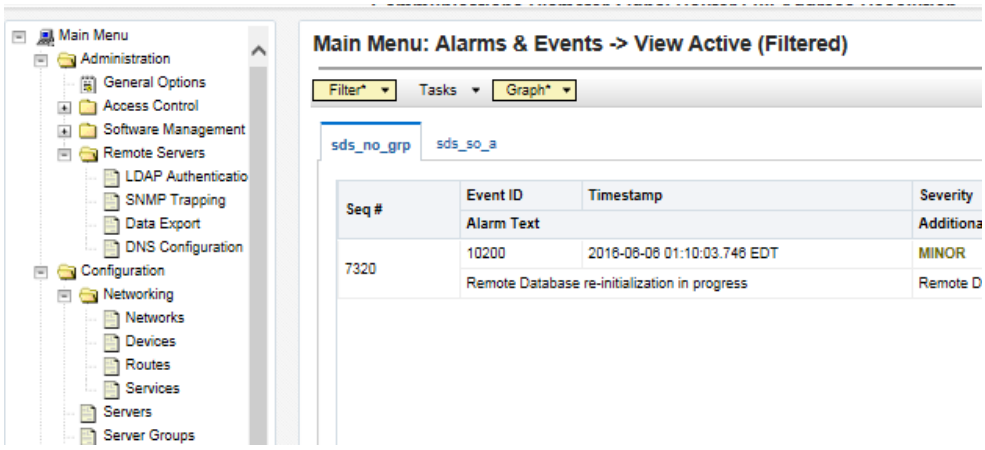
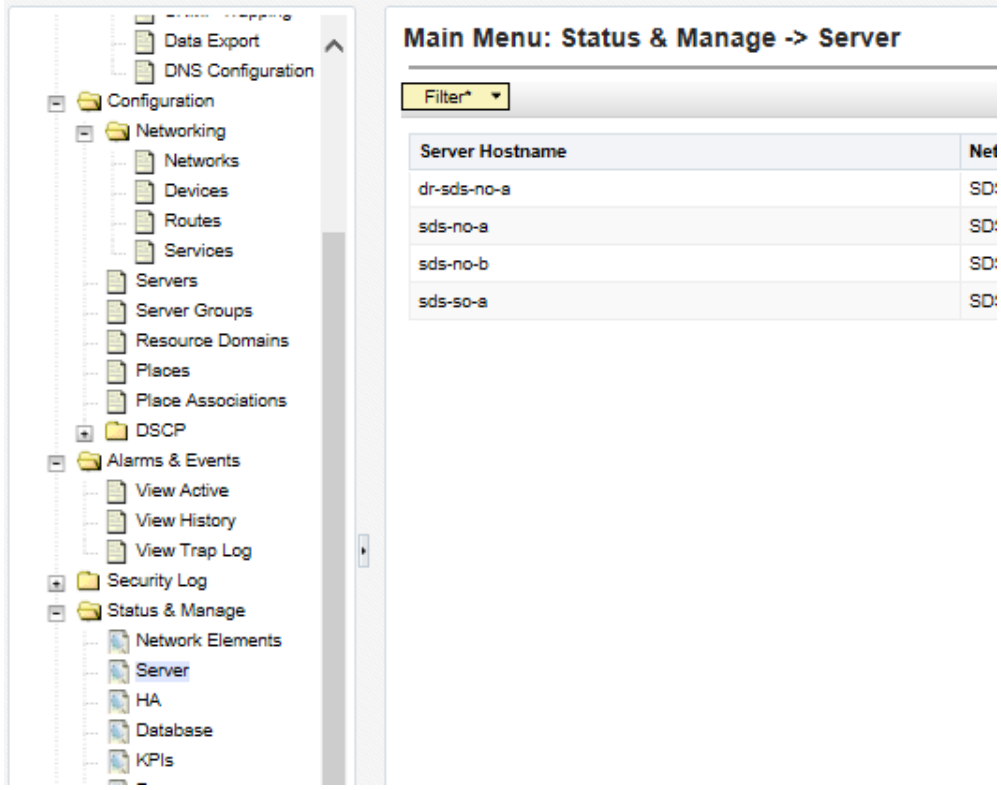
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
19. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
20. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
21. ☐	**Primary SDS VIP:** Click the **"Add"** dialogue button for the **VIP Address**.	
22. ☐	**Primary SDS VIP:** Input the **VIP Address**	
23. ☐	**Primary SDS VIP:** Click the **"Apply"** dialogue button.	

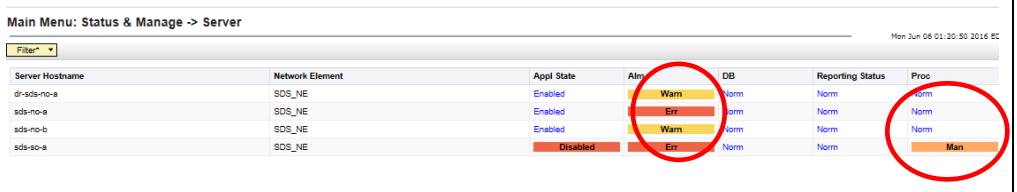
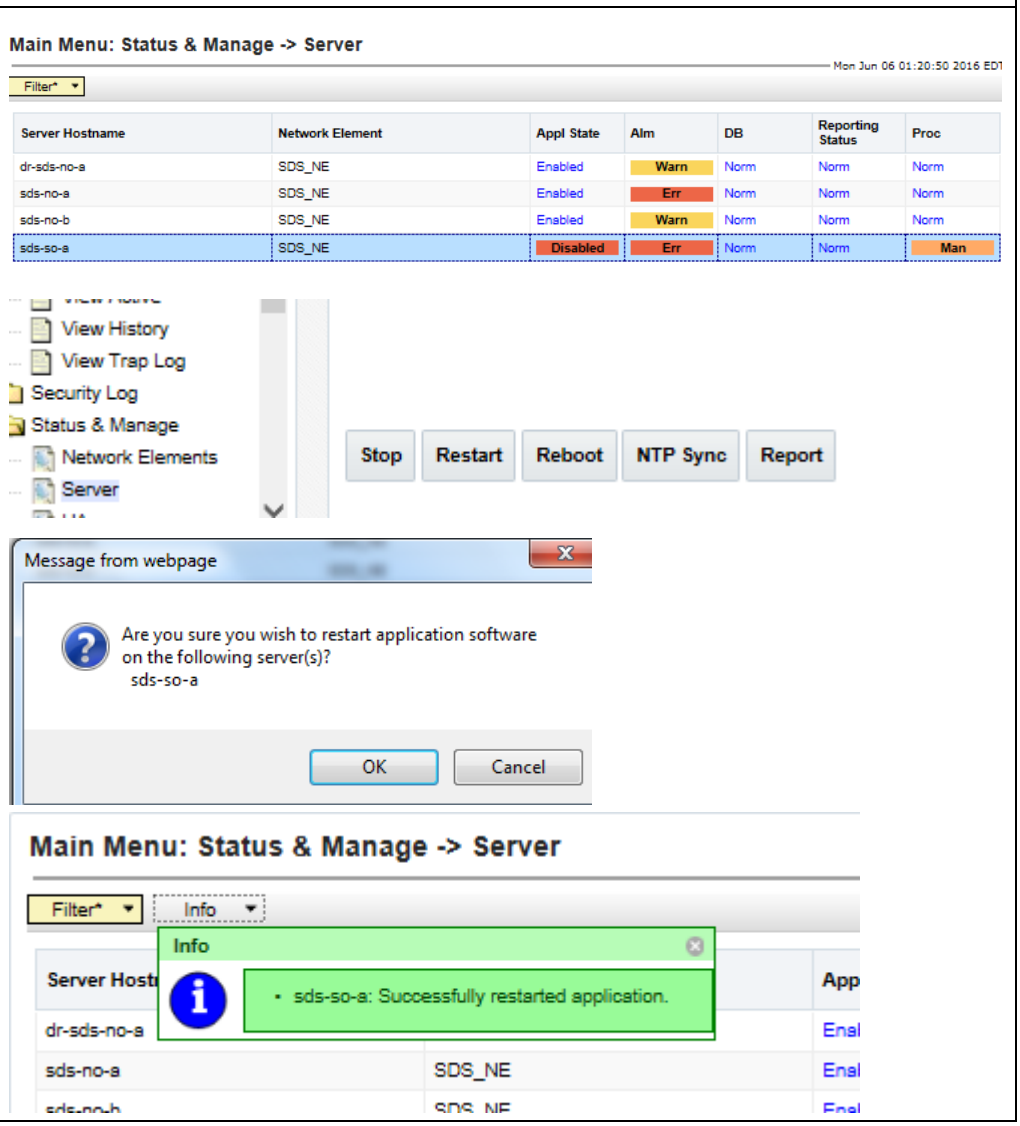
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
24. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
25. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
26.	**Primary SDS VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	

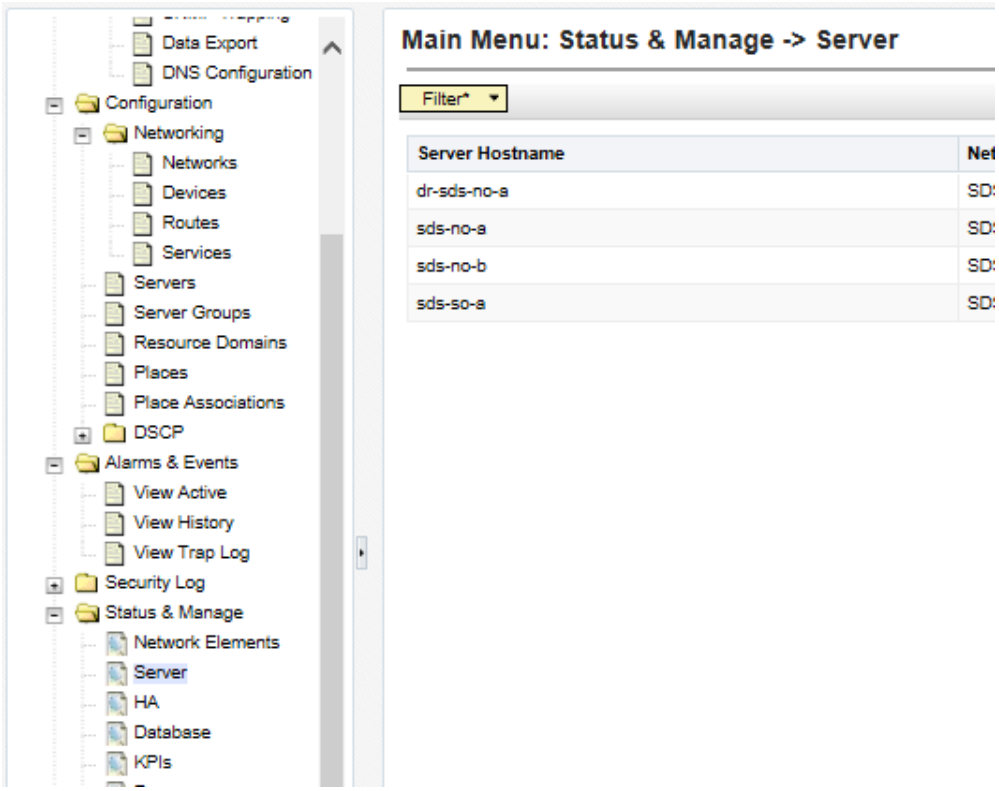
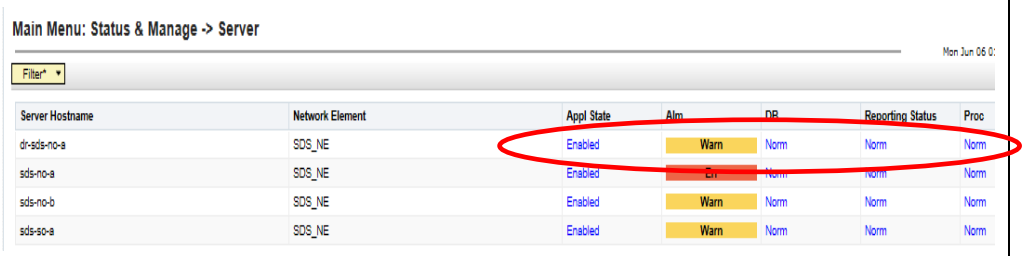
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
27.	**Primary SDS VIP:** Verify that **Event ID 10200** (*Remote Database re-initialization in progress)* alarms are present with the **SDS SOAM Server hostnames** in the **"Instance"** field..	
	MONITOR THE EVENT ID 10200 (*Remote Database re-initialization in progress)* ALARMS. **DO NOT PROCEED TO THE NEXT STEP UNTIL THE ALARM CLEAR IS RECEIVED FOR BOTH SDS SOAM SERVERS.**	
28. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	

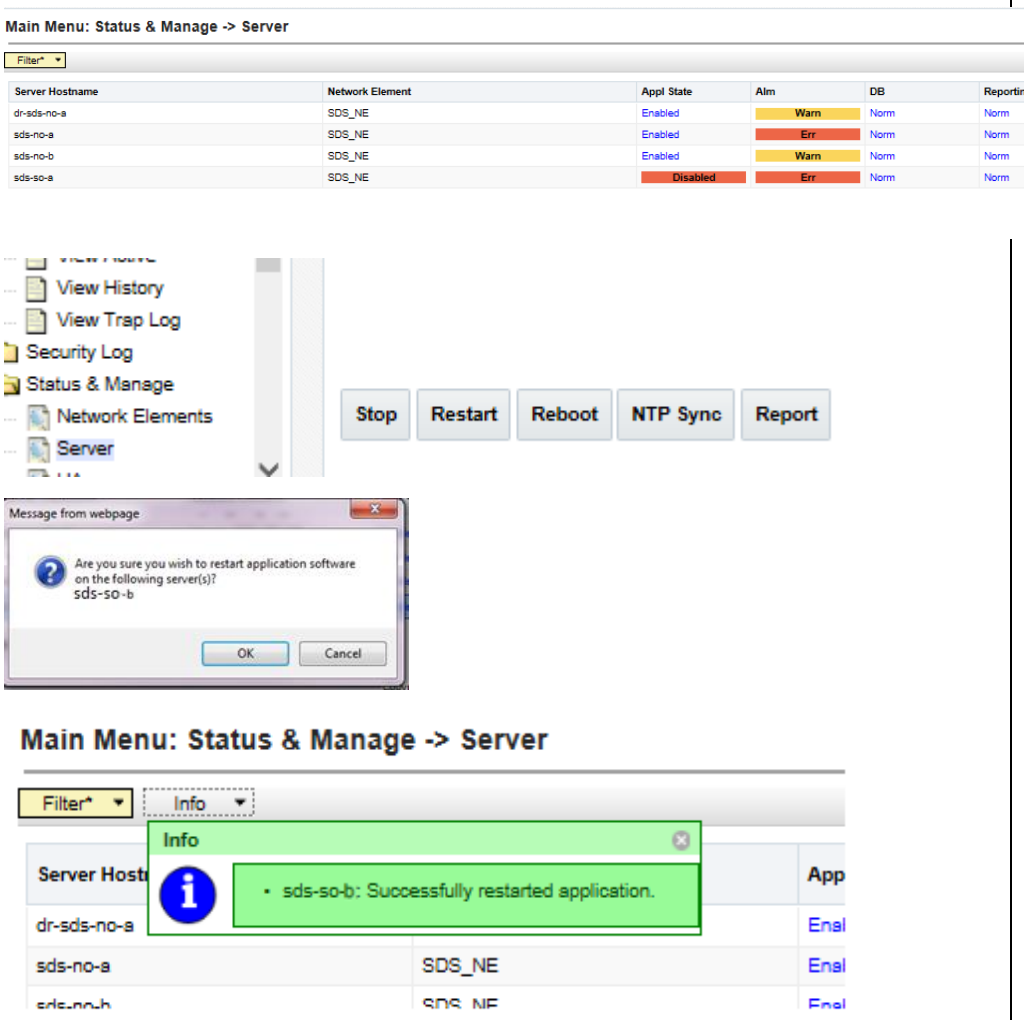
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
29. ☐	**Primary SDS VIP:** **1)** The **"A"** and **"B"** 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.	
30. ☐	**Primary SDS VIP:** **1)** Using the mouse, select **SOAM Server A**. The line entry should now be highlighted. **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 **SOAM Server A** stating: **"Successfully restarted application"**.	

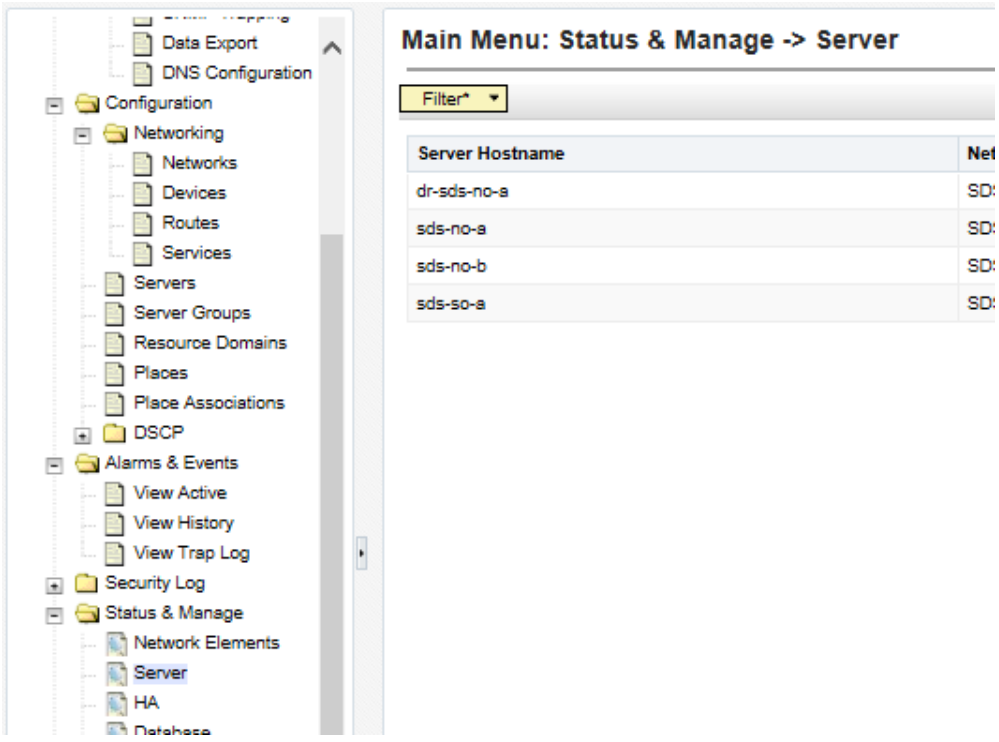
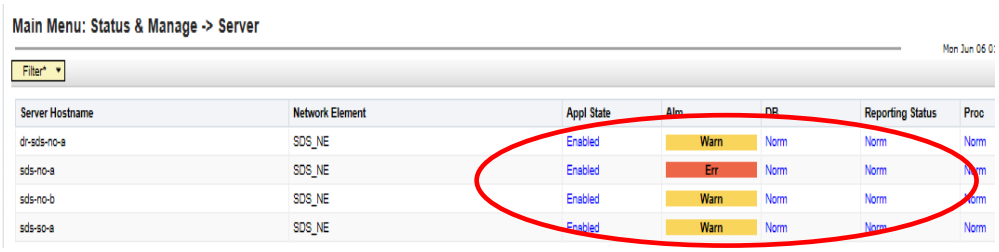
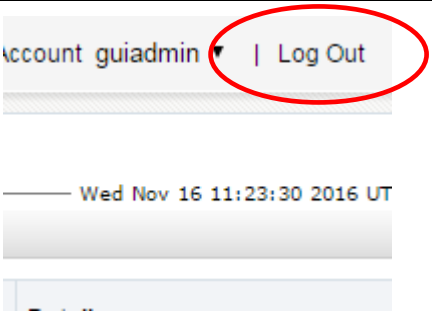
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
31. ☐	**Primary SDS VIP:** Select… **Main Menu** **→ Status & Manage** **→ *Server*** …as shown on the right.	
32. ☐	**Primary SDS VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status, & Proc"** status columns all show **"Norm"** for **SOAM 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.*	

Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
33. ☐	**Primary SDS VIP:** **1)** Using the mouse, select **SOAM Server B**. The line entry should now be highlighted. **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 **SOAM Server B** stating: **"Successfully restarted application"**.	

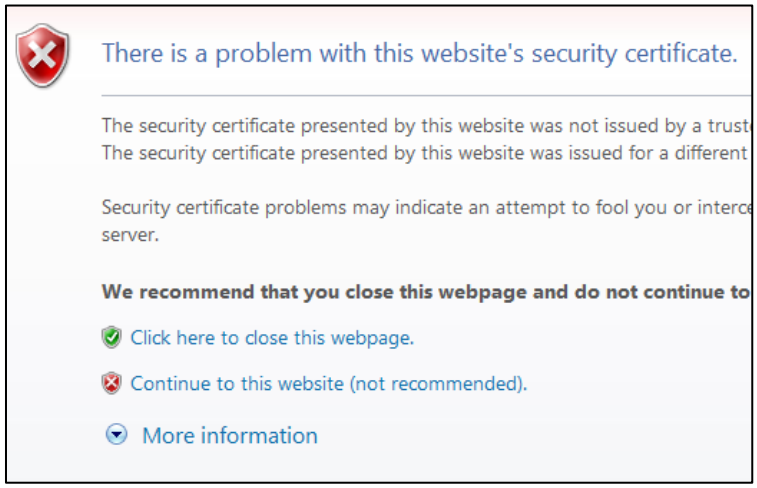
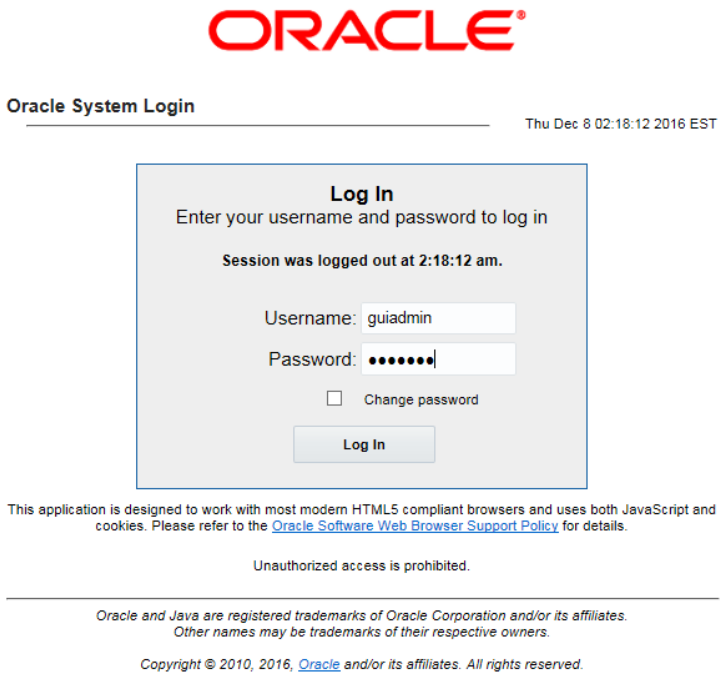
Procedure 10. Pairing the SDS SOAM Servers (All SOAM Sites)

Step	Procedure	Result
34. ☐	**Primary SDS VIP:** Select… **Main Menu** **→ Status & Manage** **→ *Server*** …as shown on the right.	
35. ☐	**Primary SDS VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for **SOAM Server A** and **Server B** 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.*
36. ☐	**Primary SDS VIP:** Click the **"Logout"** link on the SDS server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

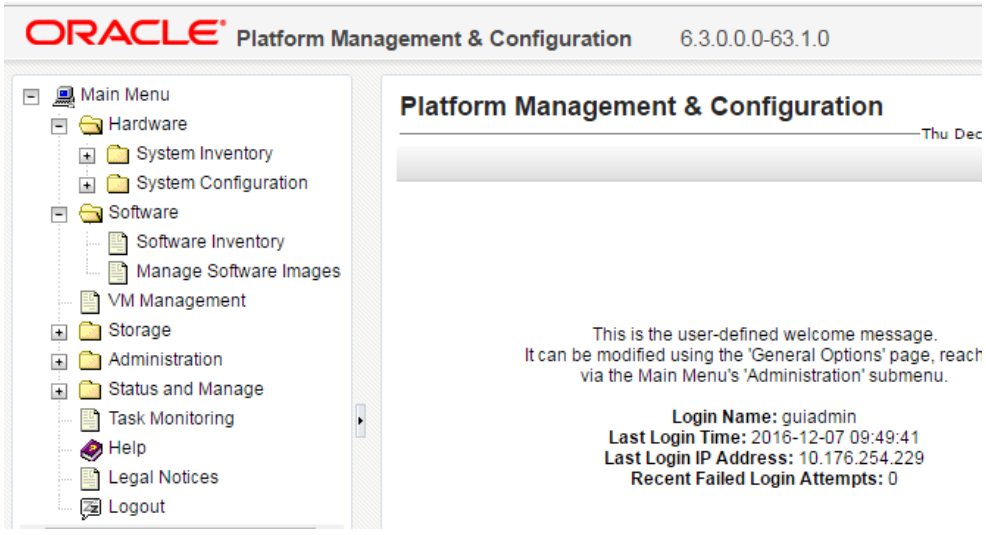
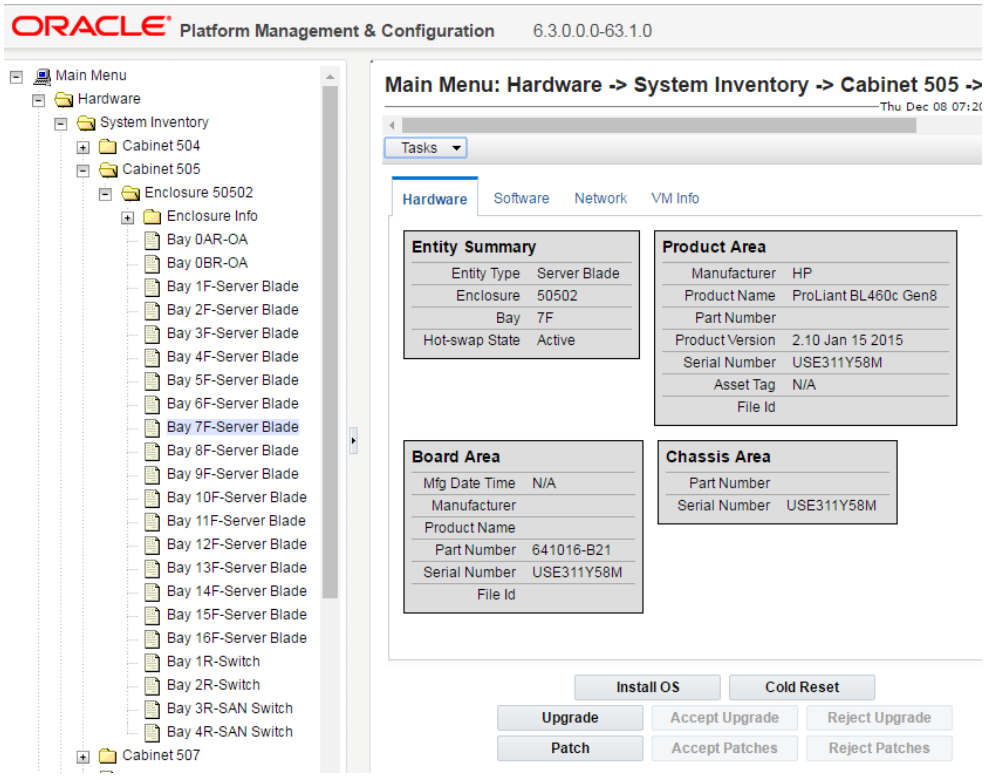
5.9 DP Installation (All SOAM Sites)

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.

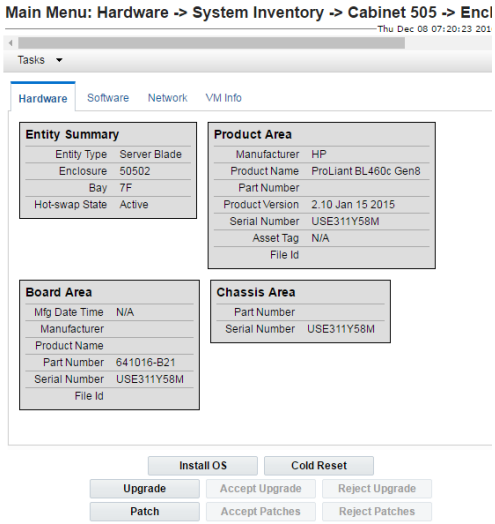
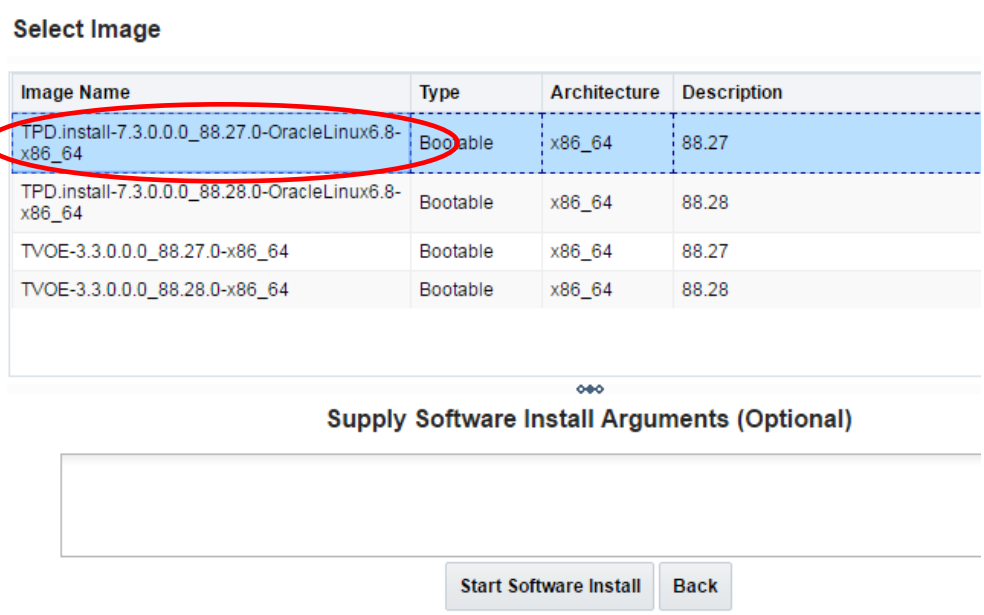
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
		EXECUTE Appendix I: (*Disable Hyperthreading for Gen8 and Gen9 (DP Only*) ON EACH DP BLADE AFTER THIS PROCEDURE.
1. ☐	**PMAC Guest VM:** Launch an approved web browser and connect to the **XMI IP Address** of the PMAC server at the SOAM site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**PMAC Guest VM:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

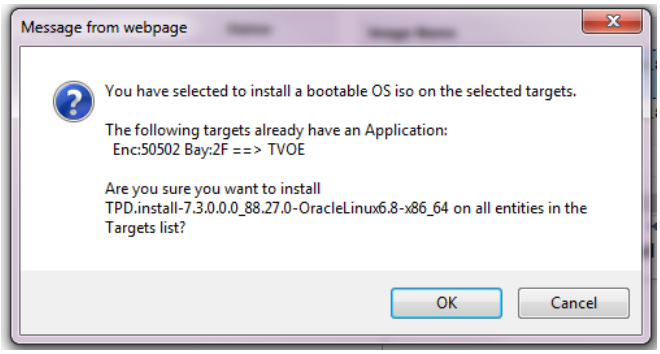
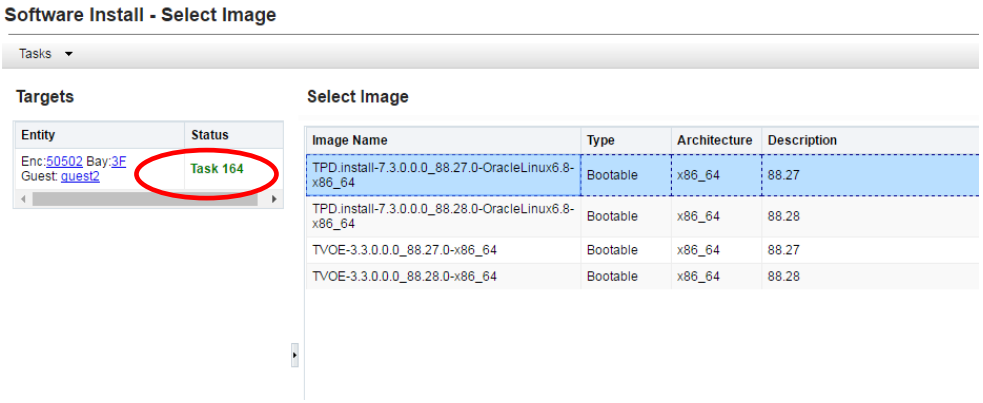
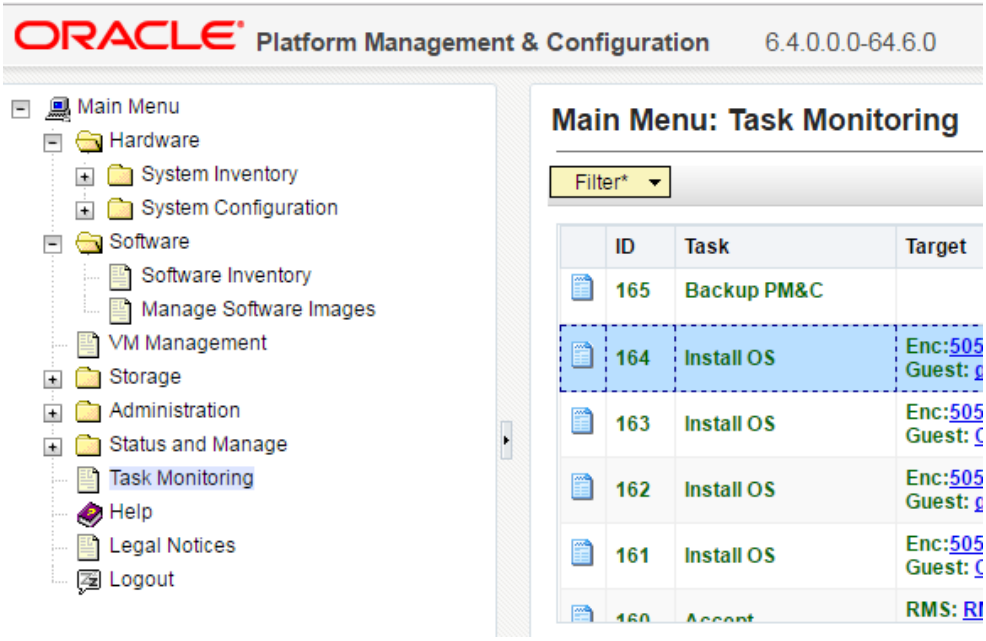
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
3. ☐	**PMAC Guest VM:** The user should be presented the PMAC Main Menu as shown on the right...	
4. ☐	**PMAC Guest VM:** Select the designated DP server blade from the Menu… **Main Menu** → **Hardware** → **System Inventory** → **<Cabinet>** → **<Enclosure>** → **<Server Blade>** …as shown on the right.	

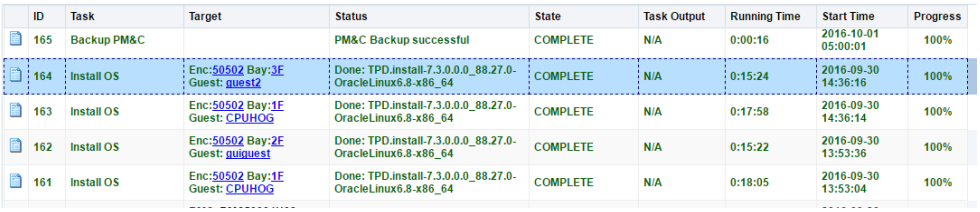
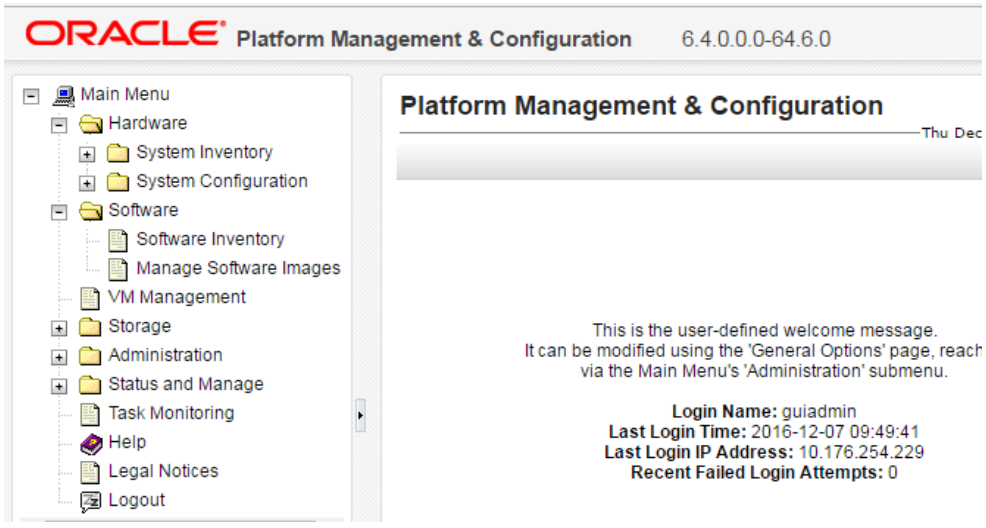
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
5. ☐	**PMAC Guest VM:** Install the operating system by clicking the **"Install OS"** dialogue button	
6. ☐	**PMAC Guest VM:** **1)** Select the desired **TPD Image** **2)** Click the **"Start Software Install"** dialogue button	

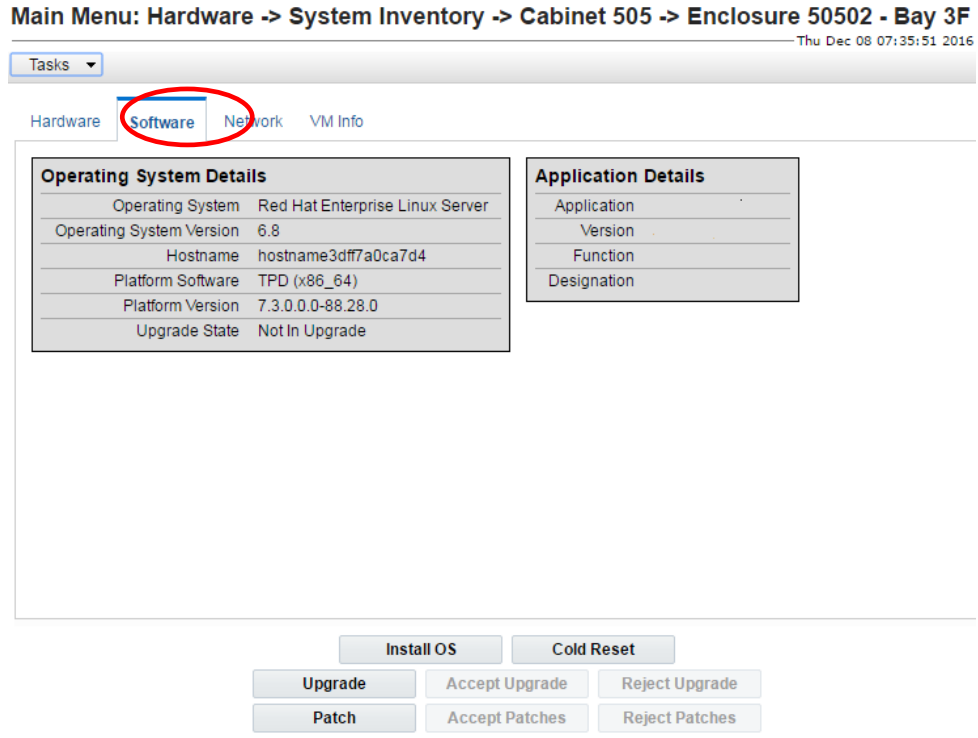
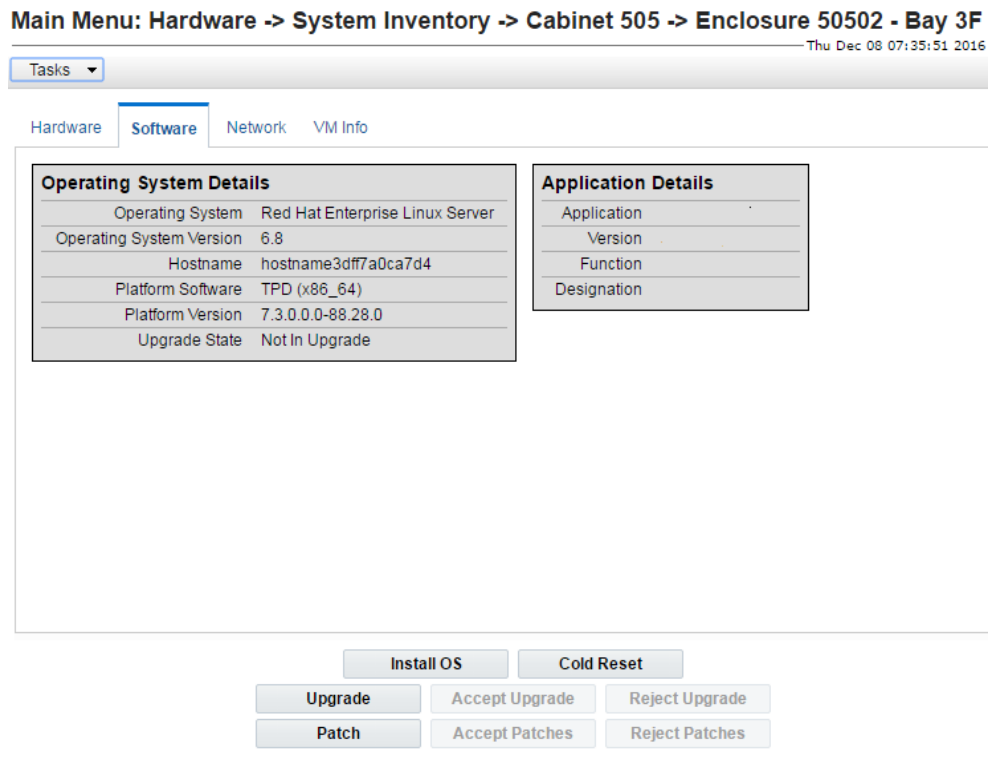
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
7. ☐	**PMAC Guest VM:** The user should be presented with an "**Are you sure you want to install**" message box as shown on the right. Click the "**OK**" dialogue button	
8. ☐	**PMAC Guest VM:** Note the task number assigned to SDS Application upgrade. This number will be used to track its progress. This task takes up to ~25 minutes.	
9. ☐	Execute **"Install OS"** for for each additional **DP** Server.	• Repeat **Steps 4 – 8** of this procedure for each additional **DP server blade** in the **SOAM** enclosure.
10. ☐	**PMAC Guest VM:** **1)** Select… **Main Menu** → **Task Monitoring** …as shown on the right.	

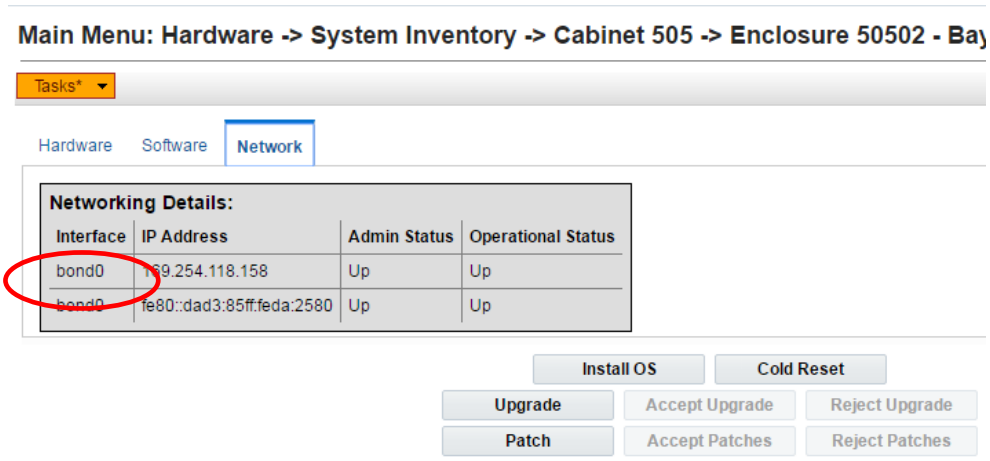
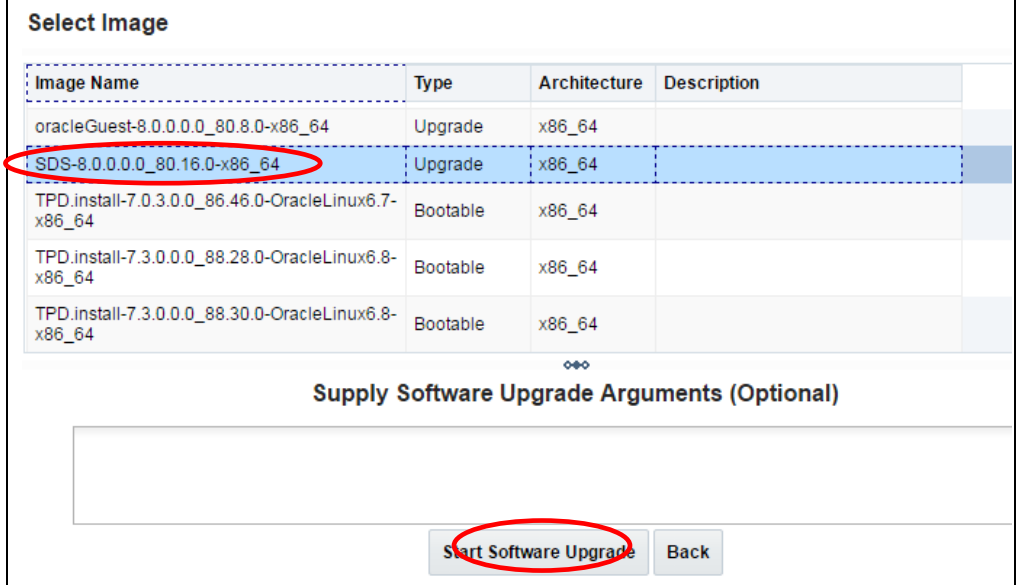
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
11. ☐	**PMAC Guest VM:** Wait till Progress is 100% with a Status of Success and a State of Complete. .... then proceed to the next step.	
12. ☐	**PMAC Guest VM:** Re-select the designated DP server blade from the Menu… **Main Menu** → **Hardware** → **System Inventory** → **<Cabinet>** → **<Enclosure>** → **<Server Blade>** …as shown on the right.	

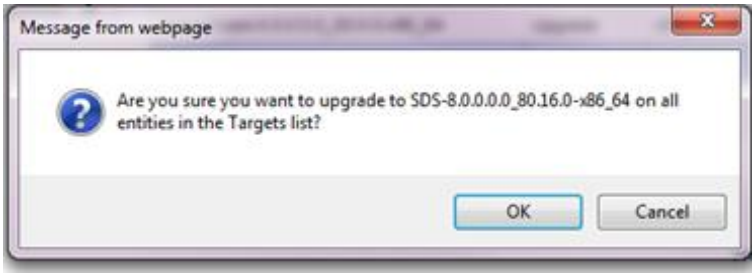
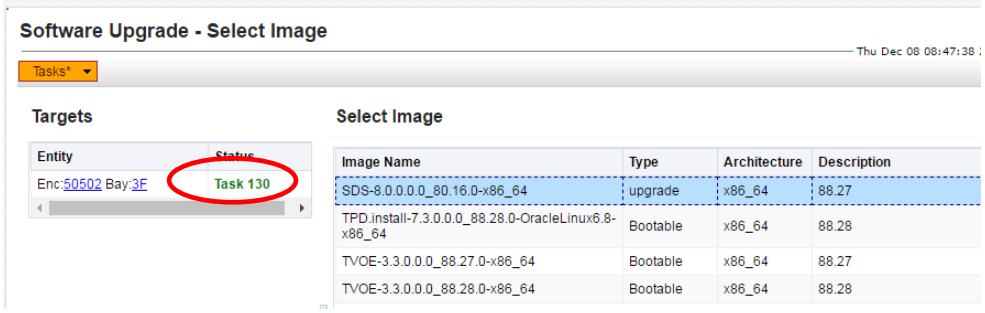
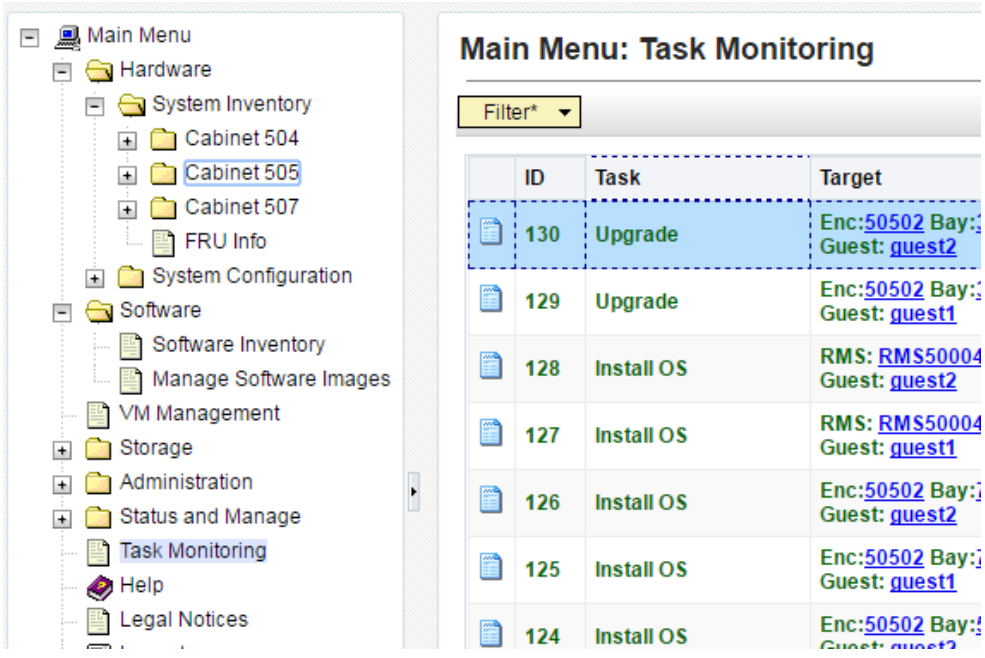
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
13. ☐	**PMAC Guest VM:** Select the “Software” tab.	
14. ☐	**PMAC Guest VM:** **1)** Verify the correct TPD is shown. **2)** Verify “**Application Details**” are blank.	

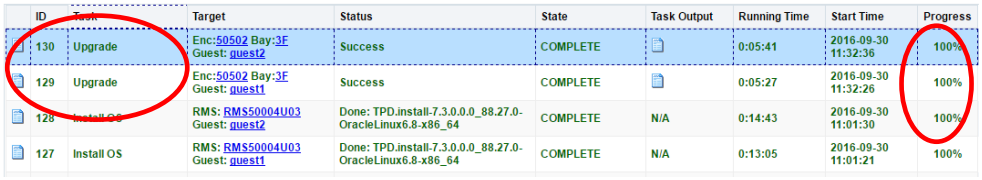
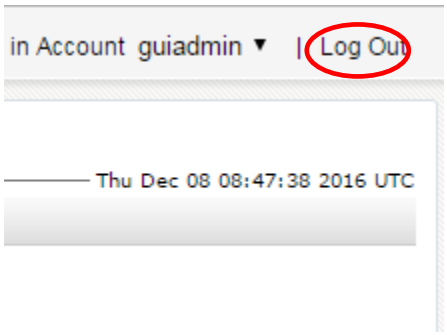
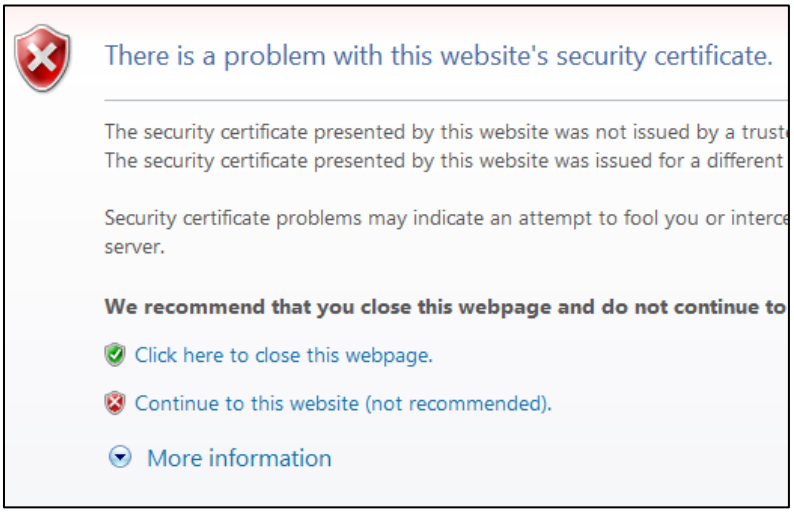
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
15. ☐	**PMAC Guest VM:** **1)** Select the "**Network**" tab. **2)** Make note of the control IP address for this DP, called "**bond0**"; it will be referenced later **3)** Select the "**Upgrade**" button.	
16. ☐	**PMAC Guest VM:** **1)** Select the correct **SDS** version from the "**Image Name"** list. The line entry should now be highlighted. **2)** Select the "**Start Software Upgrade**" dialogue button	

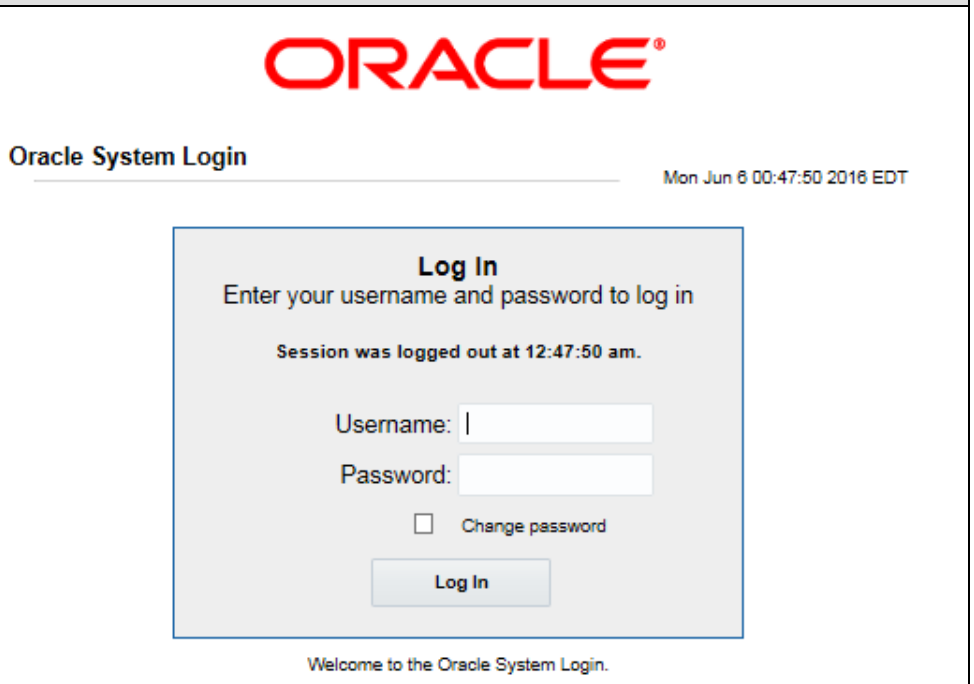
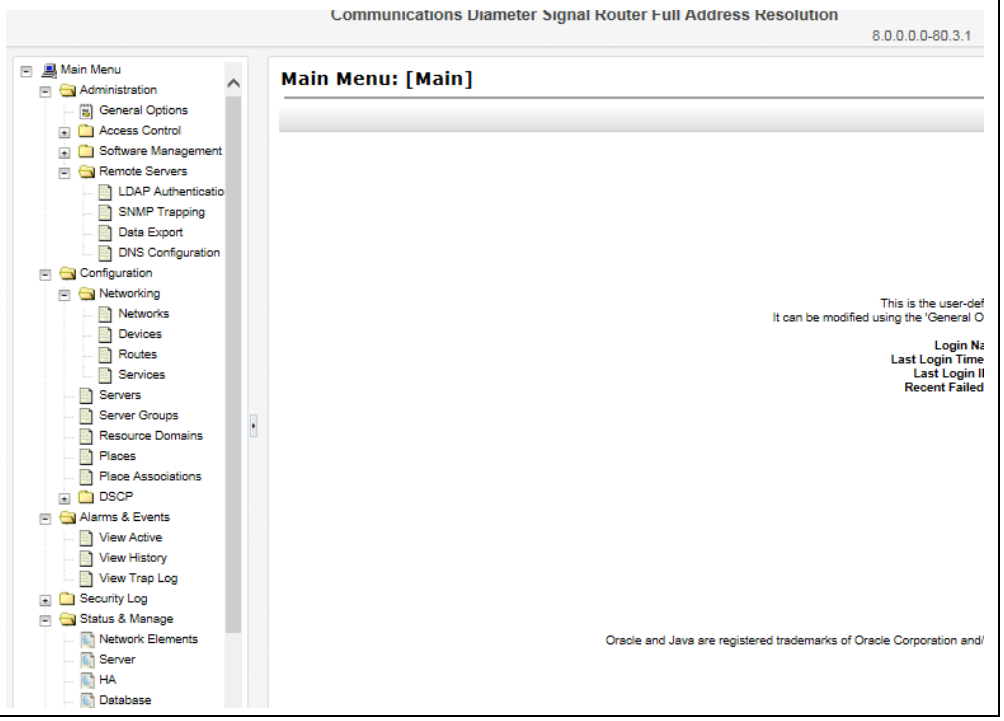
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
17. ☐	**PMAC Guest VM:** The user should be presented with an "**Are you sure you want to upgrade**" message box ....as shown on the right. Click the "**OK**" dialogue button.	
18. ☐	**PMAC Guest VM:** Note the task number assigned to upgrade SDS application . This number will be used to track its progress. This task takes up to ~20 minutes.	
19. ☐	Install SDS SW on each remaining DP server blade.	• Repeat **Steps 10 – 18** of this procedure for each additional **DP server blade** installed in the **SOAM** enclosure.
20. ☐	**PMAC Guest VM:** Select… **Main Menu** → **Task Monitoring** …as shown on the right.	

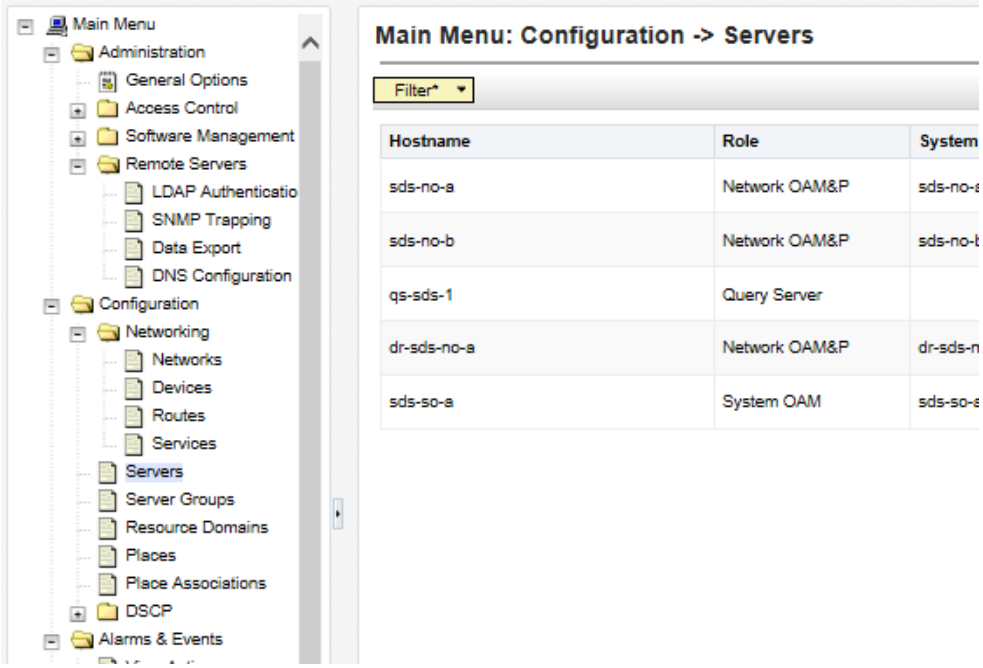
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
21. ☐	**PMAC Guest VM:** Wait till Progress is 100% with a Status of Success and a State of Complete. .... then proceed to the next step.	
22. ☐	**PMAC Guest VM::** Click the **"Logout"** link on the PMAC server GUI.	
23. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP address (VIP) assigned to Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	

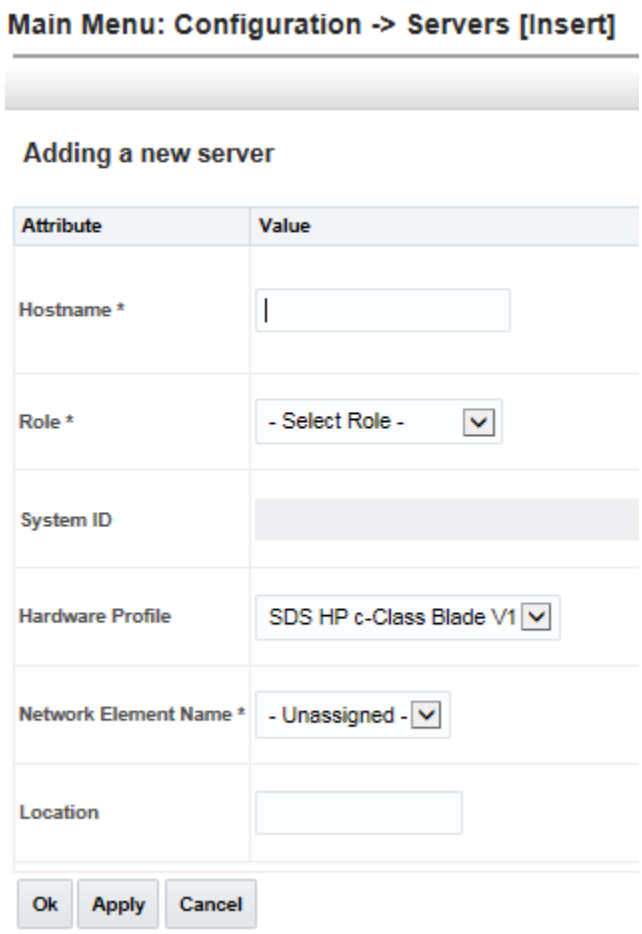
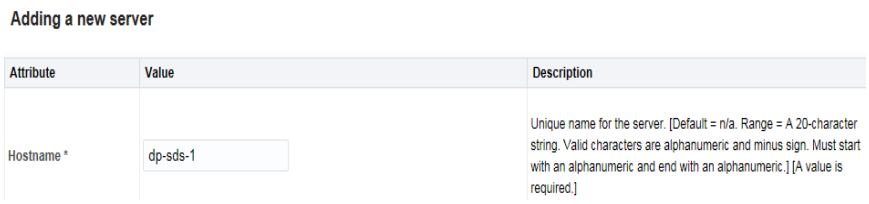
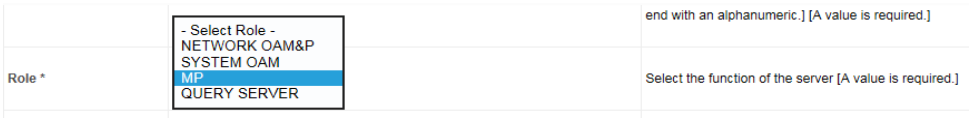
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
24. ☐	**Primary SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
25. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
26. ☐	**Primary SDS VIP:** 1) Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right 2) Select the **"Insert"** dialogue button.	

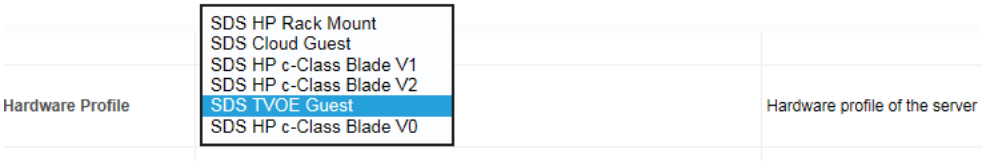
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
27. ☐	**Primary SDS VIP:** The user is now presented with the **"Adding a new server"** configuration screen.	
28. ☐	**Primary SDS VIP:** Input the assigned "**hostname"** for the Database Processor **(DP)**.	
29. ☐	**Primary SDS VIP:** Select **"MP"** for the server **Role** from the pull-down menu.	

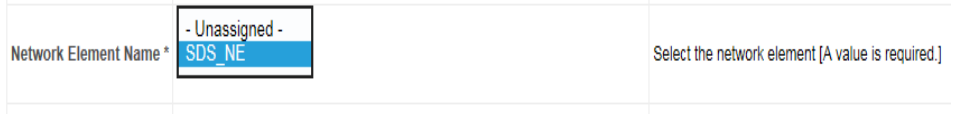
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>30. ☐</td><td>Primary SDS VIP:

Using the chart provided, select the DP Hardware Profile which is appropriate to your installation from the pull-down menu.

NOTE: The choice of DP HW Profile is dictated by the placement of the XMI switch pair in the c-Class enclosure.</td><td> 

<table>
<tr><th>DP HW Profile</th><th>Network</th><th>Bonded Interfaces</th><th>Comments</th></tr>
<tr><td rowspan="2">SDS HP c-Class Blade V0</td><td>IMI</td><td rowspan="2">Bond0 (eth01, eth02)</td><td rowspan="2">Use when both XMI and IMI are to be VLAN tagged.</td></tr>
<tr><td>XMI</td></tr>
<tr><td rowspan="2">SDS HP c-Class Blade V1</td><td>IMI</td><td>Bond0 (eth01, eth02)</td><td rowspan="2">Use when XMI enclosure switches are connected to DP blade mezzanine card ports eth23 / eth24.</td></tr>
<tr><td>XMI</td><td>bond1 (eth23, eth24)</td></tr>
<tr><td rowspan="2">SDS HP c-Class Blade V2</td><td>IMI</td><td>Bond0 (eth01, eth02)</td><td rowspan="2">Use when XMI enclosure switches are connected to DP blade mezzanine card ports eth21 / eth22.</td></tr>
<tr><td>XMI</td><td>bond1 (eth21, eth22)</td></tr>
</table></td></tr>
<tr><td>31. ☐</td><td>Primary SDS VIP:

Select the Network Element Name of the SOAM site where the DP is physically located from the list of available NEs in the pull-down menu</td><td> 

NOTE: After the Network Element Name is selected, the Interfaces fields will be displayed, as seen in Step 33</td></tr>
<tr><td>32. ☐</td><td>Primary SDS VIP:

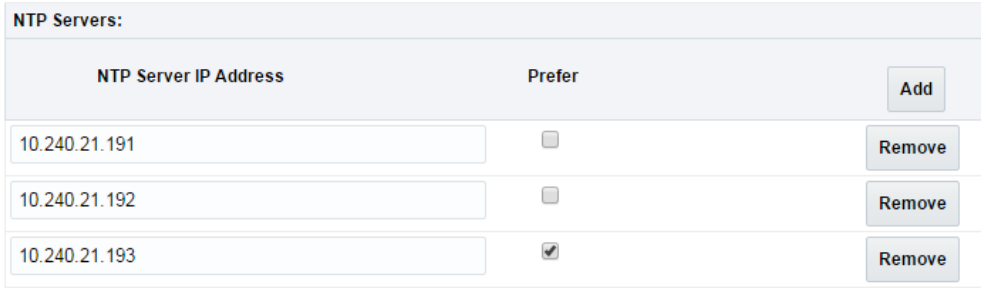
Enter the site location.

NOTE: Location is an optional field.</td><td> 
</td></tr>
</table>

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>33. ☐</td><td>Primary SDS VIP:

1) Enter the IMI IP address for the DP Server.

2) Set the IMI Interface to “bond0” and “check” the VLAN checkbox.</td><td>


<table>
<tr><th>DP Server</th><th>Network</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td>DP</td><td>IMI</td><td>bond0</td><td>✓</td></tr>
</table>
</td></tr>
<tr><td>34.</td><td>1) Enter the customer assigned XMI IP address for the DP Server.

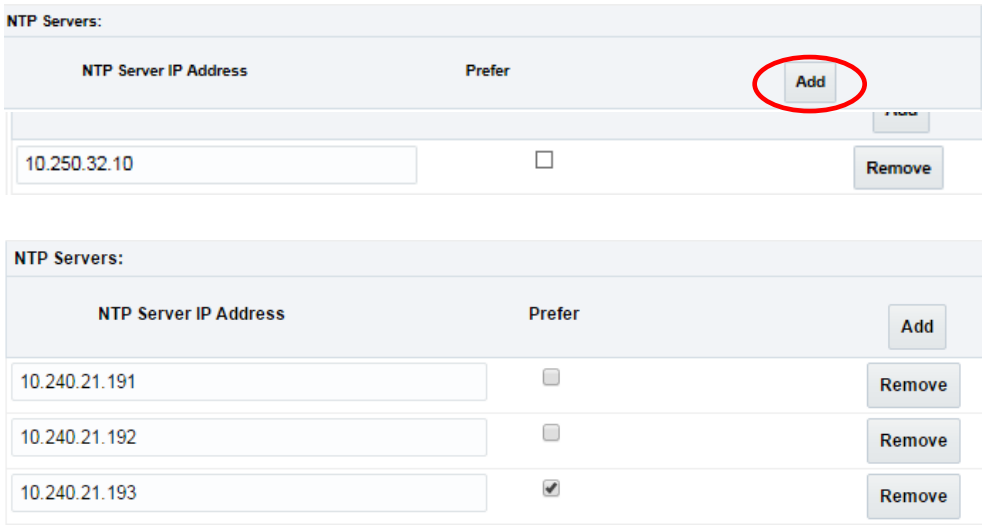
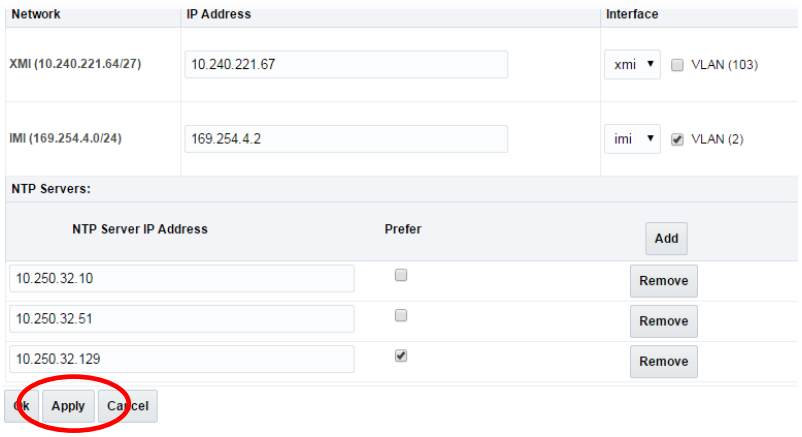
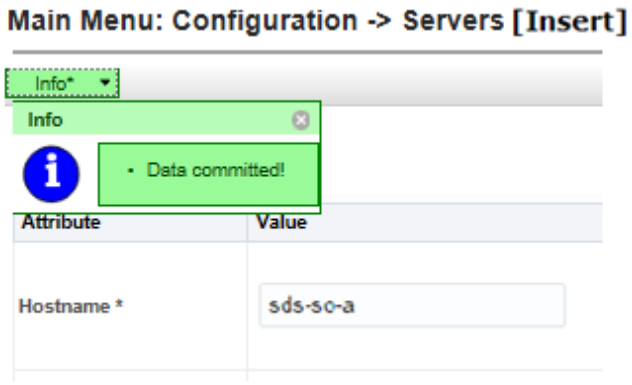
Layer 3
(No VLAN tagging used for XMI)

2) Set the XMI Interface to “bond1” and “DO NOT check” the VLAN checkbox.
- OR -

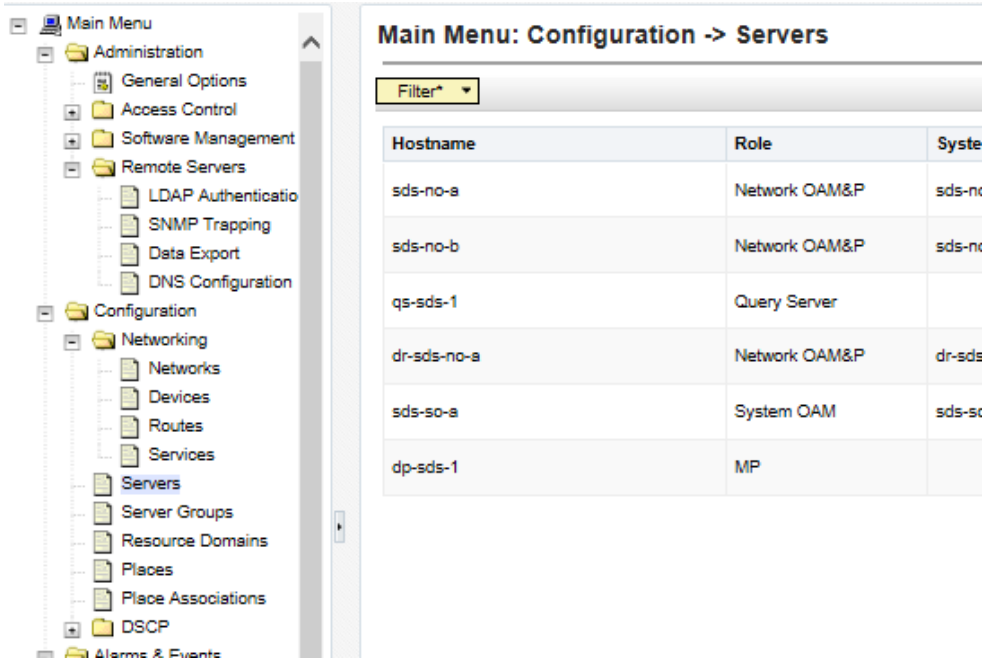
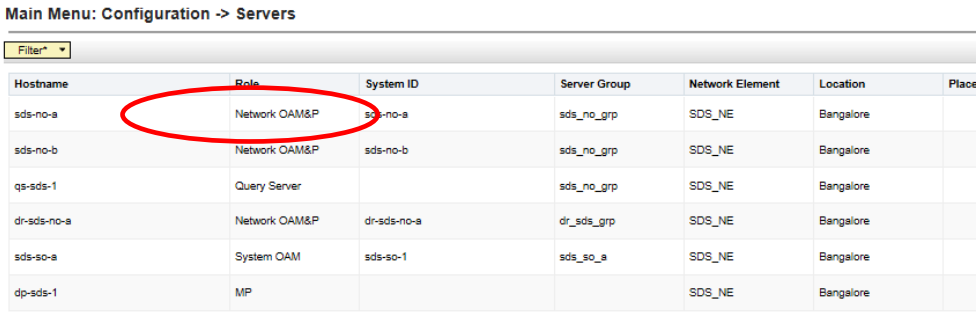
Layer 2
(VLAN tagging used for XMI)

2) Set the XMI Interface to “bond0” and “check” the VLAN checkbox.</td><td>
<table>
<tr><th>DP Server</th><th>Network</th><th>VLAN tagging
(on XMI network)</th><th>Interface</th><th>VLAN Checkbox</th></tr>
<tr><td rowspan="2">DP</td><td rowspan="2">XMI</td><td>No</td><td>bond1</td><td>✗</td></tr>
<tr><td>Yes</td><td>bond0</td><td>✓</td></tr>
</table>
!!! CAUTION !!!
It is crucial that the correct network configuration be selected in Steps 33 – 34 of this procedure. Choosing an incorrect configuration will result in the need to re-install the OS and restart the DP Server instalation procedure over from the beginning.
</td></tr>
</table>

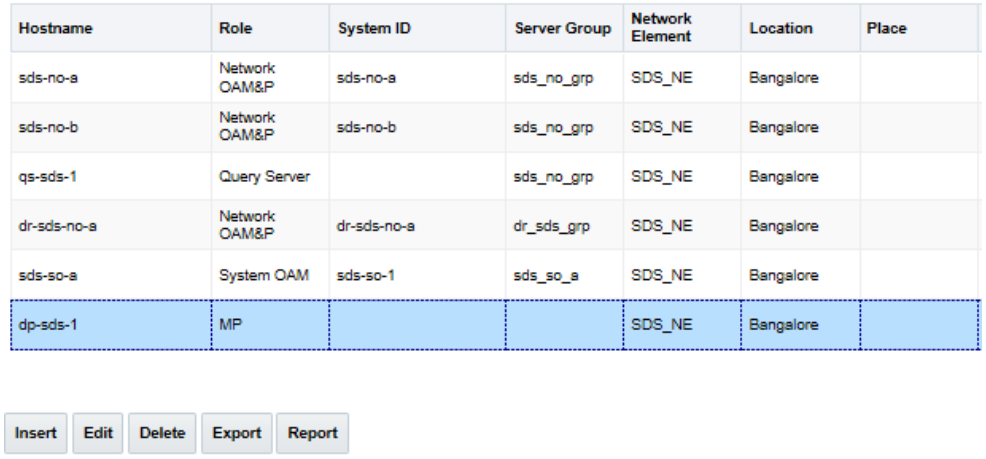
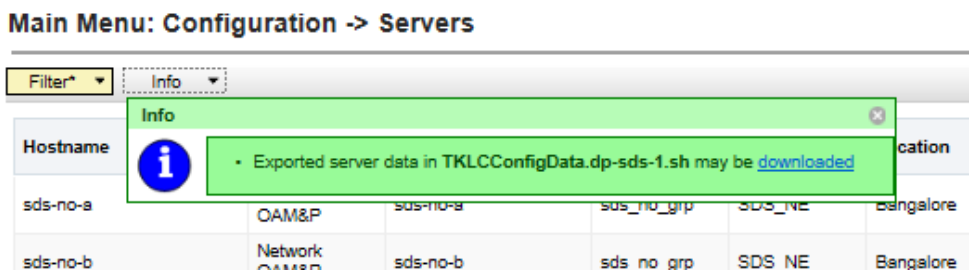
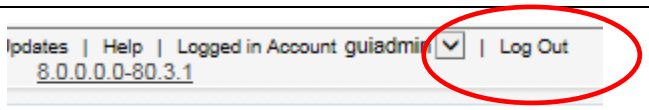
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
35. ☐	**Primary SDS VIP:** **1)** Click the "**NTP Servers:**" **"Add"** dialogue button. **2)** Enter the **NTP Server IP Address** for an NTP Server. **3)** Enter 3 NTP Server **IP address**, repeat (1) and (2) to enter it. **4)** Optionally, click the "**Prefer**" checkbox to prefer one NTP Server over the other.	
36. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"Apply"** dialogue button...	
37. ☐	**Primary SDS VIP:** If the values provided match the network ranges assigned to the NE, the user must select the Info box to receive a banner information message showing that the data has been committed to the DB.	

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
38. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Servers*** …as shown on the right.	
39. ☐	**Primary 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.	

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
40. ☐	**Primary SDS VIP:** 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. **2)** Click the **"Export"** dialogue button from the bottom left corner of the screen.	
41. ☐	**Primary SDS VIP:** The user must select the Info box to receive a banner information message showing a download link for the "**MP**" configuration data.	
42. ☐	Configure/Export the each additional DP server to be installed for this SOAM site.	• Repeat **Steps 26 – 41** of this procedure for each additional **DP** server installed in the SOAM cabinet.
43. ☐	**Primary SDS VIP:** Click the **"Logout"** link on the SDS server GUI.	

44. ☐	**Primary SDS VIP:**
	
	1) SSH to the **Primary SDS NOAM VIP** and access the command prompt.
	
	2) Log into the server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

45. ☐	**Primary SDS VIP:** Change directory to filemgmt	`$ cd /var/TKLC/db/filemgmt`

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result

46. ☐	**Primary SDS VIP:**
	Attain directory listing. Look for the configuration file(s) that have just been generated for the DP(s). This should appear toward the bottom of the output.
		`$ ls -ltr TKLCConfigData*.sh`
		***** TRUNCATED OUTPUT *****
		`-rw-rw-rw- 1 admusr admusr 2042 Dec 20 10:54 TKLCConfigData.dp-carync-1.sh`
		`-rw-rw-rw- 1 admusr admusr 2042 Dec 20 10:57 TKLCConfigData.dp-carync-2.sh`

47. ☐	**Primary SDS VIP:**
	Use **scp** to copy the file(s) to the PMAC server.
		`$sudo scp -p <configuration_file-1> <configuration_file-2> admusr@<PMAC_Mgmt_IP>:/tmp/`
		`Password: <admusr_password>`
		`TKLCConfigData.dp-carync-1.sh 100% 1757 1.7KB/s 00:00`
		`TKLCConfigData.dp-carync-2.sh 100% 1757 1.7KB/s 00:00`
		`$`

48.	**Primary SDS VIP:** Logout of the Primary SDS CLI.	`$ exit`
49. ☐	**PMAC Server CLI:** Use **SSH** to login to the **PMAC Guest** VM server as the **admusr.**	`login: admusr` `Password: <admusr_password>`
50.	**PMAC Guest VM:** **Key exchange with DP control IP**	$ keyexchange admusr@<DP_Control_IP> Example: [admusr@nassau-enc-pmac-1 ~]$ keyexchange admusr@192.168.1.22 The server does not know of 192.168.1.22. Will just exchange host keys for the name given! Password of admusr: Could not get authorized keys file from remote (192.168.1.22). Maybe it does not exist. Continuing... The server does not know of 192.168.1.22. Will just exchange host keys for the name given! ssh is working correctly. [admusr@nassau-enc-pmac-1 ~]$

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result

51. ☐	**PMAC Guest VM:**
	Copy the server configuration file to the Control IP for the DP.
	
	Note: The Control IP for each DP is obtained in **Step 15** of this procedure.
		`$ sudo scp -p /tmp/<configuration_file> admusr@<DP_Control_IP>:/var/TKLC/db/filemgmt/`
		`Password: <admusr_password>`
		`TKLCConfigData.dp-carync-1.sh 100% 1757 1.7KB/s 00:00`

52. ☐	**PMAC Guest VM:** Connect to the DP server console from the PMAC Server Console.	`$ ssh <DP_Control_IP>` `Password: <admusr_password>`
53. ☐	**DP Server:** Copy the **SDS DP** configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname (shown in red) from the file name.	***Example:*** TKLCConfigData<.server_hostname>.sh ➔ will translate to ➔TKLCConfigData.sh `$ sudo cp -p /var/TKLC/db/filemgmt/TKLCConfigData.dp-carync-1.sh /var/tmp/TKLCConfigData.sh` **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*

54. ☐	**DP Server:**
	After the script completes, a broadcast message will be sent to the terminal.
		***** NO OUTPUT FOR ≈ 3-20 MINUTES *****
		`Broadcast message from admusr (Mon Dec 14 15:47:33 2009):`
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		`Please remove the USB flash drive if connected and reboot the server.`
		<ENTER>

55.	**DP Server:** Verify that the desired Time Zone is currently in use.	`$ date` `Mon Aug 10 19:34:51 UTC 2015`

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
56.	**DP Server:** If the desired Time Zone was not presented in the previous step… **Configure the Time Zone.** Otherwise, skip to the next step.	***Example:*** `$ sudo set_ini_tz.pl <time_zone>` **NOTE:** *The following command example sets the time to the "UTC" (aka GMT) time zone which is recommneded for all sites.* *The user may replace, as appropriate, with the customer requested time zone for this site installation. See* ***Appendix G*** *for a list of valid time zones.* `$ sudo set_ini_tz.pl "Etc/UTC"`
57. ☐	**DP Server:** Initiate a reboot of the DP.	`$ sudo init 6`
58. ☐	**DP Server:** Output similar to that shown on the right may be observed as the server initiates a reboot.	`$ Connection to 192.168.1.226 closed by remote host.` `Connection to 192.168.1.226 closed.`
59. ☐	**PMAC Guest VM:** After the DP server has completed reboot… Re-connect to the DP server console from the PMAC Server Console	`$ sudo ssh <DP_Control_IP>` `Password: <admusr_password>`

60. ☐	**DP Server:**
	
	1) Verify that the **XMI IP address** input in **Step 33** has been applied to **"bond1"**.
	
	2) Verify that the **IMI IP address** input in **Step 33** has been applied to **"bond0.4"**.
	
	NOTE: *Exact bond configuration may vary for custom network implementations.*
		`$ ifconfig |grep in`
		`bond0  Link encap:Ethernet  HWaddr B4:99:BA:AC:BD:64`
		`inet addr:192.168.1.226 Bcast:192.168.1.255 Mask:255.255.255.0`
		`bond0.4 Link encap:Ethernet  HWaddr B4:99:BA:AC:BD:64`
		`inet addr:10.240.38.82 Bcast:10.240.38.127 Mask:255.255.255.192`
		`bond1  Link encap:Ethernet  HWaddr B4:99:BA:AC:BD:64`
		`inet addr:10.240.39.154 Bcast:10.240.39.255 Mask:255.255.255.128`
		`eth01  Link encap:Ethernet  HWaddr B4:99:BA:AC:BD:64`
		`eth02  Link encap:Ethernet  HWaddr B4:99:BA:AC:BD:64`
		`lo  Link encap:Local Loopback`
		`inet addr:127.0.0.1  Mask:255.0.0.0`

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result

61. ☐	**DP Server:**
	
	From the **DP Server**, **"ping"** the **IMI IP address** of the **SOAM-A** Guest.
		`$ ping -c 5 10.240.38.78`
		`PING 10.240.38.78 (10.240.38.78) 56(84) bytes of data.`
		`64 bytes from 10.240.38.78: icmp_seq=1 ttl=64 time=0.031 ms`
		`64 bytes from 10.240.38.78: icmp_seq=2 ttl=64 time=0.017 ms`
		`64 bytes from 10.240.38.78: icmp_seq=3 ttl=64 time=0.031 ms`
		`64 bytes from 10.240.38.78: icmp_seq=4 ttl=64 time=0.028 ms`
		`64 bytes from 10.240.38.78: icmp_seq=5 ttl=64 time=0.030 ms`
		`64 bytes from 10.240.38.78: icmp_seq=6 ttl=64 time=0.028 ms`
		
		`--- 10.240.38.78 ping statistics ---`
		`6 packets transmitted, 6 received, 0% packet loss, time 5000ms`
		`rtt min/avg/max/mdev = 0.017/0.027/0.031/0.007 ms`

62. ☐	**DP Server:**
	
	From the **DP Server**, **"ping"** the local **XMI Gateway address** associated with the SOAM NE.
		`$ ping -c 5 10.240.39.1`
		`PING 10.240.39.1 (10.240.39.1) 56(84) bytes of data.`
		`64 bytes from 10.240.39.1: icmp_seq=1 ttl=64 time=0.024 ms`
		`64 bytes from 10.240.39.1: icmp_seq=2 ttl=64 time=0.033 ms`
		`64 bytes from 10.240.39.1: icmp_seq=3 ttl=64 time=0.032 ms`
		`64 bytes from 10.240.39.1: icmp_seq=4 ttl=64 time=0.026 ms`
		`64 bytes from 10.240.39.1: icmp_seq=5 ttl=64 time=0.027 ms`
		`64 bytes from 10.240.39.1: icmp_seq=6 ttl=64 time=0.026 ms`
		
		`--- 10.240.39.1 ping statistics ---`
		`6 packets transmitted, 6 received, 0% packet loss, time 5004ms`
		`rtt min/avg/max/mdev = 0.024/0.028/0.033/0.003 ms`

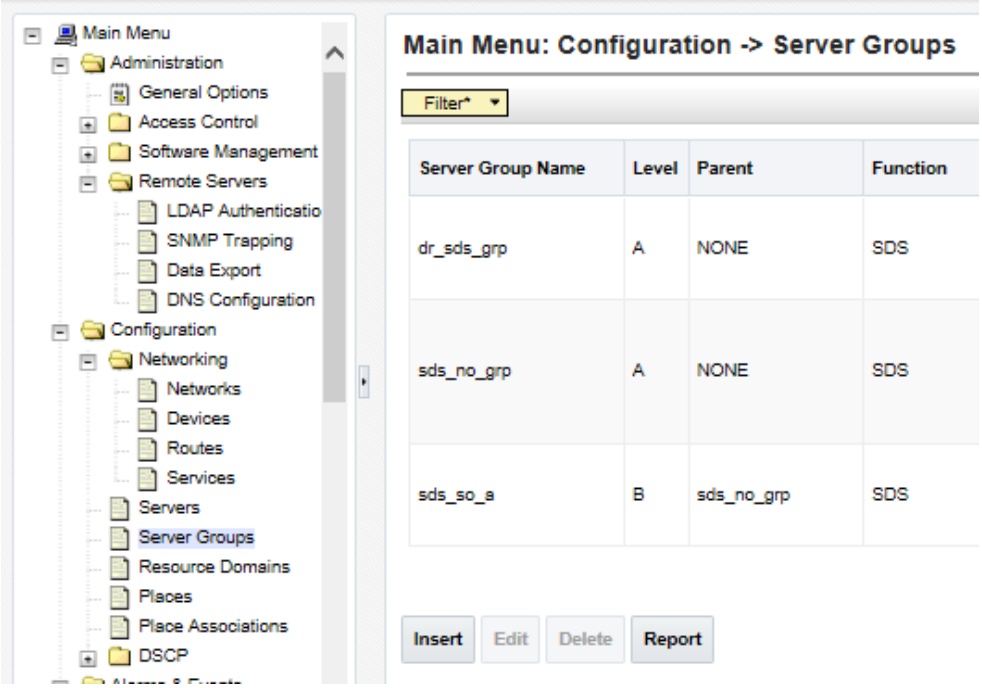
63. ☐	**DP Server:**
	
	Use the **"ntpq"** command to verify connectivity to the assigned Primary and Secondary NTP server(s).
		`$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`+10.250.32.10 192.5.41.209 2 u 139 1024 377 2.008 1.006 1.049`
		`*10.250.32.51 192.5.41.209 2 u 979 1024 377 0.507 1.664 0.702`

64. ☐	**DP Server:**
	
	Execute a **"syscheck"** to verify the current health of the server.
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

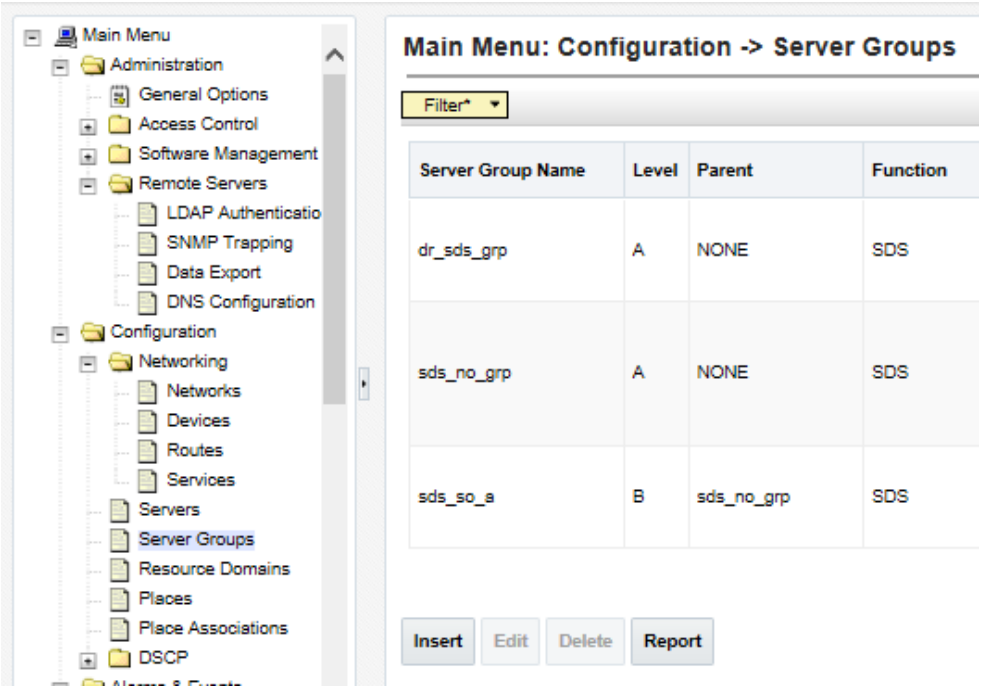
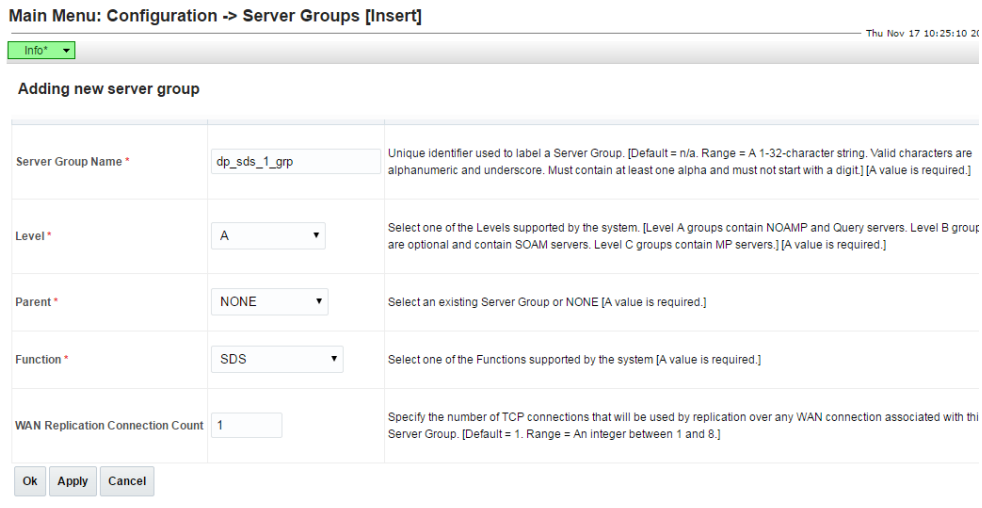
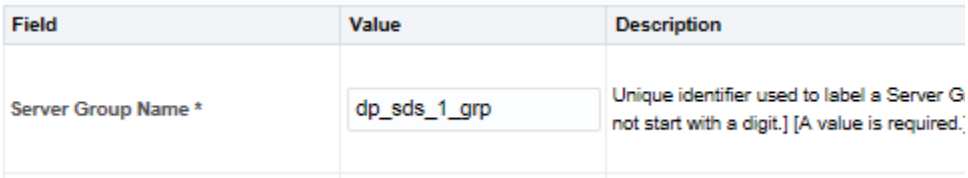
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
65.	**DP Server:** Accept upgrade to the Application Software. Use "q" key to exit the screen session.	**[admusr@nassau-dp-2 ~]$ sudo /var/TKLC/backout/accept** **Called with options: --accept** **Loading Backout::BackoutType::RPM** **Accepting Upgrade** **Executing common accept tasks** **Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info.** **Cleaning backout directory.** **Clearing Upgrade Accept/Reject alarm.** **Cleaning message from MOTD.** **No patch pending alarm on server so no MOTD update.** **Cleaning up RPM config backup files...** **Checking /** **Checking /boot** **Checking /tmp** **Checking /usr** **Checking /var** **Checking /var/TKLC** **Checking /tmp/appworks_temp** **Checking /usr/openv** **Checking /var/TKLC/appw/logs/Process** **Checking /var/TKLC/appw/logs/Security** **Checking /var/TKLC/db/filemgmt** **Checking /var/TKLC/rundb** **Starting cleanup of RCS repository.** **INFO: Removing '/etc/my.cnf' from RCS repository** **INFO: Removing '/etc/pam.d/password-auth' from RCS repository** **INFO: Removing '/etc/pam.d/system-auth' from RCS repository** **INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0' from RCS repository** **INFO: Removing '/etc/php.d/zip.ini' from RCS repository** **INFO: Removing '/var/lib/prelink/force' from RCS repository** **=== Window terminated (Thu Feb 2 20:07:21 2017) ===** **screen session: use 'screen -x upgrade' to reconnect** **Type the letter "q" on the keyboard to exit the screen session.** **[screen is terminating]** **[admusr@nassau-dp-2 ~]$** **NOTE:** **EXECUTE Appendix I: Disable Hyperthreading (DP Only) on server before exiting.**
66. ☐	**DP Server:** Exit from the command line to return the server console to the login prompt.	$ **exit** Connection to 192.168.1.199 closed.

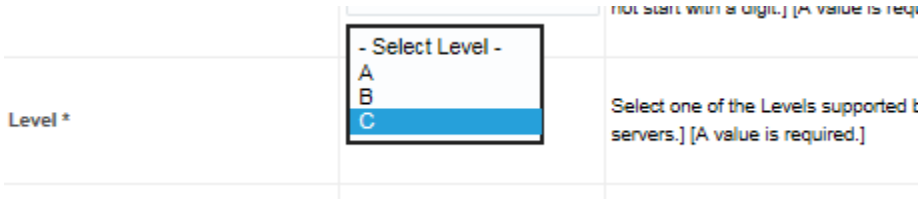
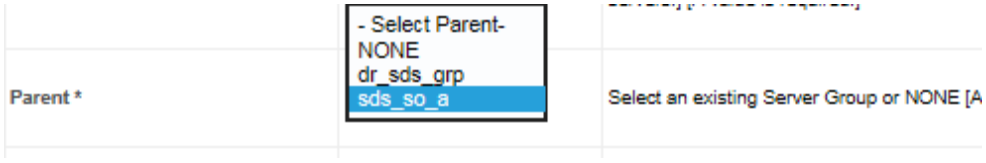
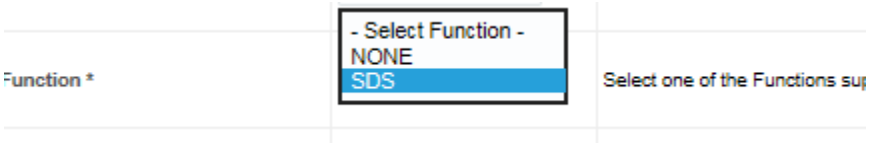
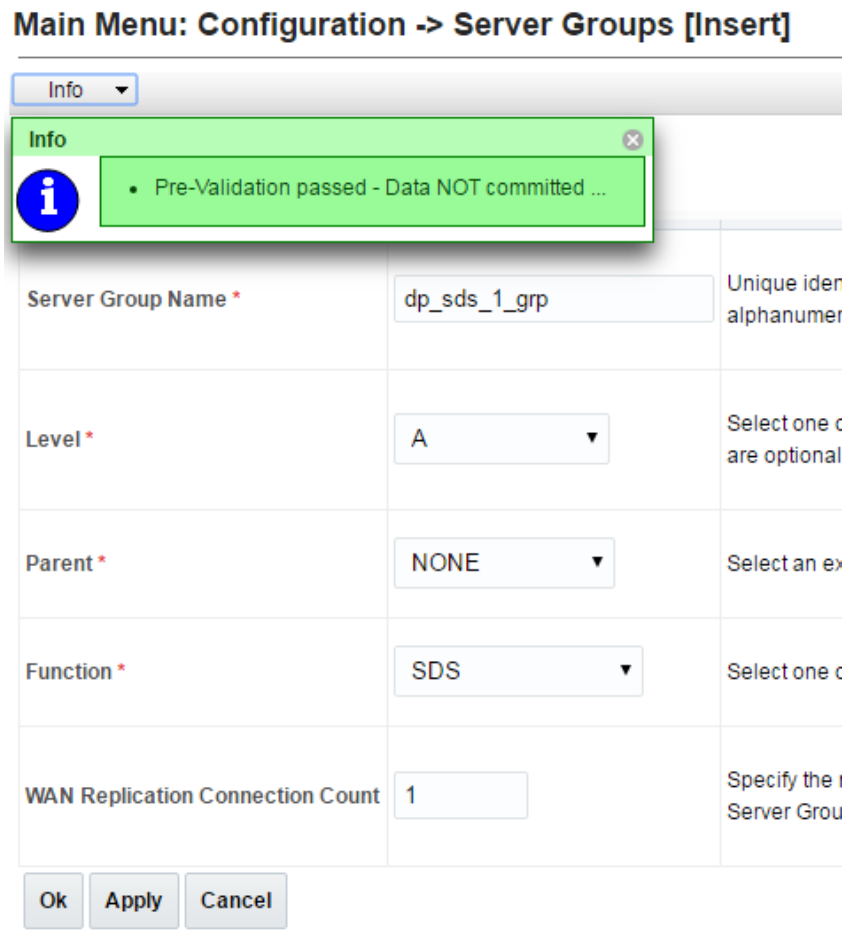
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
67. ☐	Apply the configuration file for each additional DP server installed at the SOAM site.	Repeat Steps 51 – 66 of this procedure for each subtending DP server installed in the same SOAM enclosure.
68. ☐	**PMAC Guest VM:** Exit from the PMAC server.	`$ exit`
69. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right.	

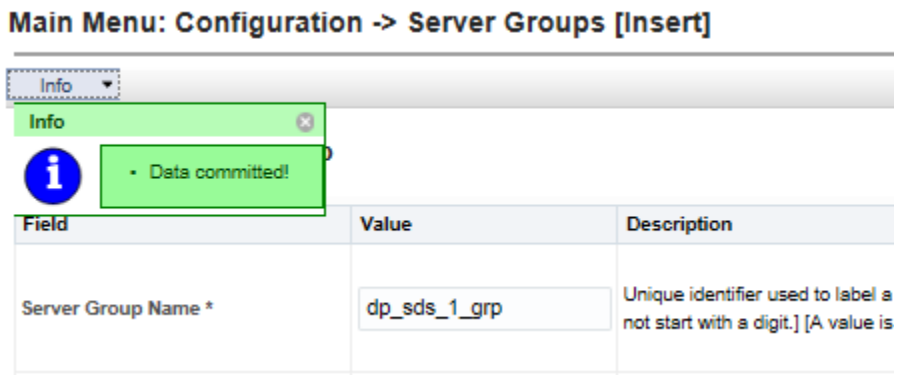
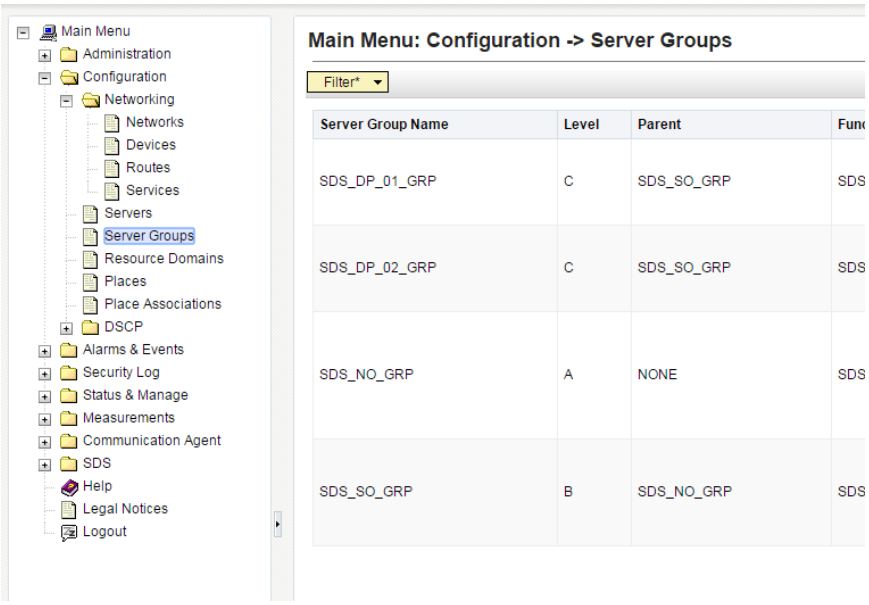
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
70. ☐	**Primary 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.	
71. ☐	**Primary 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).*	
72. ☐	**Primary SDS VIP:** 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.*

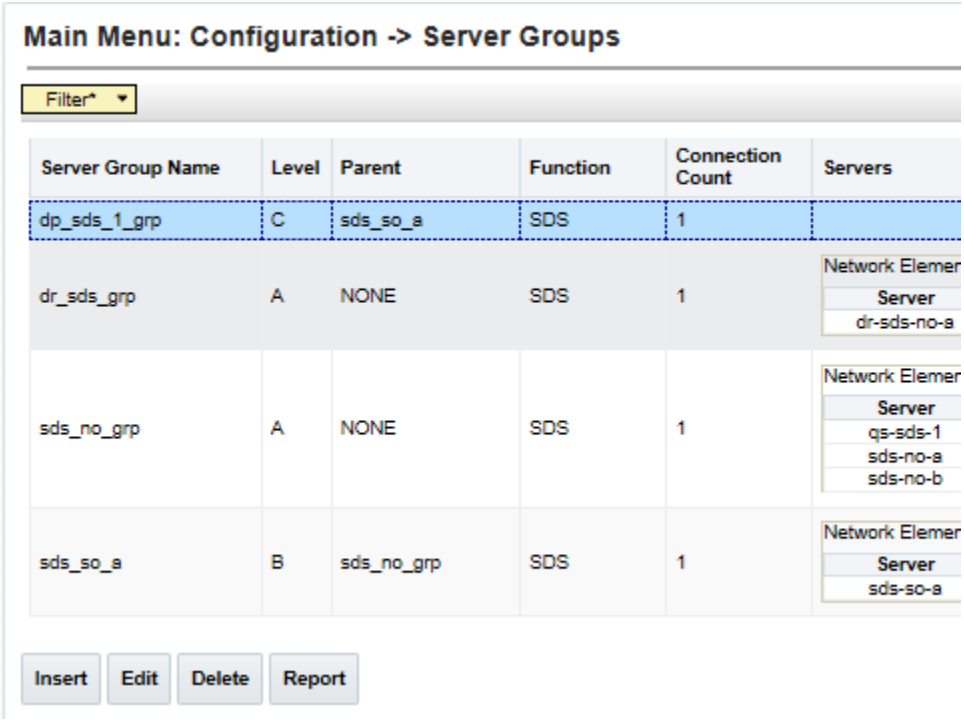
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
73. ☐	**Primary SDS VIP:** Select **"C"** on the **"Level"** pull-down menu.	
74. ☐	**Primary SDS VIP:** Select **System OAM group** on the **"Parent"** pull-down menu.	
75. ☐	**Primary SDS VIP:** Select **"SDS"** on the **"Function"** pull-down menu.	
76. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	

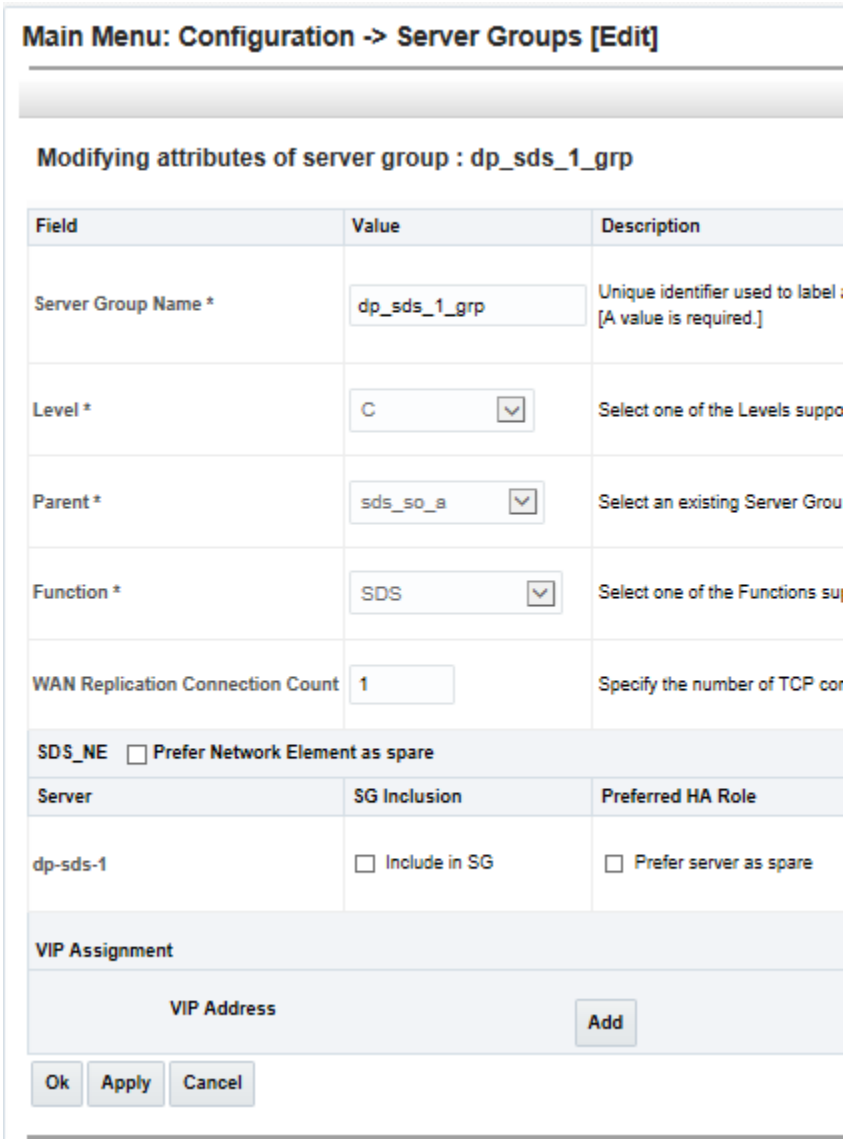
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
77. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
78. ☐	**Primary SDS VIP:** **1)** Select… **Main Menu** → **Configuration** → ***Server Groups*** …as shown on the right **2)** The user will be presented with the **"Configuration → Server Groups"** screen as shown on the right.	

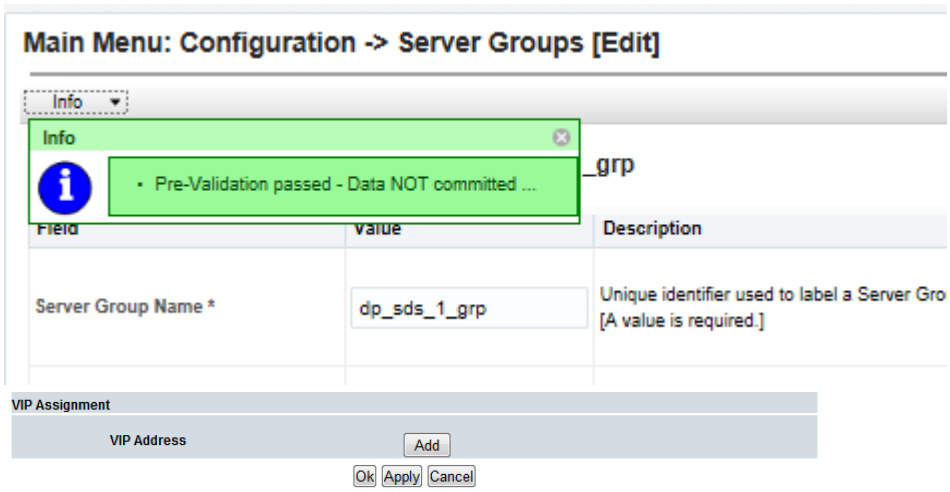
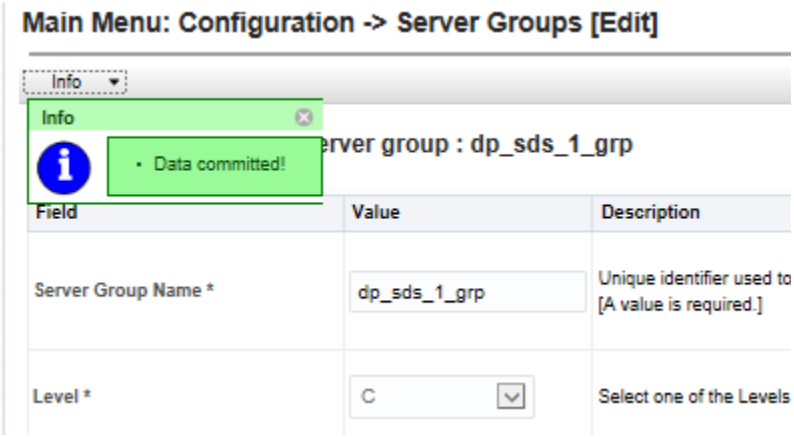
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
79. ☐	**Primary 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.	

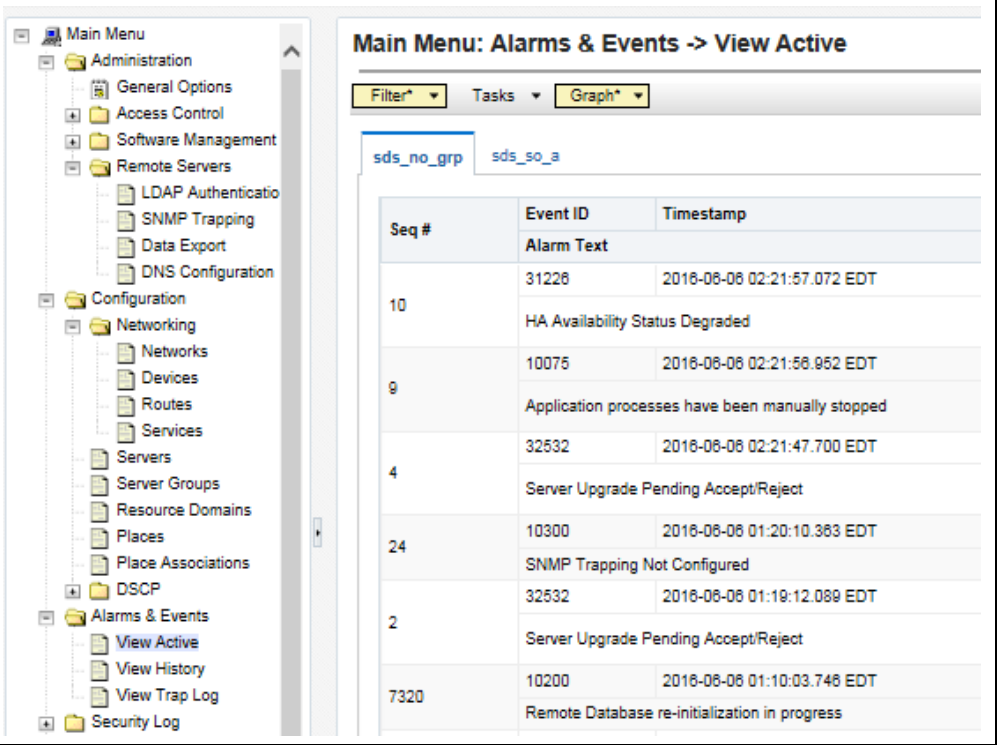
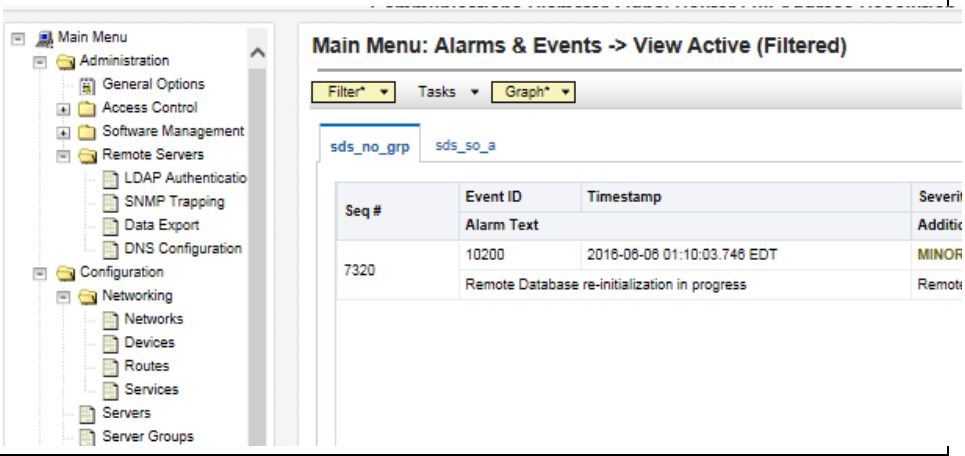
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
80. ☐	**Primary SDS VIP:** The user will be presented with the **"Configuration → Server Groups [Edit]"** screen as shown on the right	
81. ☐	**Primary SDS VIP:** Select the **"DP"** server from the list of **"Servers"** by clicking the check box next its name.	

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
82. ☐	**Primary SDS VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"Apply"** dialogue button.	
83. ☐	**Primary SDS VIP:** The user should be presented with a banner information message stating **"Data committed"**.	
84. ☐	Place each additional DP Server into its respective DP Server Group.	Repeat **Steps 69 – 83** of this procedure for each subtending **DP** server installed in the same SOAM enclosure, *using a unique group for each **DP***.

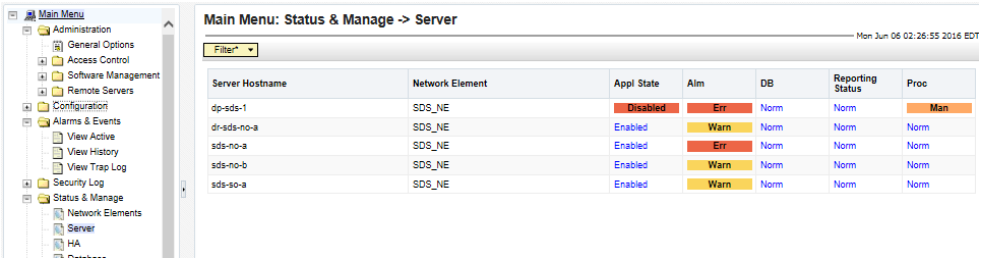
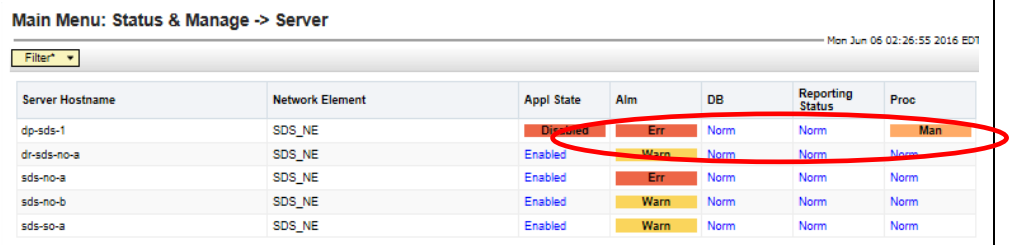
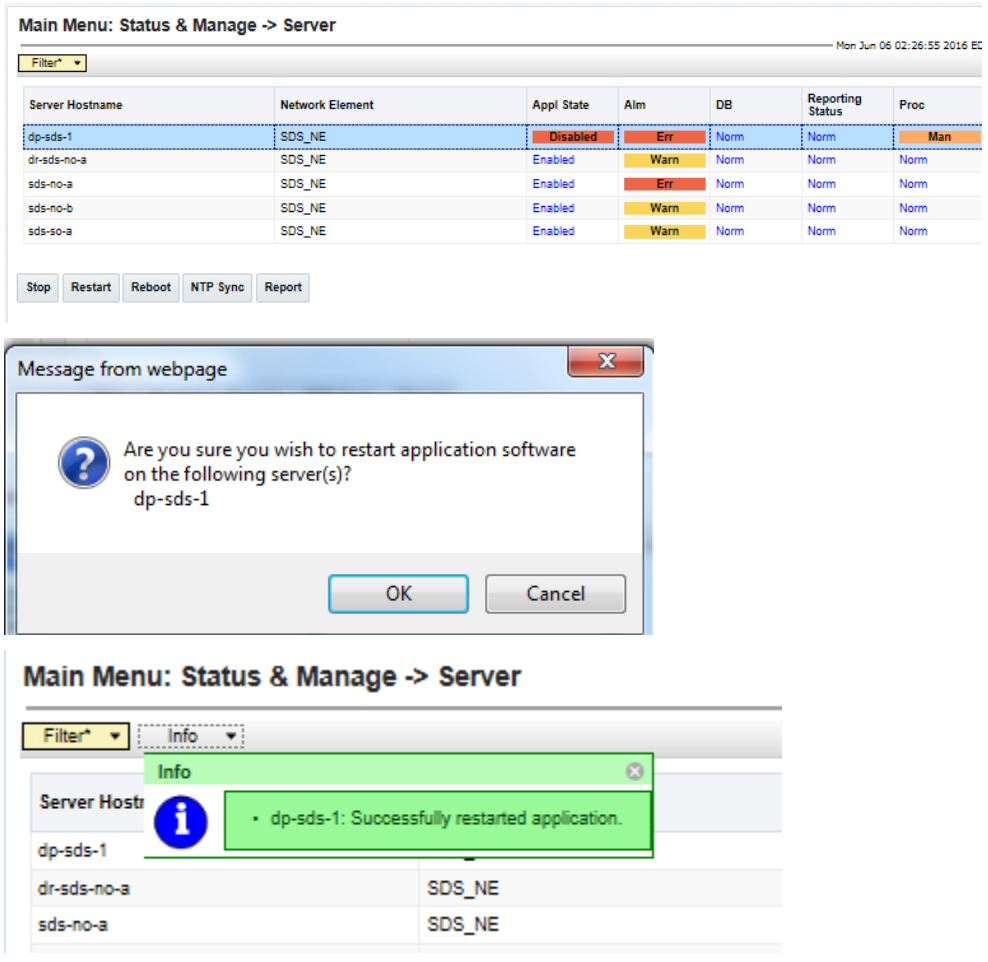
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
85.	**Primary SDS VIP:** Select… **Main Menu** → **Alarms & Events** → ***View Active*** …as shown on the right.	
86.	**Primary SDS VIP:** Verify that **Event ID 10200** (*Remote Database re-initialization in progress)* alarms are present with the **DP Server hostnames** in the **"Instance"** field..	

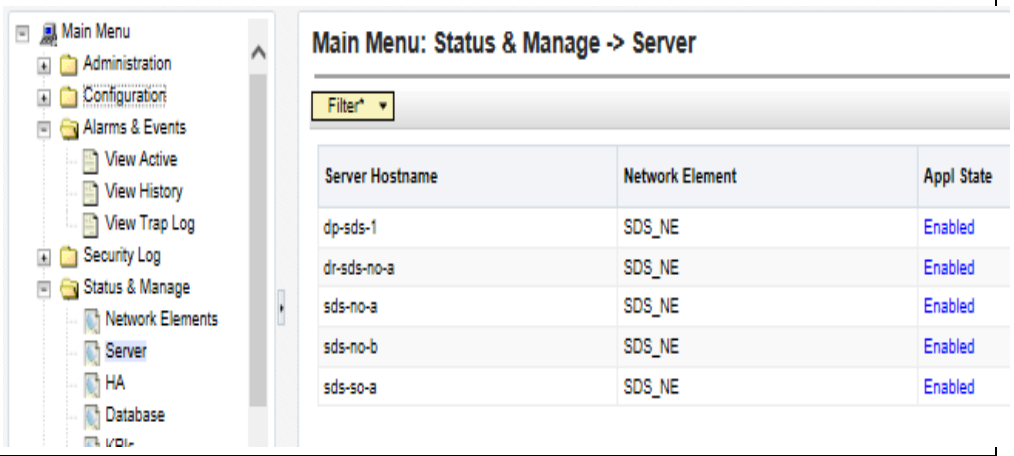
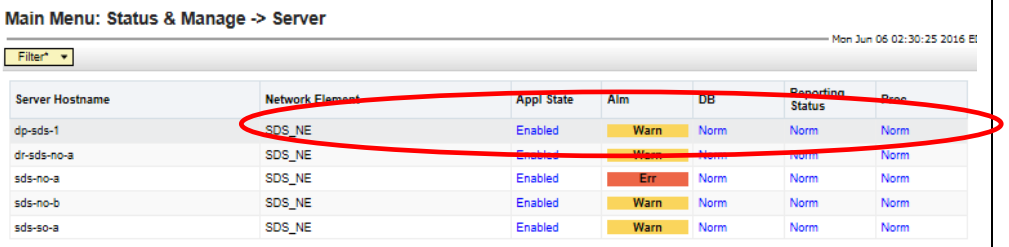
MONITOR THE EVENT ID 10200 (*Remote Database re-initialization in progress)* ALARMS.

DO NOT PROCEED TO THE NEXT STEP UNTIL THE ALARM CLEAR IS RECEIVED FOR ALL DP SERVERS.

Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
87. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	
88. ☐	**Primary SDS VIP:** Verify that the **"DB & Reporting"** status columns all show **"Norm"** for the **DP** at this point. The **"Proc"** column should show **"Man"**.	
89. ☐	**Primary SDS VIP:** **1)** Using the mouse, select the **"DP"** hostname. The line entry should now be highlighted. **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.*	

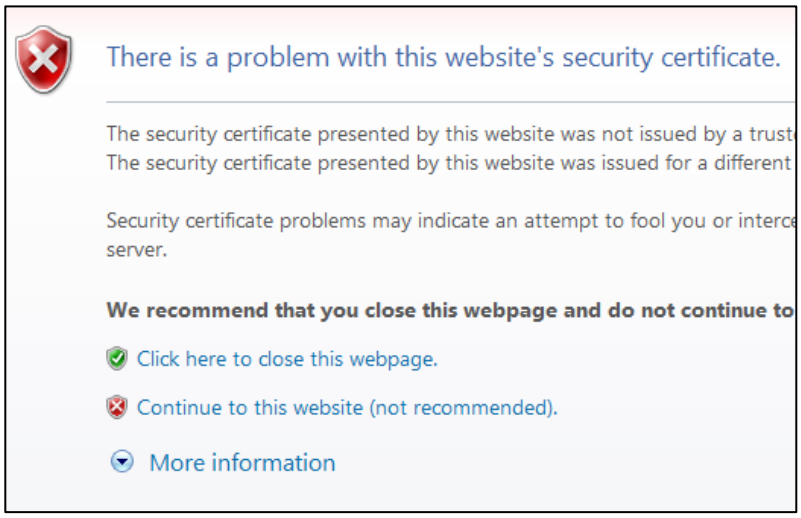
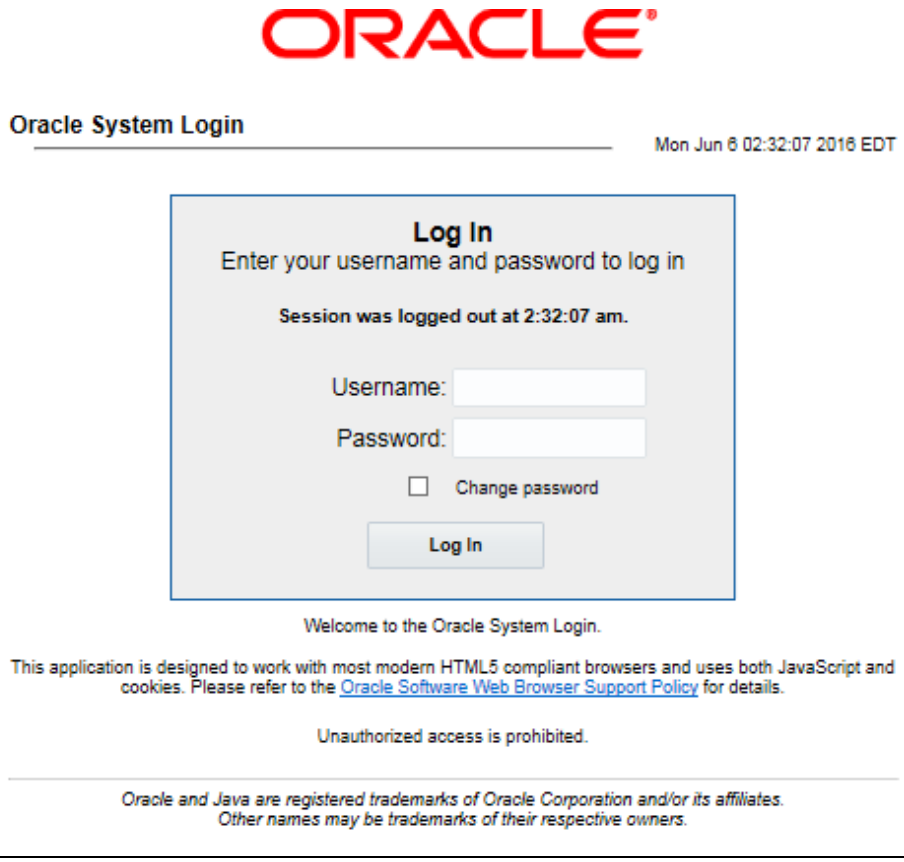
Procedure 11. Installing the Data Processor Blade (All SOAM Sites)

Step	Procedure	Result
90. ☐	**Primary SDS VIP:** Select… **Main Menu** → **Status & Manage** → ***Server*** …as shown on the right.	
91. ☐	**Primary 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"**.	
92. ☐	Repeat this procedure for each additional **DP** Server.	Repeat Steps 87 – 91 of this procedure for each additional DP server installed in the SOAM cabinet.
THIS PROCEDURE HAS BEEN COMPLETED		

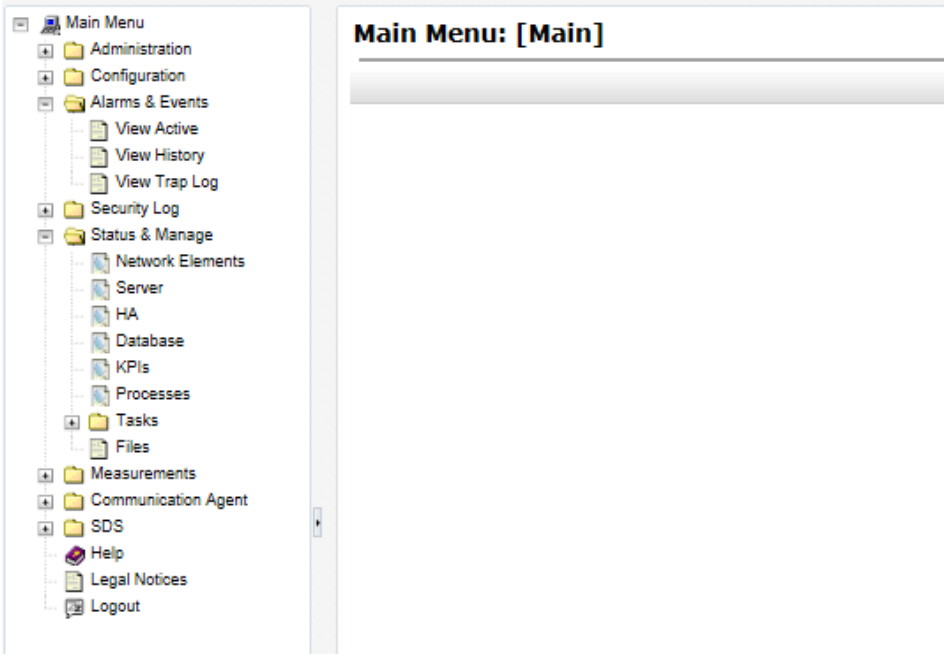
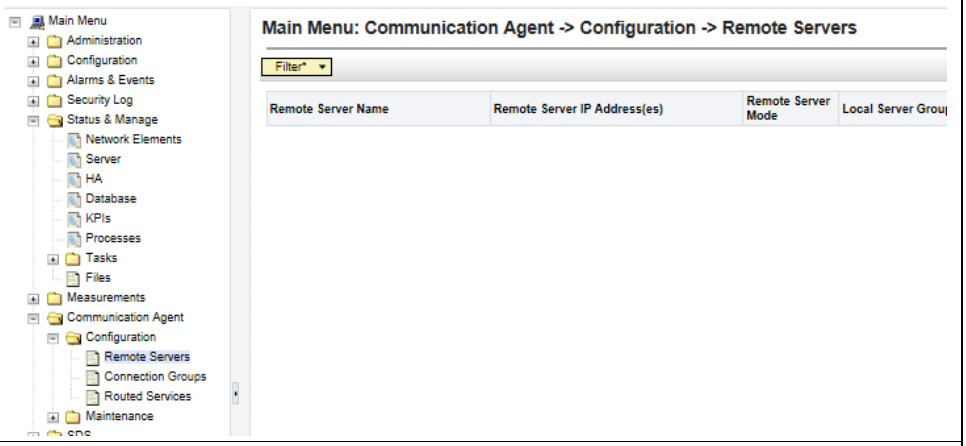
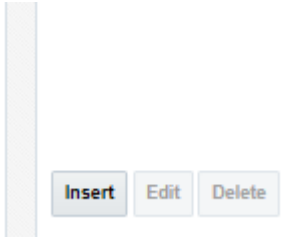
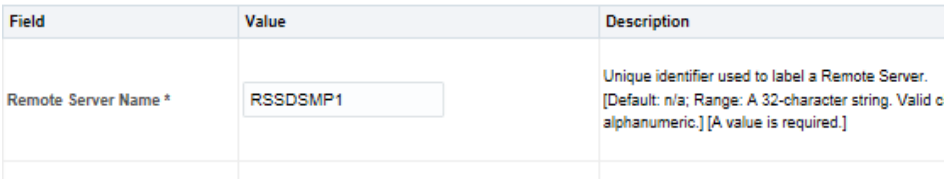
5.10 Configuring ComAgent

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.

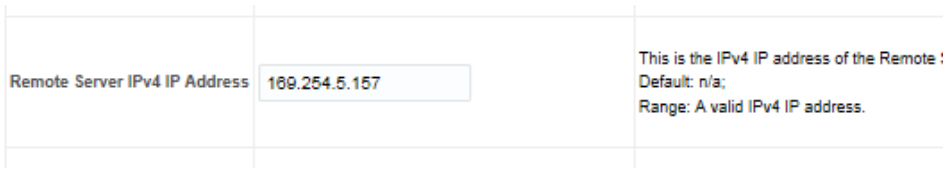
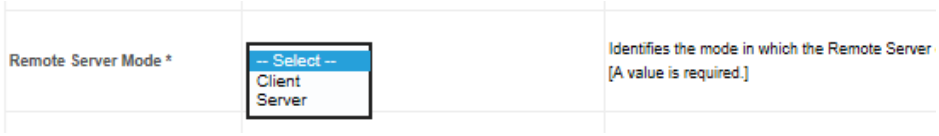
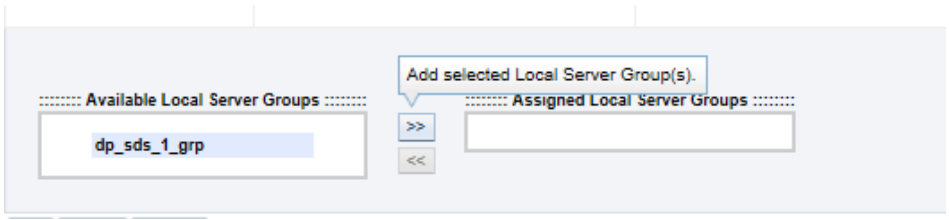
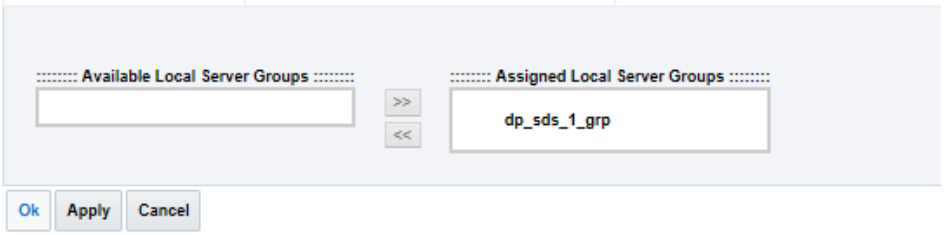
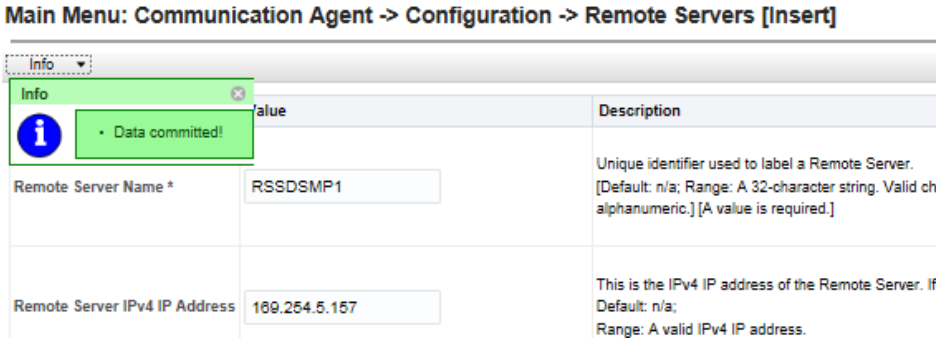
Procedure 12. Configuring ComAgent (All SOAM Sites)

Step	Procedure	Result
1. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP Address (VIP) of the SDS **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
2. ☐	**Primary 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 12. Configuring ComAgent (All SOAM Sites)

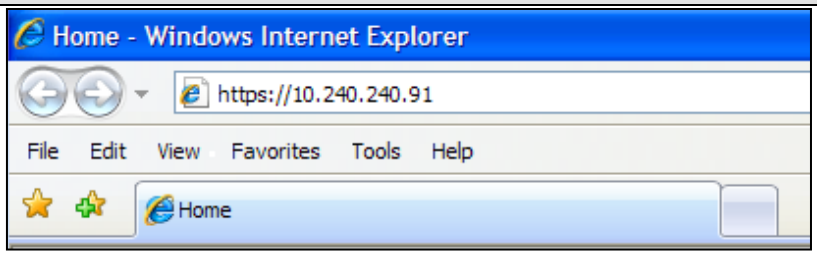
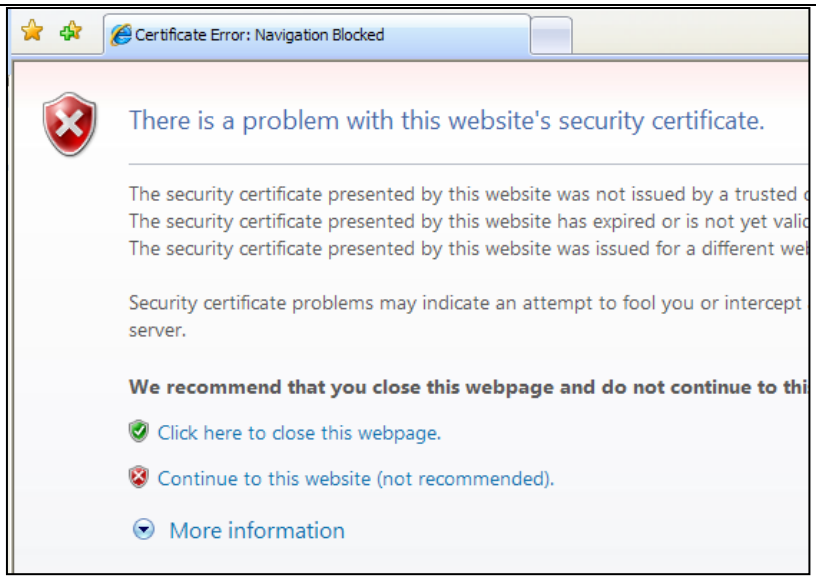
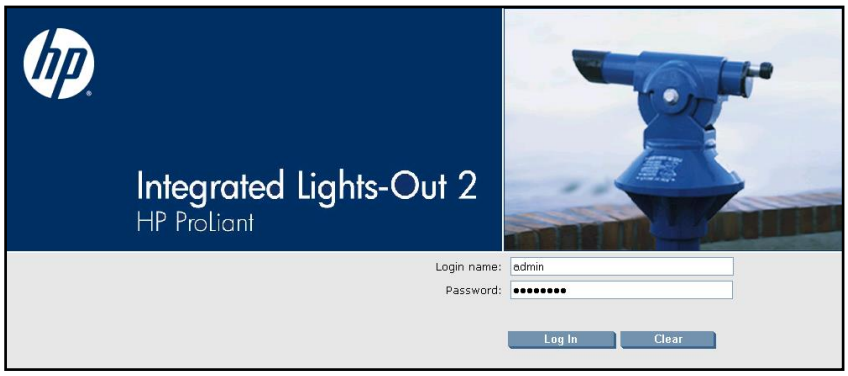
3. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	
4. ☐	**Primary SDS VIP:** Select… **Main Menu** **→Communication Agent** **→Configuration** **→Remote Servers** …as shown on the right.	
5. ☐	**Primary SDS VIP:** Select the "**Insert**" dialogue button	
6. ☐	**Primary SDS VIP:** Enter the "**Remote Server Name**" for the DSR Message Processer server	

Procedure 12. Configuring ComAgent (All SOAM Sites)

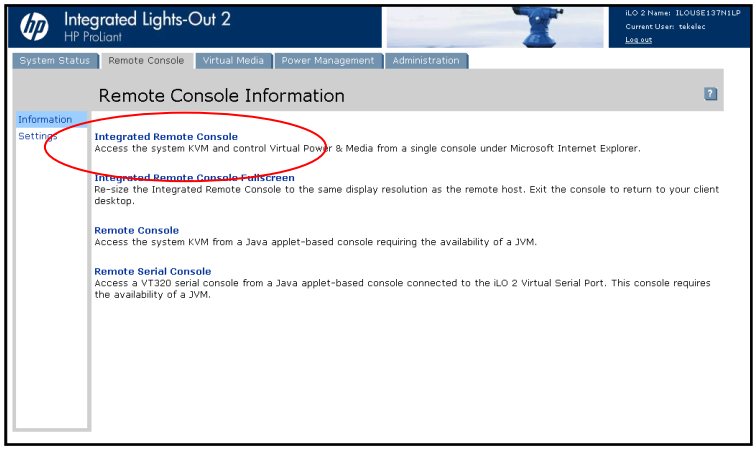
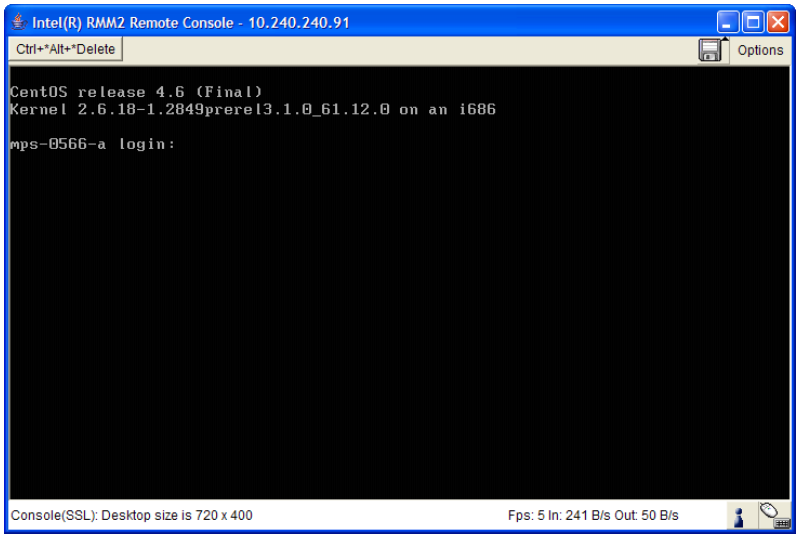
7. ☐	**Primary SDS VIP:** Enter the "**Remote Server IMI IP Address**".	 **NOTE:** *This should be the IMI IP address of the MP blade.*
8. ☐	**Primary SDS VIP:** Select "**Client**" for the **Remote Server Mode** from the pull-down menu.	
9. ☐	**Primary SDS VIP:** Select the **Local Server Group** for the SDS Data Processer server group	
10. ☐	**Primary SDS VIP:** Click the "**Apply**" dialogue button	
11. ☐	**Primary SDS VIP:** Under the "Info" banner option, the user should be presented with a message stating **"Data committed"**	
12. ☐	Repeat steps 5 – 11 of this procedure for each additional remote DA-MP in the associated DSR SOAM NE.	
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix A. Accessing the iLO VGA Redirection Window

Procedure 13. Accessing the iLO VGA Redirection Window

Step	Procedure	Result
1. ☐	Launch an approved web browser and connect to the iLO interface **NOTE:** *Always use https:// for iLO GUI access.*	
2. ☐	The web browser will display a warning message regarding the Security Certificate. **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
3. ☐	Login to the iLO console as "Administrator"	

Procedure 13. Accessing the iLO VGA Redirection Window

4. ☐	The admin GUI is displayed. Select the "**Remote Console**" tab in the upper left corner of the GUI.	
5. ☐	The Remote Console Information GUI is displayed Click on the "**Integrated Remote Console**" option	
6. ☐	The iLO Console window is displayed. **NOTE:** *The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.*	
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix B. Creating Temporary External IP Address for Accessing SDS GUI

This procedure creates a temporary external IP address that will be used for accessing the SDS GUI prior to configuring the first SDS server. This procedure assumes that the user has access to the ILO and can access an external (XMI) network at the customer site.

Procedure 14. Creating Temporary External IP Address for Accessing SDS GUI

Step	In this procedure you will configure a temporary external IP Address for SDS Server A for the 1st SDS site. The user will use this IP Address in a web browser to access the GUI to configure the first SDS server.	
1. ☐	Log onto the SDS NOAM Server A ILO as indicated in Appendix A ***Note***: Output similar to that shown on the right will appear.	CentOS release 5.6 (Final) Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.22.0 on an x86_64 hostname1260476221 login: **admusr** Password: **<*admusr_password*>**
2. ☐	For Gen8: Delete bond0 For Gen9: Delete bond0	$ sudo **netAdm delete --device=bond0** eth01 was successfully removed from bond0 eth11 was successfully removed from bond0 Interface bond0 removed For Gen9: $ sudo **netAdm delete --device=bond0** eth01 was successfully removed from bond0 eth02 was successfully removed from bond0 Interface bond0 removed

3. ☐	Add XMI IP address to the first SDS server
	(SDS NOAM-A) and have it use interface eth02 for Gen8 and eth03 for Gen9
		For Gen8:
		$ sudo **netAdm set --device=eth02 --onboot=yes --netmask=255.255.255.0 --address=<XMI_IP_Address_for_SDS_A>**
		Interface eth02 updated
		For Gen9:
		$ sudo **netAdm set --device=eth03 --onboot=yes --netmask=255.255.255.0 --address=<XMI_IP_Address_for_SDS_A>**
		Interface eth03 updated

4. ☐	Add route to the default gateway for the first SDS site	For Gen8:
		$ sudo **netAdm add --device=eth02 --route=default --gateway=<XMI_IP_Address_for_default_gateway>**
		Route to eth02 added
		For Gen9:
		$ sudo **netAdm add --device=eth03 --route=default --gateway=<XMI_IP_Address_for_default_gateway>**
		Route to eth03 added

5. ☐	Wait a few minutes and then ping the default gateway to ensure connectivity.	$ **ping <XMI_IP_Address_for_default_gateway>**

Procedure 14. Creating Temporary External IP Address for Accessing SDS GUI

6. ☐	Log off the ILO	`$ exit`
7. ☐	Important ***Note***: This interface must be un-configured	***Note***: If this method is used, then the For Gen8 `eth02(0r eth03 for Gen9)` interface must be un-configured in Step **Error! Reference ource not found.** in Procedure 3 of Section 5.1 Configuring SDS Servers A and B (1st SDS NOAM Site Only)
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix C. Establish a Local Connection for Accessing the SDS GUI

This procedure contains steps to connect a laptop to the SDS NOAM-A server via a directly cabled Ethernet connection and setting the IP address of the laptop. This procedure enables the user to use the laptop for accessing the SDS GUI prior to configuring the first SDS server.

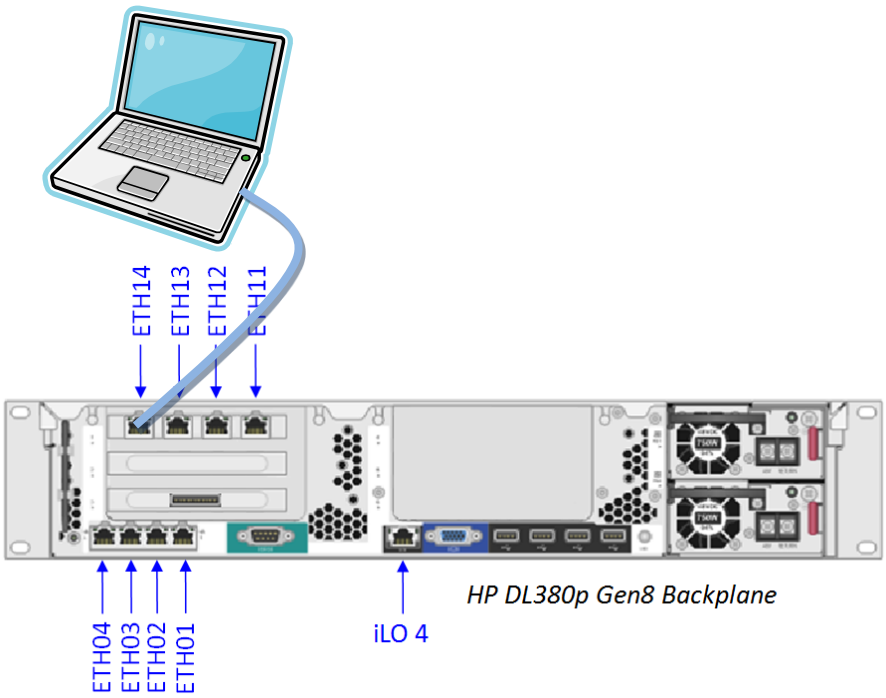
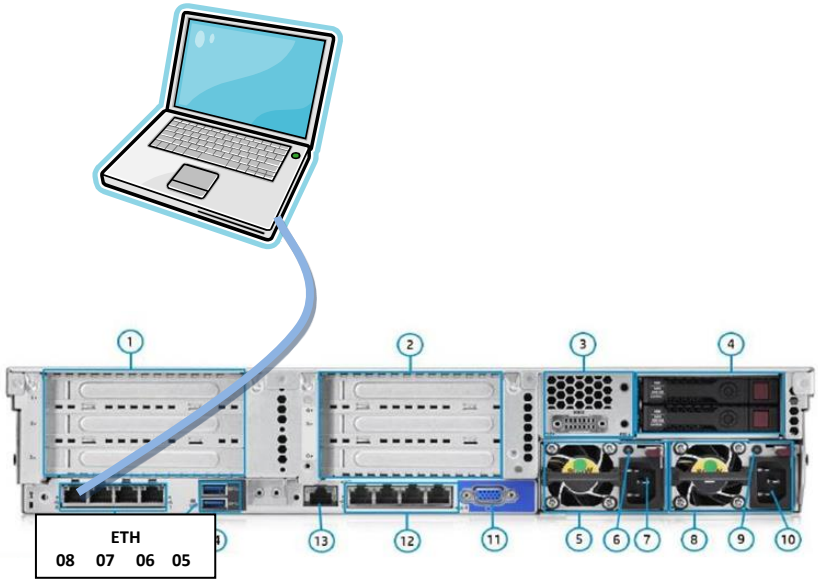
Procedure 15. Establish a Local Connection for Accessing SDS GUI

Step	In this procedure you will configure a temporary external IP Address for SDS Server NOAM A for the 1st SDS site. The user will use this IP Address in a web browser to access the GUI to configure the first SDS server.	
1. ☐	Access the SDS NOAM-A server's console.	Connect to the SDS NOAM-A server's console using one of the access methods described in **Section 2.3.**

2. ☐	**1)** Access the command prompt.
	2) Log into the SDS NOAM-A server as the "**admusr**" user.
		`CentOS release 5.6 (Final)`
		`Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.22.0 on an x86_64`
		
		`hostname1260476221 login: admusr`
		`Password: <admusr_password>`

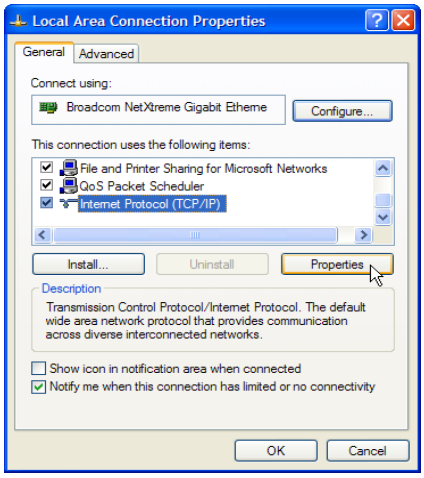
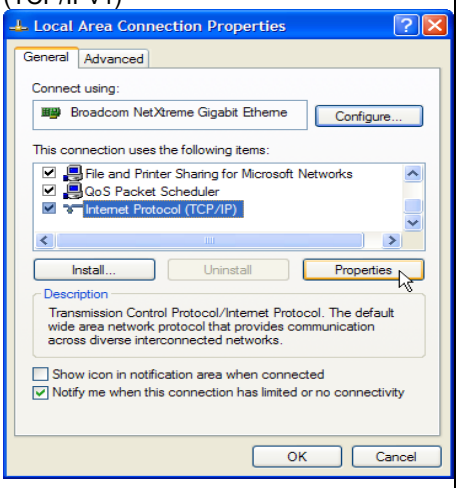
3. ☐	***This step, DL380 Gen8 only!*** Configure static IP 192.168.100.11 on the eth14 port of the SDS NOAM-A server.	`$ sudo netAdm set --device=eth14 --address=192.168.100.11 --netmask=255.255.255.0 --onboot=yes`
4. ☐	***This step, DL380 Gen9 only!*** Configure static IP 192.168.100.11 on the eth08 port of the SDS NOAM-A server.	`$ sudo netAdm set --device=eth08 --address=192.168.100.11 --netmask=255.255.255.0 --onboot=yes`

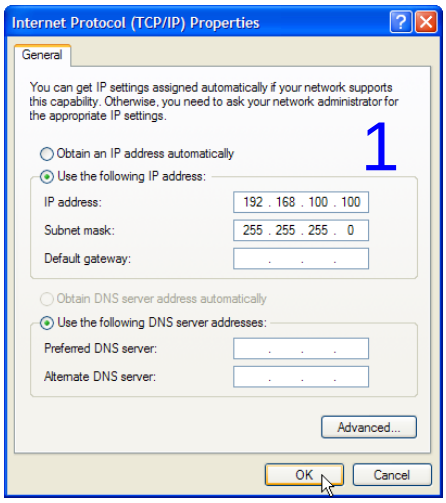
Procedure 15. Establish a Local Connection for Accessing SDS GUI

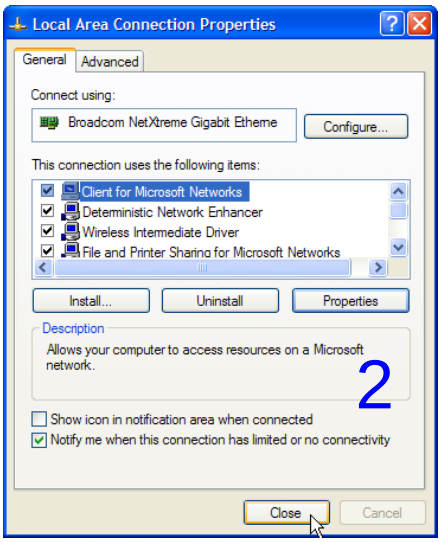
5. ☐	**Execute this step for HP DL380 Gen8:** **1)** Plug in one end of the Ethernet cable (straight-thru) into the back of SDS NOAM-A server ETH14 (top left port). **2)** Plug the other end of the Ethernet cable into the laptop's Ethernet jack.	 **Figure 16 – HP DL380 Gen9: DC (Rear Panel)**
☐	**Execute this step** **For HP DL380 Gen9:** **1)** Plug in one end of the Ethernet cable (straight-thru) into the back of SDS NOAM-A server **ETH08** (bottom left port). **2)** Plug the other end of the Ethernet cable into the laptop's Ethernet jack.	

Procedure 15. Establish a Local Connection for Accessing SDS GUI

<table>
<tr>
<td>6. ☐</td>
<td>Access the laptop network interface card's TCP/IP "Properties" screen.

NOTE: For this step follow the instruction specific to the laptop's OS (XP, Vista or Win 7).</td>
<td>Windows XP
• Go to Control Panel
• Double-click on Network Connections
• Right-click the wired Ethernet Interface icon and select "Properties"
Select "Internet Protocol (TCP/IP)" and select "Properties"
 
</td>
<td>Windows Vista / Win 7
• Go to Control Panel.
• Double-click on Network and Sharing Center
• Select Manage Network Connections (left menu)
• Right-click the wired Ethernet Interface icon and select "Properties"
Select "Internet Protocol Version 4 (TCP/IPv4)"
 
</td>
</tr>
<tr>
<td>7. ☐</td>
<td>1) Set the IP address and netmask of the laptop's network interface card to an IP address within the same network subnet as the statically assigned IP address used in Step 3 of this procedure (192.168.100.100 is suggested) and click "OK".

2) Click "Close" from the network interface card's main "Properties" screen.</td>
<td colspan="2"> 


</td>
</tr>
<tr>
<td colspan="4">THIS PROCEDURE HAS BEEN COMPLETED</td>
</tr>
</table>

The user can now launch an approved web browser on this laptop and connect to https://192.168.100.11 to access the SDS GUI using a temporary IP address.

Appendix D. Configure Cisco 4948E-F Aggregation Switches

These switch configuration procedures require that the SDS hardware (servers and switches) are installed in a frame as indicated in the below picture:

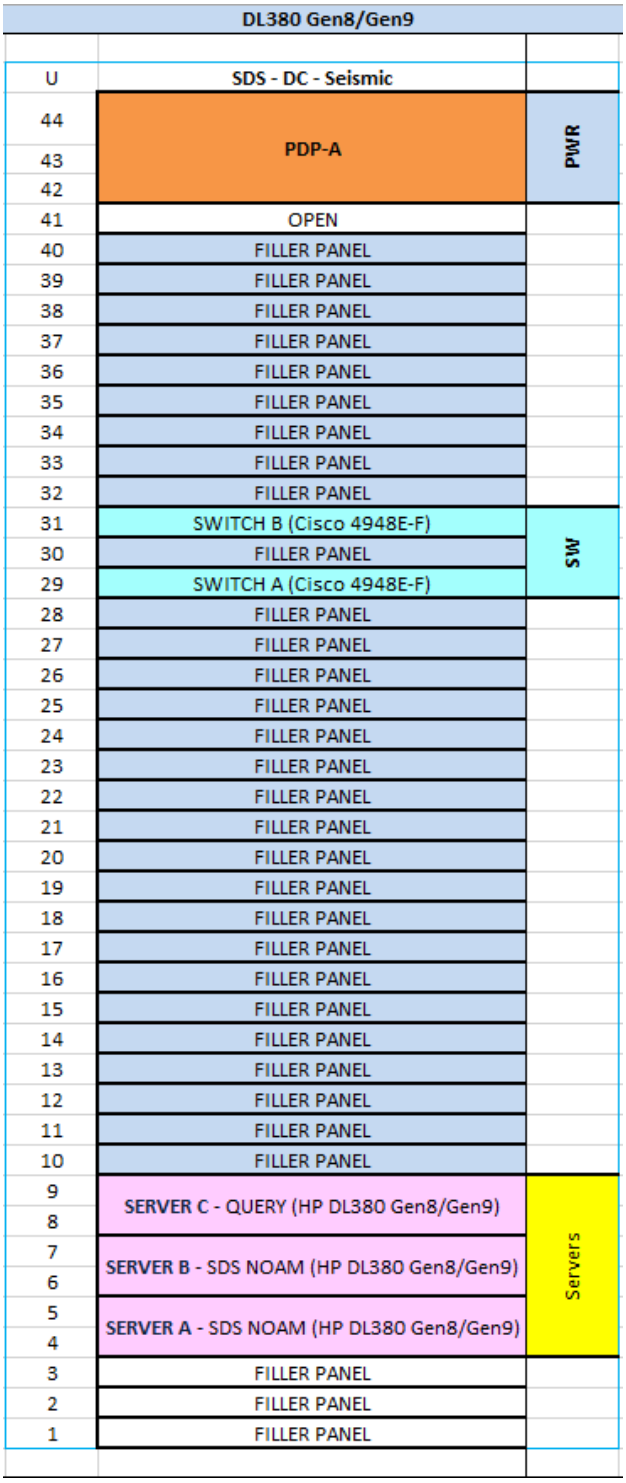
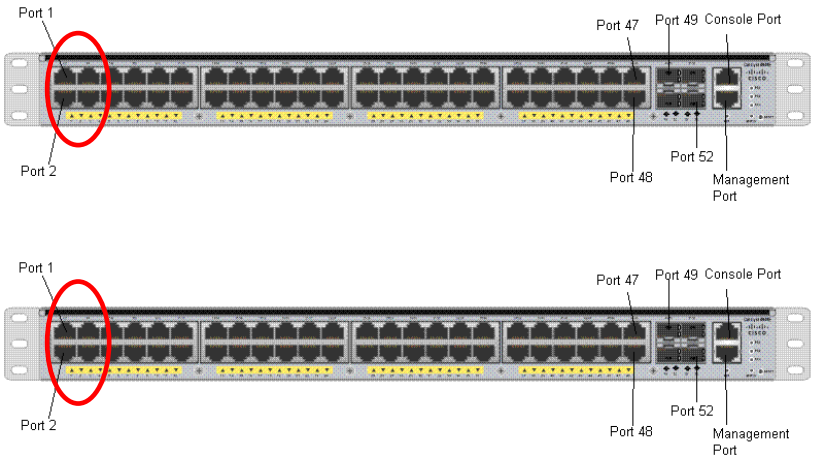
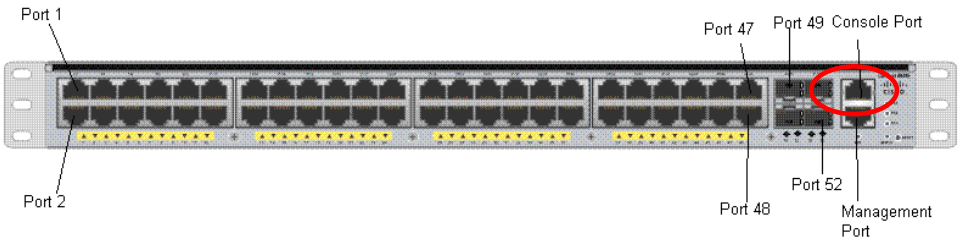


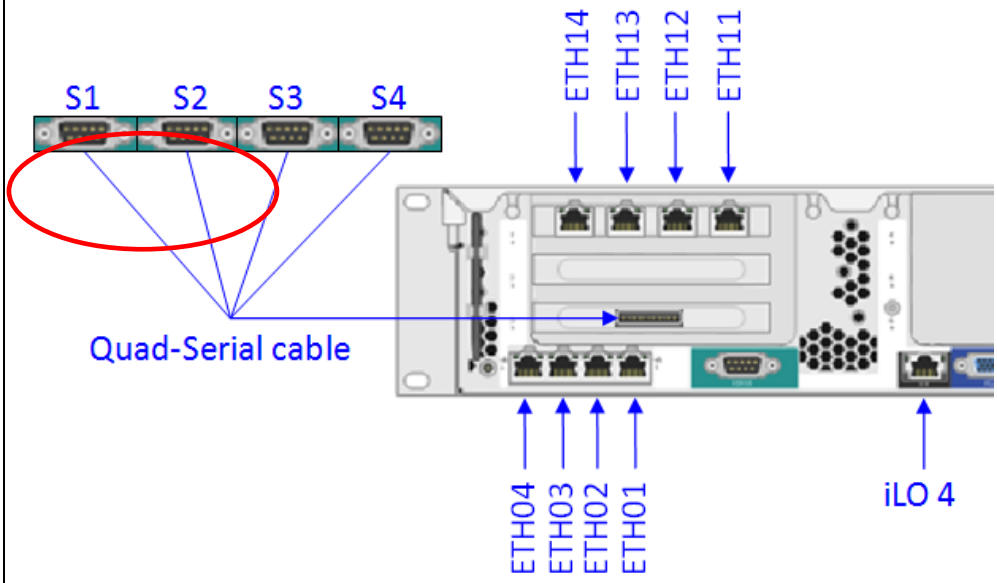
Figure 17 – SDS Frame Layout

D-1. Verifying Cisco Switch Wiring (All SDS NOAM Sites)

Procedure 16. Verifying Cisco Switch Wiring (SDS Sites)

Step	Procedure	Result
1.	Set/Verify the following cable configuration at the **Cisco 4948E-F switches**: ☐ **1)** Verify that the ISL **switch1A, Port 1** to **switch1B, Port 1** is **CONNECTED**. ☐ **2)** Verify that the ISL **switch1A, Port 2** to **switch1B, Port 2** is **CONNECTED**. ☐ **3)** Verify that the ISL **switch1A, Port 3** to **switch1B, Port 3** is **CONNECTED**. **4)** Verify that the ISL **switch1A, Port 4** to **switch1B, Port 4** is **CONNECTED**.	1B **switch1B** (Top) 1A **switch1A** (Bottom)  **Figure 18 – Cisco 4948E-F Switch ISL Connections**
2.	**DL380 Gen8 only :** Verify that **SERVER A** has the Quad-Serial card interface ports connected to the **Console Port** each switch port.	 **Figure 19 – Cisco 4948E-F Switch (Console Port)**

Procedure 16. Verifying Cisco Switch Wiring (SDS Sites)

Step	Procedure	Result
☐ ☐	**1)** Verify that the **switch1A, Console Port** is **CONNECTED** to **SERVER A, Quad-Serial Port S1** using Cable 830-1229-xx**.** **2)** Verify that the **switch1B, Console Port** is **CONNECTED** to **SERVER A, Quad-Serial Port S2** using Cable 830-1229-xx**.**	 **Figure 20 – HP DL380 Gen8: Rear Panel (Quad-Serial Ports)**
3. ☐	***This step, DL380 Gen8 only!*** **1)** Verify that **switch1A, Port 5** is **CONNECTED to SERVER A, ETH01**.	

Procedure 16. Verifying Cisco Switch Wiring (SDS Sites)

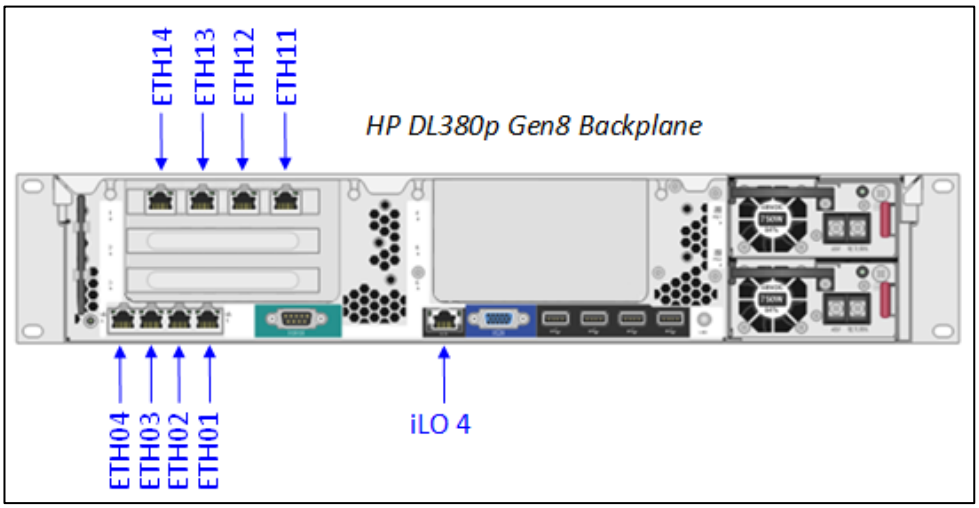
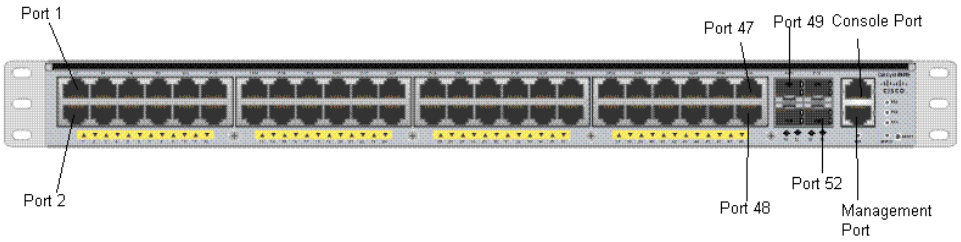
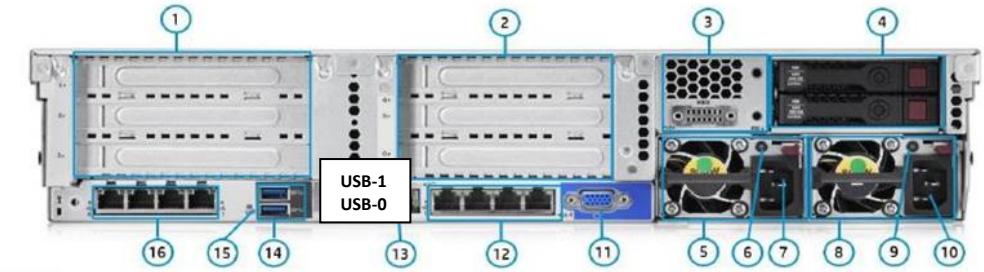
Step	Procedure	Result
☐	**2)** Verify that **switch1B, Port 5** is **CONNECTED to SERVER A, ETH11**.	
☐	**3)** Verify that **switch1A, Port 6** is **CONNECTED to SERVER B, ETH01**.	
☐	**4)** Verify that **switch1B, Port 6** is **CONNECTED to SERVER B, ETH11**.	
☐	**5)** Verify that **switch1A, Port 7** is **CONNECTED to SERVER C, ETH01**.	
☐	**6)** Verify that **switch1B, Port 7** is **CONNECTED to SERVER C, ETH11**.	

Figure 21 – HP DL380 Gen8: Rear Panel (Ethernet)

Procedure 16. Verifying Cisco Switch Wiring (SDS Sites)

Step	Procedure	Result
4. ☐	***This step, DL380 Gen9 only!*** **1)** Verify that the **switch1A, Console Port** is **CONNECTED** to **SERVER A, USB Port USB0** **2)** Verify that the **switch1B, Console Port** is **CONNECTED** to **SERVER A, USB Port USB1**	 **Figure 22 – Cisco 4948E-F Switch (Console Port)**  **Figure 23 – HP DL380 Gen9: DC (Rear Panel)**

Procedure 16. Verifying Cisco Switch Wiring (SDS Sites)

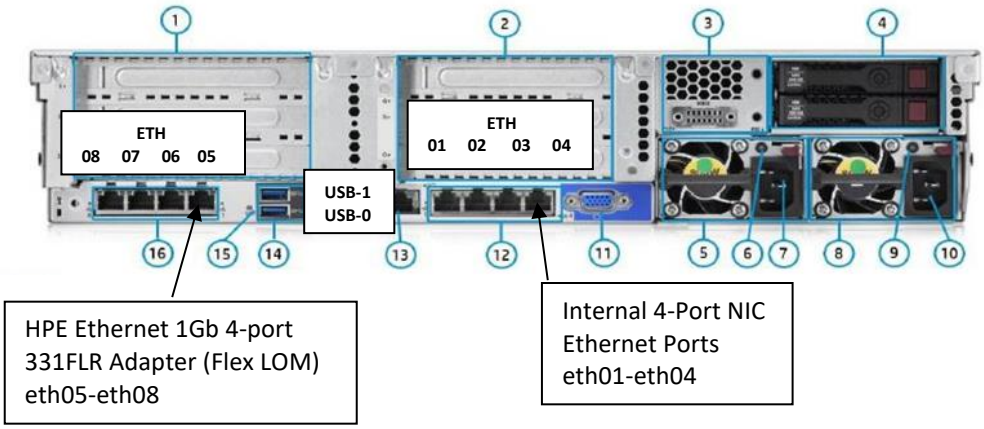
Step	Procedure	Result
5.	***This step, DL380 Gen9 only!***	
☐	**1)** Verify that **switch1A, Port 5** is **CONNECTED to** **SERVER A, ETH01**	
☐	**2)** Verify that **switch1B, Port 5** is **CONNECTED to** **SERVER A, ETH02**	
☐	**3)** Verify that **switch1A, Port 6** is **CONNECTED to** **SERVER B, ETH01**	
☐	**4)** Verify that **switch1B, Port 6** is **CONNECTED to** **SERVER B, ETH02**	
☐	**5)** Verify that **switch1A, Port 7** is **CONNECTED to** **SERVER C, ETH01**	
	6) Verify that **switch1B, Port 7** is **CONNECTED to** **SERVER C, ETH02**	
THIS PROCEDURE HAS BEEN COMPLETED		

Figure 24 – HP DL380 Gen9: DC (Rear Panel)

D-2. Configure Cisco 4948E-F Aggregation Switches

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

CAUTION!! All netConfig commands must be typed ***exactly*** as they are shown here! Input is case sensitive, there is no input validation, and some terminal clients will inject bad characters if you backspace! Use **Ctrl-C** to exit netConfig if you make a mistake on any field and re-run that command.

Variable	Management Server	Serial Port (DL380 Gen8)	Serial Port (DL380 Gen9)
<switch1A_serial_port>	SERVER A	ttyS4	ttyUSB0
<switch1B_serial_port>	SERVER A	ttyS5	ttyUSB1

Variable	
<IOS_image_file>	Fill in the appropriate value from [5]: _____

Variable	Value
<switch_platform_username>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).
<switch_platform_password>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).
<switch_console_password>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).
<switch_enable_password>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).
<SERVER A_mgmtVLAN_ip_address >	*Primary SDS:* 169.254.1.11 *DR SDS:* 169.254.1.14
< SERVER B_mgmtVLAN_ip_address>	*Primary SDS:* 169.254.1.12 *DR SDS:* 169.254.1.15
<switch_mgmtVLAN_id>	2
<switch1A_mgmtVLAN_ip_address>	169.254.1.1
<netmask>	255.255.255.0
<switch1B_mgmtVLAN_ip_address>	169.254.1.2
<management_server_mgmtInterface>	bond0.2
<SERVER A_iLO_ip> (See NAPD documentation for IP Address) [1]	_____
< SERVER B_iLO_ip > (See NAPD documentation for IP Address) [1]	_____

Ethernet Interface	DL380 Gen8 /	DL380 Gen9
<ethernet_interface_1>	bond0.2 (eth01, eth11)	bond0.2 (eth01, eth02)
<ethernet_interface_2>	bond0.4 (eth01, eth11)	bond0.4 (eth01, eth02)

Variable	Value
<platcfg_password>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).
<management_server_mgmtInterface>	bond0.2
<switch_backup_user>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS)..
<switch_backup_user_password>	Contact Oracle's Customer Support Accessing My Oracle Support (MOS).

Note: Uplinks, if present, must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Refer to Figure 17 – SDS Frame Layout for determining which cables are used for customer uplink.

Needed Material:

- HP Misc. Firmware DVD
- HP Solutions Firmware Upgrade Pack Release Notes [4]
- Application specific documentation (documentation that referred to this procedure)
- Switch A and B initialization xml files and SDS switch configuration xml file located on the NOAM server in the /usr/TKLC/plat/etc/switch/xml/ directory ISO.
- Application ISO's with netConfig and its required RPMs.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the Customer Care Center section of this document.

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result
1. ☐	**SERVER A:** Access the **SERVER A** console.	Connect to the **SERVER A** console using one of the access methods described in **Section 2.3.**

2. ☐	**SERVER A:**
	Log into the HP DL380 server as the "**admusr**" user.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

3. ☐ ☐ ☐	**SERVER A:**
	Verify the switch1A initialization file exists
	Verify the switch1B initialization file exists
	Verify the switch configuration files exist
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E_E-F_init.xml`
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/switch1B_SDS_4948E_E-F_init.xml`
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/Primary_switch1A_SDS_4948E_E-F_configure.xml`
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/Primary_switch1B_SDS_4948E_E-F_configure.xml`
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/DR_switch1A_SDS_4948E_E-F_configure.xml`
		`$ ls -l /usr/TKLC/plat/etc/switch/xml/DR_switch1B_SDS_4948E_E-F_configure.xml`
		
		If any file does not exist, contact Customer Care Center for assistance.

4. ☐	**SERVER A:**
	DL 380 GEN 8:
	Verify quad-serial port mappings *(quad-dongle S1 = ttyS4, quad-dongle S2 = ttyS5)*
		`$ sudo setserial -g /dev/ttyS{1..12}`
		`/dev/ttyS1, UART: 16550A, Port: 0x02f8, IRQ: 3`
		`/dev/ttyS2, UART: unknown, Port: 0x03e8, IRQ: 4`
		`/dev/ttyS3, UART: unknown, Port: 0x02e8, IRQ: 3`
		`/dev/ttyS4, UART: 16950/954, Port: 0x0000, IRQ: 24`
		`/dev/ttyS5, UART: 16950/954, Port: 0x0000, IRQ: 24`
		`/dev/ttyS6, UART: 16950/954, Port: 0x0000, IRQ: 24`
		`/dev/ttyS7, UART: 16950/954, Port: 0x0000, IRQ: 24`
		`/dev/ttyS8, UART: unknown, Port: 0x0000, IRQ: 0`
		`/dev/ttyS9, UART: unknown, Port: 0x0000, IRQ: 0`
		`/dev/ttyS10, UART: unknown, Port: 0x0000, IRQ: 0`
		`/dev/ttyS11, UART: unknown, Port: 0x0000, IRQ: 0`
		`/dev/ttyS12, UART: unknown, Port: 0x0000, IRQ: 0`
		
		Output should match the example shown above; if not, contact Customer Care Center for assistance.

5.	**SERVER A:**
	For GEN 9:
	Verify serial port mapping from USB0 and USB1.
		`$ sudo setserial -g /dev/ttyUSB*`
		`/dev/ttyUSB0, UART: unknown, Port: 0x0000, IRQ: 0, Flags: low_latency`
		`/dev/ttyUSB1, UART: unknown, Port: 0x0000, IRQ: 0, Flags: low_latency`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result
6. ☐	**SERVER A:** For Gen8: Setup conserver serial console access for switch1A	$ **sudo conserverSetup -i -s <SERVER_A_mgmtVLAN_ip_address>** Example: $ **sudo conserverSetup -i -s 169.254.1.11** Enter your platcfg username, followed by [ENTER]:**platcfg** Enter your platcfg password, followed by [ENTER]: Target address is local to this host. Running conserverSetup in local mode. Checking Platform Revision for local TPD installation... The local machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Enter the switch name for this console connection (default: "switch1A_console"), followed by [ENTER]: **switch1A_console** Enter the serial device designation for switch1A_console (default: "ttyUSB0"), followed by [ENTER]:**ttyS4** Configure additional serial consoles [Y/n]? [press ENTER for default <Y>]:n Configuring switch 'switch1A_console' console server...Configured. Configuring console repository service......Configured. Remote host has the following available interfaces: bond0 bond0.4 bond1 eth01 eth02 eth11 eth12 Enter the name of the bond on the remote server(default: "bond0"), followed by [ENTER]: ...No entry provided for bond. Resorting to default. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth11

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result
7.	**SERVER A:** Note: For DL380 Gen9 only: Setup conserver serial console access for switch1A	$ **sudo conserverSetup -i -u <SERVER_A_mgmtVLAN_ip_address>** Example: $ **sudo conserverSetup -i -u 169.254.1.11** Enter your platcfg username, followed by [ENTER]:**platcfg** Enter your platcfg password, followed by [ENTER]: Target address is local to this host. Running conserverSetup in local mode. Checking Platform Revision for local TPD installation... The local machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Enter the switch name for this console connection (default: "switch1A_console"), followed by [ENTER]: **switch1A_console** Enter the serial device designation for switch1A_console (default: "ttyUSB0"), followed by [ENTER]:ttyUSB0 Configure additional serial consoles [Y/n]? [press ENTER for default <Y>]:n Configuring switch 'switch1A_console' console server...Configured. Configuring console repository service......Configured. Remote host has the following available interfaces: bond0 bond0.4 bond1 eth01 eth02 eth11 eth12 Enter the name of the bond on the remote server(default: "bond0"), followed by [ENTER]: ...No entry provided for bond. Resorting to default. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result
8.	**SERVER A:** Note: For DL380 Gen8: Setup conserver serial console access for switch1B	$ **sudo conserverSetup -i -s <SERVER_A_mgmtVLAN_ip_address>** Example: $ **sudo conserverSetup -i -s 169.254.1.11** Enter your platcfg username, followed by [ENTER]:platcfg Enter your platcfg password, followed by [ENTER]: Checking Platform Revision for local TPD installation... The local machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Enter the switch name for this console connection (default: "switch1A_console"), followed by [ENTER]:**switch1B_console** Enter the serial device designation for switch1B_console (default: "ttyUSB0"), followed by [ENTER]:**ttyS5** Configure additional serial consoles [Y/n]? [press ENTER for default <Y>]:**n** Configuring switch 'switch1B_console' console server...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: 169.254.1.11 ...Configured. Remote host has the following available interfaces: bond0 bond0.2 bond0.4 bond1 eth01 eth02 eth11 eth12 eth13 eth14 Enter the name of the bond on the remote server(default: "bond0"), followed by [ENTER]: ...No entry provided for bond. Resorting to default. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth11

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result
9. ☐	**SERVER A:** **Note : For DL380 Gen9** Setup conserver serial console access for switch1B	$ **sudo conserverSetup -i -u <SERVER_A_mgmtVLAN_ip_address>** Example: $ **sudo conserverSetup -i -u 169.254.1.11** Enter your platcfg username, followed by [ENTER]:platcfg Enter your platcfg password, followed by [ENTER]: Checking Platform Revision for local TPD installation... The local machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: SDS Base Distro Release: 7.0.0.0.0_86.14.0 Enter the switch name for this console connection (default: "switch1A_console"), followed by [ENTER]:**switch1B_console** Enter the serial device designation for switch1B_console (default: "ttyUSB0"), followed by [ENTER]:**ttyUSB1** Configure additional serial consoles [Y/n]? [press ENTER for default <Y>]:**n** Configuring switch 'switch1B_console' console server...Configured. Configuring iptables for port(s) 782...Configured. Configuring iptables for port(s) 1024:65535...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: 169.254.1.11 ...Configured. Remote host has the following available interfaces: bond0 bond0.2 bond0.4 bond1 eth01 eth02 eth11 eth12 eth13 eth14 Enter the name of the bond on the remote server(default: "bond0"), followed by [ENTER]: ...No entry provided for bond. Resorting to default. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

10. ☐	**SERVER A:**
	
	Add a repository for SSH service
		`$ sudo netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`SSH host IP? 169.254.1.11`
		`SSH username: admusr`
		`SSH password? <user_password>`
		`Verify password: <user_password>`
		`Add service for ssh_service successful`

11. ☐	**SERVER A:**
	
	Verify you have entered the information correctly for SSH service
		`$ sudo netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 169.254.1.11`
		`Options:`
		`password: 615EBD88232A2EFD0080AC990393083D`
		`user: admusr`

12. ☐	**SERVER A:**
	
	Add a repository for TFTP service
		`$ sudo netConfig --repo addService name=tftp_service`
		`Service type? (tftp, ssh, conserver, oa) tftp`
		`Service host? 169.254.1.11`
		`Directory on host? /var/lib/tftpboot/`
		`Add service for tftp_service successful`

13. ☐	**SERVER A:**
	
	Verify that you have entered the information correctly for TFTP service
		`$ sudo netConfig --repo showService name=tftp_service`
		`Service Name: tftp_service`
		`Type: tftp`
		`Host: 169.254.1.11`
		`Options:`
		`dir: /var/lib/tftpboot/`

14. ☐	**SERVER A:**
	
	Create console service for switch1A
		`$ sudo netConfig --repo addService name=switch1A_consvc`
		
		`Service type? (tftp, ssh, conserver, oa) conserver`
		`Conserver host IP? 169.254.1.11`
		`Conserver username? platcfg`
		`Service password? <platcfg_password>`
		`Verify password: <platcfg_password>`
		`Add service for switch1A_consvc successful`

15. ☐	**SERVER A:**
	
	Verify you have entered the information correctly for switch1A console service
		`$ sudo netConfig --repo showService name=switch1A_consvc`
		`Service Name: switch1A_consvc`
		`Type: conserver`
		`Host: 169.254.1.11`
		`Options:`
		`password: 0B902ECD13D5BD2F1B57B5BFC6E95FE9`
		`user: platcfg`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

16. ☐	**SERVER A:**
	
	Add repository for switch1B console service
		`$ sudo netConfig --repo addService name=switch1B_consvc`
		
		`Service type? (tftp, ssh, conserver, oa) conserver`
		`Conserver host IP? 169.254.1.11`
		`Conserver username? platcfg`
		`Service password?: <platcfg_password>`
		`Verify password: <platcfg_password>`
		`Add service for console_service successful`

17. ☐	**SERVER A:**
	
	Verify you have entered the information correctly for switch1B console service
		`$ sudo netConfig --repo showService name=switch1B_consvc`
		`Service Name: switch1B_consvc`
		`Type: conserver`
		`Host: 169.254.1.11`
		`Options:`
		`password: 0B902ECD13D5BD2F1B57B5BFC6E95FE9`
		`user: platcfg`

18. ☐	**SERVER A:**
	
	Verify and remove the service named “console_service” if present
		`$ sudo netConfig --repo showService name=console_service`
		`Services:`
		`Service Name: console_service`
		`Type: conserver`
		`Host: 169.254.1.11`
		`Options:`
		`password: 0B902ECD13D5BD2F1B57B5BFC6E95FE9`
		`user: platcfg`
		
		If service named “console_service is present, then remove it. Otherwise skip to the next step.
		
		`$ sudo netConfig --repo deleteService name=console_service`
		`Are you sure you want to delete console_service (y/n)? y`
		`Deleting service console_service...`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

19. ☐	**SERVER A:**
	
	Add repository for switch1A
		`$ sudo netConfig --repo addDevice name=switch1A --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? 4948E-F`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: 169.254.1.1/24`
		`Is the management interface a port or a vlan? [vlan]:vlan`
		`What is the VLAN ID of the management VLAN? [2]: 2`
		`What is the name of the management VLAN? [management]: management`
		`What switchport connects to the management server? [GE40]: GE5`
		`What is the switchport mode (access|trunk) for the management server port? [trunk]: trunk`
		`What are the allowed vlans for the management server port? [1,2]: 1-4`
		`Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.WO.bin]:`
		`Enter the name of the upgrade file transfer service: tftp_service`
		`File transfer service to be used in upgrade: tftp_service`
		`WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.`
		
		`Should the init oob adapter be added (y/n)? y`
		
		`Adding consoleInit protocol for switch1A using oob...`
		`What is the name of the service used for OOB access? switch1A_consvc`
		`What is the name of the console for OOB access? switch1A_console`
		`What is the platform access username? platcfg`
		`What is the device console password?`
		`Verify password:`
		
		`What is the platform user password?`
		`Verify password:`
		
		`What is the device privileged mode password?`
		`Verify password:`
		
		`Should the live network adapter be added (y/n)? y`
		
		`Adding cli protocol for switch1A using network...`
		`Network device access already set: 169.254.1.1`
		
		`Should the live oob adapter be added (y/n)? y`
		
		`Adding cli protocol for switch1A using oob...`
		`OOB device access already set: switch1A_consvc`
		`Device named switch1A successfully added.`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

20. ☐	**SERVER A:**
	
	Add repository for switch1B
		`$ sudo netConfig --repo addDevice name=switch1B --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? 4948E-F`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: 169.254.1.2/24`
		`Is the management interface a port or a vlan? [vlan]:vlan`
		`What is the VLAN ID of the management VLAN? [2]: 2`
		`What is the name of the management VLAN? [management]: management`
		`What switchport connects to the management server? [GE40]: GE5`
		`What is the switchport mode (access|trunk) for the management server port? [trunk]: trunk`
		`What are the allowed vlans for the management server port? [1,2]: 1-4`
		`Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.WO.bin]:`
		`Enter the name of the upgrade file transfer service: tftp_service`
		`File transfer service to be used in upgrade: tftp_service`
		`WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.`
		
		`Should the init oob adapter be added (y/n)? y`
		
		`Adding consoleInit protocol for switch1A using oob...`
		`What is the name of the service used for OOB access? switch1B_consvc`
		`What is the name of the console for OOB access? switch1B_console`
		`What is the platform access username? platcfg`
		`What is the device console password?`
		`Verify password:`
		
		`What is the platform user password?`
		`Verify password:`
		
		`What is the device privileged mode password?`
		`Verify password:`
		
		`Should the live network adapter be added (y/n)? y`
		
		`Adding cli protocol for switch1A using network...`
		`Network device access already set: 169.254.1.2`
		
		`Should the live oob adapter be added (y/n)? y`
		
		`Adding cli protocol for switch1A using oob...`
		`OOB device access already set: switch1B_consvc`
		`Device named switch1B successfully added.`

Procedure 17. Configuring Cisco 4948E-F Switches (All SDS NOAM Sites)

Step	Procedure	Result

21. ☐	**SERVER A:**
	
	Verify you have entered the information correctly
		`$ sudo netConfig --repo listDevices`
		`Devices:`
		
		`Device: switch1A`
		`Vendor: Cisco`
		`Model: 4948E-F`
		`Access: Network: 169.254.1.1`
		`Access: OOB:`
		`Service: switch1A_consvc`
		`Console: switch1A_console`
		`Init Protocol Configured`
		`Live Protocol Configured`
		
		`Device: switch1B`
		`Vendor: Cisco`
		`Model: 4948E-F`
		`Access: Network: 169.254.1.2`
		`Access: OOB:`
		`Service: switch1B_consvc`
		`Console: switch1B_console`
		`Init Protocol Configured`
		`Live Protocol Configured`

22. ☐	**SERVER A:**
	
	Log in to switch1A
		Example:
		`console -M <SERVER A_mgmtVLAN_ip_address> -l platcfg switch1A_console`
		
		`$ /usr/bin/console -M 169.254.1.11 -l platcfg switch1A_console`
		
		`Enter platcfg@pmac5000101's password: <platcfg_password>`
		`[Enter `^Ec?' for help]`
		Press <Enter>

23. ☐	**switch1A:**
	
	Note the image version for comparison in a following step.
		`Switch> show version | include image`
		`System image file is "bootflash:cat4500e-entservicesk9-mz.122-54.XO.bin"`
		
		Note the image version for comparison in a following step.

IF THE SWITCH1A (4948E-F) IOS DOES NOT DISPLAY THE CORRECT VERSION IN THE ABOVE STEP, THEN STOP AND EXECUTE THE FOLLOWING STEPS:

1) Appendix D-3 Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)

2) Return to this Procedure and continue with the following Step. **Beginning with Step 43.**

NOTE: *For each switch, compare the IOS version from previous steps with the IOS version specified in the Firmware Upgrade Pack Release Notes [4] for the switch model being used.*

If the version from previous steps is equal or greater than the version from the release notes and has "k9" in the name, denoting support for crypto, then continue with the next step, there is no upgrade necessary for this switch.

Procedure 18. Configure Cisco 4948E-F Aggregation Switches (All SDS NOAM Sites)

Step	Procedure	Result
24. ☐	**Switch1A:** Execute "**show bootflash**" to verify that only the correct bootflash is present.	Switch> **show bootflash** -#- --length-- -----date/time------ path 1 25771102 Nov 29 2011 08:53:46 cat4500e-entservicesk9-mz.122-54.XO.bin 95072256 bytes available (33210368 bytes used) Note the image version for comparison in a following step
25. ☐	**Switch1A:** Reset switch back to factory defaults by deleting the VLANs.	Switch>**en** Password: Switch#**write erase** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] **<ENTER>** [OK] Erase of nvram: complete Switch# *Jan 26 12:53:06.547: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram **<ENTER>** Switch#**config t** Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no vlan 2-1024** %Default VLAN 1002 may not be deleted. %Default VLAN 1003 may not be deleted. %Default VLAN 1004 may not be deleted. %Default VLAN 1005 may not be deleted. Switch(config)#**config-register 0x2101** Switch(config)#**end** Switch#
26. ☐	**Switch1A:** Reload the switch.	Switch#**reload** System configuration has been modified. Save? [yes/no]: **no** Proceed with reload? [confirm] **<ENTER>**

Step	Procedure	Result
27. ☐	**Switch1A:** Monitor the switch reboot until it returns to a login prompt.	cisco WS-C4948E-F (MPC8548) processor (revision 5) with 1048576K bytes of memory. Processor board ID CAT1529S91B MPC8548 CPU at 1GHz, Cisco Catalyst 4948E-F Last reset from Reload 1 Virtual Ethernet interface 48 Gigabit Ethernet interfaces 4 Ten Gigabit Ethernet interfaces 511K bytes of non-volatile configuration memory. Press RETURN to get started! **<ENTER>** Switch>
28. ☐	**Switch1A:** Enter "enable" mode.	Switch#**enable** Switch#
29. ☐	**Switch1A:** Verify that you see the correct IOS version listed in the bootflash.	Switch#**dir bootflash:** Directory of bootflash:/ 7 -rw- 25771102 Jan 31 2012 07:45:56 +00:00 cat4500e-entservicesk9-mz.122-54.XO.bin 128282624 bytes total (72122368 bytes free) Switch#
30. ☐	**Switch1A:** Close connection to switch.	Switch#**quit** Switch con0 is now available Press RETURN to get started.
31. ☐	**switch1A:** Note the image version for comparison in a following step.	Exit from console by typing **CTRL+E+c+.** (combination control character and 'e' character, followed by sequence 'c' character, then 'period' character) and you will be returned to the server prompt.
32. ☐	**SERVER A:** Log in to switch1B	***Example:*** **console -M <SERVER A_mgmtVLAN_ip_address> -l platcfg switch1B_console** $ **/usr/bin/console -M 169.254.1.11 -l platcfg switch1B_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** [Enter `^Ec?' for help] Press <Enter>

Step	Procedure	Result
33. ☐	**Switch1B:** Note the image version for comparison in a following step.	Switch> **show version | include image** System image file is "bootflash:cat4500e-entservicesk9-mz.122-54.XO.bin" Note the image version for comparison in a following step.

IF THE SWITCH1B IOS DOES NOT DISPLAY THE CORRECT VERSION IN THE ABOVE STEP, THEN STOP AND EXECUTE THE FOLLOWING STEPS:

1) **Appendix D-3** Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites); **Beginning with Step 26.**

2) Return to this Procedure and continue with the following Step.

NOTE: *For each switch, compare the IOS version from previous steps with the IOS version specified in the Firmware Upgrade Pack Release Notes [4] for the switch model being used.*

If the version from previous steps is equal or greater than the version from the release notes and has "k9" in the name, denoting support for crypto, then continue with the next step, there is no upgrade necessary for this switch.

Step	Procedure	Result
34. ☐	**Switch1B:** Execute "**show bootflash**" to verify that only the correct bootflash is present.	Switch> **show bootflash** -#- --length-- -----date/time------ path 1 25771102 Nov 29 2011 09:04:04 cat4500e-entservicesk9-mz.122-54.XO.bin 95072256 bytes available (33210368 bytes used) Note the image version for comparison in a following step
35. ☐	**Switch1B:** Reset switch back to factory defaults by deleting the VLANs.	Switch>**en** Password: Switch#**write erase** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] **<ENTER>** [OK] Erase of nvram: complete Switch# *Jan 26 12:53:06.547: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram **<ENTER>** Switch#**config t** Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no vlan 2-1024** %Default VLAN 1002 may not be deleted. %Default VLAN 1003 may not be deleted. %Default VLAN 1004 may not be deleted. %Default VLAN 1005 may not be deleted. Switch(config)#**config-register 0x2101** Switch(config)#**end** Switch#

Step	Procedure	Result
36. ☐	**Switch1B:** Reload the switch.	Switch#**reload** System configuration has been modified. Save? [yes/no]: **no** Proceed with reload? [confirm] **<ENTER>**
37. ☐	**Switch1B:** Monitor the switch reboot until it returns to a login prompt.	cisco WS-C4948E-F (MPC8548) processor (revision 5) with 1048576K bytes of memory. Processor board ID CAT1529S91B MPC8548 CPU at 1GHz, Cisco Catalyst 4948E-F Last reset from Reload 1 Virtual Ethernet interface 48 Gigabit Ethernet interfaces 4 Ten Gigabit Ethernet interfaces 511K bytes of non-volatile configuration memory. Press RETURN to get started! **<ENTER>** Switch>
38. ☐	**Switch1B:** Enter “enable” mode.	Switch#**enable** Switch#
39. ☐	**Switch1B:** Verify that you see the correct IOS version listed in the bootflash.	Switch#**dir bootflash:** Directory of bootflash:/ 7 -rw- 25771102 Jan 31 2012 07:45:56 +00:00 cat4500e-entservicesk9-mz.122-54.XO.bin 128282624 bytes total (72122368 bytes free) Switch#
40. ☐	**Switch1B:** Close connection to switch.	Switch#**quit** Switch con0 is now available Press RETURN to get started.
41. ☐	**Switch1B:** Note the image version for comparison in a following step.	Exit from console by typing **CTRL+E+c+.** (combination control character and ‘e’ character, followed by sequence ‘c’ character, then ‘period’ character) and you will be returned to the server prompt.

Step	Procedure	Result

42.		**Open firewall with command:**
		
		sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s 169.254.1.0/24 -p udp --dport 69 -j ACCEPT" --location=1
		
		Turn on tftp:
		
		`$ tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`
		
		`$`

43. ☐	**SERVER A:**
	
	Initialize switch 1A
		`$ sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E_E-F_init.xml`
		
		`Processing file: /usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E-F_init.xml`
		
		`$`
		
		Note: This step takes about 2-3 minutes to complete
		
		Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
		
		A successful completion of netConfig will return the user to the prompt.

44. ☐	**SERVER A:**
	
	Initialize switch 1B
		`$ sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/switch1B_SDS_4948E_E-F_init.xml`
		
		`Processing file: /usr/TKLC/plat/etc/switch/xml/switch1B_SDS_4948E-F_init.xml`
		
		`$`
		
		Note: This step takes about 2-3 minutes to complete
		
		Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
		
		A successful completion of netConfig will return the user to the prompt.

Step	Procedure	Result

45. ☐	**SERVER A:**
	
	Ping switch 1A's SVI (router interface) addresses to verify switch initialization.
	
	Note: VIP addresses are not yet available.
		`$ ping -c 15 169.254.1.1`
		
		`PING 169.254.1.1 (169.254.1.1) 56(84) bytes of data.`
		
		`64 bytes from 169.254.1.1: icmp_seq=1 ttl=255 time=3.09 ms`
		`64 bytes from 169.254.1.1: icmp_seq=2 ttl=255 time=0.409 ms`
		`64 bytes from 169.254.1.1: icmp_seq=3 ttl=255 time=0.417 ms`
		`64 bytes from 169.254.1.1: icmp_seq=4 ttl=255 time=0.418 ms`
		`64 bytes from 169.254.1.1: icmp_seq=5 ttl=255 time=0.419 ms`
		`64 bytes from 169.254.1.1: icmp_seq=6 ttl=255 time=0.419 ms`
		`64 bytes from 169.254.1.1: icmp_seq=7 ttl=255 time=0.429 ms`
		`64 bytes from 169.254.1.1: icmp_seq=8 ttl=255 time=0.423 ms`
		`64 bytes from 169.254.1.1: icmp_seq=9 ttl=255 time=0.381 ms`
		`64 bytes from 169.254.1.1: icmp_seq=10 ttl=255 time=0.416 ms`
		`64 bytes from 169.254.1.1: icmp_seq=11 ttl=255 time=0.381 ms`
		`64 bytes from 169.254.1.1: icmp_seq=12 ttl=255 time=0.426 ms`
		`64 bytes from 169.254.1.1: icmp_seq=13 ttl=255 time=0.420 ms`
		`64 bytes from 169.254.1.1: icmp_seq=14 ttl=255 time=0.415 ms`
		`64 bytes from 169.254.1.1: icmp_seq=15 ttl=255 time=0.419 ms`
		
		`--- 169.254.1.1 ping statistics ---`
		
		`15 packets transmitted, 15 received, 0% packet loss, time 14006ms`
		
		`rtt min/avg/max/mdev = 0.381/0.592/3.097/0.669 ms $`

46. ☐	**SERVER A:**
	
	Ping switch 1B's SVI (router interface) addresses to verify switch initialization.
	
	Note: VIP addresses are not yet available.
		`$ ping -c 15 169.254.1.2`
		
		`PING 169.254.1.2 (169.254.1.2) 56(84) bytes of data.`
		
		`64 bytes from 169.254.1.2: icmp_seq=9 ttl=255 time=2.76 ms`
		`64 bytes from 169.254.1.2: icmp_seq=10 ttl=255 time=0.397 ms`
		`64 bytes from 169.254.1.2: icmp_seq=11 ttl=255 time=0.448 ms`
		`64 bytes from 169.254.1.2: icmp_seq=12 ttl=255 time=0.382 ms`
		`64 bytes from 169.254.1.2: icmp_seq=13 ttl=255 time=0.426 ms`
		`64 bytes from 169.254.1.2: icmp_seq=14 ttl=255 time=0.378 ms`
		`64 bytes from 169.254.1.2: icmp_seq=15 ttl=255 time=0.431 ms`
		
		`--- 169.254.1.2 ping statistics ---`
		
		`15 packets transmitted, 7 received, +6 errors, 53% packet loss, time 14003ms`
		
		`rtt min/avg/max/mdev = 0.378/0.747/2.769/0.825 ms, pipe 3`
		
		! WARNING !: The user needs to verify that the above ping is successful before continuing on to the next step. If the ping continues to receive "Destination Host Unreachable", then stop this procedure and contact MOS My Oracle Support.

Step	Procedure	Result

47. ☐	**SERVER A:**
	Configure switch 1A
		`$ sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/Primary_switch1A_SDS_4948E_E-F_configure.xml`
		
		`Processing file: /usr/TKLC/plat/etc/switch/xml/Primary_switch1A_SDS_4948E-F_configure.xml`
		
		`$`
		
		Note: This step takes about 2-3 minutes to complete.
		
		• Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
		• A successful completion of netConfig will return the user to the prompt.

48.	**SERVER A:**
	Configure switch 1B
		`$ sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/Primary_switch1B_SDS_4948E_E-F_configure.xml`
		
		`Processing file: /usr/TKLC/plat/etc/switch/xml/Primary switch1B_SDS_4948E-F_configure.xml`
		
		`$`
		
		Note: This step takes about 2-3 minutes to complete.
		
		• Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
		• A successful completion of netConfig will return the user to the prompt.

49. ☐	**SERVER A:**
	Undo the temporary changes.
		`$ tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp`
		
		`Login on Remote: platcfg`
		
		`Password of platcfg: <platcfg_password>`
		
		`1`

50.	Close firewall.	Close firewall with command: sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s 169.254.1.0/24 -p udp --dport 69 -j ACCEPT" --location=1

Step	Procedure	Result

51. ☐	**SERVER A:**
	
	Verify the switch is using the correct IOS image per platform version.
		`$ sudo netConfig --device=switch1A listFirmware`
		
		`Image: cat4500e-entservicesk9-mz.122-54.XO.bin`
		
		`$ sudo netConfig --device=switch1B listFirmware`
		
		`Image: cat4500e-entservicesk9-mz.122-54.XO.bin`

52. ☐	**SERVER A:**
	
	Execute the "**service network restart**" to restore SERVER A networking to original state.
	
	Output similar to that shown on the right may be observed.
		`$ sudo service network restart`
		
		`[admusr@mrsvnc-sds-NO-a xml]$ sudo service network restart`
		
		`Shutting down interface bond0.2: [ OK ]`
		
		`Shutting down interface bond0.4: [ OK ]`
		
		`Shutting down interface bond0: [ OK ]`
		
		`Shutting down interface bond1: [ OK ]`
		
		`Shutting down loopback interface: [ OK ]`
		
		`Bringing up loopback interface: [ OK ]`
		
		`Bringing up interface bond0: [ OK ]`
		
		`Bringing up interface bond1: Determining if ip address 10.75.160.146 is already in use for device bond1...`
		
		`[ OK ]`
		
		`Bringing up interface bond0.2: Determining if ip address 169.254.1.11 is already in use for device bond0.2...`
		
		[OK]
		Bringing up interface bond0.4: Determining if ip address 169.254.100.11 is already in use for device bond0.4...
		[OK]
		
		`$`

Step	Procedure	Result

53. ☐	**SERVER A:**
	
	Ping switch 1A's SVI (router interface) addresses to verify switch configuration.
	
	Note: VIP addresses are not yet available.
		`$ ping -c 5 169.254.1.1`
		
		`PING 169.254.1.1 (169.254.1.1) 56(84) bytes of data.`
		
		`64 bytes from 169.254.1.1: icmp_seq=1 ttl=255 time=0.430 ms`
		`64 bytes from 169.254.1.1: icmp_seq=2 ttl=255 time=0.426 ms`
		`64 bytes from 169.254.1.1: icmp_seq=3 ttl=255 time=0.427 ms`
		`64 bytes from 169.254.1.1: icmp_seq=4 ttl=255 time=0.426 ms`
		
		`64 bytes from 169.254.1.1: icmp_seq=5 ttl=255 time=0.431 ms`
		
		`--- 169.254.1.1 ping statistics ---`
		
		`5 packets transmitted, 5 received, 0% packet loss, time 4003ms`
		
		`rtt min/avg/max/mdev = 0.426/0.428/0.431/0.002 ms`
		
		`$`

54. ☐	**SERVER A:**
	
	Ping switch 1B's SVI (router interface) addresses to verify switch configuration.
	
	Note: VIP addresses are not yet available
		`$ ping -c 5 169.254.1.2`
		
		`PING 169.254.1.2 (169.254.1.2) 56(84) bytes of data.`
		`64 bytes from 169.254.1.2: icmp_seq=1 ttl=255 time=0.401 ms`
		`64 bytes from 169.254.1.2: icmp_seq=2 ttl=255 time=0.394 ms`
		`64 bytes from 169.254.1.2: icmp_seq=3 ttl=255 time=0.407 ms`
		`64 bytes from 169.254.1.2: icmp_seq=4 ttl=255 time=0.393 ms`
		`64 bytes from 169.254.1.2: icmp_seq=5 ttl=255 time=0.401 ms`
		
		`--- 169.254.1.2 ping statistics ---`
		
		`5 packets transmitted, 5 received, 0% packet loss, time 3999ms`
		
		`rtt min/avg/max/mdev = 0.393/0.399/0.407/0.013 ms`
		
		`$`

55. ☐	**SERVER A:**
	
	Verify SSH capability from server A to switch 1A.
		`$ ssh platcfg@169.254.1.1`
		
		`The authenticity of host '169.254.1.1 (169.254.1.1)' can't be established.`
		
		`RSA key fingerprint is fd:83:32:34:3f:06:2f:12:e0:ea:e2:73:e2:c1:1e:6e.`
		
		`Are you sure you want to continue connecting (yes/no)? yes`
		
		`Warning: Permanently added '169.254.1.1' (RSA) to the list of known hosts.`
		
		`Password: <switch_platform_password>`

56. ☐	**SERVER A:**
	
	Close SSH connection to switch 1A.
		`$ quit`
		
		`Connection to 169.254.1.1 closed.`

Step	Procedure	Result

57. ☐	**SERVER A:**
	Verify SSH capability from server A to switch 1B
		`$ ssh platcfg@169.254.1.2`
		
		`The authenticity of host '169.254.1.2 (169.254.1.2)' can't be established.`
		
		`RSA key fingerprint is 3a:1b:e0:92:99:73:9d:04:92:3f:72:37:c0:1c:a6:95.`
		
		`Are you sure you want to continue connecting (yes/no)? yes`
		
		`Warning: Permanently added '169.254.1.2' (RSA) to the list of known hosts.`
		
		`Password: <switch_platform_password>`

58. ☐	**SERVER A:**
	Close SSH connection to switch 1A.
		`$ quit`
		
		`Connection to 169.254.1.2 closed.`

59. ☐	**SERVER B:**
	Ping switch 1A's SVI (router interface) addresses to verify switch configuration.
	
	Note: VIP addresses are not yet available.
		`$ ping -c 5 169.254.1.1`
		
		`PING 169.254.1.1 (169.254.1.1) 56(84) bytes of data.`
		`64 bytes from 169.254.1.1: icmp_seq=1 ttl=255 time=0.430 ms`
		`64 bytes from 169.254.1.1: icmp_seq=2 ttl=255 time=0.426 ms`
		`64 bytes from 169.254.1.1: icmp_seq=3 ttl=255 time=0.427 ms`
		`64 bytes from 169.254.1.1: icmp_seq=4 ttl=255 time=0.426 ms`
		`64 bytes from 169.254.1.1: icmp_seq=5 ttl=255 time=0.431 ms`
		`--- 169.254.1.1 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 4003ms`
		`rtt min/avg/max/mdev = 0.426/0.428/0.431/0.002 ms`

60. ☐	**SERVER B:**
	Ping switch 1B's SVI (router interface) addresses to verify switch configuration.
	
	Note: VIP addresses are not yet available
		`$ ping -c 5 169.254.1.2`
		
		`PING 169.254.1.2 (169.254.1.2) 56(84) bytes of data.`
		`64 bytes from 169.254.1.2: icmp_seq=1 ttl=255 time=0.401 ms`
		`64 bytes from 169.254.1.2: icmp_seq=2 ttl=255 time=0.394 ms`
		`64 bytes from 169.254.1.2: icmp_seq=3 ttl=255 time=0.407 ms`
		`64 bytes from 169.254.1.2: icmp_seq=4 ttl=255 time=0.393 ms`
		`64 bytes from 169.254.1.2: icmp_seq=5 ttl=255 time=0.401 ms`
		`--- 169.254.1.2 ping statistics ---`
		`5 packets transmitted, 5 received, 0% packet loss, time 3999ms`
		`rtt min/avg/max/mdev = 0.393/0.399/0.407/0.013 ms`

Step	Procedure	Result

61. ☐	**SERVER B:**
	Verify SSH capability from server B to switch 1A.
		`$ ssh platcfg@169.254.1.1`
		`The authenticity of host '169.254.1.1 (169.254.1.1)' can't be established.`
		`RSA key fingerprint is fd:83:32:34:3f:06:2f:12:e0:ea:e2:73:e2:c1:1e:6e.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added '169.254.1.1' (RSA) to the list of known hosts.`
		`Password: <switch_platform_password>`

62. ☐	**SERVER B:** Close SSH connection to switch 1A.	`switch1A> quit` `Connection to 169.254.1.1 closed.`

63. ☐	**SERVER B:**
	Verify SSH capability from server B to switch 1B
		`$ ssh platcfg@169.254.1.2`
		`The authenticity of host '169.254.1.2 (169.254.1.2)' can't be established.`
		`RSA key fingerprint is 3a:1b:e0:92:99:73:9d:04:92:3f:72:37:c0:1c:a6:95.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added '169.254.1.2' (RSA) to the list of known hosts.`
		`Password: <switch_platform_password>`

64. ☐	**SERVER B:** Close SSH connection to switch 1B.	`switch1B> quit` `Connection to 169.254.1.2 closed.`
65. ☐	**SERVER A:** **Run Appendix D-4 to backup switch configuration.**	

66. ☐	**SERVER A:**
	Exit from the command line to return the server console to the login prompt.
		`$ exit`
		`logout`
		`CentOS release 5.6 (Final)`
		`Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.22.0 on an x86_64`

THIS PROCEDURE HAS BEEN COMPLETED		

D-3. Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
1. ☐	**SERVER A:** Access the **SERVER A** console.	Connect to the **SERVER A** console using one of the access methods described in **Section 2.3.**
2. ☐	**SERVER A:** **1)** Access the command prompt. **2)** Log into the HP DL380 server as the "**admusr**" user.	CentOS release 5.6 (Final) Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.20.0 on an x86_64 hostname1260476221 login: **admusr** Password: ***<admusr_password>***
3. ☐	**SERVER A:** Output similar to that shown on the right will appear as the server access the command prompt.	***** TRUNCATED OUTPUT ***** VPATH=/opt/TKLCcomcol/runcm5.16:/opt/TKLCcomcol/cm5.16 PRODPATH= RELEASE=5.16 RUNID=00 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds PRODPATH=/opt/comcol/prod RUNID=00 [admusr@hostname1260476221 ~]$
4. ☐	**SERVER A:** Verify IOS images on the system	$ **ls /var/lib/tftpboot/** **<IOS_image_file>** If the correct IOS version is displayed, skip forward to **Step 8**.

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
5. ☐	**SERVER A:** Place **USB drive** containing the the **HP Misc Firmware** image with the correct 4948E-F IOS version into the **SERVER A** front panel USB port.	 **Figure 25 – HP DL380 Gen8: Front Panel (USB Port)**  **Figure 26 – HP DL380 Gen9: Front Panel (USB Port)**

6. ☐	**SERVER A:**
	
	Copy IOS image onto the system
		`$ mount /dev/scd0 /media/cdrom`
		`$ cp /media/cdrom/files/<New_IOS_image_file> /var/lib/tftpboot/`
		`$ chmod 644 /var/lib/tftpboot/<New_IOS_image_file>`
		`$ umount /media/cdrom`

7.	Open firewall	Open firewall with command: `sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s 169.254.1.0/24 -p udp --dport 69 -j ACCEPT" --location=1`

8. ☐	**SERVER A:**
	
	Prepare the system for IOS transfer.
		`$ tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`
		`$`

9. ☐	**SERVER A:**
	
	Verify the current bonded interface configuration.
		`$ ifconfig |grep bond`
		`bond0 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6C`
		`bond0.2 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6C`
		`bond0.4 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6C`
		`bond1 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6E`
		`$`
		
		Execute one of the following options:
		
		• *If **bond0** & **bond0.2** are both present, skip to **Step 11**.*
		
		• *If only **bond0** is present, continue with the following step.*

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
10. ☐	**SERVER A:** **For Gen8:** Create the bond0.2 and add interfaces eth01 & eth11 to it. **For Gen9:** Create the bond0.2 and add interfaces eth01 & eth02 to it.	**For Gen8:** **$ sudo netAdm delete --device=bond0** **$ sudo netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --bootproto=none** **$ sudo netAdm set --device=eth01 --bootproto=none --type=Ethernet --master=bond0 --slave=yes --onboot=yes** **$ sudo netAdm set --device=eth11 --bootproto=none --type=Ethernet --master=bond0 --slave=yes --onboot=yes** Add the <SERVER A_mgmtVLAN_IP_address> to bond0.2 **$ sudo netAdm add --device=bond0.2 --address=169.254.1.11 --netmask=255.255.255.0 --onboot=yes** **For Gen9:** **$ sudo netAdm delete --device=bond0** **$ sudo netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --bootproto=none** **$ sudo netAdm set --device=eth01 --bootproto=none --type=Ethernet --master=bond0 --slave=yes --onboot=yes** **$ sudo netAdm set --device=eth02 --bootproto=none --type=Ethernet --master=bond0 --slave=yes --onboot=yes** Add the <SERVER A_mgmtVLAN_IP_address> to bond0.2 **$ sudo netAdm add --device=bond0.2 --address=169.254.1.11 --netmask=255.255.255.0 --onboot=yes**

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>11.
☐</td><td>SERVER A:

Disable the bond0.2 interface to switch1B and verify the bond0.2 IP address.</td><td>On SERVER A ensure that the interface connected to switch1A is the only interface available and obtain the IP address of <SERVER A_mgmtVLAN_Interface> by performing the following commands:

For Gen8:

<pre>$ sudo ifdown eth11
$ sudo ifup eth01
$ sudo ifconfig bond0.2
bond0.2 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6C
    inet addr:169.254.1.11
Bcast:169.254.1.255Mask:255.255.255.0
    inet6 addr: fe80::9a4b:e1ff:fe6e:876c/64 Scope:Link
    UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
    RX packets:99384 errors:0 dropped:0 overruns:0 frame:0
    TX packets:105440 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:4603240 (4.3 MiB) TX bytes:55536818 (52.9 MiB)</pre>

The command output should contain the IP address of the <SERVER A_mgmtVLAN_ip_address>.

For Gen9:

<pre>$ sudo ifdown eth02
$ sudo ifup eth01
$ sudo ifconfig bond0.2
bond0.2 Link encap:Ethernet HWaddr 98:4B:E1:6E:87:6C
    inet addr:169.254.1.11
Bcast:169.254.1.255Mask:255.255.255.0
    inet6 addr: fe80::9a4b:e1ff:fe6e:876c/64 Scope:Link
    UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
    RX packets:99384 errors:0 dropped:0 overruns:0 frame:0
    TX packets:105440 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:4603240 (4.3 MiB) TX bytes:55536818 (52.9 MiB)</pre>

The command output should contain the IP address of the <SERVER A_mgmtVLAN_ip_address>.</td></tr>
<tr><td>12.
☐</td><td>SERVER A:

Connect to switch1A console</td><td>
<pre>console -M <SERVER A_mgmtVLAN_ip_address> -l platcfg switch1A_console

$ /usr/bin/console -M 169.254.1.11 -l platcfg switch1A_console

Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]</pre>
Press <Enter></td></tr>
</table>

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
13. ☐	**switch1A:** Enter enable mode	Switch> **enable** Switch#
14. ☐	**switch1A:** Configure switch port with this sequence of commands	Switch# **conf t** Switch(config)# **vlan 2** Switch(config)# **int vlan 2** Switch(config-if)# **ip address 169.254.1.1 255.255.255.0** Switch(config-if)# **no shut** Switch(config-if)# **int gi1/5** Switch(config-if)# **switchport mode trunk** Switch(config-if)# **spanning-tree portfast trunk** Switch(config-if)# **end**
15. ☐	**switch1A:** Test connectivity	**ping <SERVER A_mgmtVLAN_ip_address>** Switch# **ping 169.254.1.11** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to <SERVER A_mgmtVLAN_ip_address>, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms *If ping is not 100% successful the first time, repeat the ping. If unsuccessful again, double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Customer Care Center.*
16. ☐	**switch1A:** Upload IOS image to switch	Switch# **copy tftp: bootflash:** Address or name of remote host []? **<SERVER A_mgmtVLAN_ip_address>** Source filename []? **<New_IOS_image_file>** Destination filename [<New_IOS_image_file>]? **<ENTER>** Press <Enter> here, you do NOT want to change the filename Accessing tftp://<SERVER A_mgmtVLAN_ip address>/<IOS_image_file>... Loading <IOS_image_file> from <SERVER A_mgmtVLAN_ip_address> (via Vlan2): !! [OK - 45606 bytes] 45606 bytes copied in 3.240 secs (140759 bytes/sec)
17. ☐	**switch1A:** Locate old IOS image to be removed	Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin 2 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-ipbasek9-mz.122-54.WO.bin 60817408 bytes total (43037392 bytes free) ***NOTE**: Here, you should note which IOS you uploaded, and the one which was already on the switch. Note the one that was already on the switch, this will be the one to delete, as notated by the variable <OLD_IOS_image>*

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
18. ☐	**switch1A:** Remove old IOS image	Switch# **delete /force /recursive bootflash:<OLD_IOS_image>** Switch#
19. ☐	**switch1A:** Locate old IOS image to be removed	Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin 60817408 bytes total (43037392 bytes free) ***NOTE**: Here, you should see only the IOS version you uploaded.*
20. ☐	**Switch1A:** Reset switch back to factory defaults by deleting the VLANs.	Switch#**write erase** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] **<ENTER>** [OK] Erase of nvram: complete Switch# *Jan 26 12:53:06.547: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#**config t** Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no vlan 2-1024** %Default VLAN 1002 may not be deleted. %Default VLAN 1003 may not be deleted. %Default VLAN 1004 may not be deleted. %Default VLAN 1005 may not be deleted. Switch(config)#**config-register 0x2101** Switch(config)#**end** Switch#
21. ☐	**switch1A:** Reload the switch	Switch#**reload** System configuration has been modified. Save? [yes/no]: **no** Proceed with reload? [confirm] **<ENTER>** **! WARNING!:** *It is extremely important to answer **"no"** to the above "Save?" option.*
22. ☐	**switch1A:** After the reload, enter *enable* mode.	Switch> **enable** Switch#
23. ☐	**switch1A:** Wait until the switch is reloaded, then confirm the correct IOS image.	Switch> **show version | include image** System image file is "bootflash:cat4500-entservicesk9-mz.122-54.WO.bin" Switch> ***NOTE**: Here, you should see only the IOS version you uploaded. If the IOS version is not at the correct version, stop here and contact Customer Care Center.*

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result

24. ☐	**switch1A:**
	
	Locate old IOS image to be removed.
		`Switch# dir bootflash:`
		`Directory of bootflash:/`
		`1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin`
		`60817408 bytes total (43037392 bytes free)`
		
		***NOTE**: Here, you should see only the IOS version you uploaded.*

25. ☐	**switch1A:** Exit the switch1A console session.	`Switch#` <CTRL-e><c><.> **Hot Key sequence:** Ctrl-E, C, period

26. ☐	**SERVER A:**
	
	Disable the bond0.2 interface to switch1A.
		On SERVER A ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of <*SERVER A_mgmtInterface*> by performing the following commands:
		
		`For Gen8:`
		`$ sudo ifup eth11`
		`$ sudo ifdown eth01`
		
		For Gen9:
		`$ ifup eth02`
		`$ ifdown eth01`
		
		***NOTE**: The command output should contain the IP address of the variable **<SERVER A_mgmtVLAN_ip_address>**.*

27. ☐	**SERVER A:**
	
	Connect to switch1B console
		`console -M <SERVER A_mgmtVLAN_ip_address> -l platcfg switch1B_console`
		
		`$ /usr/bin/console -M 169.254.1.11 -l platcfg switch1B_console`
		
		`Enter platcfg@pmac5000101's password: <platcfg_password>`
		`[Enter `^Ec?' for help]`
		Press <Enter>

28. ☐	**switch1B:** Enter enable mode	`Switch> enable` `Switch#`

29. ☐	**switch1B:**
	
	Configure switch port with this sequence of commands
		`Switch# conf t`
		`Switch(config)# vlan 2`
		`Switch(config)# int vlan 2`
		`Switch(config-if)# ip address 169.254.1.2 255.255.255.0`
		`Switch(config-if)# no shut`
		`Switch(config-if)# int gi1/5`
		`Switch(config-if)# switchport mode trunk`
		`Switch(config-if)# spanning-tree portfast trunk`
		`Switch(config-if)# end`

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
30. ☐	**switch1B:** Test connectivity	**ping <management_SERVER A_mgmtVLAN_ip_address>** Switch# **ping 169.254.1.11** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to <SERVER A_mgmtVLAN_ip_address>, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms ***NOTE**: If ping is not 100% successful the first time, repeat the ping. If unsuccessful again, double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Customer Care Center*.
31. ☐	**switch1B:** Upload IOS image to switch	Switch# **copy tftp: bootflash:** Address or name of remote host []? **<management_SERVER A_mgmtVLAN_ip_address>** Source filename []? **<New_IOS_image_file>** Destination filename [<New_IOS_image_file>]? **<ENTER>** Press <Enter> here, you do NOT want to change the filename Accessing tftp://<management_SERVER B_mgmtVLAN_ip address>/<IOS_image_file>... Loading <IOS_image_file> from <SERVER A_mgmtVLAN_ip_address> (via Vlan2): !! [OK - 45606 bytes] 45606 bytes copied in 3.240 secs (140759 bytes/sec)
32. ☐	**switch1B:** Locate old IOS image to be removed	Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin 2 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-ipbasek9-mz.122-54.WO.bin 60817408 bytes total (43037392 bytes free) ***NOTE**: Here, you should note which IOS you uploaded, and the one which was already on the switch. Note the one that was already on the switch, this will be the one to delete, as notated by the variable <OLD_IOS_image>*
33. ☐	**switch1B:** Remove old IOS image	Switch# **delete /force /recursive bootflash:<OLD_IOS_image>** Switch#
34. ☐	**switch1B:** Locate old IOS image to be removed	Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin 60817408 bytes total (43037392 bytes free) Here, you should see only the IOS version you uploaded.

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result
35. ☐	**Switch1B:** Reset switch back to factory defaults by deleting the VLANs.	Switch#**write erase** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] **<ENTER>** [OK] Erase of nvram: complete Switch# *Jan 26 12:53:06.547: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#**config t** Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no vlan 2-1024** %Default VLAN 1002 may not be deleted. %Default VLAN 1003 may not be deleted. %Default VLAN 1004 may not be deleted. %Default VLAN 1005 may not be deleted. Switch(config)#**config-register 0x2101** Switch(config)#**end** Switch#
36. ☐	**switch1B:** Reload the switch	Switch# **reload** Proceed with reload? [confirm] **<ENTER>** System config modified. save? [**yes/no]:no** ! WARNING !: It is extremely important to answer "no" to the above "Save?" option. Proceed with reload? [confirm] <ENTER>
37. ☐	**switch1B:** Wait until the switch is reloaded, then confirm the correct IOS image	Switch> **show version | include image** System image file is "bootflash:cat4500-entservicesk9-mz.122-54.WO.bin" Switch>
38. ☐	**switch1B:** Enter enable mode	Switch> **enable** Switch#
39. ☐	**switch1B:** Locate old IOS image to be removed	Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-54.WO.bin 60817408 bytes total (43037392 bytes free) Here, you should see only the IOS version you uploaded.
40. ☐	**switch1A:** Exit the switch1A console session.	Switch# <CTRL-e><**c**><.> **Hot Key sequence:** Ctrl-E, C, period

Procedure 19. Cisco 4948E-F IOS Upgrade (SDS Sites)

Step	Procedure	Result

41. ☐	**SERVER A:**
	
	Re-enable the bond0.2 interface to switch1A.
		On SERVER A ensure that the both bond0.2 interfaces are up:
		
		For Gen8:
		
		`$ sudo ifup eth11`
		`$ sudo ifup eth01`
		
		For Gen9:
		
		`$ sudo ifup eth02`
		`$ sudo ifup eth01`

42.	Close firewall	`$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s 169.254.1.0/24 -p udp --dport 69 -j ACCEPT" --location=1`

43. ☐	**SERVER A:**
	
	Stop the "tftp" service.
		`$ tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp`
		
		`Login on Remote: platcfg`
		
		`Password of platcfg: <platcfg_password>`
		
		`1`

44.	Return to Appendix D-2	
THIS PROCEDURE HAS BEEN COMPLETED		

D-4. Cisco 4948E-F Configuration Backup (All SDS NOAM sites)

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	
<switch_backup_user_password> (also needed in switch configuration procedure)	
<switch_name>	hostname of the switch
<switch_backup_directory>	/usr/TKLC/plat/etc/switch/backup

Procedure 20. Cisco 4948E-F Backup (SDS Sites)

Step	Procedure	Result
1. ☐	**SERVER A:** Access the **SERVER A** console.	Connect to the **SERVER A** console using one of the access methods described in **Section 2.3.**
2. ☐	**SERVER A:** Log into server as the "**admusr**" user.	login: **admusr** Using keyboard-interactive authentication. Password: ***<admusr_password>***
3. ☐	**SERVER A:** Verify hostname of the switch1A	$ **sudo netConfig --device=<switch_name> getHostname** Hostname: switch1A **Note:** The value beside "Hostname:" should be the same as the <switch_name> variable
4. ☐	**SERVER A:** Verify SSH service	$ **sudo netConfig --repo showService name=ssh_service** Service Name: ssh_service Type: ssh Host: 169.254.1.11 Options: password: 615EBD88232A2EFD0080AC990393083D user: admusr
5. ☐	**SERVER A:** Run backup command	$ **sudo netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup**
6. ☐	**SERVER A:** Verify backup and inspect its contents to ensure they reflect the configured values	$ **ls /home/admusr/<switch_name>-backup*** Example Output: /home/admusr/switch1A-backup /home/admusr/switch1A-backup.info $ $ **cat /home/admusr/<switch_name>-backup** Verify that the backup information looks correct.
7. ☐	**Repeat steps 3-6 for switch1B.**	
8. ☐	**SERVER A:** Copy the switch1A and switch1B backup files to the permanent backup storage directory	**$ sudo cp -p /home/admusr/switch*-backup* /usr/TKLC/plat/etc/switch/backup/** **ls -al /usr/TKLC/plat/etc/switch/backup/** **[admusr@hostnamecf48ffa1d812 xml]$ ls -al** **-rw------- 1 admusr admgrp 7368 Mar 1 10:37 switch1A-backup** **-rw------- 1 admusr admgrp 88 Mar 1 10:37 switch1A-backup.info** **-rw------- 1 admusr admgrp 7368 Mar 1 10:37 switch1B-backup** **-rw------- 1 admusr admgrp 88 Mar 1 10:37 switch1B-backup.info**

Procedure 20. Cisco 4948E-F Backup (SDS Sites)

Step	Procedure	Result
9. ☐	**SERVER A:** Delete switch1A and switch1B backup files from the admusr directory	`$ sudo rm /home/admusr/*backup*`
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix E. Creating an XML File for Installing 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 (NOAM & SOAM). The format for each of these XML files is identical. Below is an example of the **SDS_NO_NE.xml** file.

- **THE HIGHLIGHTED VALUES IN EACH TABLE MUST BE UPDATED BY THE USER FOR EACH NETWORK ELEMENT *(SITE)*.**

NOTE_1: *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.*

NOTE_2: *The **MGMT_VLAN** network should only be implemented when (2) dedicated **Aggregation Switches** (typically Cisco 4948E-F) are used exclusively for the **SDS NOAM** and **Query Server** (RMS) **IMI network.** The **MGMT_VLAN** network should be **removed** from the Network Element XML file when SDS Aggregation Switches are not part of the implemention.*

NOTE_3: *When installing **IPv6** for the **XMI** or **IMI** networks, please note that the **MGMT_VLAN** (if implemented) should remain in the **IPv4** format only.*

NOTE_4: *When creating the SDS **SOAM NE XML** file, the user should be aware that the **XMI** and **IMI** networks subnets chosen **MUST EXACTLY MATCH** those used by the associated **DSR NE** within the same SOAM enclosure.*

Table 4 – SDS Network Element Configuration File (IPv4)

XML File Text	Description
<?xml version="1.0"?>	
<networkelement>	
<name>**NO_RLGHNC**</name>	[Range = 1-32 character string] – Must be alphanumeric or underscore.
<networks>	
<network>	
<name>**MGMNT_VLAN**</name>	Name of customer management network. **Note**: Do NOT change this name.
<vlanId>**2**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**169.254.1.0**</ip>	[Range = A valid IP address] – The network address of this VLAN
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
</network>	
<network>	
<name>**XMI**</name>	Name of customer external network. **Note**: Do NOT change this name.
<vlanId>**3**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**10.250.55.0**</ip>	[Range = A valid IP address] – This network must be the same as the associated DSR NE XMI network subnet within the same SOAM enclosure.
<mask>**255.255.255.0**</mask>	Must be the same as the associated DSR NE XMI netmask within the same SOAM enclosure.
<gateway>**10.250.55.1**</gateway>	[Range = A valid IP address] – This gateway address must be the same as the associated DSR NE XMI network gateway within the same SOAM enclosure.
<isDefault>true</isDefault>	[Range = true/false] – true if this is the network with the default gateway.
</network>	
<network>	
<name>**IMI**</name>	Name of customer internal network. **Note**: Do NOT change this name.
<vlanId>**4**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**169.254.100.0**</ip>	[Range = A valid IP address] – This network must be the same as the DSR IMI network subnet within the SOAM enclosure.
<mask>**255.255.255.0**</mask>	Must be the same as the DSR IMI netmask within the SOAM enclosure.
<nonRoutable>**true**</nonRoutable>	[Range = true / false] – Determines whether or not the IMI network subnet is treated as a routable network.
</network>	
</networks>	
</networkelement>	

Table 5 – SDS Network Element Configuration File (IPv6)

XML File Text	Description
<?xml version="1.0"?>	
<networkelement>	
<name>**NO_RLGHNC**</name>	[Range = 1-32 character string] – Must be alphanumeric or underscore.
<networks>	
<network>	
<name>**MGMNT_VLAN**</name>	Name of customer management network. **Note**: Do NOT change this name.
<vlanId>**2**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**169.254.1.0**</ip>	[Range = A valid IP address] – The network address of this VLAN
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
</network>	
<network>	
<name>**XMI**</name>	Name of customer external network. **Note**: Do NOT change this name.
<vlanId>**3**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**2001:db8:0:241::0**</ip>	[Range = A valid IP address] – This network must be the same as the associated DSR NE XMI network subnet within the same SOAM enclosure.
<mask>**/64**</mask>	Must be the same as the associated DSR NE XMI netmask within the same SOAM enclosure.
<gateway>2001:db8:0:241::1</gateway>	[Range = A valid IP address] – This gateway address must be the same as the associated DSR NE XMI network gateway within the same SOAM enclosure.
<isDefault>true</isDefault>	[Range = true/false] – true if this is the network with the default gateway.
</network>	
<network>	
<name>**IMI**</name>	Name of customer internal network. **Note**: Do NOT change this name.
<vlanId>**4**</vlanId>	[Range = 2-4094.] – The VLAN ID to use for this VLAN.
<ip>**fd01::0**</ip>	[Range = A valid IP address] – This network must be the same as the associated DSR NE XMI network subnet within the same SOAM enclosure.
<mask>**/64**</mask>	Must be the same as the associated DSR NE XMI netmask within the same SOAM enclosure.
<nonRoutable>**true**</nonRoutable>	[Range = true / false] – Determines whether or not the IMI network subnet is treated as a routable network.
</network>	
</networks>	
</networkelement>	

Appendix F. NetBackup Client Installation

This section contains procedures for configuration of additional services to Appworks-based application servers.

Procedure 21. NetBackup Client Installation

Step	This procedure will download and install NetBackup Client software on the server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE'S ACCESSING MY ORACLE SUPPORT (MOS). AND ASK FOR ASSISTANCE.	

1. ☐	Install **Netbackup** Client Software	Execute Section *3.10.5 Application NetBackup Client Procedures* of reference [7] to complete this step.
		
		NOTE: If installing Netbackup client software, it must be installed and configured on all SDS servers (Primary SDS and DR SDS servers only).
		
		NOTE: Location of the bpstart_notify and bpend_notify scripts is required for the execution of this step. These scripts are located as follows:
		`/usr/TKLC/appworks/sbin/bpstart_notify`
		`/usr/TKLC/appworks/sbin/bpend_notify`

2. ☐	Link notify scripts to well-known path stated in the above step	Link the notify scripts to well-known path stated in the above step
		
		`ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify`
		
		`ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify`

3. ☐	Verify if the Netbackup port 1556 is opened for IPv4 protocol	Verify if the NetBackup port 1556 is opened on IPv4 protocol:
		`iptables -L 60sds-INPUT -n | grep 1556`
		
		If there is no output, then enable the port 1556 for NetBackup on IPv4:
		
		`iptablesAdm append --type=rule --protocol=ipv4 --domain=60sds --table=filter --chain=INPUT --match='-m state --state NEW -m tcp -p tcp --dport 1556 -j ACCEPT' --persist=yes`

4. ☐	Verify if the Netbackup port 1556 is opened for IPv6 protocol	Verify if the NetBackup port 1556 is opened on IPv6 protocol:
		`ip6tables -L 60sds-INPUT -n | grep 1556`
		
		If there is no output, then enable the port 1556 for NetBackup on IPv6 protocol:
		
		`iptablesAdm append --type=rule --protocol=ipv6 --domain=60sds --table=filter --chain=INPUT --match='-m state --state NEW -m tcp -p tcp --dport 1556 -j ACCEPT' --persist=yes`

Appendix G. 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 blade timezone. For an exhaustive list of **ALL** timezones, log onto the PMAC server console and view the text file: **`/usr/share/zoneinfo/zone.tab`**

Table 6 – List of Selected Time Zone Values

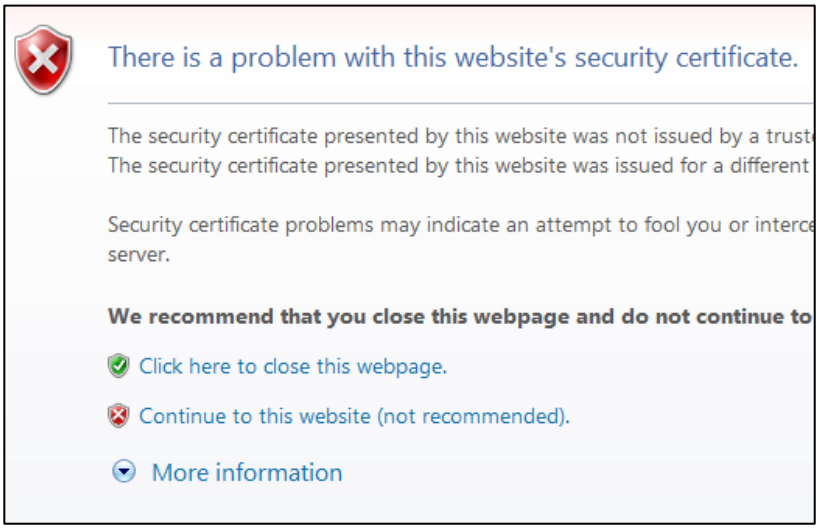
Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08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

Time Zone Value	Description	Universal Time Code (UTC) Offset
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

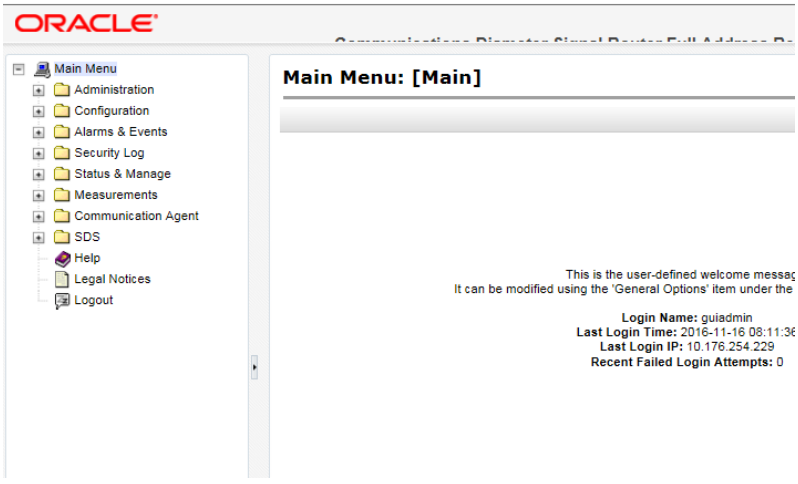
Appendix H. Accepting Installation Through SDS NOAM GUI

This section will accept an application installation through SDS NOAM GUI.

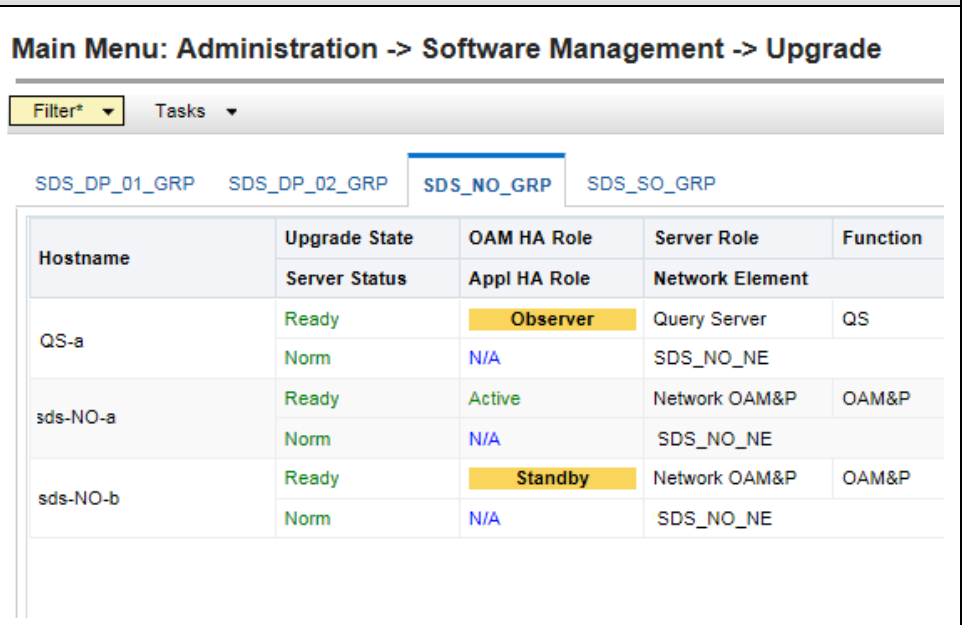
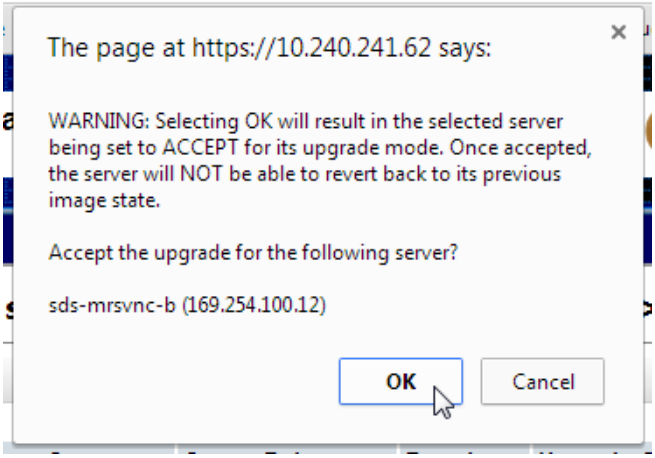
Procedure 22. Accepting Installation Through SDS NOAM GUI

Step	Procedure	Result
1. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active SDS site** **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	

Procedure 22. Accepting Installation Through SDS NOAM GUI

Step	Procedure	Result
2. ☐	**Primary 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. ☐	**Primary SDS VIP:** The user should be presented the SDS Main Menu as shown on the right.	

Procedure 22. Accepting Installation Through SDS NOAM GUI

Step	Procedure	Result
4. ☐	**Primary SDS VIP:** Using the cursor **left-click**, select the row containing the Server(s) for which you would like to **"Accept"** upgrade. **NOTE:** *Multi-select is available by holding down the **"CTRL"** key while using the cursor to **left-click** multiple rows.*	
5. ☐	**Primary SDS VIP:** Using the cursor **left-click**, select the **"Accept"** dialogue button.	
6. ☐	**Primary SDS VIP:** The user is presented with a dialogue box stating that the **"Accept Upgrade"** action is **irreversible** and locks the Server on the current software release *(i.e. Backout to the previous release is no longer allowed).* If the user wishes to continue, use the cursor **left-click** to select the **"OK"** dialogue button.	
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix I. Disable Hyperthreading for Gen8 and Gen9 (DP Only)

Procedure 23. Gen8: Disable Hyerthreading (DP Only)

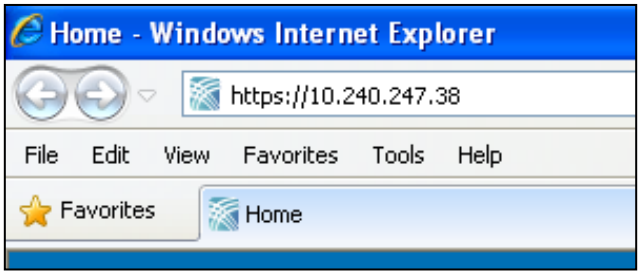
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1.
☐</td><td>DP Server XMI IP (SSH):

Access the command prompt via DP blade's XMI IP address and log into the server as the "admusr" user.</td><td>login: admusr
Password: <admusr_password></td></tr>
<tr><td>2.
☐</td><td>DP Server XMI IP (SSH):

Execute "hpasmcli" command to determine status of hyperthreading for the DP blade.</td><td>$ sudo hpasmcli -s "show ht"

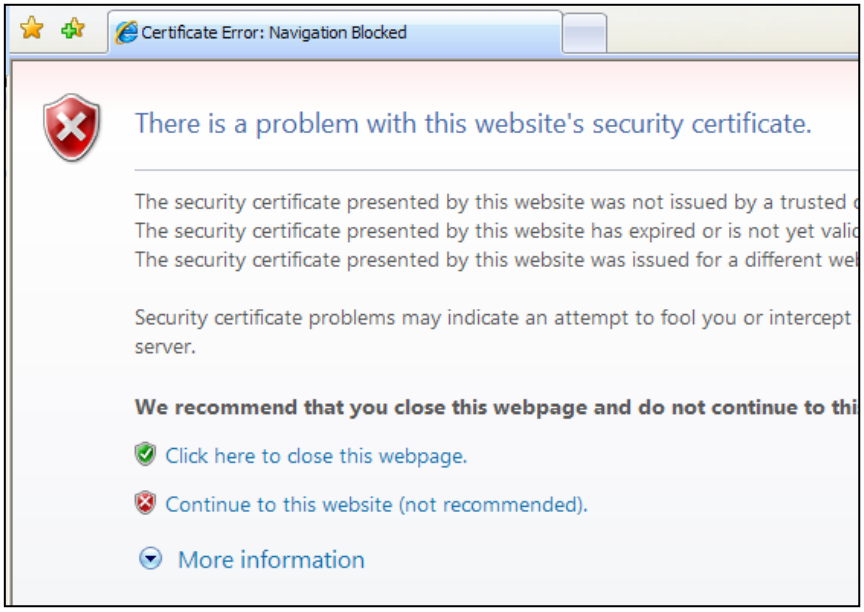
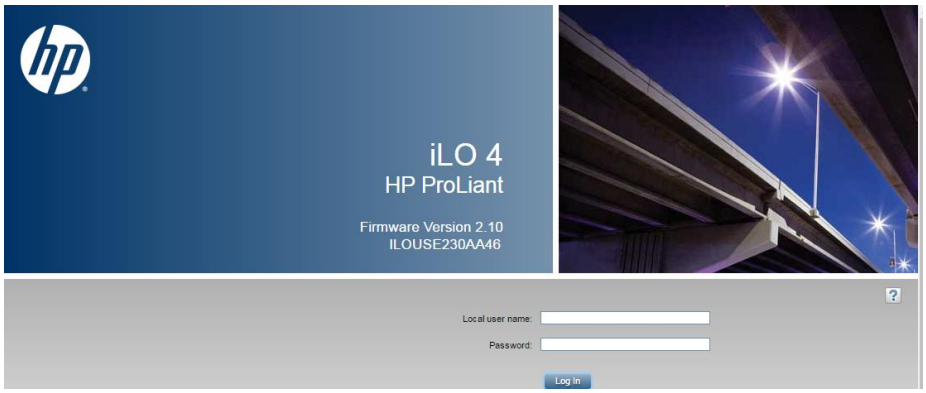
Processor hyper-threading is currently enabled.

Note: Output returned may state "enabled" or "disabled".</td></tr>
<tr><td>3.
☐</td><td colspan="2"> 
• If output from Step 2 shows that hyperthreading is currently "enabled", then continue with Step 4 of this procedure.
• If output from Step 2 shows that hyperthreading is currently "disabled", then STOP and restart Appendix Procedure 23 for the next installed DP blade.</td></tr>
<tr><td>4.
☐</td><td>Launch the Internet Explorer web browser and connect to the DP-iLO GUI interface.

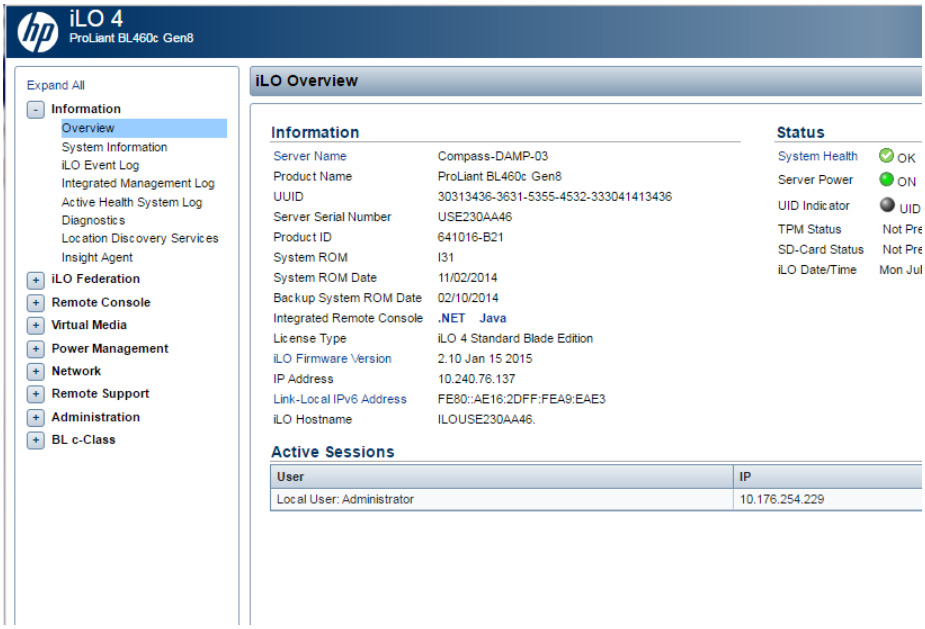
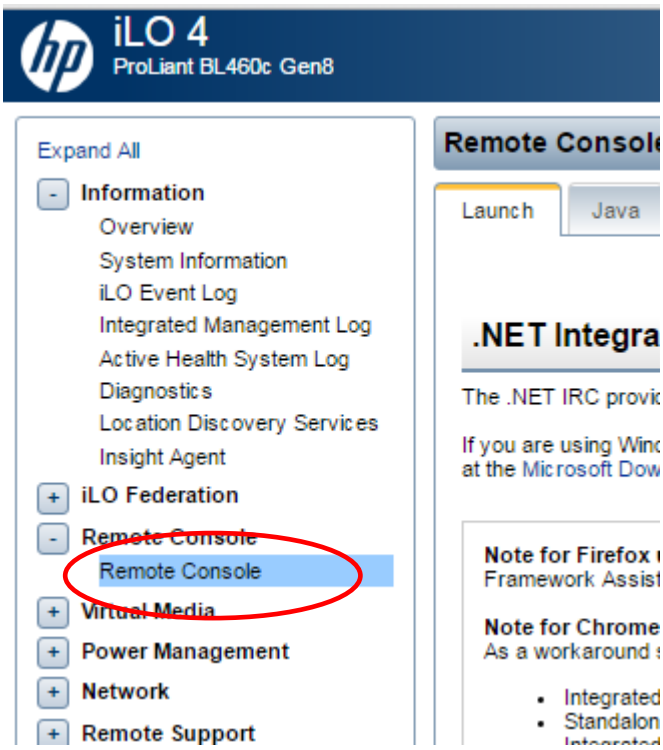
Note: Always use https:// for iLO GUI access.</td><td> 

<u>!!! WARNING !!!</u>
Verify the DP-iLO IP address before proceeding. The user must login using the DP-iLO IP address only.</td></tr>
</table>

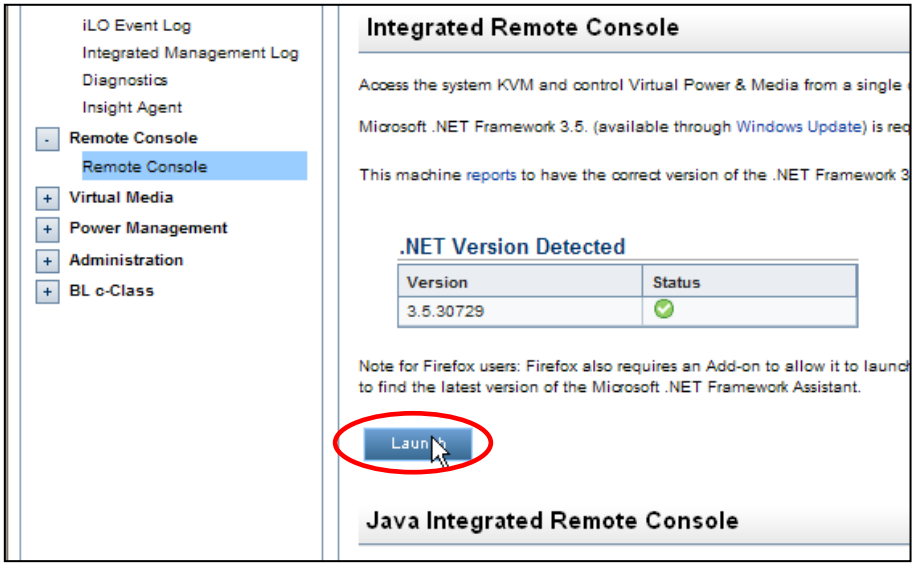
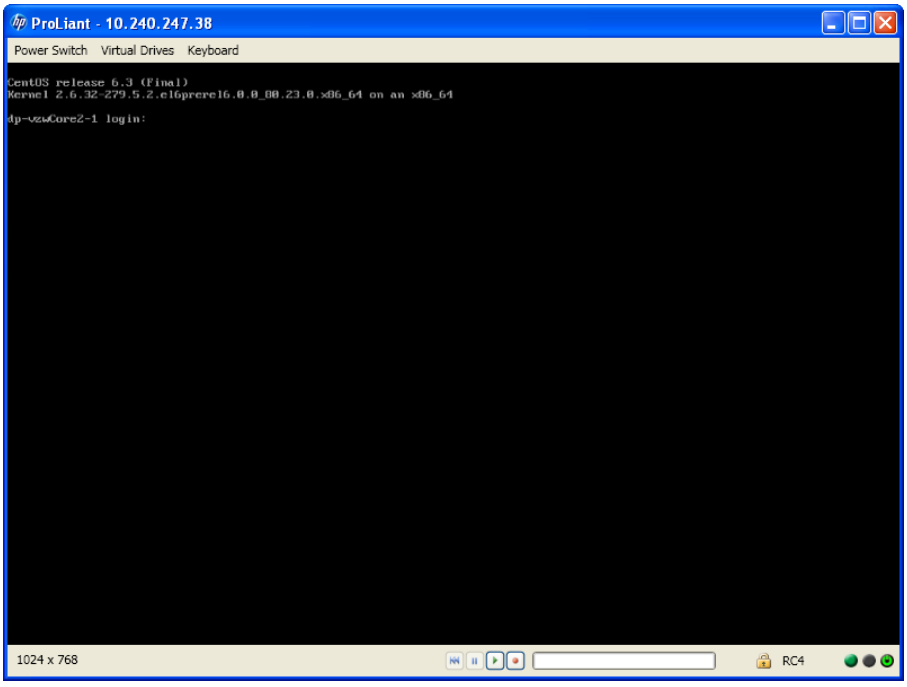
Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
5. ☐	The web browser will display a warning message regarding the Security Certificate. ***Note***: If presented with the "security certificate" warning screen shown to the right, choose the following option: **"Continue to this website (not recommended)".**	
6. ☐	Log into the iLO console as "Administrator" and enter the configured password.	

Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
7. ☐	The admin GUI is displayed. Select the "**Remote Console**" tab in the upper left corner of the GUI.	
8. ☐	The Remote Console Information GUI is displayed Click on the "**Remote Console**" menu option	

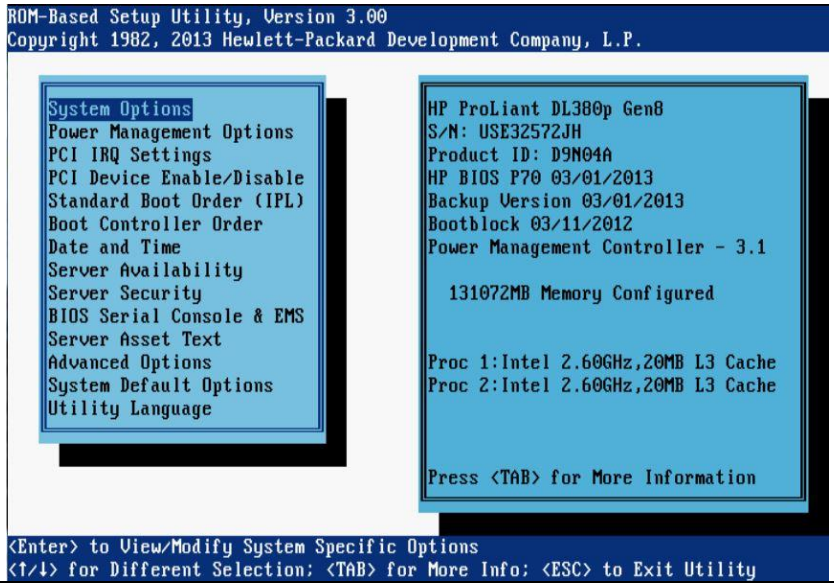
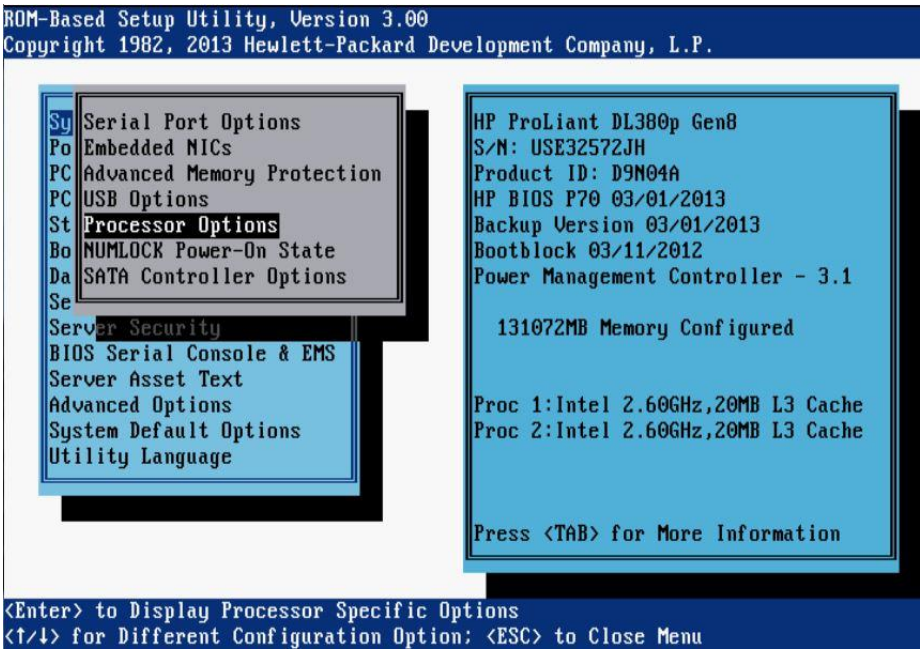
Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
9. ☐	Under the **"Integrated Remote Console"** section in the top of the right panel, click on the **"Launch"** dialogue button. ***Note***: Answer **"Yes/OK"** to any pop-up windows that might appear.	
10. ☐	The iLO Console window is displayed. ***Note***: The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.	
11.	**DP Server XMI IP (SSH):** Access the command prompt via DP blade's **XMI IP** address and log into the server as the "**admusr**" user.	`login: admusr` `Password: <admusr_password>`

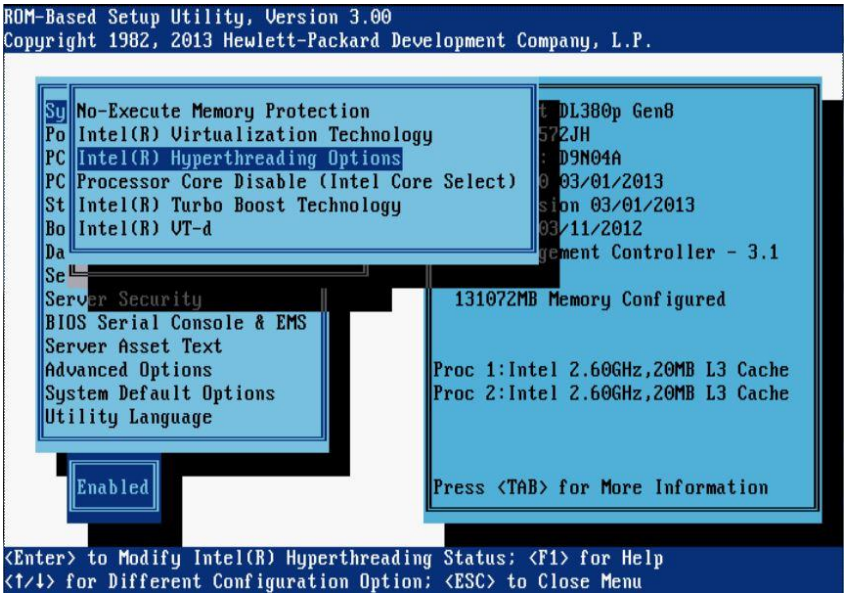
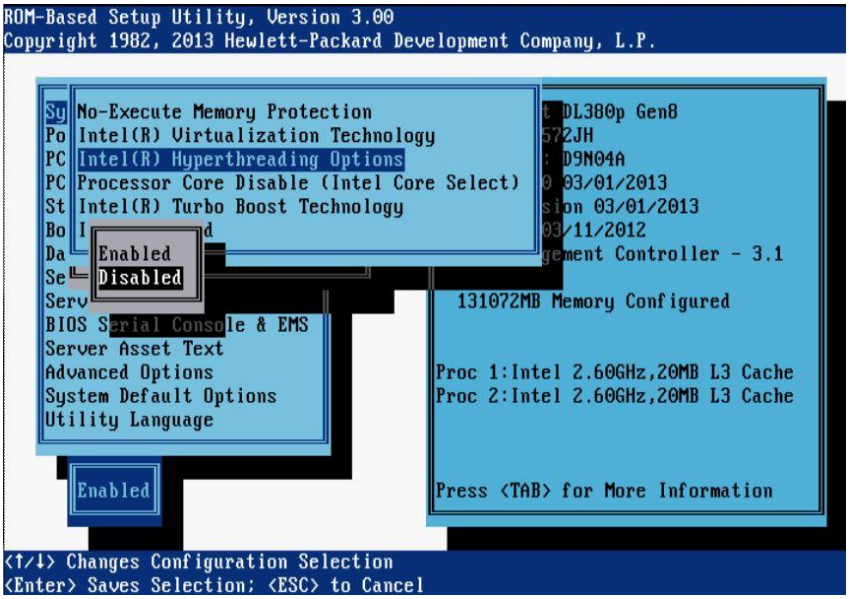
Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
12. ☐	Reboot the server. This can be achieved by logging in as the **“ ”** user and executing **init 6** command **a**t the command prompt.	`$ sudo init 6` ***Note***: It is normal for the Remote Console window to stay blank for up to **3 minutes** before initial output appears.
13. ☐	Access the Server BIOS by pressing **F9** key	Reboot the server. This can be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see **`F9=Setup`** in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below.  **Expected Result:** *ROM-Based Setup Utility is accessed and the ROM-Based Setup Utility menu will be displayed*. ***Note***: It is normal for a period of 2 minutes or more to occur between pressing the F9 key and entering the Blade BIOS screen

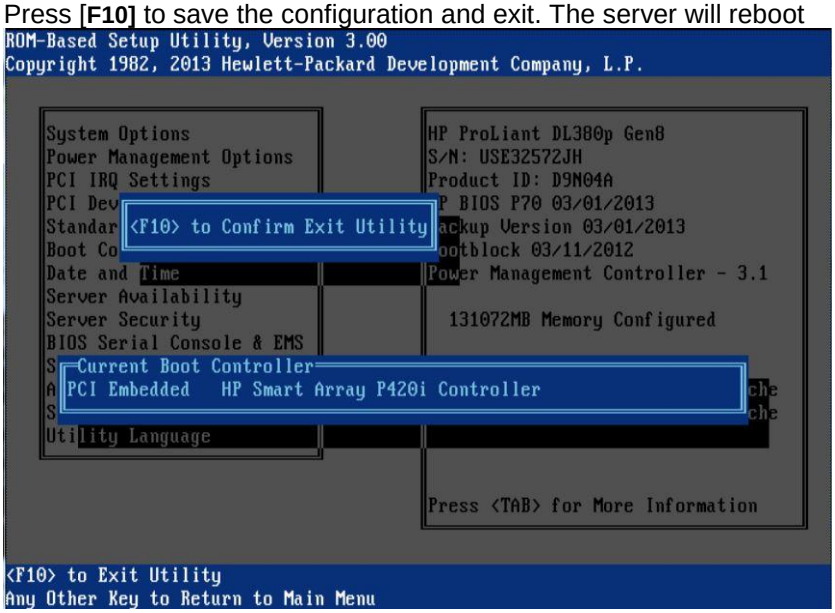
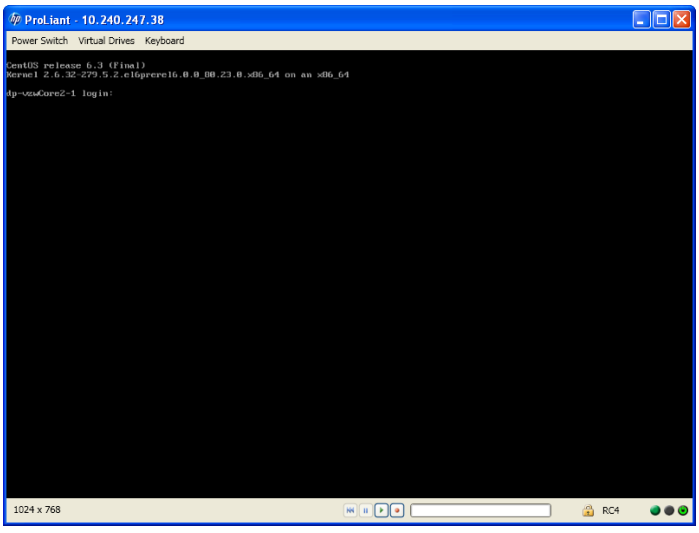
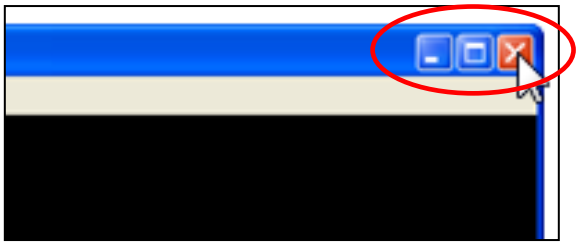
Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
14. ☐	Select System Options	Scroll to ***System Options*** and press **[ENTER]** 
15. ☐	Select Processor Options	Select ***Processor Options*** option and press **[ENTER]** 

Procedure 23. Gen8: Disable Hyerthreading (DP Only)

Step	Procedure	Result
16. ☐	Select Hyperthreading Options	**Select *Intel® Hyperthreading Options*** and press **[ENTER]**. 
17. ☐	Set hyperthreading to **Disabled**.	Select ***Disabled*** option and press [ENTER]**.** 

Procedure 23. Gen8: Disable Hyerthreading (DP Only)

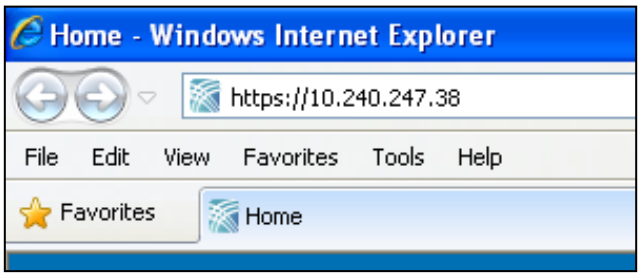
Step	Procedure	Result
18. ☐	Save Configuration and Exit. ***Note***: It is normal for the Remote Console window to stay blank for up to **3 minutes** before initial output appears.	Press [**F10**] to save the configuration and exit. The server will reboot  **Expected Result:** *Settings are saved and server reboots*.
19. ☐	Continue to monitor the server boot process until the screen returns to the login prompt.	
20. ☐	Close the Remote Console window.	
THIS PROCEDURE HAS BEEN COMPLETED		

Procedure 24. Gen9: Disable Hyperthreading (DP Only)

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1. ☐</td><td>DP Server XMI IP (SSH):
Access the command prompt via DP blade's XMI IP address and log into the server as the "admusr" user.</td><td>login: admusr
Password: <admusr_password></td></tr>
<tr><td>2. ☐</td><td>DP Server XMI IP (SSH):
Execute "hpasmcli" command to determine status of hyperthreading for the DP blade.</td><td>$ sudo hpasmcli -s "show ht"

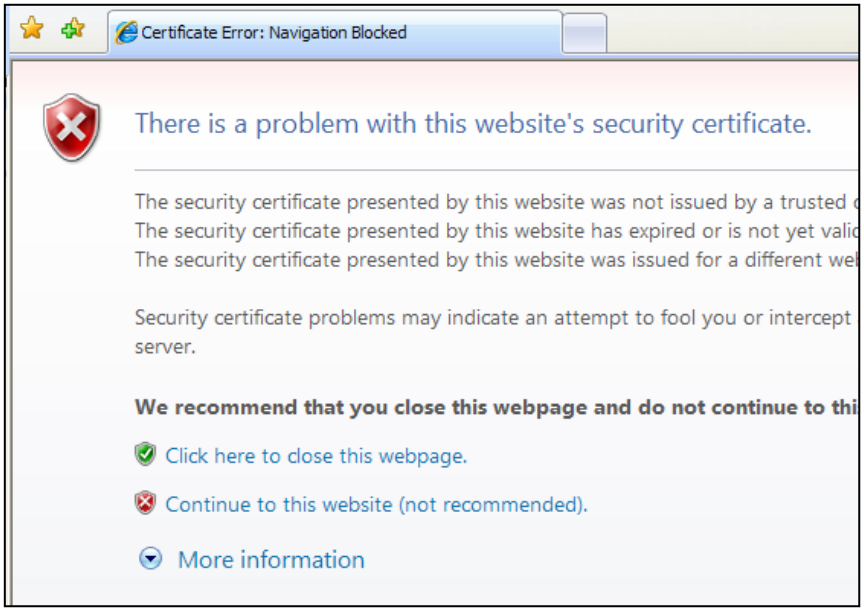
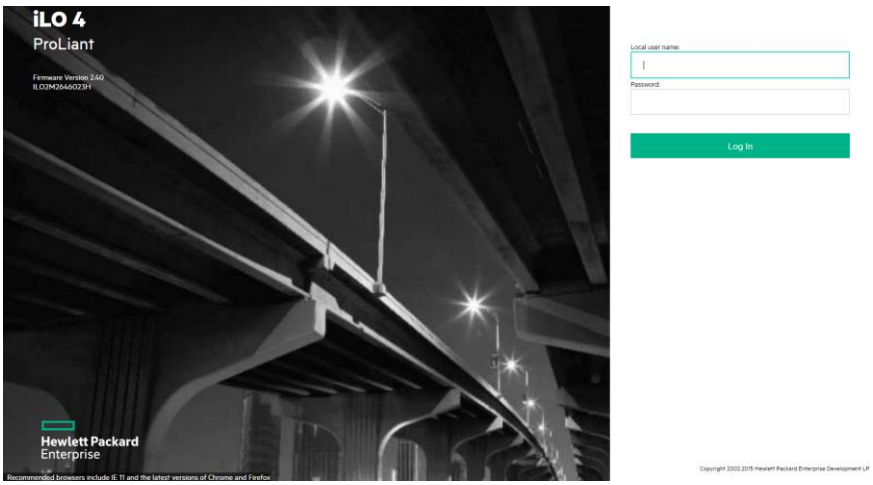
Processor hyper-threading is currently enabled.

NOTE: Output returned may state "enabled" or "disabled".</td></tr>
<tr><td>3. ☐</td><td colspan="2"> 
• If output from Step 2 shows that hyperthreading is currently "enabled", then continue with Step 4 of this procedure.
• If output from Step 2 shows that hyperthreading is currently "disabled", then STOP and restart Appendix Procedure 24 for the next installed DP blade.</td></tr>
<tr><td>4. ☐</td><td>Launch the Internet Explorer web browser and connect to the DP-iLO GUI interface.

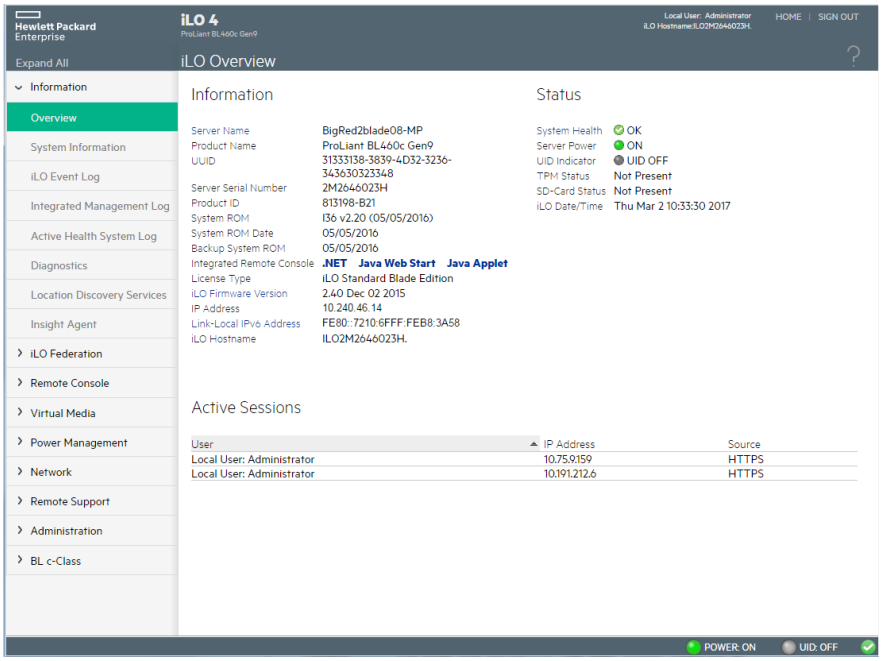
NOTE: Always use https:// for iLO GUI access.</td><td> 

<u>!!! WARNING !!!</u>
Verify the DP-iLO IP address before proceeding. The user must login using the DP-iLO IP address only.</td></tr>
</table>

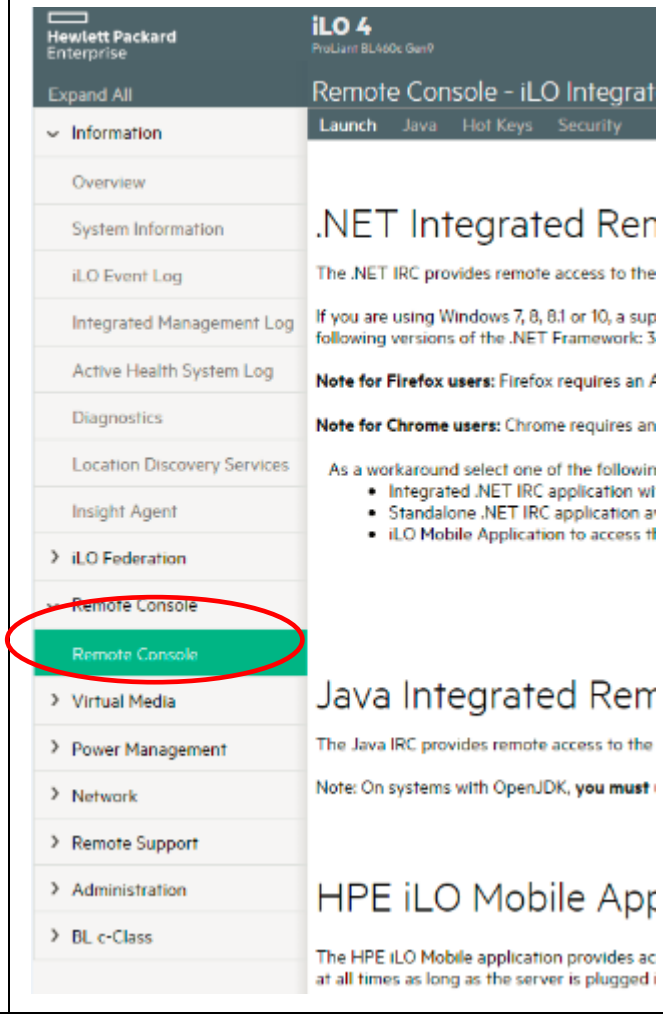
Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
5. ☐	The web browser will display a warning message regarding the Security Certificate. ***Note***: If presented with the "security certificate" warning screen shown to the right, choose the following option: **"Continue to this website (not recommended)".**	
6. ☐	Log into the iLO console as "Administrator" and enter the configured password.	

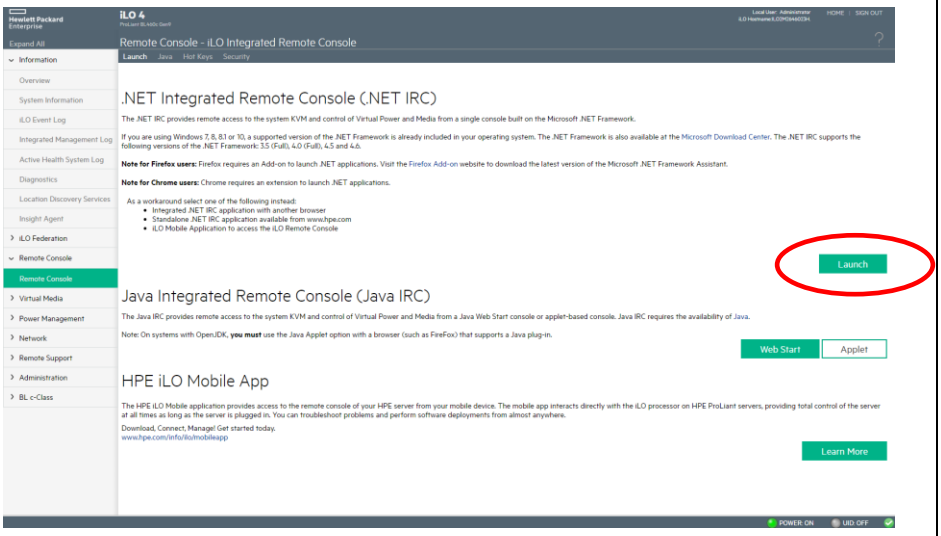
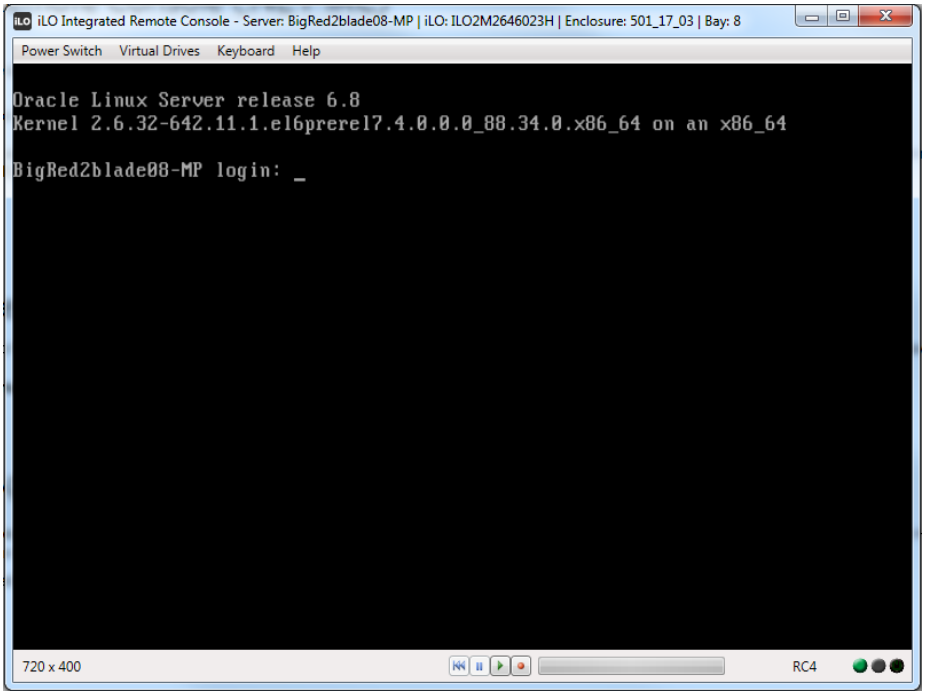
Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
7. ☐	The admin GUI is displayed. Select the "**Remote Console**" tab in the upper left corner of the GUI.	

Procedure 24. Gen9: Disable Hyperthreading (DP Only)

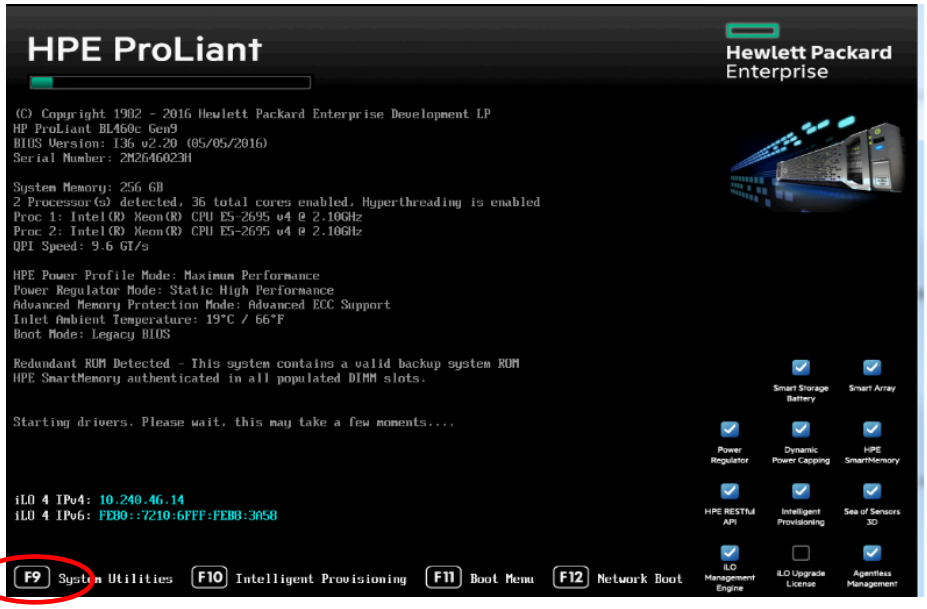
Step	Procedure	Result
8. ☐	The Remote Console Information GUI is displayed Click on the "**Remote Console**" menu option	

Procedure 24. Gen9: Disable Hyperthreading (DP Only)

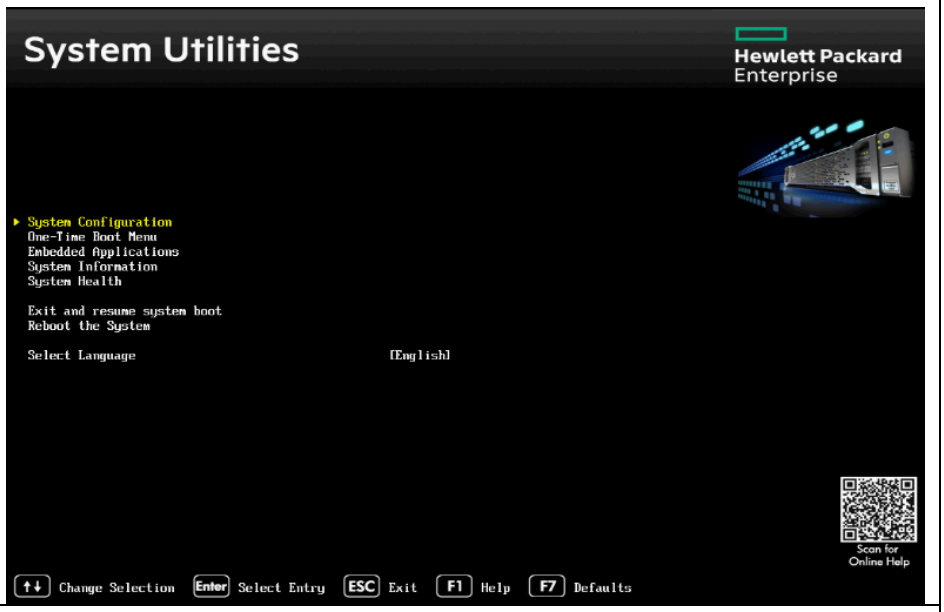
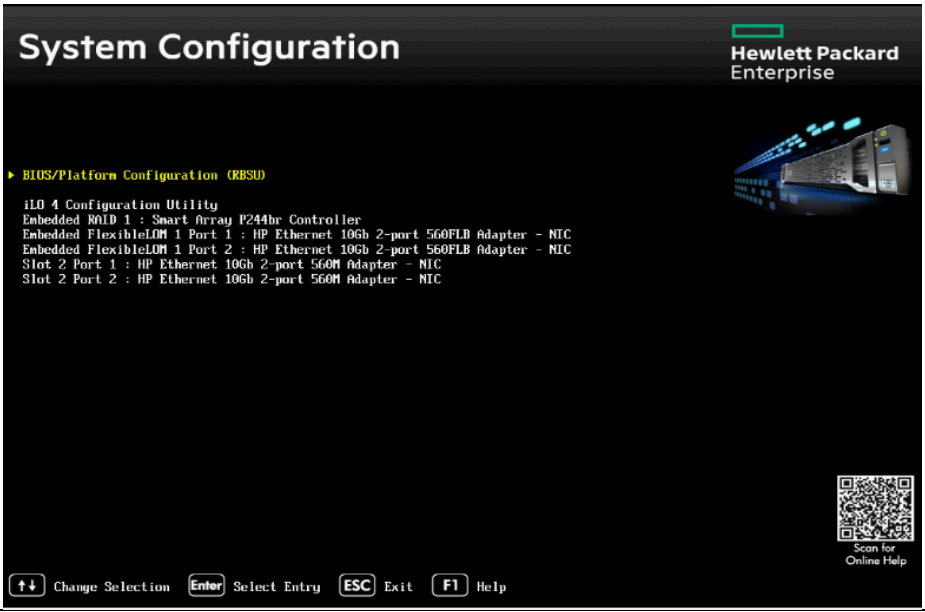
Step	Procedure	Result
9. ☐	Under the **"Integrated Remote Console"** section in the top of the right panel, click on the **"Launch"** dialogue button. ***Note***: Answer **"Yes/OK"** to any pop-up windows that might appear.	
10. ☐	The iLO Console window is displayed. ***Note***: The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.	

11.	**DP Server XMI IP (SSH):**
	
	Access the command prompt via DP blade's **XMI IP** address and log into the server as the "**admusr**" user.
		`login: admusr`
		
		`Password: <admusr_password>`

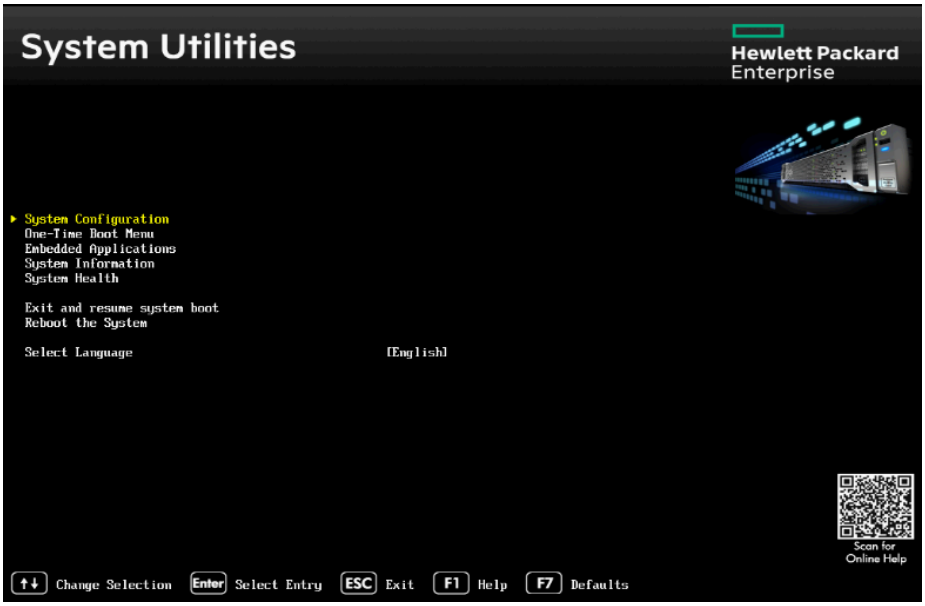
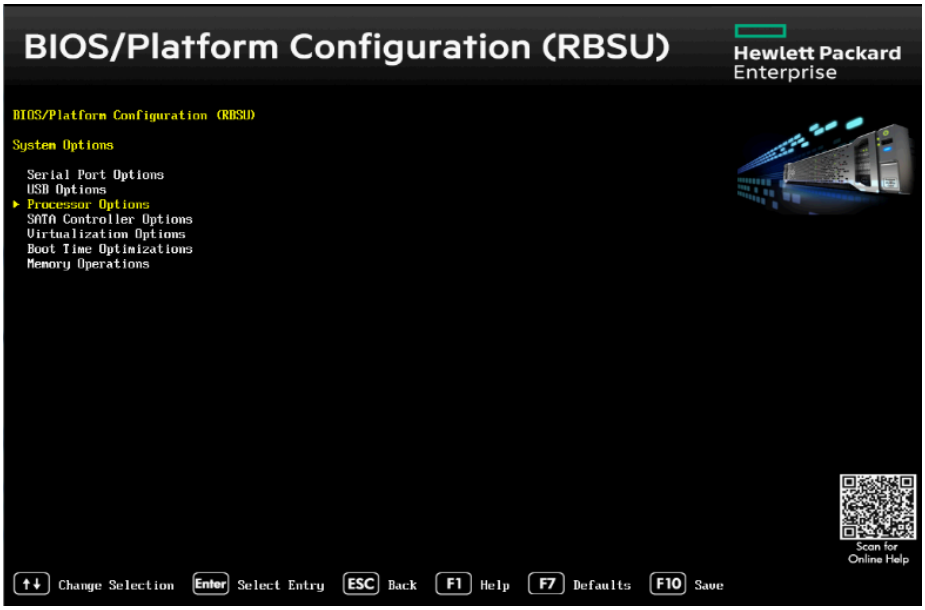
Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
12. ☐	Reboot the server. This can be achieved by logging in as the **“ ”** user and executing **init 6** command **a**t the command prompt.	`$ sudo init 6` ***Note***: It is normal for the Remote Console window to stay blank for up to **3 minutes** before initial output appears.
13. ☐	Access the Server BIOS by pressing **F9** key	Reboot the server. This can be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see **`F9=Setup`** in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below.  **Expected Result:** *ROM-Based Setup Utility is accessed and the ROM-Based Setup Utility menu will be displayed*. ***Note***: It is normal for a period of **2 minutes** or more to occur between pressing the **F9** key and entering the Blade BIOS screen.

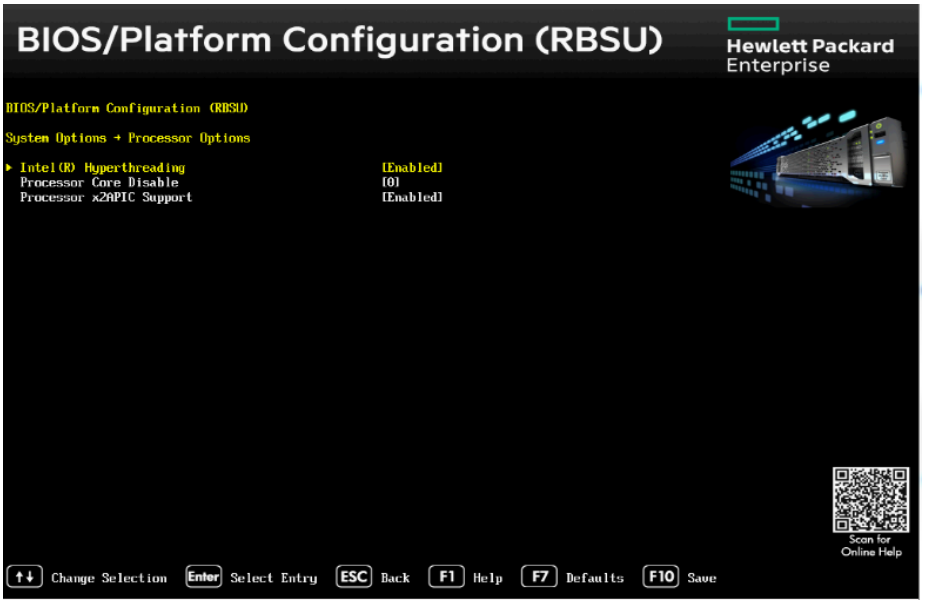
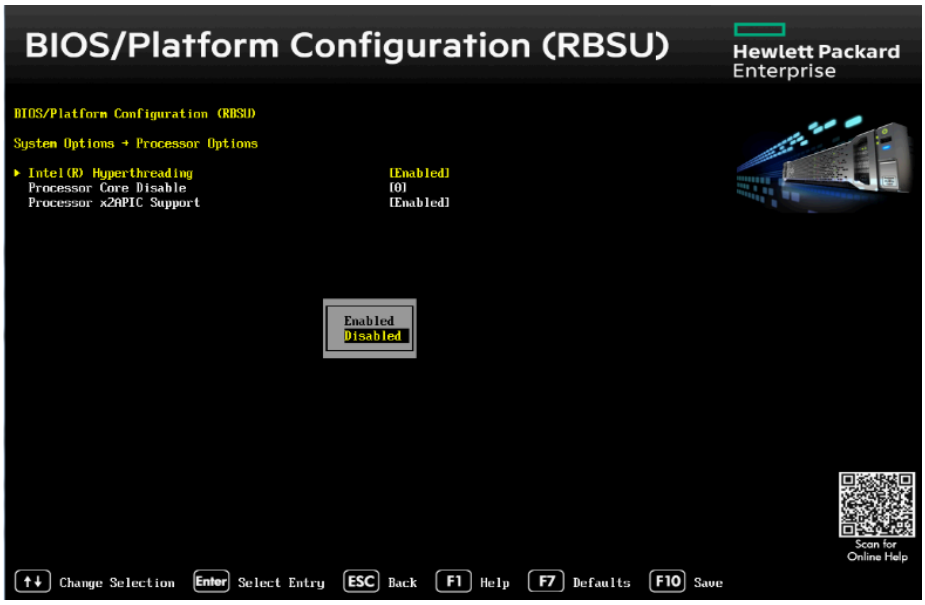
Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
14.	Scroll to ***System Configuration***	Scroll to ***System Configuration*** and press **[ENTER]** 
15.	Scroll to ***BIOS/Platform Configuration***	Scroll to ***BIOS/Platform Configuration*** and press **[ENTER]** 

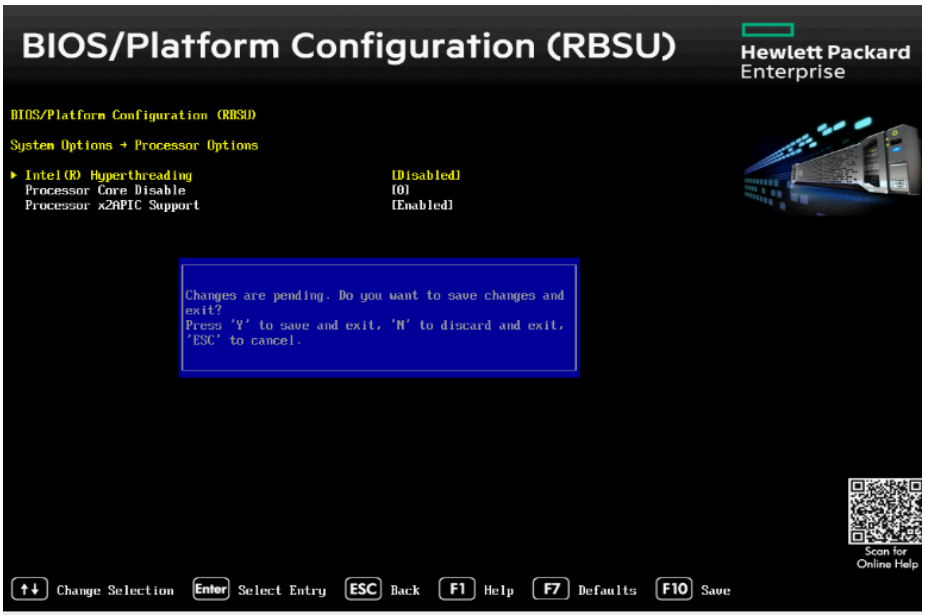
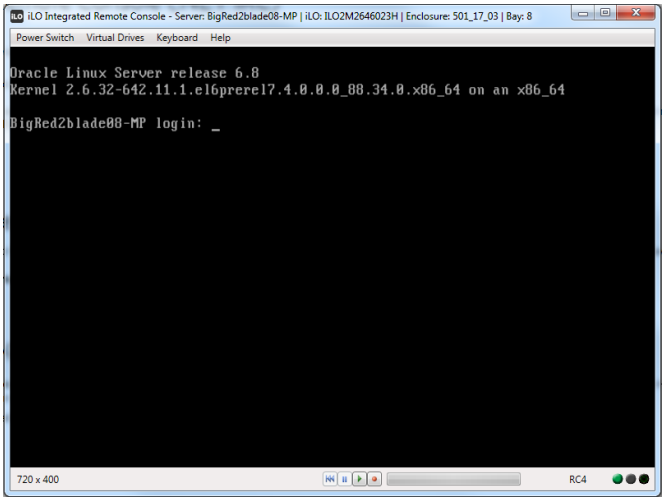
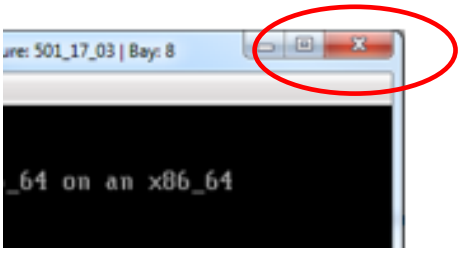
Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
16. ☐	Select System Configuration	Scroll to ***System Configuration*** and press **[ENTER]** 
17. ☐	Select Processor Options	Select ***Processor Options*** option and press **[ENTER]** 

Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
18. ☐	Select Hyperthreading Options	**Select *Intel® Hyperthreading Options*** and press **[ENTER]**. 
19. ☐	Set hyperthreading to **Disabled**	Select ***Disabled*** option and press [ENTER]**.** 

Procedure 24. Gen9: Disable Hyperthreading (DP Only)

Step	Procedure	Result
20. ☐	Save Configuration and Exit. ***Note***: It is normal for the Remote Console window to stay blank for up to **3 minutes** before initial output appears.	Press **[F10]** to save the configuration and exit. The server will reboot  **Expected Result:** *Settings are saved and server reboots*.
21. ☐	Continue to monitor the server boot process until the screen returns to the login prompt.	
22. ☐	Close the Remote Console window.	

Appendix J. Configure the HP DL380 (Gen8 and Gen9) Server CMOS Clock/BIOS Settings

J-1. Gen8: Configure the ILO for Rack Mount Server

J.1.1. RMS: Configure ILO

In this procedure you will be configuring Integrated Lights Out (iLO) for RMS. You will configure the NIC and TCP/IP, DNS/DHCP parameters as well as adding a new iLO user.

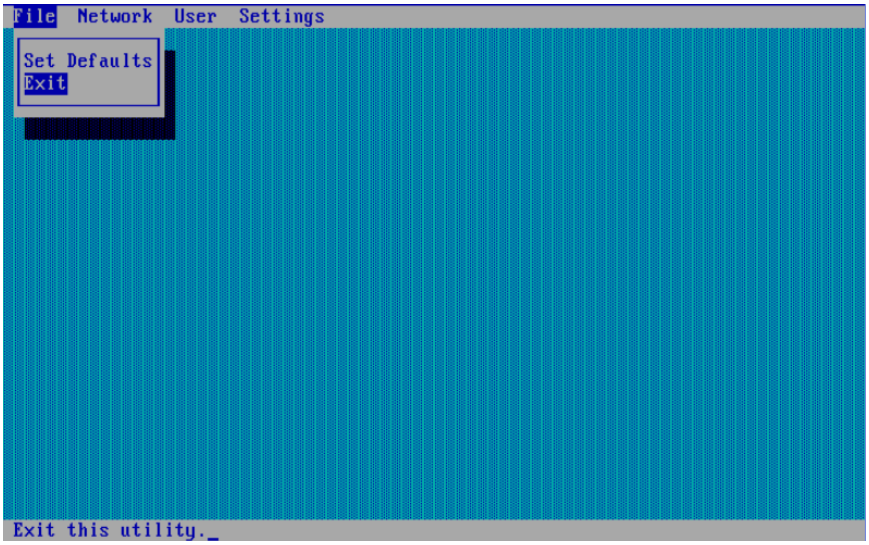
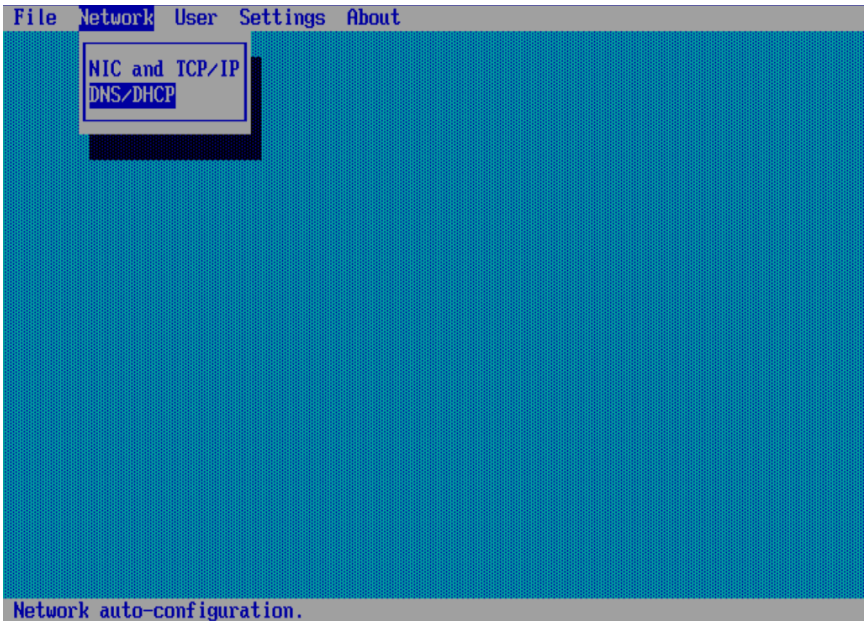
Prerequisites & Requirements:

- ✓ Server powered on
- ✓ Server booting up or rebooted

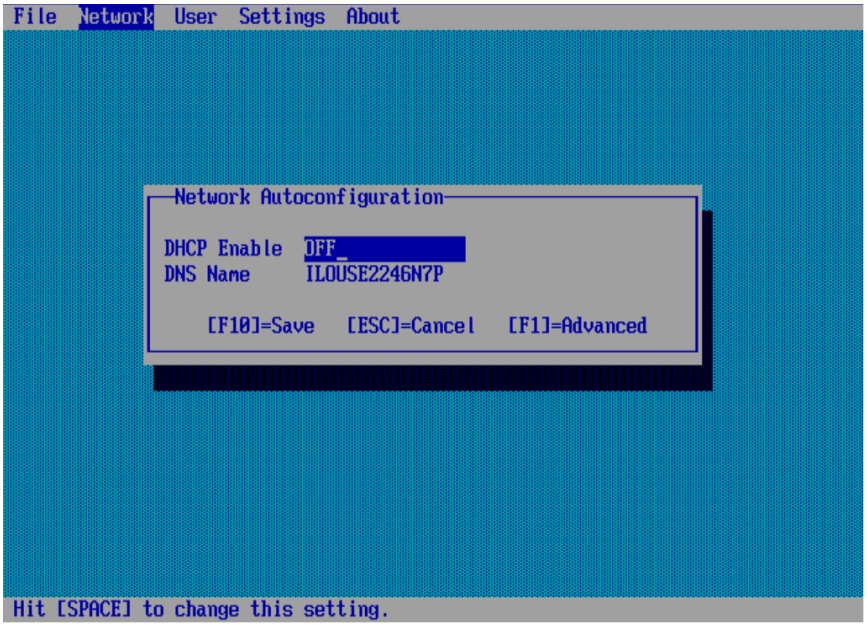
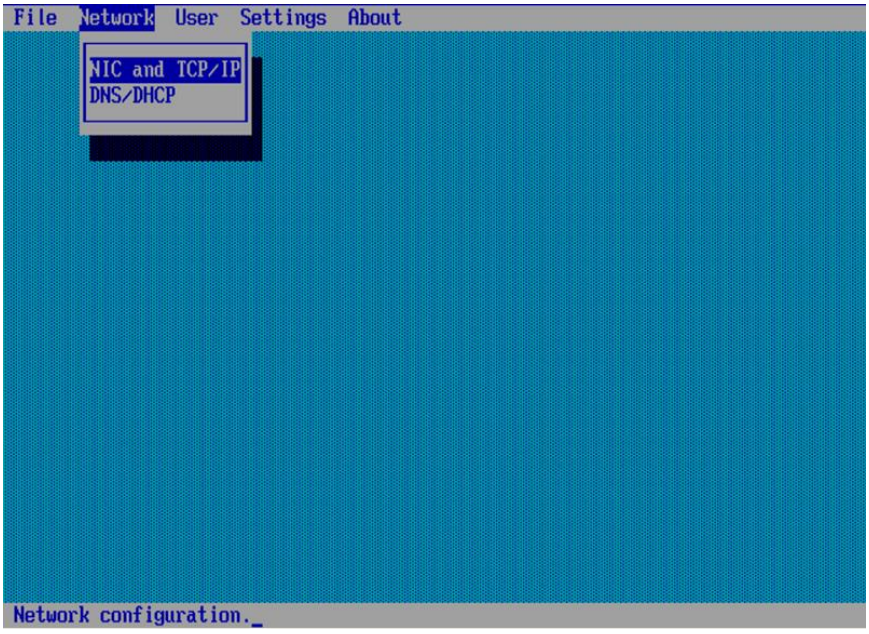
Procedure 25. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
1. ☐	**Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS):** **For HP Gen8 DL380 servers perform the following** **1. Reboot the server.** 2. When "**iLO 4 Standard press [F8] to configure**" is displayed, press **[F8]** 3. Once **[F8]** is pressed wait for the iLO Configuration screen to appear.	 **Figure 27 – iLO Configuration – Gen8: Press [F8] to configure**

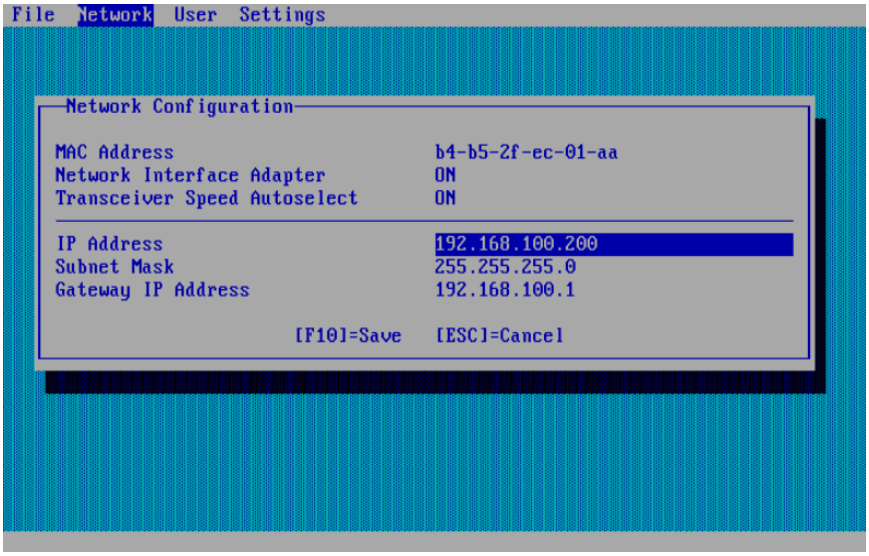
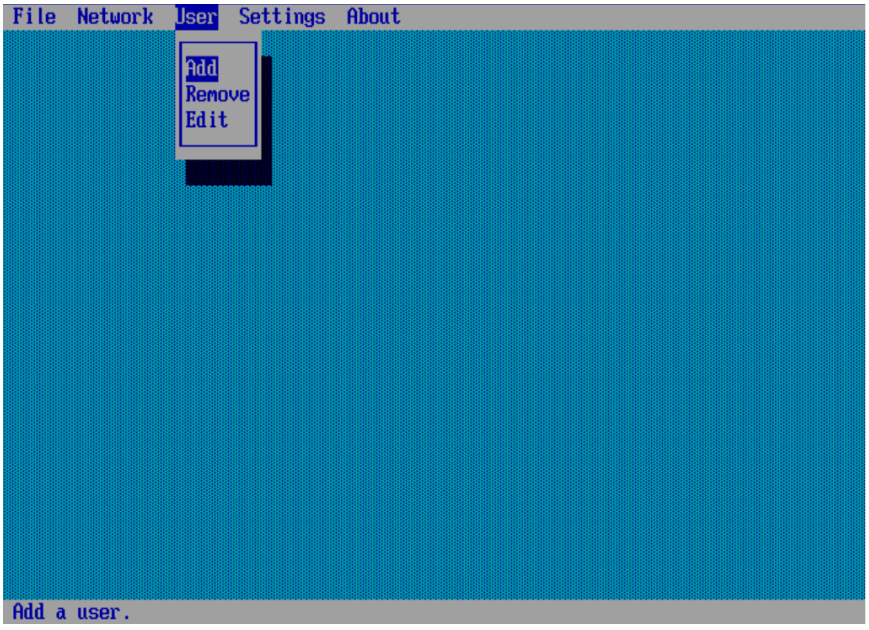
Procedure 25. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
2.	After the initial iLO configuration utility screen appears, use the arrow keys to select the Network menu	 **Figure 28 – iLO Configuration – Initial iLO Configuration Screen**
3.	Within the Network menu, select DNS/DHCP	 **Figure 29 – iLO Configuration – Select Network->DNS/DHCP**

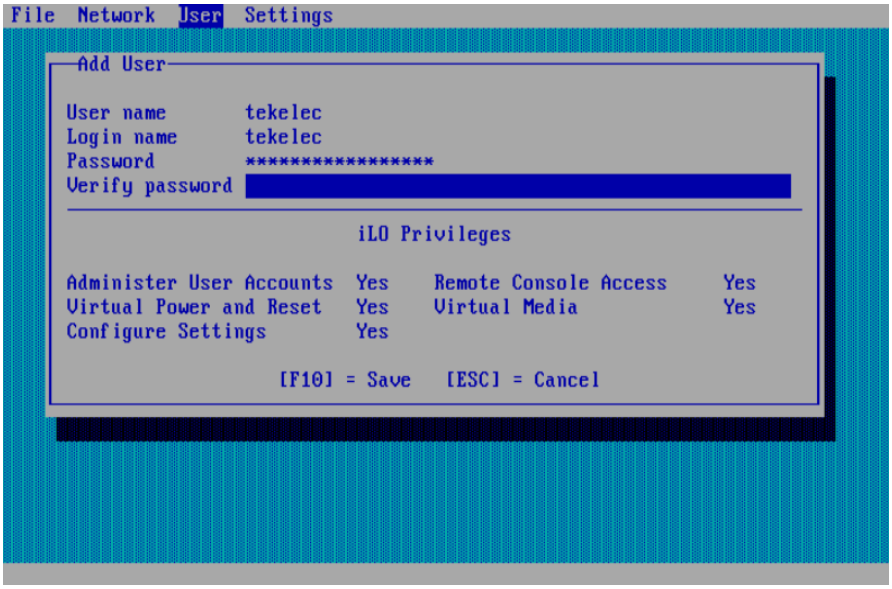
Procedure 25. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
4.	Verify that DNS/DHCP is set to OFF. If it is not set to OFF, use the [SPACE BAR] to toggle the setting to 'OFF'	 **Figure 30 – iLO Configuration – press [SPACE BAR] to turn DHCP OFF**
5.	Press [F10] to save if changes were made or [ESC] to Cancel if no changes were made. You should be returned to the Network main menu.	 **Figure 31 – iLO Configuration – Select NIC and TCP/IP**

Procedure 25. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
6.	**Press [ENTER] if required and select 'NIC and TCP/IP'**	 **Figure 32 – iLO Configuration – Select NIC and TCP/IP and configure Network**
7.	**Enter the Network Configuration information for the server. Use the arrow keys to select the field to change**	IP Address should be set based on the information in the NAPD.
8.	Once the **Network Configuration** information has been entered, press **[F10]** to save the settings. Using the arrow keys, select the **User** menu, then select **Add** and press **[ENTER]**	 **Figure 33 – iLO Configuration – Select User – Add**

Procedure 25. Gen8: Configure the iLO for Rack Mount Server

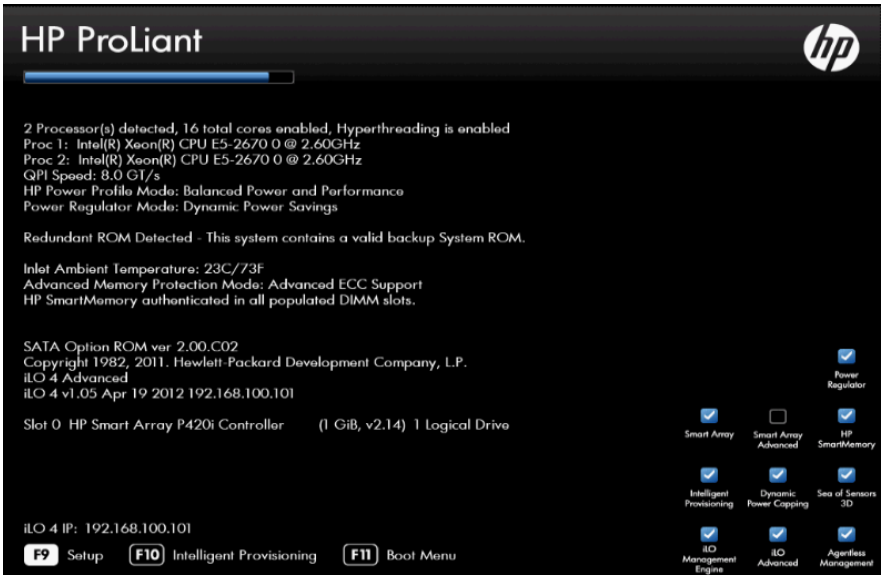
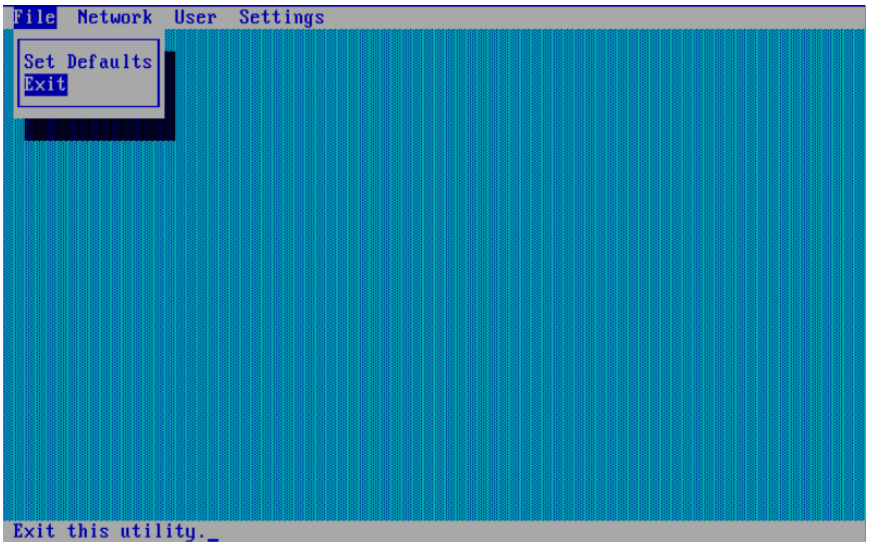
Step	Procedure	Result
9.	Add the tekelec user. Username: tekelec Login name: tekelec Password: tekelec1	
10.	Once the tekelec User has been added, press **F10** to Save the user.	
11. ☐	Repeat this procedure for other ship loose servers for the work order.	

J.1.2. Gen8: RMS BIOS Configuration, Verify Processor and Memory

Prerequisites & Requirements:

- ✓ Server powered on
- ✓ KVM connectivity to the server to get console

Procedure 26. Enter the ROM-Based Setup Utility (RBSU)

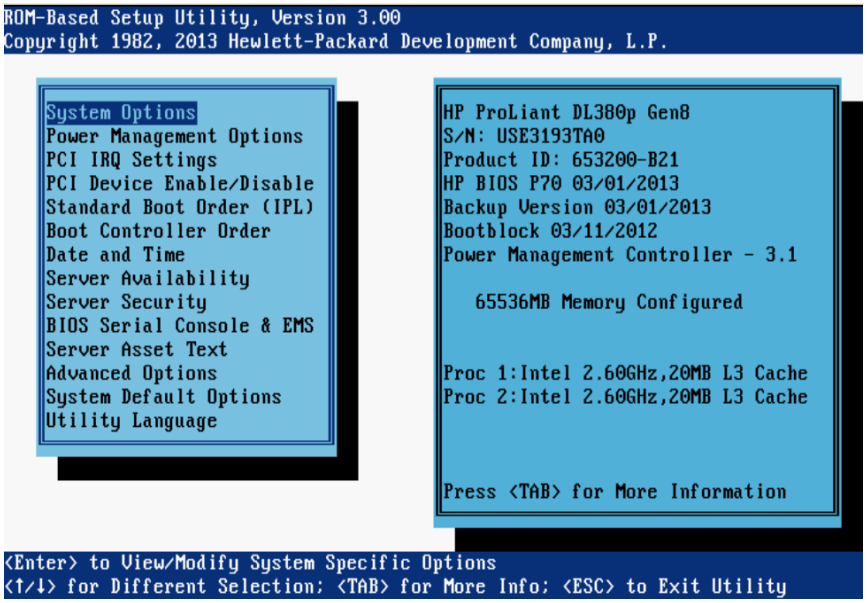
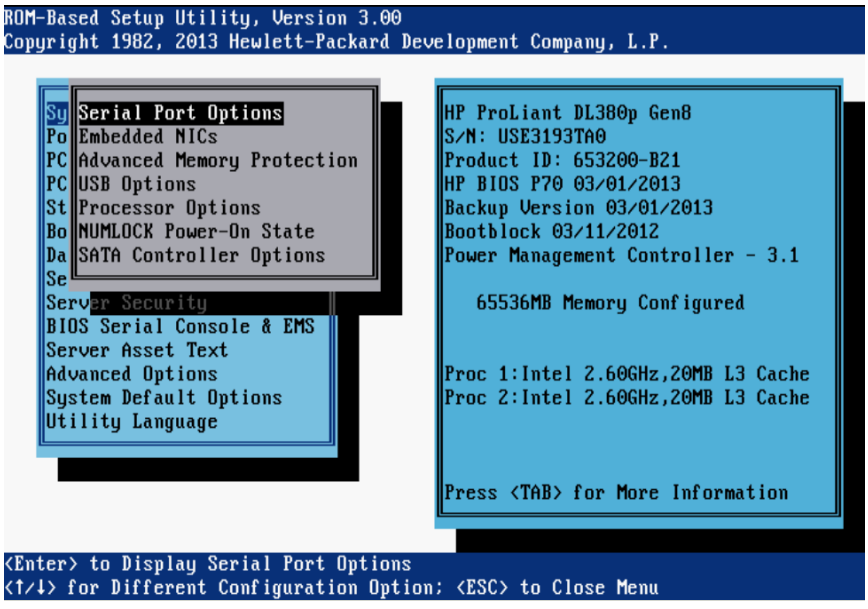
Step	Procedure	Result
1. ☐	Reboot the server. You will see an HP ProLiant screen as shown below. When prompted with the option to Press F9 for setup, do so. Once F9 is pressed, you should see "F9" selected on the screen as shown below:	 **Figure 34 – RBSU – Enter RBSU – F9 Pressed indicated in HP Splash Screen**
2.	After the initial iLO configuration utility screen appears, use the arrow keys to select the Network menu.	 **Figure 35 – iLO Configuration – Initial iLO Configuration Screen**

In this procedure you will be verifying and/or configuring the Serial Port Options for the Embedded and Virtual Serial Ports.

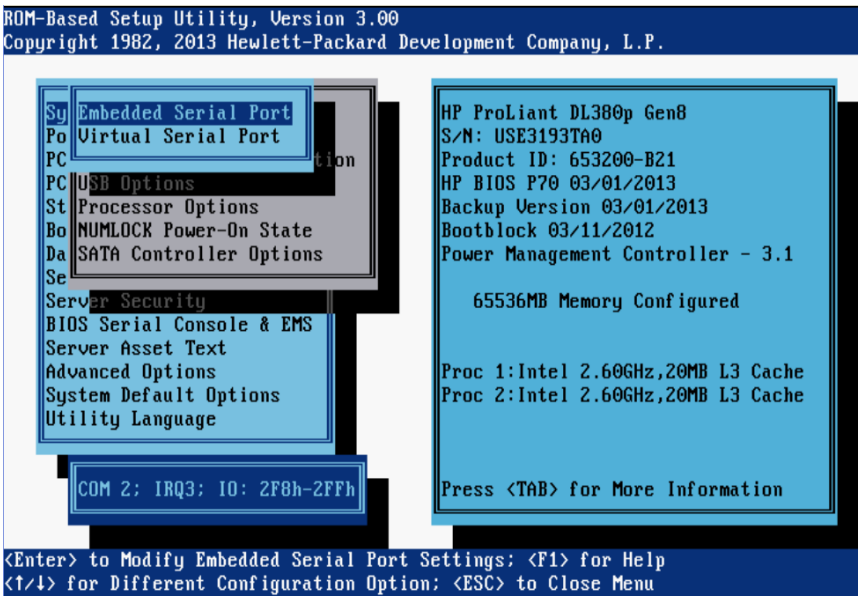
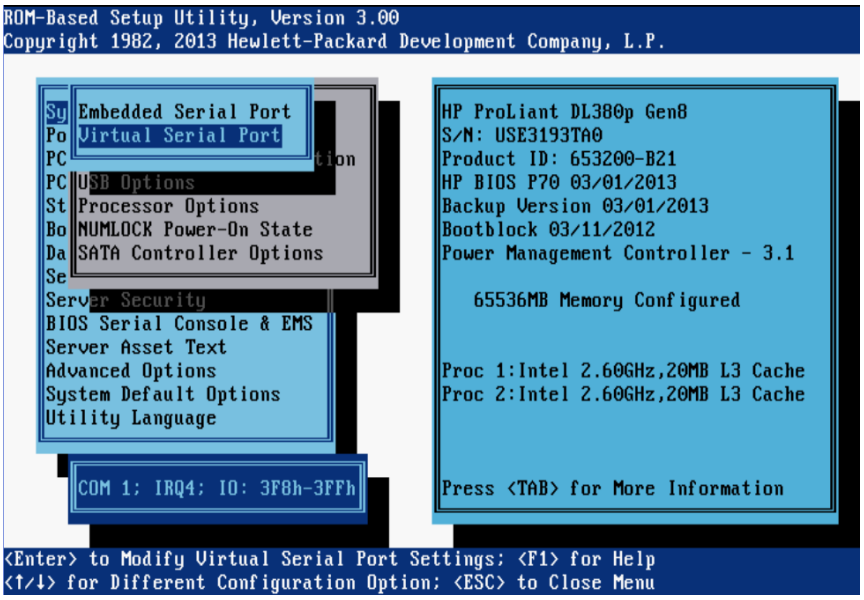
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU mode

Procedure 27. Verify/Configure Serial Port Options

Step	Procedure	Result
1. ☐	Select **System Options**, then **Serial Port Options:**	 **Figure 36 – ROM-Based Setup Utility – Initial Screen**  **Figure 37 – ROM-Based Setup Utility – Serial Port Options**

Procedure 27. Verify/Configure Serial Port Options

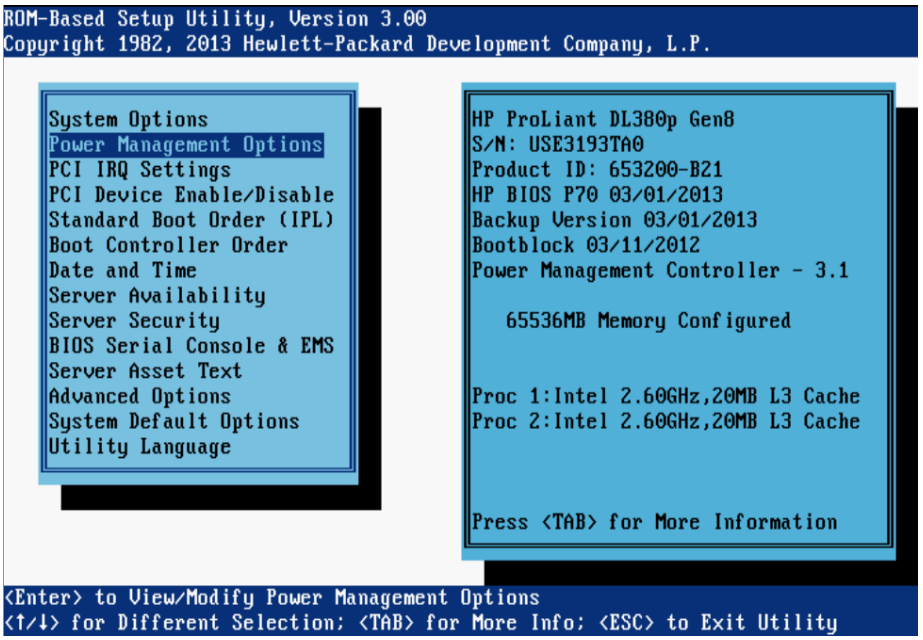
Step	Procedure	Result
2.	Verify the settings for Embedded Serial Port:	Select "**Embedded Serial Port**" and verify it is set for "**COM 2".** If it is not set to **COM 2,** press **[ENTER],** select **COM 2,** then **[ENTER].**  **Figure 38 – Verify Embedded Serial Port Setting**
3.	Verify the settings for Virtual Serial Port:	Select "**Virtual Serial Port**" and verify it is set for **COM 1.** If it is not set to **COM 1,** press **[ENTER],** select **COM 1,** then **[ENTER]** 

In this procedure you will be configuring **Power Management Options**. The server **HP Power Profile** will be verified or set to **Maximum Performance**.

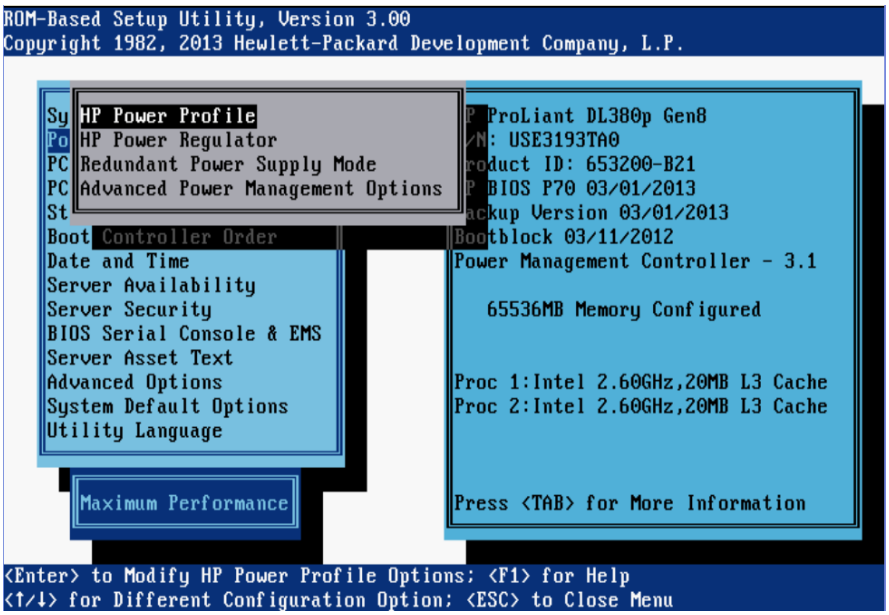
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

Procedure 28. Verify/Set Power Management

Step	Procedure	Result
1. ☐	While in **RBSU,** verify or set the **HP Power Profile**	Select "**Power Management Options**", then press **[ENTER].**  **Figure 39 – RBSU – Select Power Management Options**

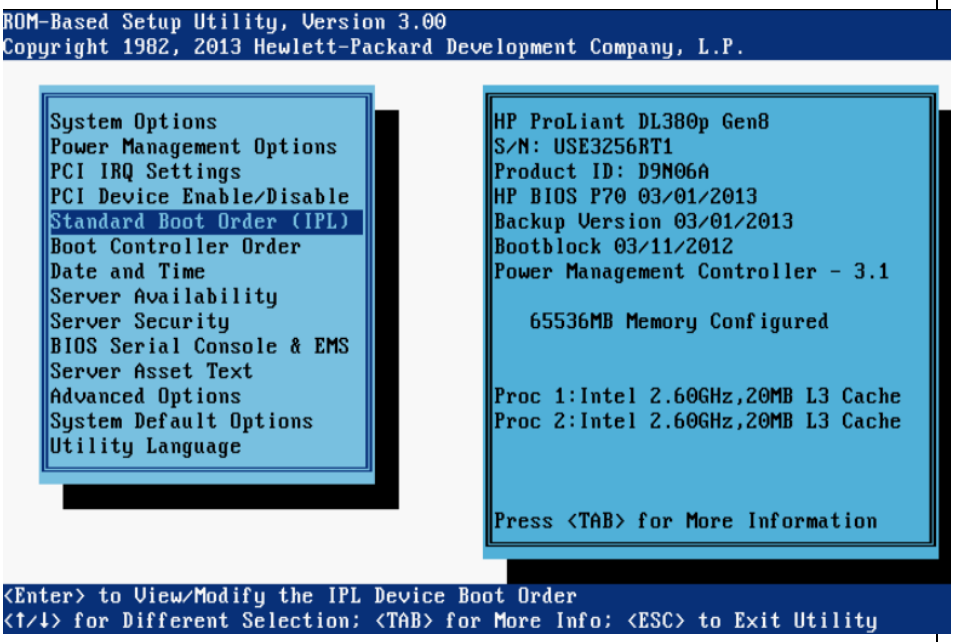
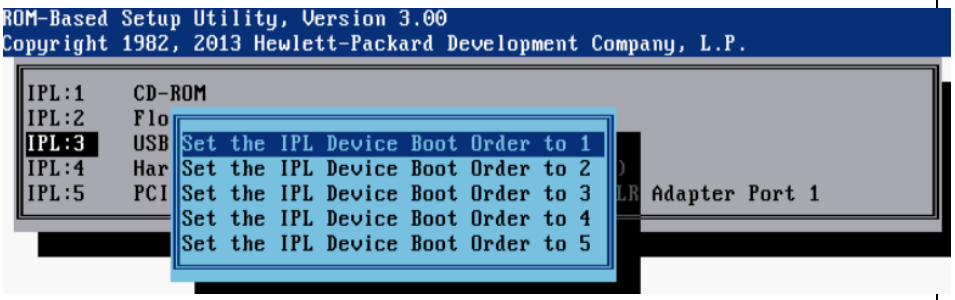
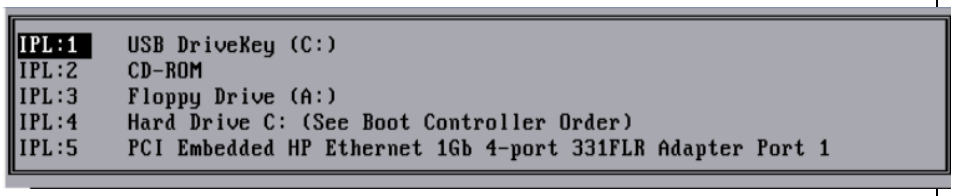
Procedure 28. Verify/Set Power Management

Step	Procedure	Result
2.	After pressing [ENTER] you will see several options to choose from such as:	*HP Power Profile, HP Power Regulator, Redundant Power Supply Mode, Advanced Power Management*.  **Figure 40 – RBSU – Select HP Power Profile and Maximum**
3.	• Select **HP Power Profile** • Verify it is set to **Maximum Performance**	
4.	If not set to **Maximum Performance**, press **[ENTER]** and select **"Maximum Performance"**, then press **[ENTER]**	

Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

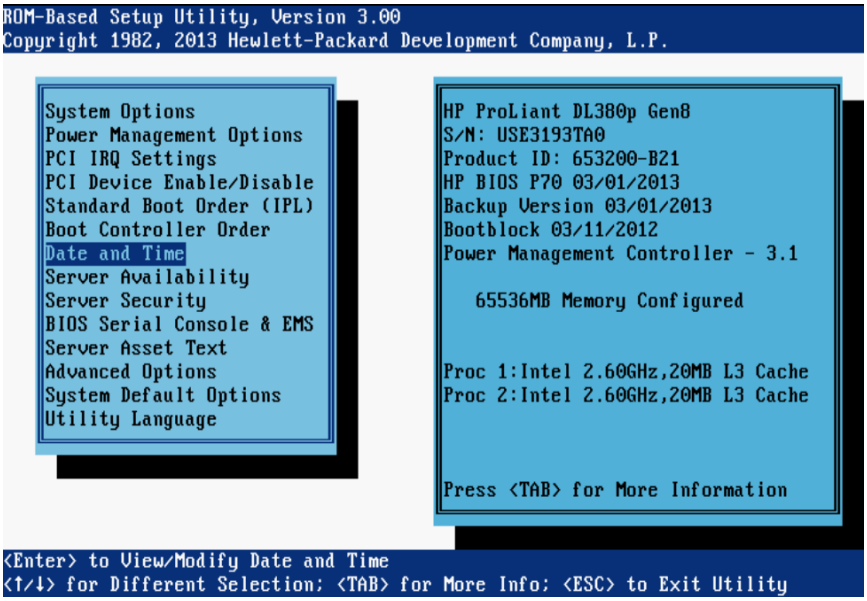
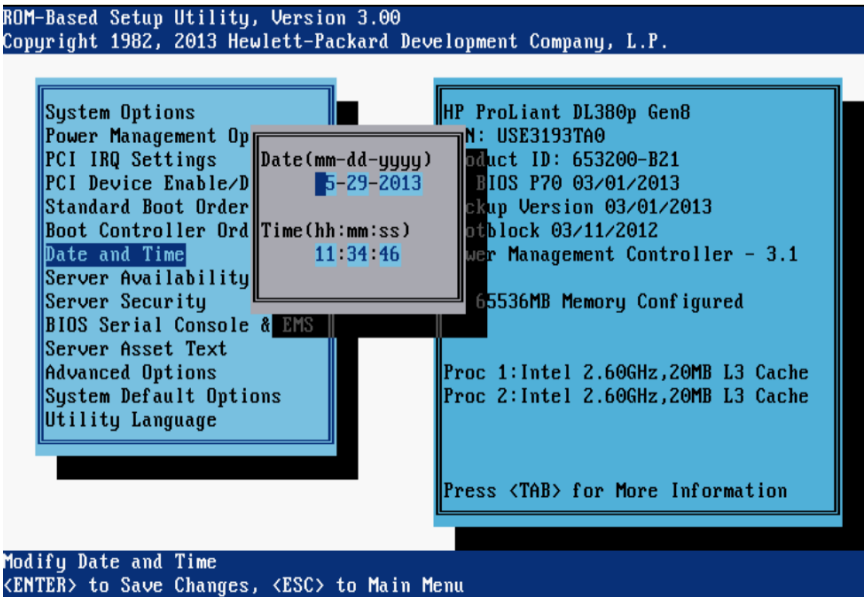
Procedure 29. Verify/Set Standard Boot Order (IPL)

Step	Procedure	Result
1. ☐	While in **RBSU,** verify or set the **Standard Boot Order**. Select **Standard Boot Order, then press [ENTER]**	Select "**Power Management Options**", then press **[ENTER].**  **Figure 41 – Select Standard Boot Order**
2.	Verify that **IPL:1** is **USB DriveKey (C:).** If **IPL:1** is not **USB DriveKey,** then select **USB DriveKey** and press **[ENTER],** then select **"Set the IPL Device Boot Order to 1**" and press **[ENTER]**	 **Figure 42 – Select Set the IP Device Boot Order to 1**
3.	Verify that **IPL:1** is **now USB DriveKey (C:)**	 **Figure 43 – IPL:1 is Now USB DriveKey (C:)**

Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

Procedure 30. Verify/Set System Date and Time

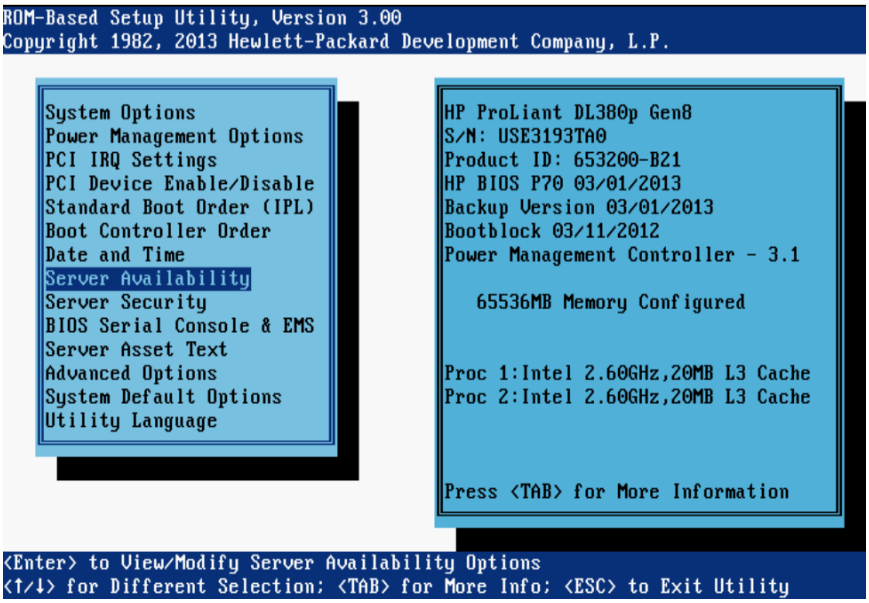
Step	Procedure	Result
1. ☐	While in RBSU, set the system Date and Time: Select "**Date and Time**", then press **[ENTER]**	 **Figure 44 – Select Date and Time**
2.	Set the current **Date and Time**. Use **UTC** for the time settings. Once the correct Date and Time has been set, press **[ENTER]** to confirm the settings.	 **Figure 45 – Set Date and Time (UTC)**

In this procedure you will be configuring **Server Availability** which determines how the server will behave following a power loss and recovery. The server will be set to **Restore Last Power State** following a power outage and recovery. In addition it will be set to power on with **No Delay**.

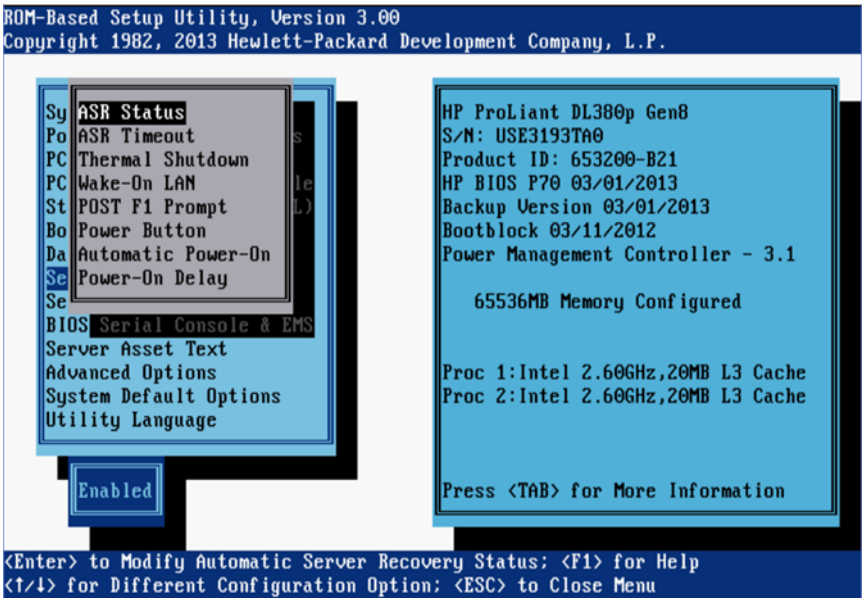
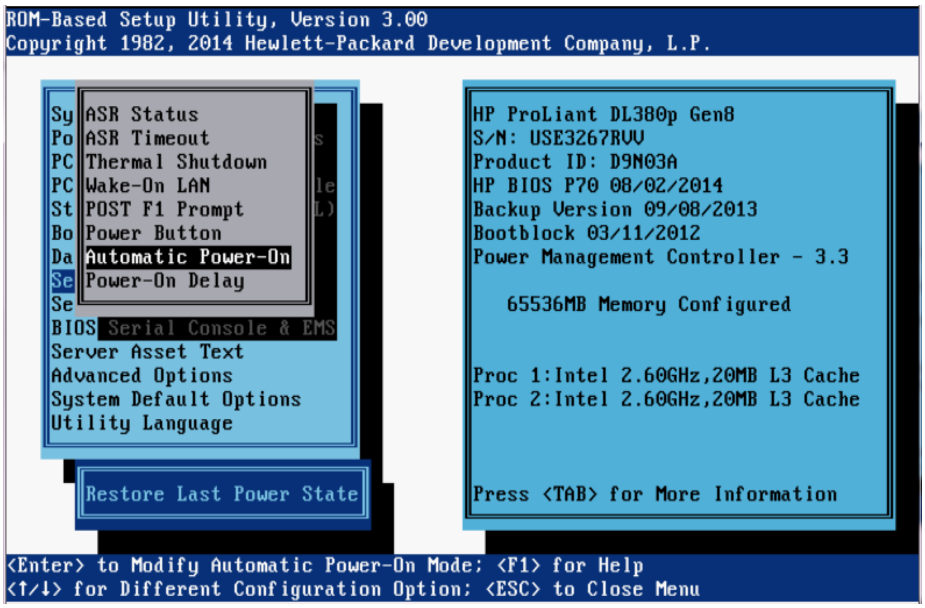
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

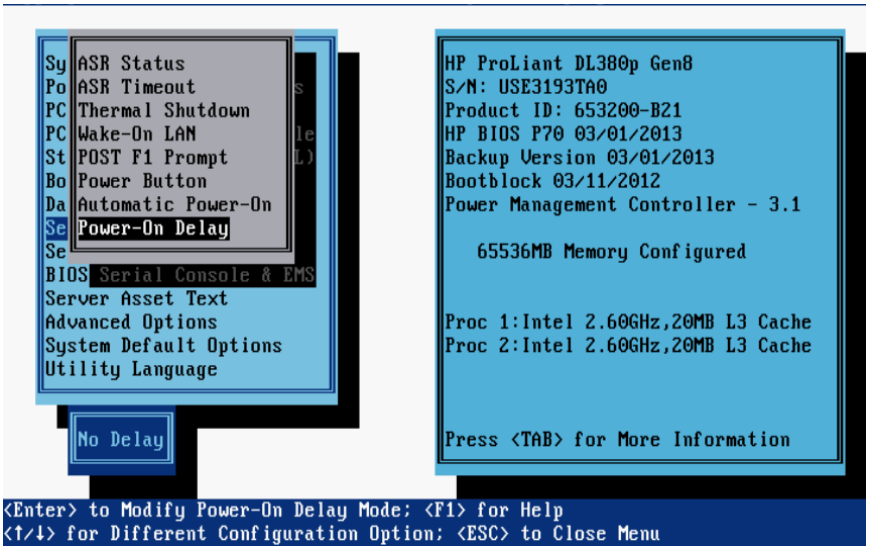
Procedure 31. Verify/Set Server Availability

Step	Procedure	Result
1. ☐	While in **RBSU,** set the **Server Availability:** Select "**Server Availability**", then press **[ENTER]**	 **Figure 46 – RBSU – Select Server Availability**
2.	After pressing **[ENTER]** you will see several options to choose from including *ASR Status, ASR Timeout, Thermal Shutdown, Wake-On LAN, POST F1 Prompt, Power Button, Automatic Power-On* and *Power-On Delay*.	
3.	✓ Select **ASR Status**. ✓ Verify it is set to **Enabled.**	

Procedure 31. Verify/Set Server Availability

Step	Procedure	Result
4.	If not set to **Enabled**, press **[ENTER]** and select **"Enabled"**, then press **[ENTER]**	 **Figure 47 – RBSU – Verify ASR Status is Set to Enabled**
5.	Select **Automatic Power-On**	 **Figure 48 – RBSU – Verify Automatic Power-On is Set to Enabled**
6.	Verify **Automatic Power-On** is set to **Restore Last Power State**	
7.	If not set to **Enabled**, press **[ENTER]** and select **"Enabled"**, then press **[ENTER]**	

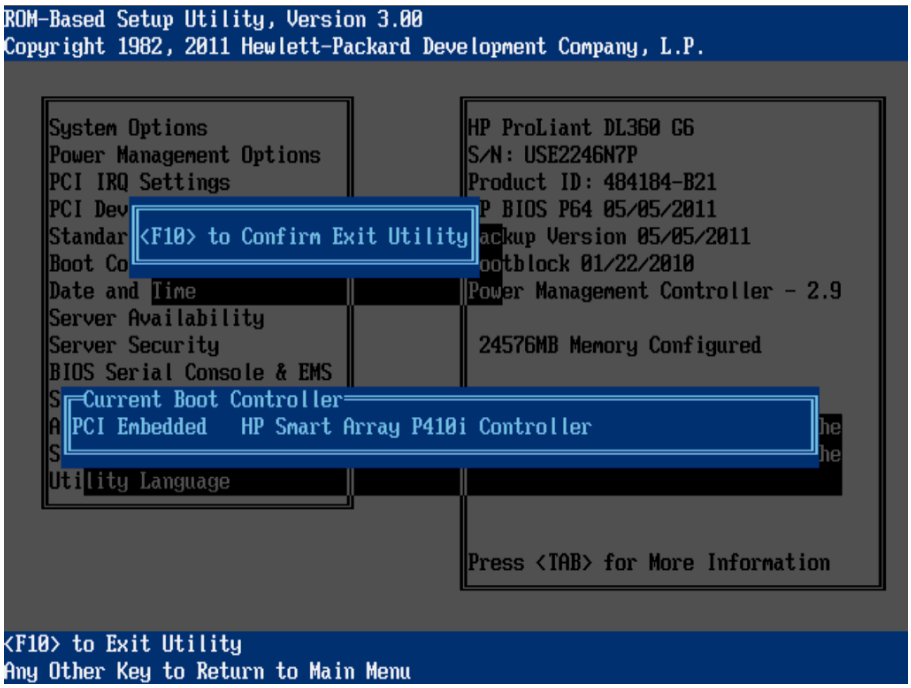
Procedure 31. Verify/Set Server Availability

Step	Procedure	Result
8.	Select **Power-On Delay**	 **Figure 49 – RBSU – Verify Power-On Delay is Set to No Delay**
9.	Verify **Power-On Delay** is set to **No Delay**	
10.	If not set to **Enabled**, press **[ENTER]** and select **"No Delay"**, then press **[ENTER]**	

Prerequisites & Requirements:

- ✓ Tasks within the RBSU have been completed.
- ✓ To **Exit** the **RBSU,** press **<ESC>** and then press **<F10>** to Confirm Exit Utility

Procedure 32. Exit the RBSU

Step	Procedure	Result
11. ☐	While in **RBSU,** set the **Server Availability:** Select "**Server Availability**", then press **[ENTER]**	 **Figure 50 – RBSU – Exit ROM-Based Setup Utility**
12.	**Expected Results:** The BIOS for the server is successfully configured, memory and processors are verified.	

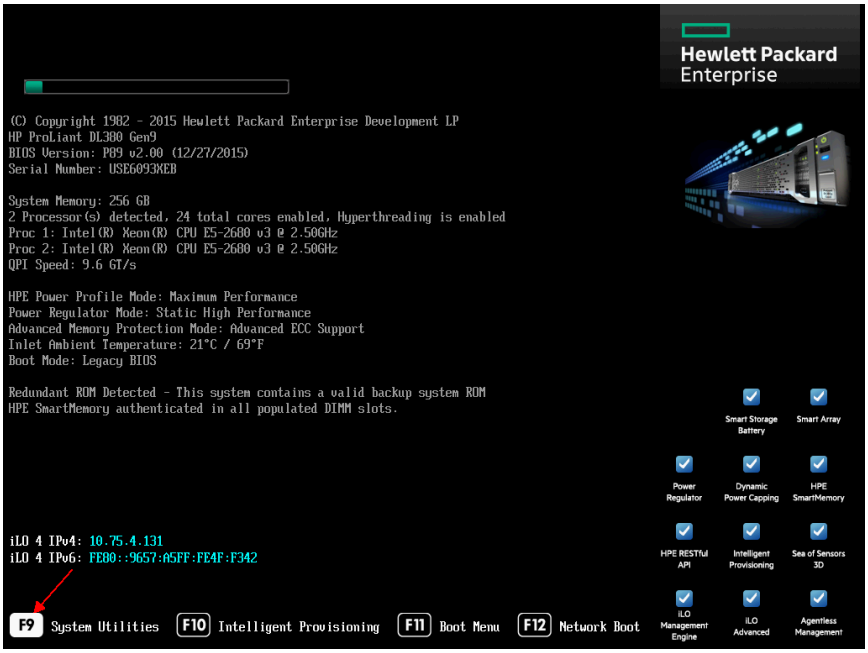
J-2. Gen9: RMS Configure iLO

J.2.1. RMS: Configure iLO

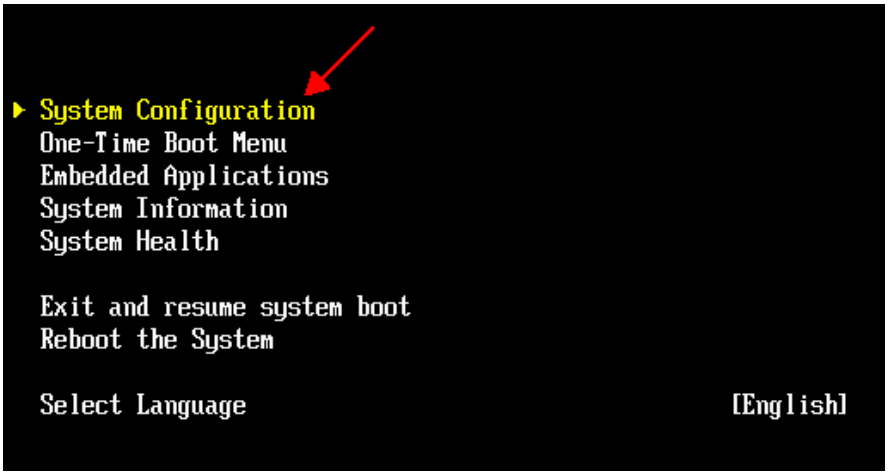
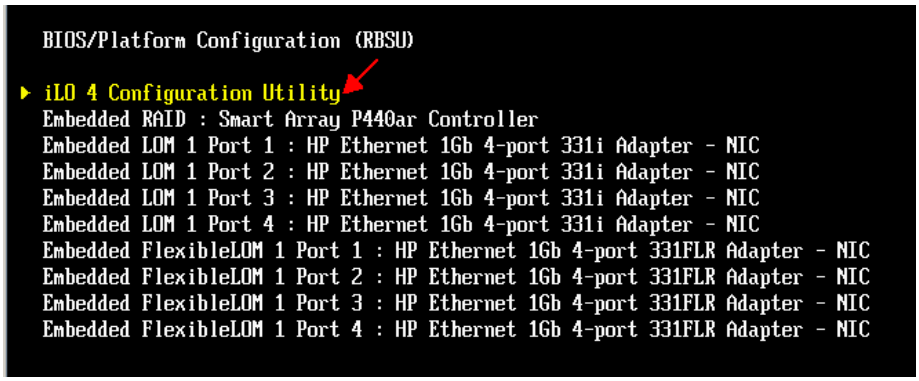
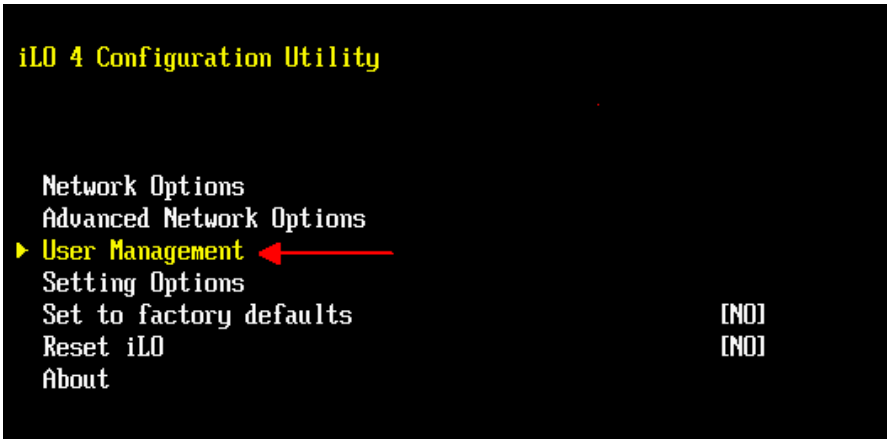
Prerequisites & Requirements:

- ✓ Server powered on
- ✓ Server booting up or rebooted

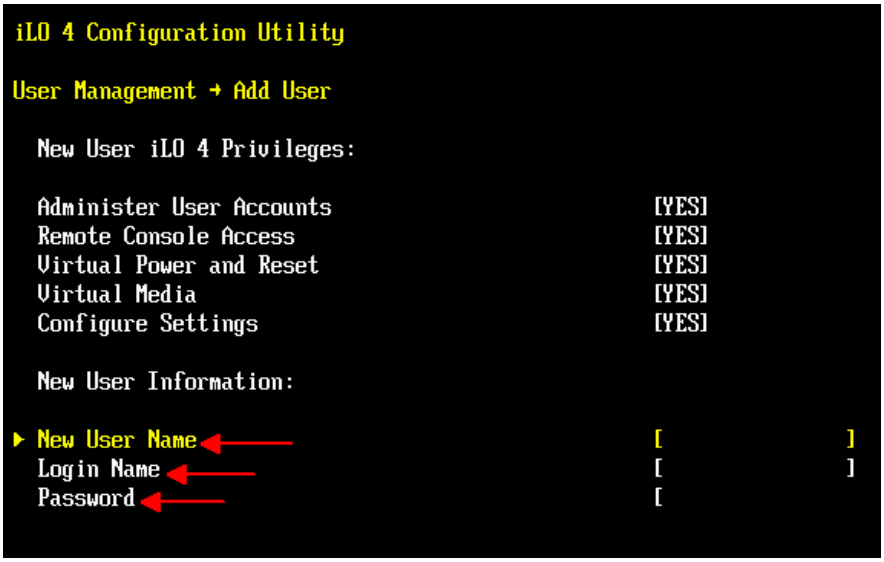
Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
1. ☐	**Reboot the server.** You will see an HP screen as shown below. When prompted with the option to **Press F9** for System Utilities, do so. Once **F9** is pressed, you should see "**F9' selected** on the screen as shown below	 **Figure 51 – Gen9: iLO Configuration – Gen9: Press [F9] to configure**

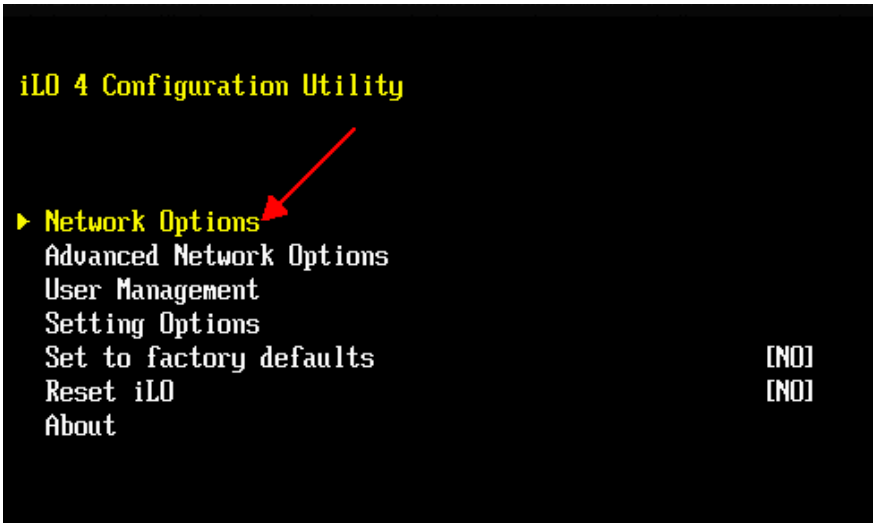
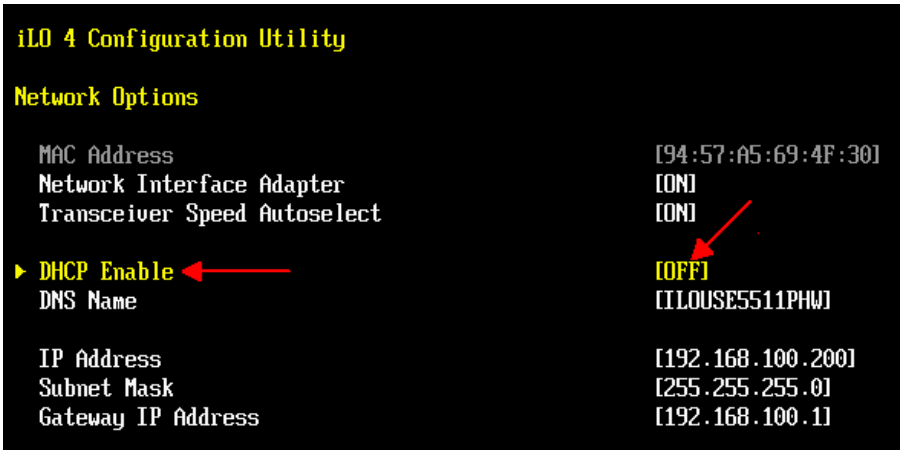
Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
2.	After **F9** is pressed select **System Configuration** then select **iLO 4 Configuration Utility**	 **Figure 52 – Gen9: iLO4 Select System Configuration**  **Figure 53 – Gen9: iLO: Select iLO4 Configuration Utility**
3.	After the initial iLO Configuration Utility screen appears, select **User Management**	 **Figure 54 – Gen9: iLO Configuration – User Management**

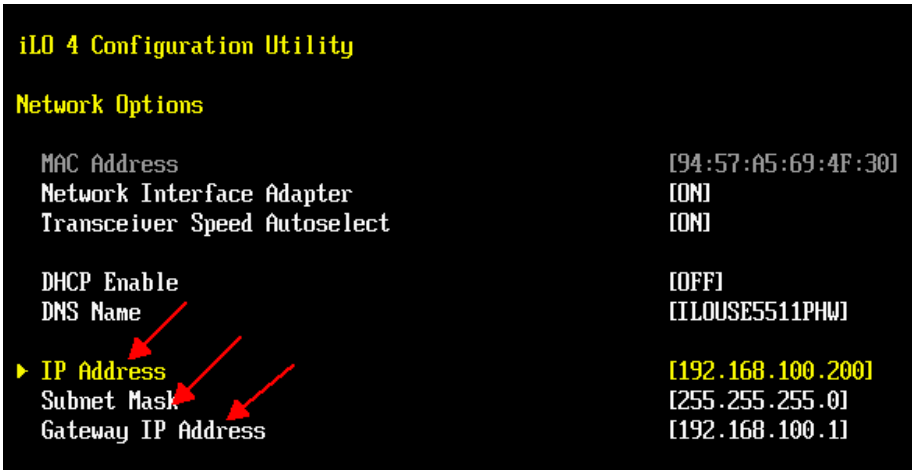
Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
4.	Select **Add User** press **[ENTER]** to add the **admusr** user.	 **Figure 55 – Gen9: iLO Configuration – Add User**
5.	Enter the **New User Name, Login Name and Password** information for **tekelec**: **New User Name:** `tekelec` **Login Name:** `tekelec` **Password:** `tekelec1`	 **Figure 56 – Gen9: iLO Configuration – Add New User Name: tekelec**

Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
6.	Press [ESC] to go back to the iLO 4 Configuration Utility menu, then select Network Options.	 **Figure 57 – Gen9: iLO Configuration – Select Network Options**
7.	Within the Network menu verify that DHCP Enable is set to [OFF]. IF not set to [OFF], press [ENTER] and arrow down to select [OFF] then press [ENTER].	 **Figure 58 – Gen9: iLO Configuration – DHCP Enable to OFF**

Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
8.	Use the arrow keys to move up/down to set the **IP Address**, **Subnet Mask** and **Gateway IP Address** for the server.	IP Address should be set based on the information in the NAPD. **Subnet Mask:** `255.255.255.0` **Gateway IP Address:** `192.168.100.1`  **Figure 59 – Gen9: iLO Configuration – Network Configuration IP, Subnet, Gateway**

Procedure 33. Gen8: Configure the iLO for Rack Mount Server

Step	Procedure	Result
9.	Press **[F10]** to save all changes, **ENTER** "**Y**" to confirm then exit out and reboot the server	 **Figure 60 – Gen9: iLO Configuration – F10 Save Changes**  **Figure 61 – Gen9: iLO Configuration – Change Reboot Message**
10.	Repeat this procedure for other ship loose servers for the work order.	

J.2.2. Gen9: RMS BIOS Configuration, verify processor & memory

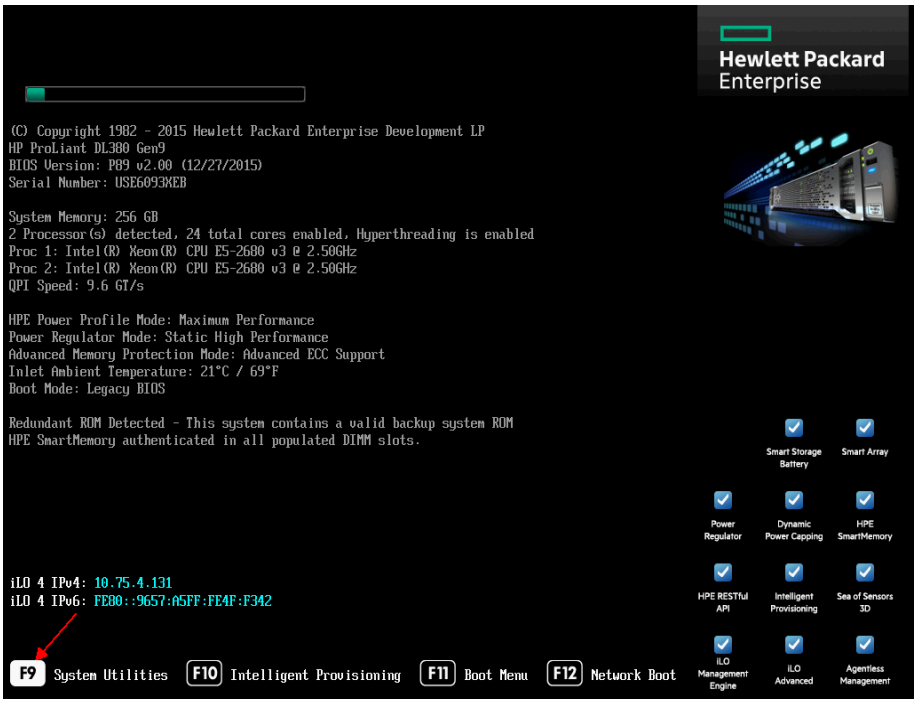
In this section you will be configuring the BIOS on the Rack Mount Server and verifying the processor and memory configuration.

Verify/Configure BIOS Settings and Verify Configured Memory

Prerequisites & Requirements:

- ✓ Server powered on
- ✓ KVM connectivity to the server to get console

Procedure 34. Gen9: Enter the ROM-Based Setup Utility (RBSU)

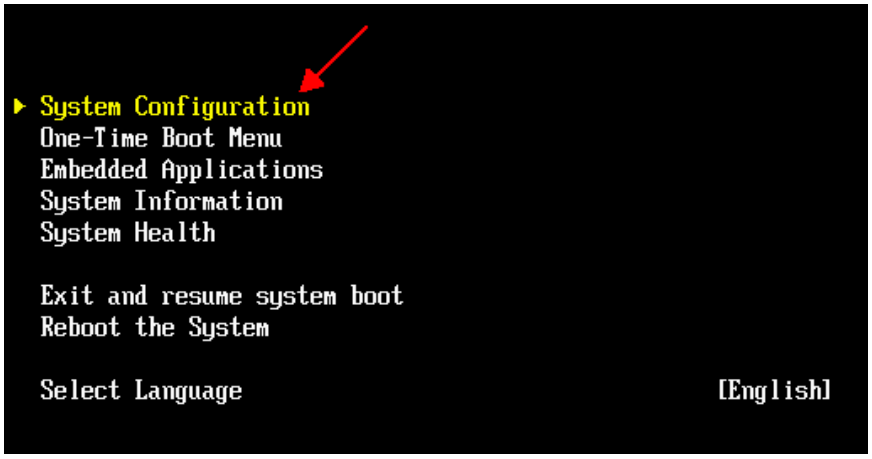
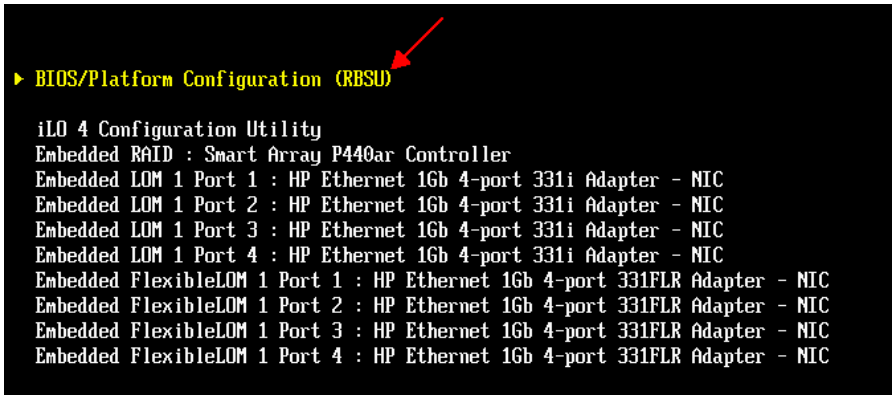
Step	Procedure	Result
1. ☐	**Reboot the server.** You will see an HP screen as shown below. When prompted with the option to **Press F9** for System Utilities, do so. Once **F9** is pressed, you should see "**F9' selected** on the screen as shown below**:**	 **Figure 62 – Gen9 RBSU – Enter RBSU – F9 Pressed indicated in HP Splash Screen**

In this procedure you will be verifying and/or configuring the Serial Port Options for the Embedded and Virtual Serial Ports.

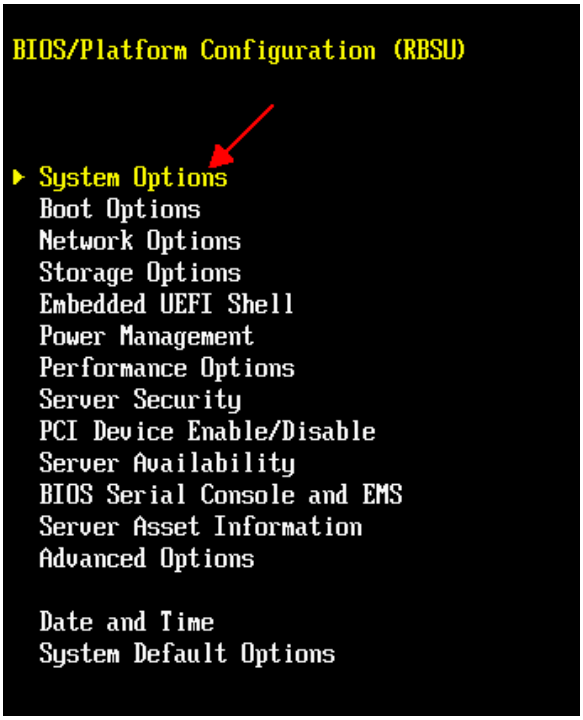
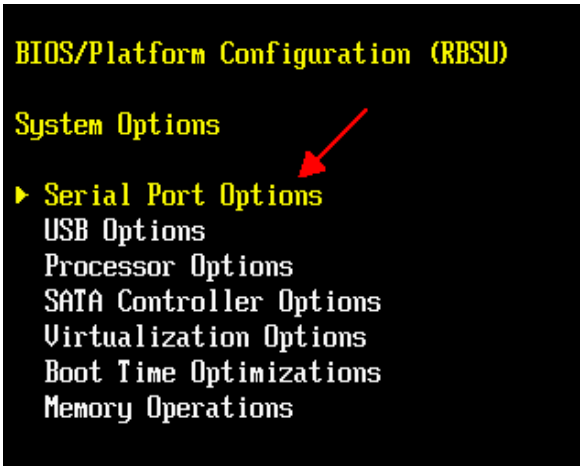
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU mode

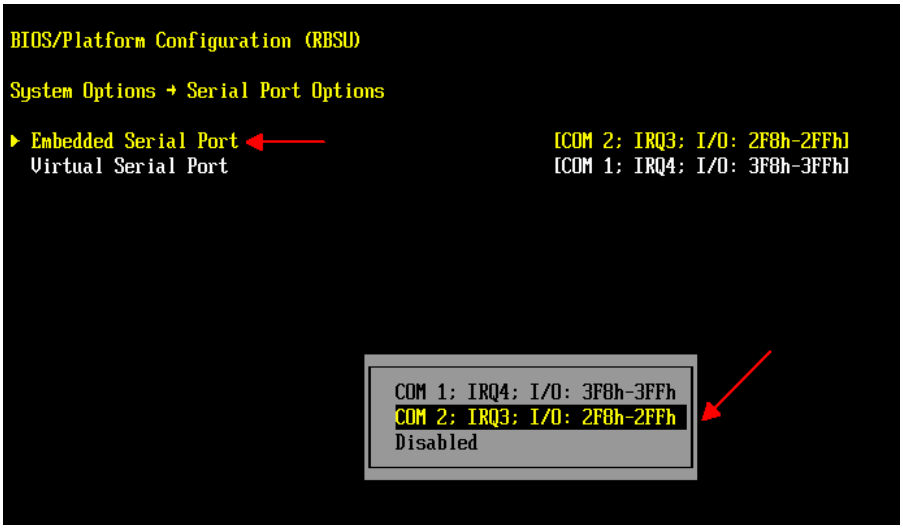
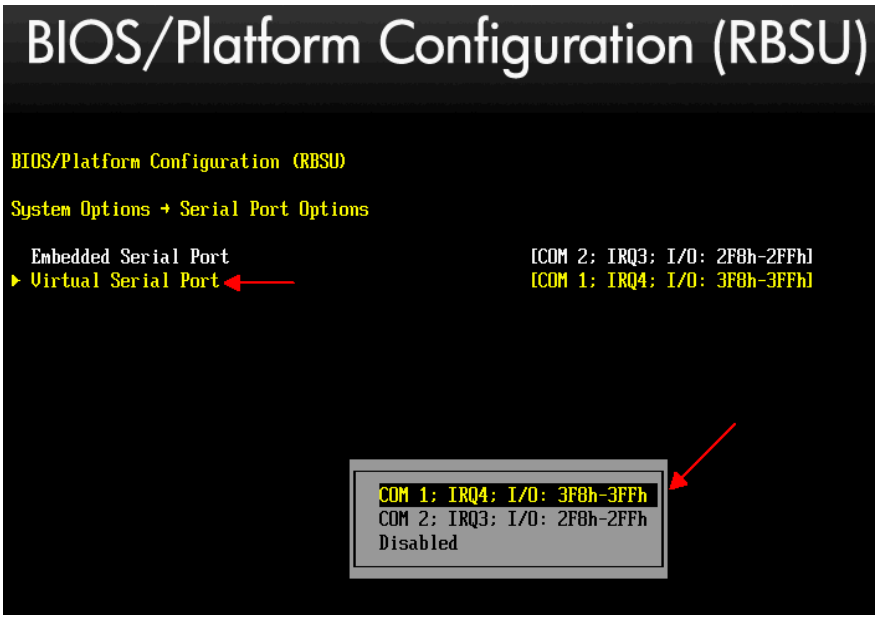
Procedure 35. Gen9: Verify/Configure Serial Port Options

Step	Procedure	Result
1. ☐	Press Enter to go into the **System Configuration** menu then select **BIOS/Platform Configuration (RBSU)**.	 **Figure 63 – Gen9: Select System Configuration**  **Figure 64 – Gen9: Select BIOS/Platform Configuration (RBSU)**

Procedure 35. Gen9: Verify/Configure Serial Port Options

Step	Procedure	Result
2.	Select **System Options** then select **Serial Port Options**	 **Figure 65 – Gen9: ROM-Based Setup Utility – System Options**  **Figure 66 – Gen9: ROM-Based Setup Utility – Serial Port Options**

Procedure 35. Gen9: Verify/Configure Serial Port Options

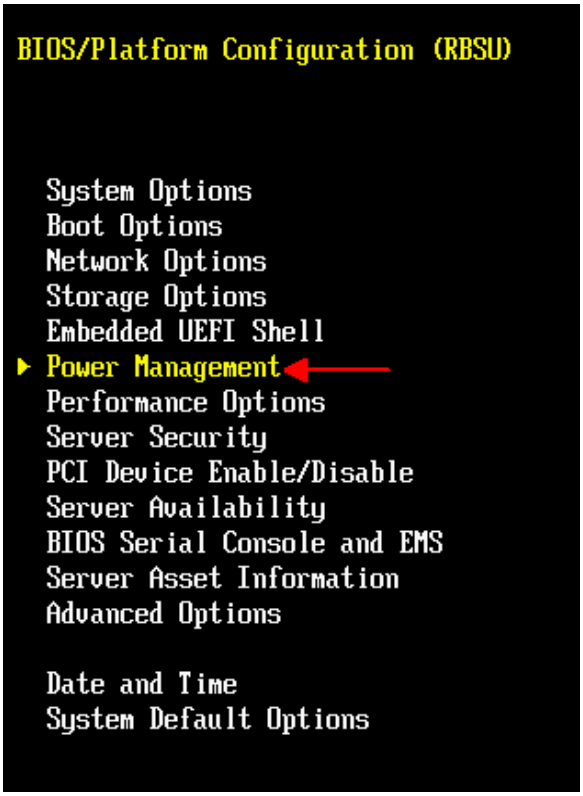
Step	Procedure	Result
3.	Verify the settings for Embedded Serial Port: Select "**Embedded Serial Port**" and verify it is set for "**COM 2".** If it is not set to **COM 2,** press **[ENTER],** select **COM 2,** then **[ENTER]**	 **Figure 67 – Gen9: Verify Embedded Serial Port Setting**
4.	Verify the settings for Virtual Serial Port: Select "**Virtual Serial Port**" and verify it is set for **COM 1.** If it is not set to **COM 1,** press **[ENTER],** select **COM 1,** then **[ENTER]**	 **Figure 68 – Gen9: Verify Virtual Serial Port Setting**

In this procedure you will be configuring **Power Management Options**. The server **HP Power Profile** will be verified/set to **Maximum Performance**.

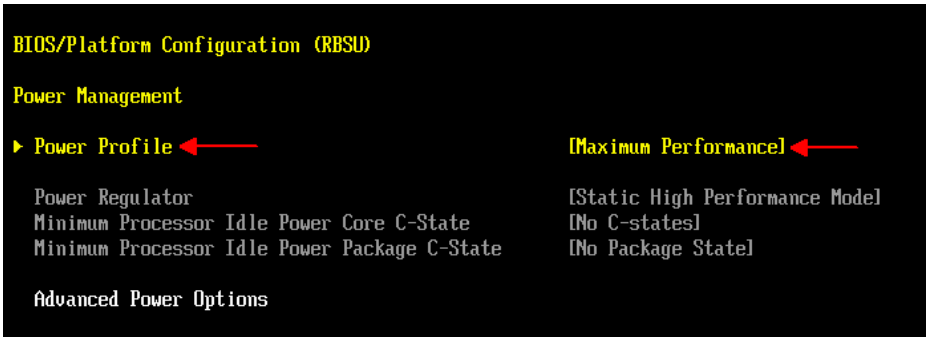
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

Procedure 36. Gen9: Verify/Set Power Management

Step	Procedure	Result
1. ☐	While in RBSU, verify/set the HP Power Profile: Select **Power Management**, then press **ENTER**.	 **Figure 69 – Gen9: RBSU – Select Power Management**

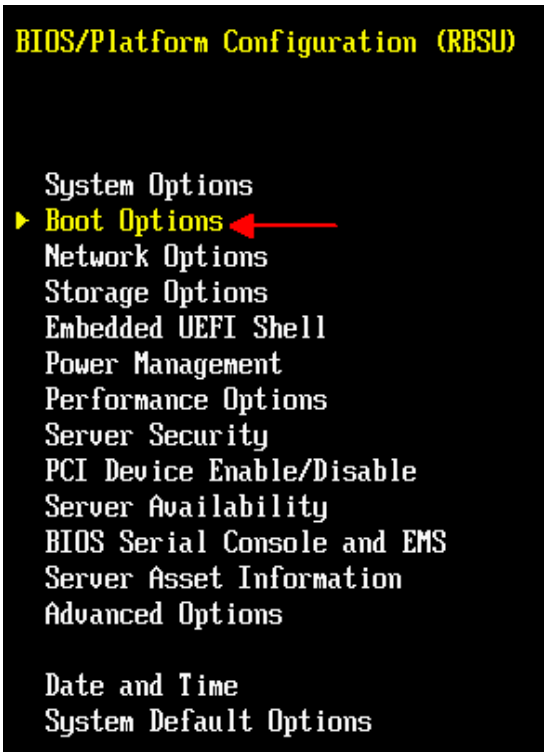
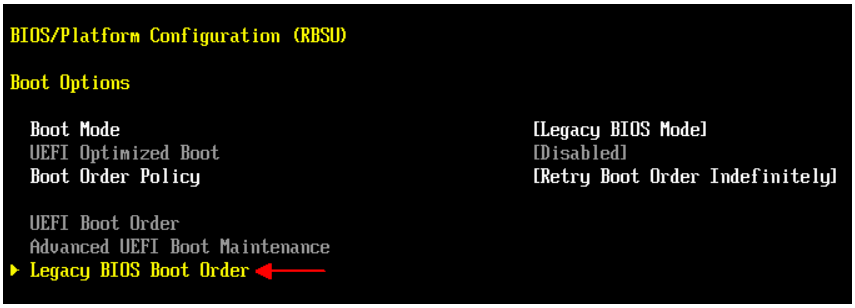
Procedure 36. Gen9: Verify/Set Power Management

Step	Procedure	Result
2.	Several options to choose from display, such as: Power Profile, Power Regulator, Minimum Processor Idle Power Core C-State, Minimum Processor Idle Power Package C-State and Advanced Power Options • Select **Power Profile**. Verify it is set to **Maximum Performance**	 **Figure 70 – Gen9: RBSU – Select HP Power Profile and Maximum Performance**
3.	If not set to **Maximum Performance**, press **ENTER** and select **Maximum Performance**, then press **ENTER**.	

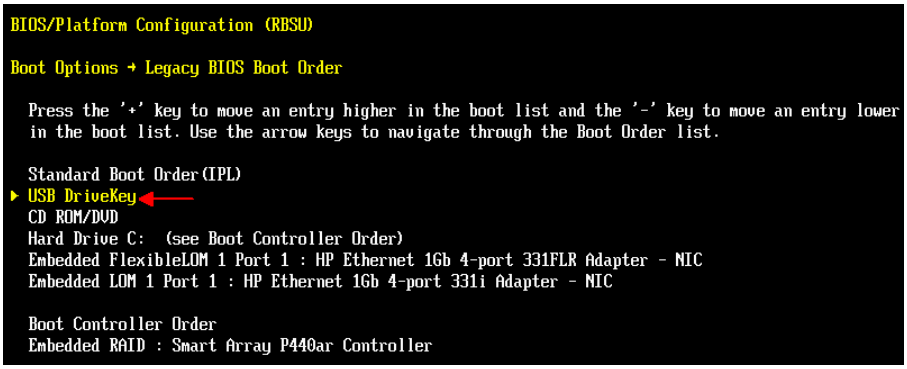
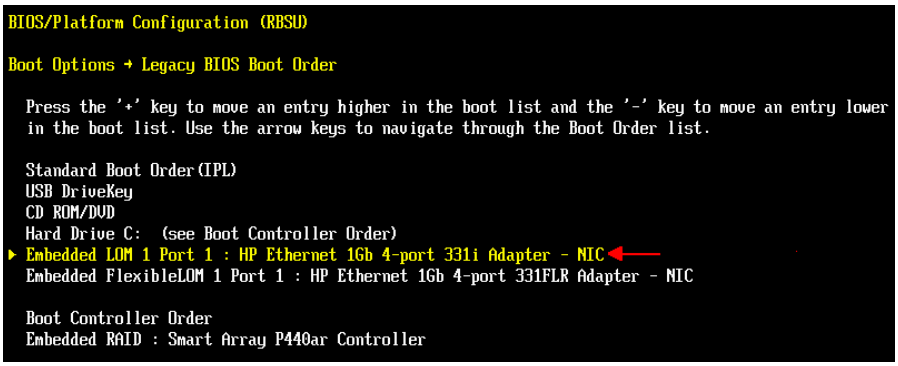
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

Procedure 37. Gen9: Verify/Set Standard Boot Order (IPL)

Step	Procedure	Result
1. ☐	While in RBSU, verify or set the Legacy BIOS Boot Order, Select **Boot Options**, then press **ENTER**, then select **Legacy BIOS Boot Order** then press **ENTER**.	 **Figure 71 – Gen9: Select Boot Options**  **Figure 72 – Gen9: Select Legacy BIOS Boot Order**

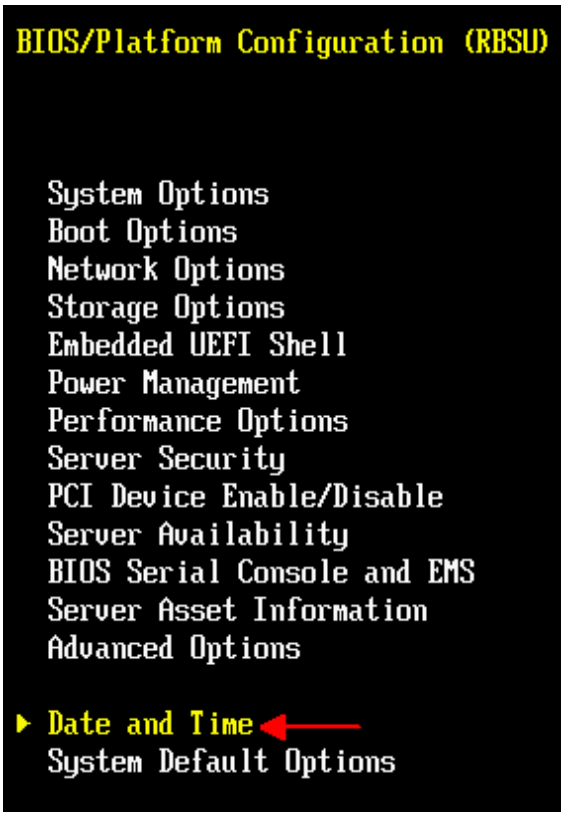
Procedure 37. Gen9: Verify/Set Standard Boot Order (IPL)

Step	Procedure	Result
2.	Verify under **Standard Boot Order (IPL)** that **USB DriveKey** is in the first position and **Embedded LOM** is in the fourth position**.** Press **"+"** or **"-"** to maneuver to the correct position.	**Legacy BIOS Boot Order:** USB DriveKey CD ROM/DVD Hard Drive C Embedded LOM 1 Port 1 Embedded FlexibleLOM 1 Port 1  **Figure 73 – Select Set the IP Device Boot Order USB DriveKey**  **Figure 74 – Select Set the IP Device Boot Order Embedded LOM 1 Port 1**

Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

Procedure 38. Gen9: Verify/Set System Date and Time

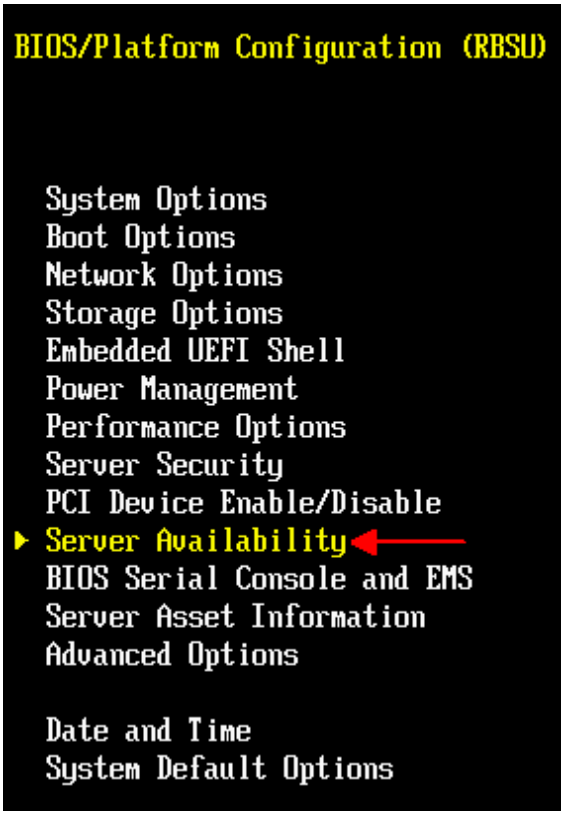
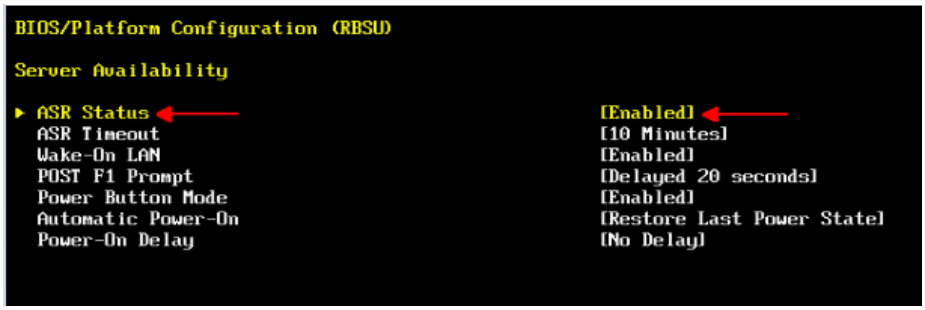
Step	Procedure	Result
1. ☐	While in RBSU, set the system Date and Time: Select **Date and Time**, then press **ENTER**.	 **Figure 75 – Gen9: Select Date and Time**
2.	Set the current Date and Time. Use **UTC** for the time settings. Once the correct Date and Time has been set, press **ENTER** to confirm the settings.	 **Figure 76 – Gen9: Set Date and Time (UTC)**

In this procedure you will be configuring **Server Availability** which determines how the server will behave following a power loss and recovery. The server will be set to **Restore Last Power State** following a power outage and recovery. In addition it will be set to power on with **No Delay**.

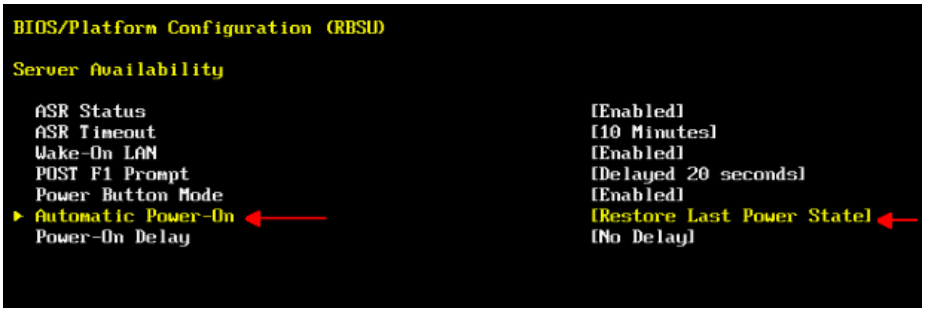
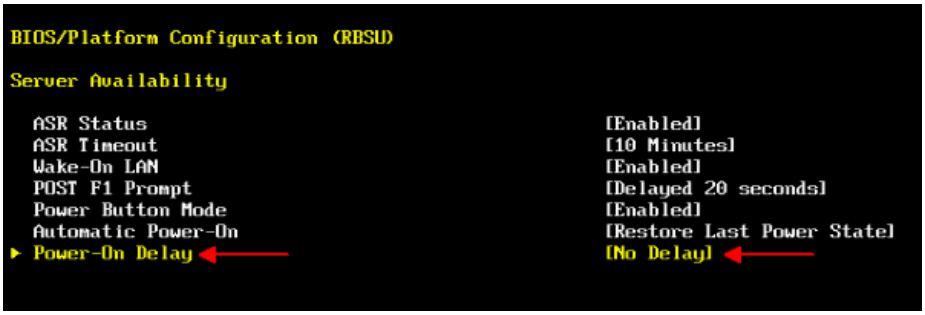
Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

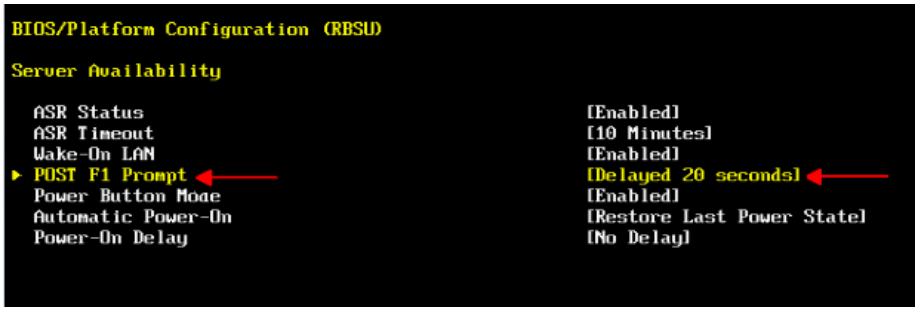
Procedure 39. Gen9: Verify/Set Server Availability

Step	Procedure	Result
1. ☐	While in **RBSU,** set the **Server Availability:** Select "**Server Availability**", then press **[ENTER]**. Several options display, including: ***ASR Status, ASR Timeout, Wake-On LAN, POST F1 Prompt, Power Button Mode, Automatic Power-On*** **and** ***Power-On Delay***. • Select **ASR Status** • Verify it is set to **Enabled**	 **Figure 77 – Gen9: RBSU – Select Server Availability**
2.	If not set to **Enabled**, press **[ENTER]** and select **"Enabled"**, then press **[ENTER]**	 **Figure 78 – Gen9: RBSU – Verify ASR Status is Set to Enabled**

Procedure 39. Gen9: Verify/Set Server Availability

Step	Procedure	Result
3.	Select **Automatic Power-On**	 **Figure 79 – Gen9: RBSU – Verify Automatic Power-On is Set to Restore Last Power State**
4.	Verify **Automatic Power-On** is set to **Restore Last Power State**	
5.	If not set to **Enabled**, press **[ENTER]** and select **"Enabled"**, then press **[ENTER]**	
6.	Select **Power-On Delay**	 **Figure 80 – Gen9: RBSU – Verify Power-On Delay is Set to No Delay**
7.	Verify **Power-On Delay** is set to **No Delay**	
8.	If not set to **Enabled**, press **[ENTER]** and select **"No Delay"**, then press **[ENTER]**	

Procedure 39. Gen9: Verify/Set Server Availability

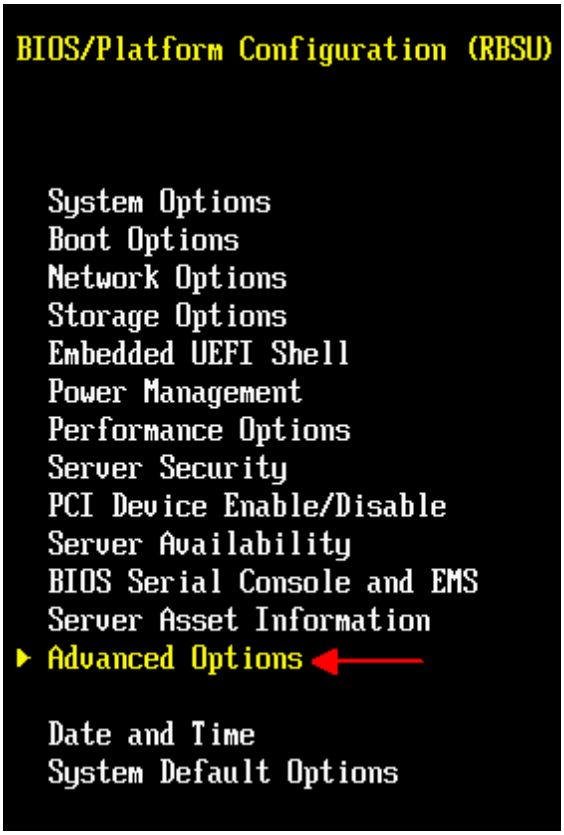
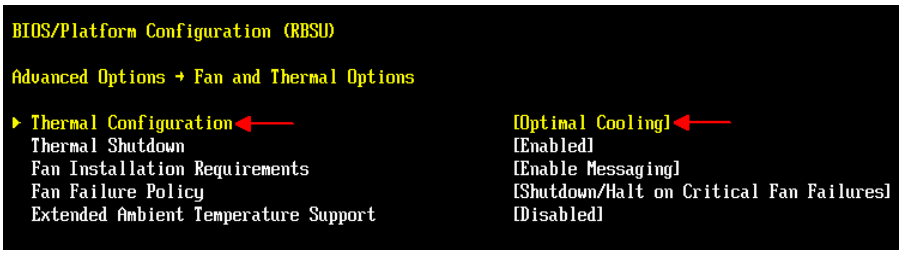
Step	Procedure	Result
9.	Select **POST F1 Prompt**	 **Figure 81 – Gen9: RBSU – Verify Post F1 Prompt is Set to Delayed 20 Seconds**
10.	Verify **Delayed 20 seconds** is set	
11.	If not set to **Delayed 20 seconds**, press **[ENTER]** and select **"Delayed 20 seconds"**, then press **[ENTER]**	

In this procedure you will be configuring **Advanced Options**. The **Fan and Thermal Options** will be verified/set to **Optimal Cooling**.

Prerequisites & Requirements:

- ✓ Server rebooted and in RBSU

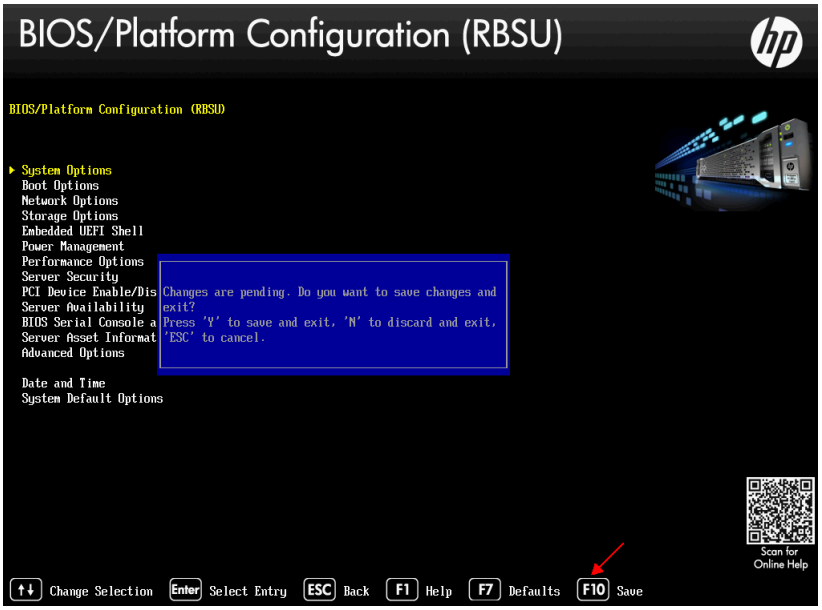
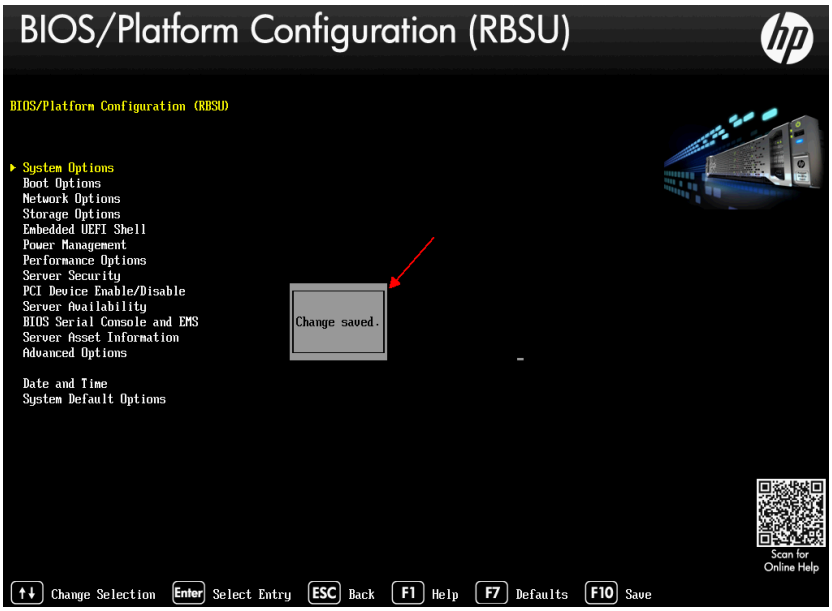
Procedure 40. Gen9: Verify Advanced Options

Step	Procedure	Result
1. ☐	While in **RBSU,** set the **Advanced Options** Select "**Advanced Options**", then press **[ENTER]**. Several options display, including: ROM Selection, Embedded Video Connection, Fan and Thermal Options, Advanced System ROM options. Select **Fan and Thermal Options**.	 **Figure 82 – Gen9: RBSU – Verify Advanced Options**
2.	Verify **Thermal Configuration** is set for **Optimal Cooling**	 **Figure 83 – Gen9: RBSU – Verify Fan and Thermal Options**
3.	If not set to **Optimal Cooling**, press **[ENTER]** and select **"Optimal Cooling"**, then press **[ENTER]**	

Prerequisites & Requirements:

Tasks within the RBSU have been completed.

Procedure 41. Gen9: Save and Exit the RBSU

Step	Procedure	Result
1. ☐	Press **F10** to save changes then Enter **"Y"** to confirm changes**.** the **RBSU,** press **<ESC>** and then press **<F10>** to Confirm Exit Utility	 **Figure 84 – Gen9: RBSU – Save Changes and Confirm**  **Figure 85 – Gen9: RBSU – Changes Saved**

Procedure 41. Gen9: Save and Exit the RBSU

Step	Procedure	Result
2.	To **Exit** the **RBSU and System Utilities,** press **<ESC>** and then press **[ENTER]** to confirm exit	 **Figure 86 – Gen9: Exit System Utilities**
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix K. Accessing My Oracle Support (MOS)

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

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

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

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

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

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

Emergency Response

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

Critical Situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability.
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system.
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations.
- Loss of system ability to provide any required critical or major trouble notification

Other problems severely affecting service, capacity/ traffic, billing, and maintenance capabilities may also be defined as critical by prior discussion and agreement with Oracle.