Oracle® Communications

Diameter Signaling Router

Subscriber Data Server (SDS) Initial Installation and Configuration Guide

Release 8.3

E93224-01

September 2018

ORACLE

Oracle Communications Diameter Signaling Router Subscriber Data Server (SDS) Initial Installation and Configuration Guide, Release 8.3.

Copyright © 2018 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. Windows® 7 and Windows® XP are trademarks or registered trademarks of Microsoft Corporation.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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

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

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

Table of Contents

1. Introduction 7
1.1 References 7
1.2 Acronyms 7
1.3 Assumptions 8
1.4 XML Files 8
1.5 How to Use This Document 8
2. Pre-Installation Setup 9
2.1 Installation Prerequisites 9
2.2 Physical Connections 10
2.3 Access Alternatives for Application Install 11
2.4 Activity Logging 11
2.5 Firmware and BIOS Settings 11
2.5.1 Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware 12
3. Installation Matrix 12
3.1 Install SDS on the Customer Network 12
4. Application Installation 14
4.1 Install the SDS Application (All SDS NOAM Sites) 14
5. Configuration Procedures 21
5.1 Configure SDS A and B (1st SDS NOAM Site Only) 21
5.2 OAM Pairing (1st SDS NOAM Site Only) 35
5.3 Query Server Installation (All SDS NOAM Sites) 43
5.4 OAM Installation for the DR SDS NOAM Site 56
5.5 OAM Pairing for DR SDS NOAM Site 68
5.6 Add SDS Software Images to PMAC Servers (All SOAM Sites) 73
5.7 OAM Installation for SOAM Sites (All SOAM Sites) 76
5.8 OAM Pairing for SDS SOAM Sites (All SOAM Sites) 96
5.9 DP Installation (All SOAM Sites) 101
5.10 Configure ComAgent 118
Appendix A. Access the iLO VGA Redirection Window 120
Appendix B. Create a Temporary External IP Address to Access SDS GUI 120
Appendix C. Establish a Local Connection for Accessing the SDS GUI 122
Appendix D. Configure Cisco 4948E-F Aggregation Switches 125
D.1 Verify Cisco Switch Wiring (All SDS NOAM Sites) 126
D.2 Configure Cisco 4948E-F Aggregation Switches 128
D.3 Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites) 151
Appendix E. Create an XML File for Installing Network Elements 160
Appendix F. Install NetBackup Client 163
Appendix G. List of Frequently Used Time Zones 164

Appendix H. Accept Installation from SDS NOAM GUI 166

Appendix I. Disable Hyperthreading for Gen8 and Gen9 (DP Only) 167

Appendix J. Configure the HP DL380 (GEN8 and GEN9) Server CMOS Clock/BIOS Settings 177

J.1 Gen8: Configure the ILO for Rack Mount Server 177

J.1.1 RMS: Configure iLO 177

J.1.2 Gen8: RMS BIOS Configuration, Verify Processor and Memory 180

J.2 Gen9: RMS Configure ILO 188

J.2.1 RMS: Configure iLO 188

J.2.2 Gen9: RMS BIOS Configuration, Verify Processor and Memory 193

J.2.2.1 Gen9: Enter the ROM-Based Setup Utility (RBSU) 193

J.2.2.2 Gen9: Verify/Configure Serial Port Options 194

Appendix K. Install OS IPM on Servers 205

Appendix L. My Oracle Support (MOS) 208

List of Tables

Table 1. Acronyms 7

Table 2. SDS Installation Matrix 13

Table 3. List of Procedures for a SDS Installation 13

Table 4. 4948-F Aggregation Switch Variables 128

Table 5. SDS Network Element Configuration File (IPv4) 161

Table 6. SDS Network Element Configuration File (IPv6) 162

Table 7. List of Selected Time Zone Values 164

List of Figures

Figure 1. Example of a Procedure Steps Used in This Document 9

Figure 2. HP DL380 Gen8, DC (Rear Panel) 10

Figure 3. HP DL380 (Gen9), DC (Rear Panel) 10

Figure 4. HP DL380 Gen8, Front Panel (USB Port) 16

Figure 5. HP DL380 Gen9, Front Panel (USB Port) 16

Figure 6. HP DL380 Gen8, Front Panel (USB Port) 29

Figure 7. HP DL380 Gen9, Front Panel (USB Port) 29

Figure 8. HP DL380 Gen8, Rear Panel (Ethernet) 34

Figure 9. HP DL380 (Gen9), DC (Rear Panel) 34

Figure 10. Cisco 4948E-F Switch (Maintenance Access Port) 34

Figure 11. HP DL380 Gen8, Front Panel (USB Port) 48

Figure 12. HP DL380 Gen9, Front Panel (USB Port) 48

Figure 13. HP DL380 Gen8, Front Panel (USB Port) 63
Figure 14. HP DL380 Gen9, Front Panel (USB Port) 63
Figure 15. HP DL380p Gen8 Backplane 123
Figure 16. HP DL380 (Gen9), DC (Rear Panel) 123
Figure 17. SDS Frame Layout 125
Figure 18. Cisco 4948E-F Switch ISL Connections – Switch 1B (Top) to Switch 1A (Bottom) 126
Figure 19. Cisco 4948E-F Switch (Console Port) 126
Figure 20. HP DL380 Gen8, Rear Panel (Quad-Serial Ports) 127
Figure 21. HP DL380 Gen8, Rear Panel (Ethernet) 127
Figure 22. Cisco 4948E-F Switch (Console Port) 127
Figure 23. HP DL380 (Gen9), DC (Rear Panel) 128
Figure 24. HP DL380 Gen8, Front Panel (USB Port) 152
Figure 25. HP DL380 Gen9, Front Panel (USB Port) 152
Figure 26. Boot from Media Screen, TPD 7.0.0.0.0 205
Figure 27. Kernel Loading Output 206
Figure 28. File System Creation Screen 206
Figure 29. Package Installation Screen 207
Figure 30. Installation Statistics Screen 207
Figure 31. Installation Complete Screen 208
Figure 32. Boot Loader Output 208

List of Procedures

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware 12
Procedure 2. Install the SDS Application (All SDS NOAM Sites) 14
Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only) 21
Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only) 35
Procedure 5. Configure the Query Server (All SDS NOAM Sites) 43
Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only) 56
Procedure 7. Pair the DR SDS NOAM Servers (DR SDS NOAM Site Only) 68
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites 73
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites) 77
Procedure 10. Pair the SDS SOAM Servers (All SOAM Sites) 96
Procedure 11. Install the Data Processor Blade (All SOAM Sites) 101
Procedure 12. Configure ComAgent (All SOAM Sites) 118
Procedure 13. Access the iLO VGA Redirection Window 120
Procedure 14. Create a Temporary External IP Address to Access SDS GUI 121

Procedure 15. Establish a Local Connection for Accessing the SDS GUI 122
Procedure 16. Verify Cisco Switch Wiring 126
Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites) 129
Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites) 151
Procedure 19. Install NetBackup Client 163
Procedure 20. Accept Installation from SDS NOAM GUI 166
Procedure 21. Gen8: Disable Hyperthreading 167
Procedure 22. Gen9: Disable Hyperthreading 172
Procedure 23. Gen8: Configure the Integrated Lights Out (iLO) for Rack Mount Server 177
Procedure 24. Enter the ROM-Based Setup Utility (RBSU) 180
Procedure 25. Verify/Configure Serial Port Options 181
Procedure 26. Verify/Set Power Management 182
Procedure 27. Verify/Set Standard Boot Order (IPL) 183
Procedure 28. Verify/Set Server Availability 185
Procedure 29. Exit the RBSU 187
Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS) 188
Procedure 31. Verify/Configure BIOS Settings and Verify Configured Memory 193
Procedure 32. Verify/Configure Serial Port Options 194
Procedure 33. Gen9: Verify/Set Power Management 197
Procedure 34. Gen9: Verify/Set Standard Boot Order (IPL) 198
Procedure 35. Gen9: Verify/Set System Date and Time 200
Procedure 36. Gen9: Verify/Set Server Availability 201
Procedure 37. Gen9: Verify/Advanced Options 203
Procedure 38. Gen9: Save and Exit RBSU 204
Procedure 39. Install OS IPM on Servers 205

1. Introduction

This document describes how to install the Oracle® Communications Diameter Signaling Router Subscriber Data Server (SDS) within a customer network. It makes use of the Platform 8.3 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 8.3 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 1.1, References.

1.1 References

[1] DSR C-Class Hardware and Software Installation Part 1

[2] DSR Software Installation & Configuration Procedure 2/2

[3] HP Solutions Firmware Upgrade Pack Release Notes, (2.2.12 or higher)

[4] Tekelec Platform Configuration Guide

[5] Platform Management and Configuration Guide

[6] TPD Initial Product Manufacture Software Installation Procedure, Latest Revision

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Description
DL	Data Link
DP	Data Processor blade
DR	Disaster Recovery
DSR	Diameter Signaling Router
HP	Hewlett Packard
IEEE	Institute of Electrical and Electronics Engineers
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NAPD	Network Architecture Planning Document
NE	Network Element
NOAM	Network Operations, Administration & Maintenance
iLO	HP Integrated Lights-Out
IP	Internet Protocol
IPM	Initial Product Manufacture
POC	Point of Contact

Acronym	Description
SDS	Subscriber Data Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
USB	Universal Serial Bus
VIP	Virtual IP
XMI	External Management Interface
XML	Extensible Markup Language

1.3 Assumptions

This procedure assumes the following;

- The user has reviewed the latest Network Architecture Planning Document (NAPD) 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 and used them to compile XML files (see Appendix E) for each SDS and SOAM site's NE before attempting to execute this procedure.
- The user conceptually understands DSR topology and SDS network configuration as described in the latest Customer specific DSR Network Planning document.
- 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 SDSs were IPM'ed with TPD Platform 7.6 of correct version as described in [6].

1.4 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.

1.5 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.

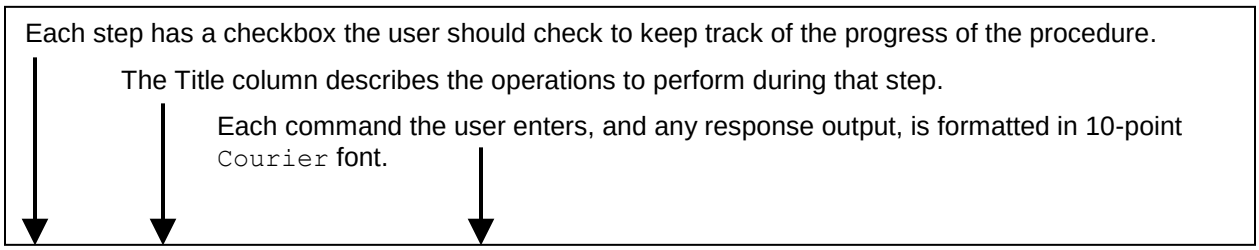
When executing this document for either purpose, there are a few points which help to ensure that the user understands the author's intent. These points are as follows;

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 L My Oracle Support (MOS), for information on contacting Oracle Customer Support.

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 through 3, and step 3.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Where it is necessary to explicitly identify the server on which a particular step is to be taken, the server name is given in the title box for the step (for example, “ServerX” in step 2 Figure 1).



	Title	Directive/Result Step
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	**ServerX**: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. `$ cu -l /dev/ttyS7`
3. ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 3. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example of a Procedure Steps Used in This Document

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 passwor
- TPD “admusr” user password

Note: When using the iLO for SSH connectivity, supported terminal Emulations are VT100 or higher (for example, 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.

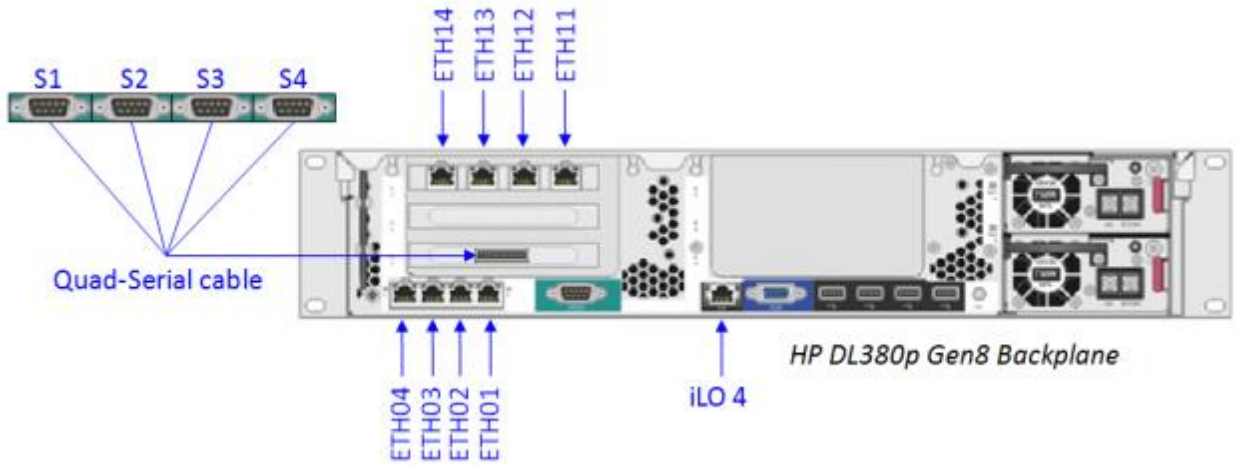


Figure 2. HP DL380 Gen8, DC (Rear Panel)

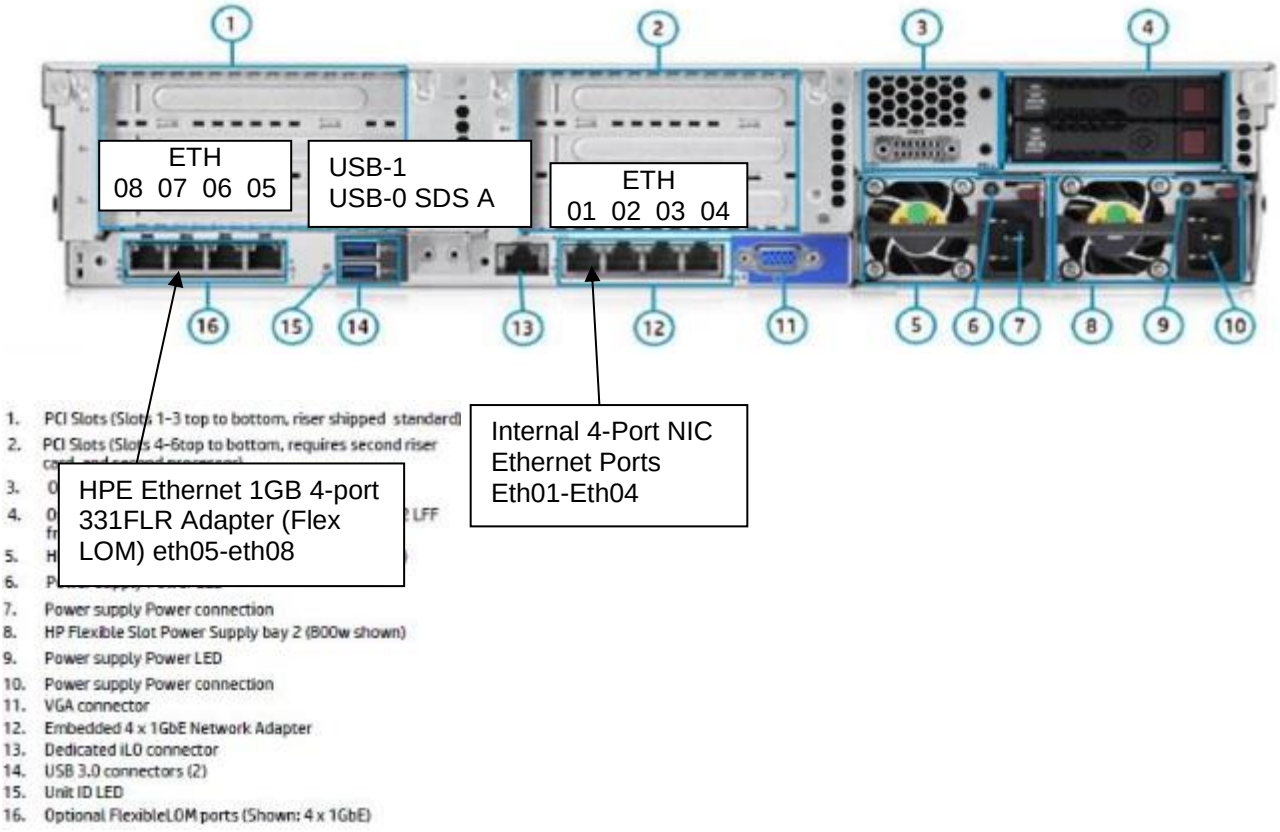


Figure 3. HP DL380 (Gen9), DC (Rear Panel)

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** may be used to initiate and monitor the SDS installation. ***Note:*** Methods 3 and 4 may only be used on a 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 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

Before 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 7.6.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 7.6.x is HP Solutions Firmware Upgrade Pack 2.2.12 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 7.6.x minimum of HP FUP 2.2.12 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 MISC Firmware ISO image

Refer to the Release Notes of the [3] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x, and (Min 2.2.12) to determine specific firmware versions needed.

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

2.5.1 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**	
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 i • Appendix J.2.2 Gen9: RMS BIOS Configuration, Verify Processor and 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 [3] HP Solutions Firmware Upgrade Pack Release Notes, (2.2.12 or higher).
3. ☐	**RMS Server**: CMOS clock, BIOS settings, and iLO IP address have been configured and firmware updated	Check off the associated checkbox in step 3 as the RMS server's CMOS clock, BIOS settings, and iLO IP address are 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. ☐	Repeat (optional)	Repeat on the disaster recovery RMS servers.

3. Installation Matrix

3.1 Install 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 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. List of Procedures for a SDS Installation

Procedure Number	Title	Page Number
Procedure 2	Install the SDS Application (All SDS NOAM Sites)	14
2	Configure SDS A and B (1st SDS NOAM Site Only)	21
3	OAM Pairing (1st SDS NOAM Site Only)	35
4	Query Server Installation (All SDS NOAM Sites)	43
5	OAM Installation for the DR SDS NOAM Site	56
6	OAM Pairing for DR SDS NOAM Site	68
7	Add SDS Software Images to PMAC Servers (All SOAM Sites)	73
8	OAM Installation for SOAM Sites (All SOAM Sites)	76
9	OAM Pairing for SDS SOAM Sites (All SOAM Sites)	96
10	DP Installation (All SOAM Sites)	101
11	Configure ComAgent	118
E.1	Figure 17. SDS Frame Layout	125
E.2	Configure Cisco 4948E-F Aggregation Switches	128
E.3	Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)	151
J	Disable Hyperthreading for Gen8 and Gen9 (DP Only)	167

4. Application Installation

4.1 Install the SDS Application (All SDS NOAM Sites)

Note: If servers are not loaded with OS (TPD), refer Appendix K for installing it.

Procedure 2. Install the SDS Application (All SDS NOAM Sites)		
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. ☐	**HP DL 380 Server**: Login	1. Access the command prompt.
		2. Log into the HP server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

3. ☐	**HP DL 380 Server**: Verify the date and time	Verify the date and time are displayed in GMT (+/- 4 min.).
		`$ date -u`
		`Wed Oct 22 14:07:12 UTC 2014`

		If the correct date and time (in GMT) are not shown in step 3. , then stop this procedure and perform Appendix J Configure the HP DL380 (GEN8 and GEN9) Server CMOS Clock/BIOS Settings and restart this procedure from the beginning. If the correct date and time (in GMT) are shown in step 3. , then continue with step 4. of this procedure.

4. ☐	**HP DL 380 Server**: Verify the TPD release	Verify the TPD release is 7.6.
		`$ getPlatRev`
		`7.6.0.0.0_88.54.0`

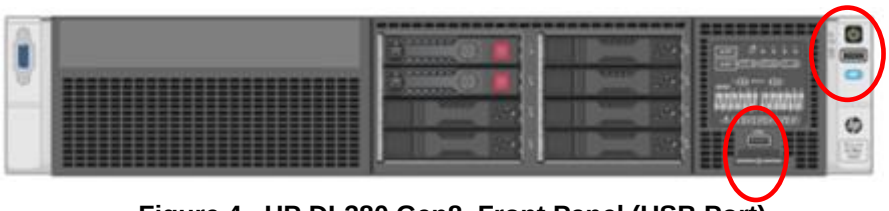
5. ☐	**HP DL 380 Server**: Verify alarm status	Execute the alarmMgr command to verify if there are any alarms on the server. `$ alarmMgr --alarmStatus` ***Note:*** This command should return no output on a healthy system. If any alarms are reported as SNMP traps, stop and contact My Oracle Support (MOS) for the assistance.

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

6. ☐	**HP DL 380 Server**: Verify system state	Execute the syscheck command to verify the state 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`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

7. ☐	**HP DL 380 Server**: Verify health of the server	Execute the verifyUpgrade command to verify the health of the server.
		`$ sudo verifyUpgrade`
		Disregard this error:
		`ERROR: No upgrade/patching transaction has been performed on this system!`
		`(/usr/share/tomcat6/webapps/ohw.war)`
		Note: This command should return no output on a healthy system. If any error are reported, stop and contact My Oracle Support (MOS) for the assistance.

8. ☐	**HP DL 380 Server**: Verify hardware ID	Verify hardware ID is ProLiant DL380 Gen8 or Gen9.
		`$ hardwareInfo | grep Hardware`
		`Hardware ID: ProLiantDL380pGen8`
		or
		`Hardware ID: ProLiantDL380Gen9`

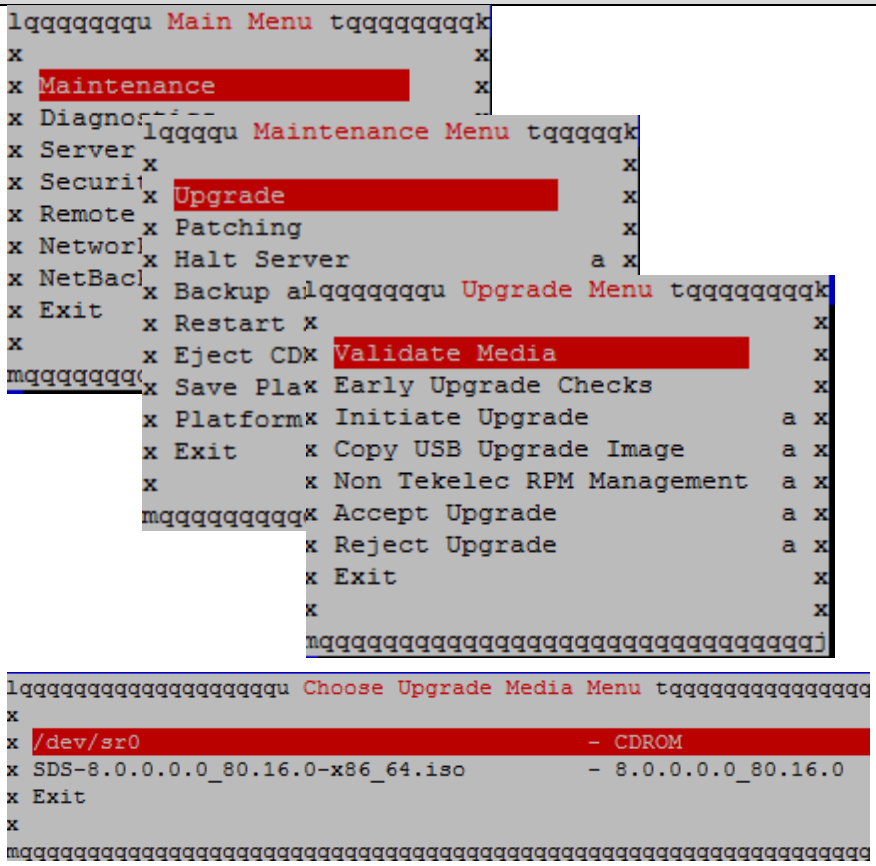
Procedure 2. Install the SDS Application (All SDS NOAM Sites)		
9. ☐	**HP DL 380 Server**: Load software	Insert the USB drive containing the SDS application software into the server's USB port.  **Figure 4. HP DL380 Gen8, Front Panel (USB Port)** **Figure 5. HP DL380 Gen9, Front Panel (USB Port)**

10. ☐	**HP DL 380 Server**: Verify software directory	Verify the USB drive has been mounted under the /media directory.
		`$ df |grep sdb`
		`/dev/sdb1 2003076 8 2003068 1% /media/sdb1`

11. ☐	**HP DL 380 Server**: Verify target release	Verify the target release is available on the USB drive.
		`$ ls /media/sdb1/`
		`SDS-8.3.0.0.0_83.15.0-x86_64.iso`

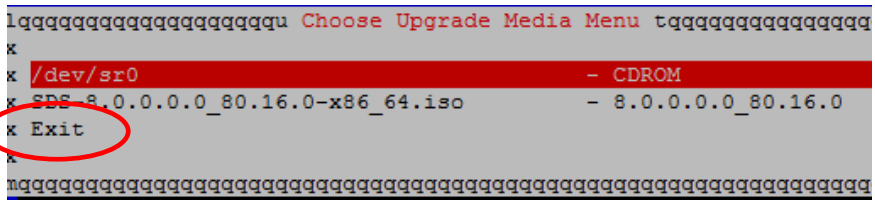
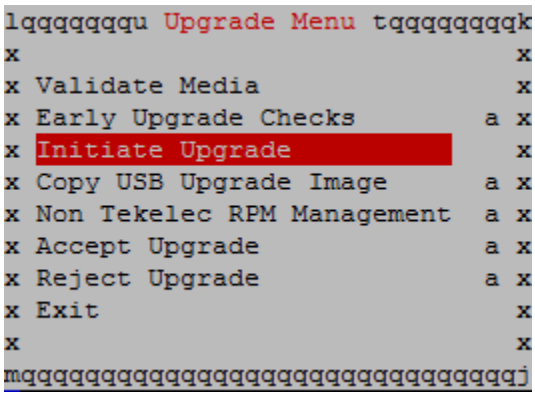
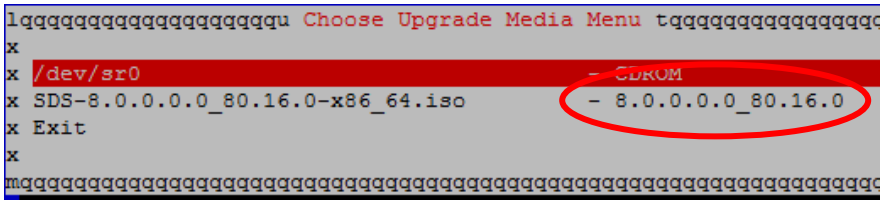
12. ☐	**HP DL 380 Server**: Copy software to directory	Copy the target release to the server's hard disk under the /var/TKLC/upgrade directory. `$ cp -p /media/sdb1/SDS-8.3.0.0.0_80.16.0-x86_64.iso /var/TKLC/upgrade/`
13. ☐	**HP DL 380 Server**: Unmount USB	1. Unmount the USB drive partition. `$ sudo umount /media/sdb1` 2. Remove the USB drive from the server's front panel.
14. ☐	Log into the platcfg utility	`$ sudo su - platcfg`
15. ☐	Validate the software	1. Navigate to **Maintenance > Upgrade > Validate Media**.

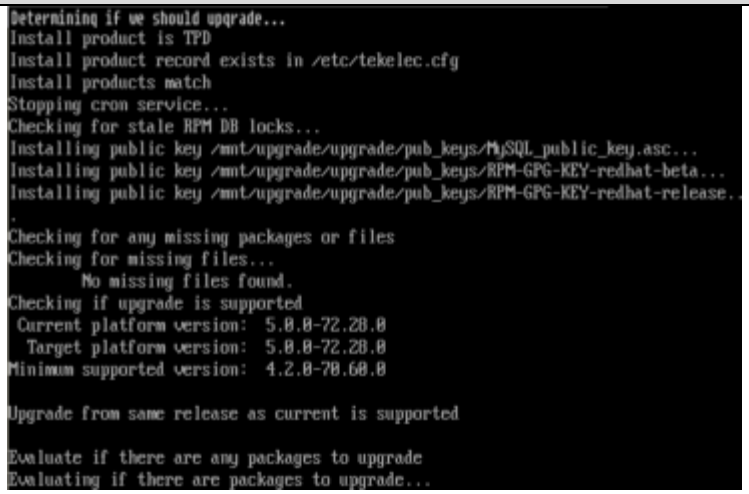
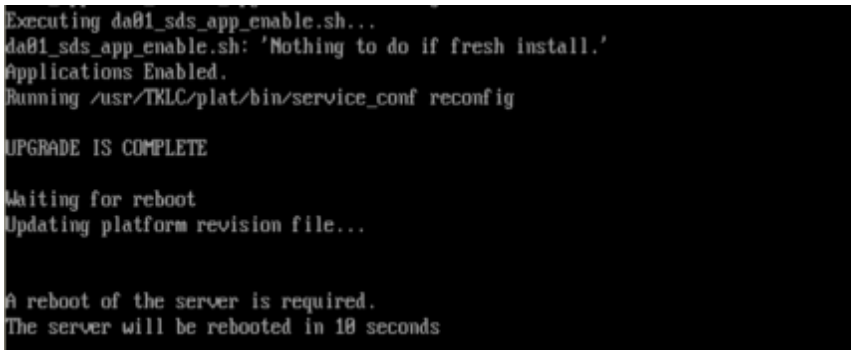
Procedure 2. Install the SDS Application (All SDS NOAM Sites)



2. Select ISO and press **Enter**.

```
Validating cdrom...
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
############################################################
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
```

Procedure 2. Install the SDS Application (All SDS NOAM Sites)		
		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. 3. When the screen displays the ISO as validated, press the ANY key. 4. Select **Exit** and press **Enter**. 
16. ☐	Initiate the upgrade	1. Select **Initiate Upgrade** and press **Enter**.  2. Verify the SDS application release matches the target release.  3. Press **Enter** to install the SDS application. Output similar to this may display.

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

17. ☐	**HP DL 380 Server**: Login	After the server has completed the reboot, log into the HP server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

18. ☐	Verify a successful installation	Verify the output contains the **Upgrade is Complete** line to indicate a successful installation of the SDS application software.
		`$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`
		`1321462900::  UPGRADE IS COMPLETE`

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

19. ☐	Verify upgrade status	1. Execute the verifyUpgrade command to verify the status of the upgrade.
		`$ sudo verifyUpgrade`
		`Disregard following error during this command execution`
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1513202476::zip error: Nothing to do!`
		`(/usr/share/tomcat6/webapps/ohw.war)`
		Note: This command should return no output on a healthy system. If any error are reported, please stop and contact My Oracle Support (MOS) for the assistance.
		2. Verify the SDS application release shown matches the target release.
		`$ rpm -qa |grep sds`
		`TKLCsds-8.1.0.0.0_80.16.0.x86_64`

20. ☐	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`

21. ☐	Put the server in trusted time mode	`$ tw.setdate –trusted` `Current time: 10/22/2014 16:25:07.869`
22. ☐	Exit	Exit from the command line to return to the server console to the login prompt. `$ exit`
23. ☐	Repeat	Repeat this procedure for each RMS server (such as, SDS NOAM A, SDS NOAM B, Query server) installed in the cabinet before continuing with the next procedure

5. Configuration Procedures

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

This procedure assumes:

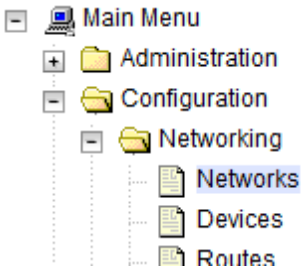
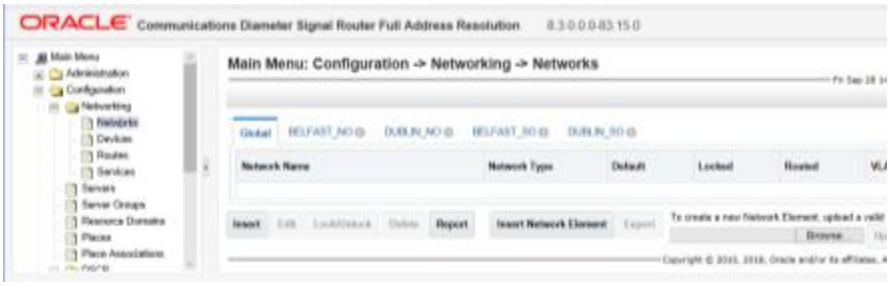
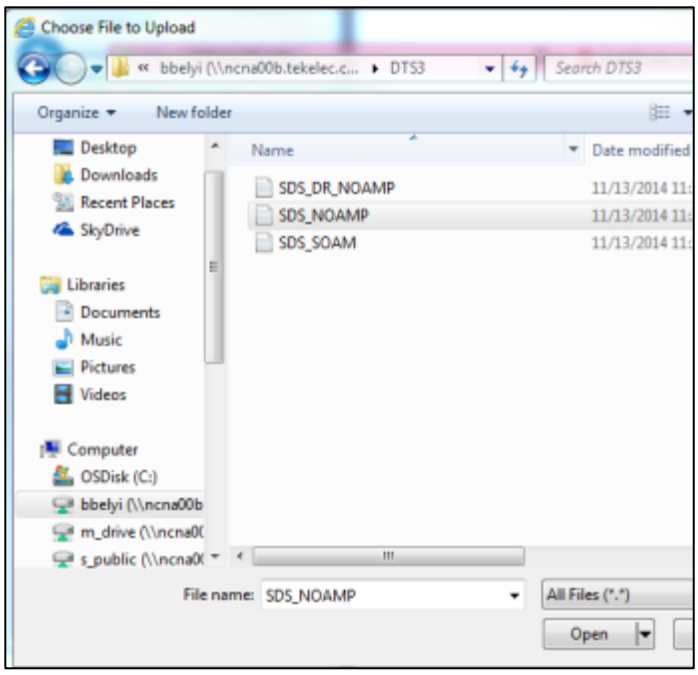
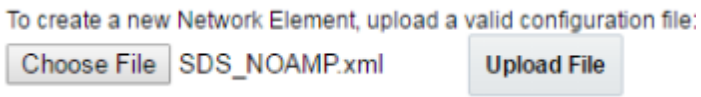
- The SDS network element XML file for the primary provisioning SDS site has been created previously as described in Appendix E.
- The network element XML files are either on a USB flash drive or the laptop's hard drive. The steps are written as if the XML files are on a USB flash drive, but the files can exist on any accessible drive.

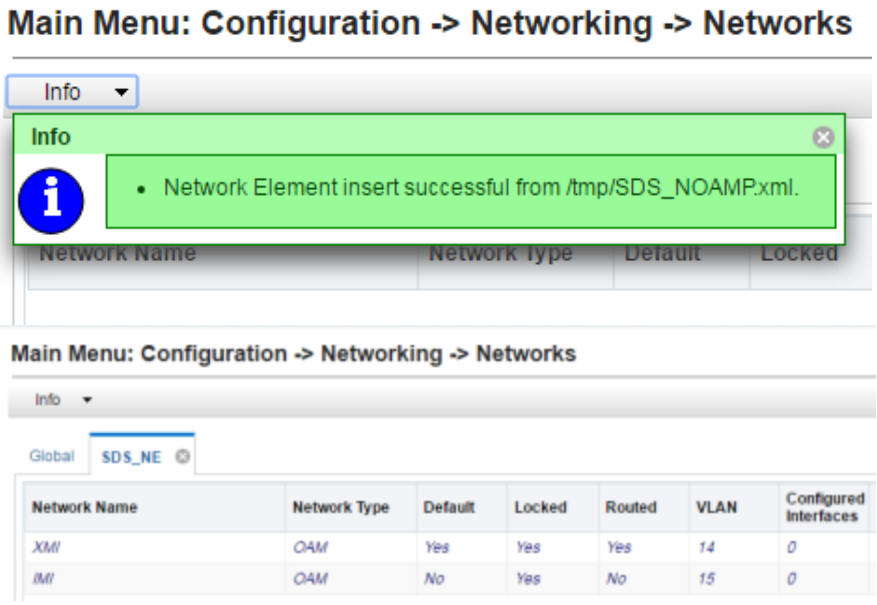
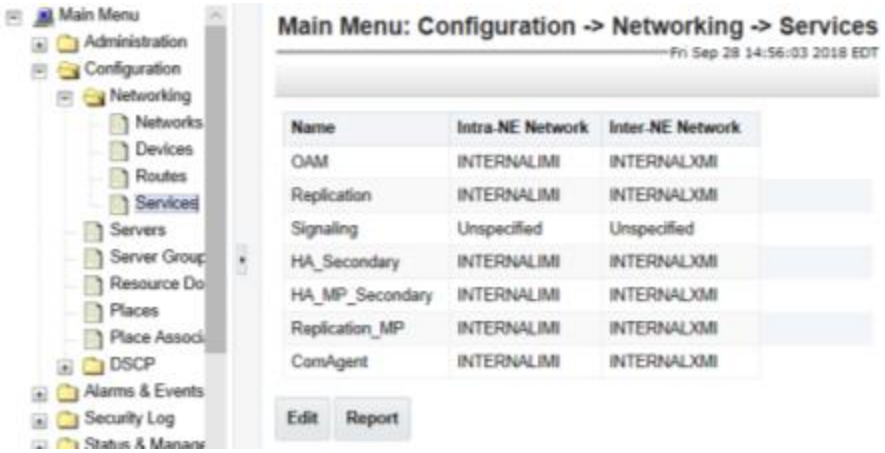
This procedure requires the user to connect to the SDS GUI before configuring the first SDS. This can be done by:

- Configuring a temporary external IP address as described in Appendix B; or
- 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.

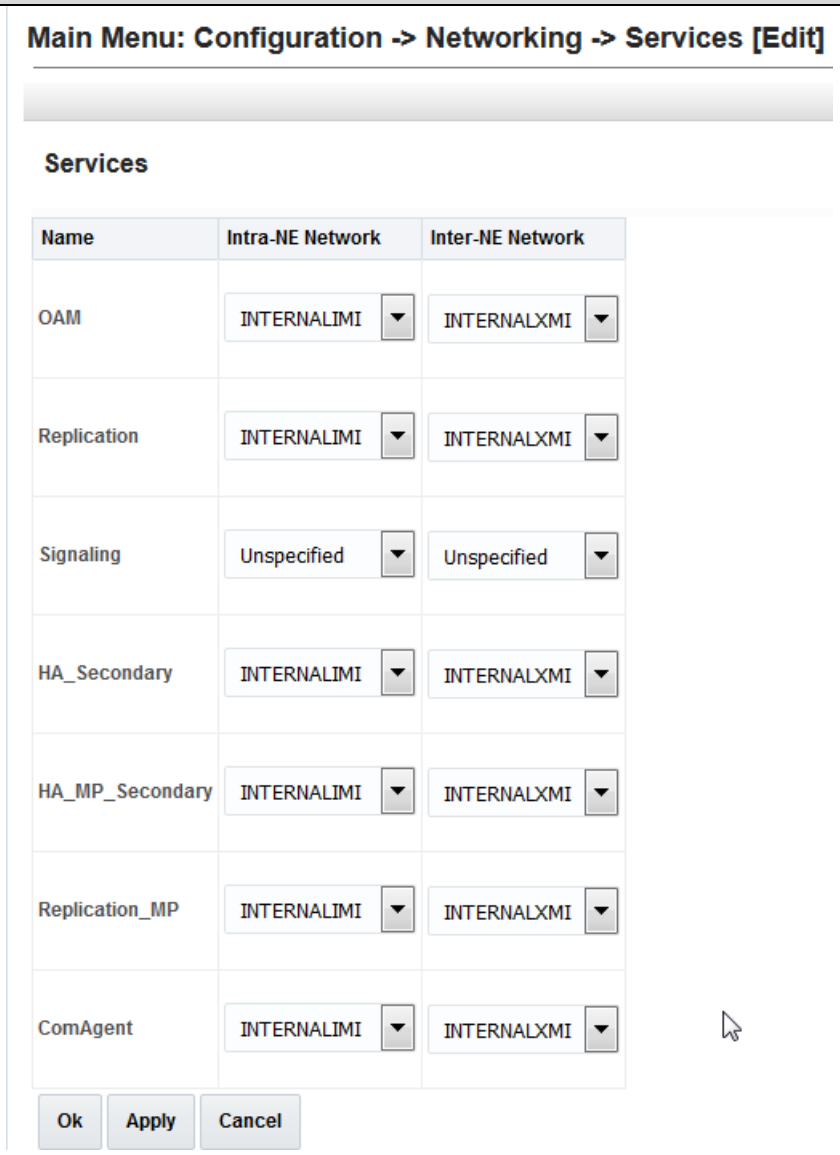
Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		
1. ☐	**SDS NOAM A**: Connect to the SDS GUI	Execute Appendix C. Establishing a Local Connection for Accessing the SDS GUI.
2. ☐	**SDS NOAM A**: Login	Log into the active SDS site with the SDS NOAM A IP address using the default user and password. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)

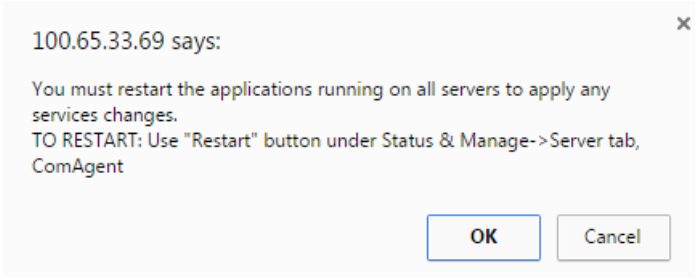
3. ☐	**SDS NOAM A**: Upload XML file	1. Navigate to **Configuration > Networking > Networks**.  2. Click **Browse**.  ***Note:*** This step assumes the XML file was previously prepared as described in Appendix E. 3. Locate the XML file, select it, and click **Open**.  4. Click **Upload File**. 

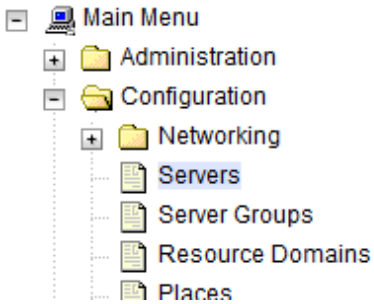
Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		
4. ☐	**SDS NOAM A**: Validate the file	Click **Info** to see the banner information showing that the data has been successfully validated and committed to the DB. 
5. ☐	**SDS NOAM A**: Edit the network services	1. Navigate to **Configuration > Networking > Services**. 2. Click **Edit**.  3. With the exception of Signaling, which is left as Unspecified, make sure all Intra-NE Network traffic is directed across IMI and all Inter-NE Network traffic is directed across XMI.

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)



4. Click **Apply**.
5. Click **OK** in the pop-up screen.



Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		
6. ☐	**SDS NOAM A or B**: Configure server ***Note***: This step through to the last step of this procedure needs to be done for both the SDS NOAM A and SDS NOAM B servers.	1. Navigate to **Configuration > Servers**.  1. Click **Insert**. 2. Fill in the fields: **Hostname**: Name for the SDS NOAM A or B server **Role**: NETWORK OAM&P **System ID**: Name of the Hostname again for the SDS NOAM A or B server **Hardware Profile**: For Gen8: SDS HP Rack Mount For Gen9: SDS HP Gen9 Rack Mount **Network Element Name**: Select the NE **Location**: (Optional) Enter the location of the server.

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)

7. ☐ **SDS NOAM A or B**: Configure server

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

1. Type the SDS IP address for the the **MgmtVLAN** IP address, select **bond0** as the Interface, and mark the **VLAN** checkbox.
2. Type the SDS IP address for the the **IMI** network, select **bond0** as the Interface, and mark the **VLAN** checkbox.

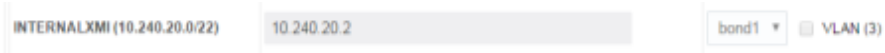
SDS (Primary NOAM)	Network	IP Address	Interface	VLAN Checkbox
SDS-A	MgmtVLAN	169.254.1.11	bond0	✓
	IMI	169.254.100.11		
SDS-B	MgmtVLAN	169.254.1.12	bond0	✓
	IMI	169.254.100.12		

Notes:

- These IP addresses are based on the information in the NAPD and the network element configuration file.
- The MgmtVLAN only displays when the 4948E-F aggregation switches are deployed with SDS NOAM/Query Server RMS. If the MgmtVLAN does not display, the IMI network values still apply.

3. Type the SDS IP address for the the **XMI** network.
   - For Layer 3, where no VLAN tagging is used for XMI, select **bond1** as the Interface and do NOT mark the VLAN checkbox.

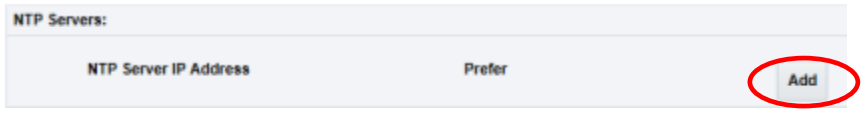
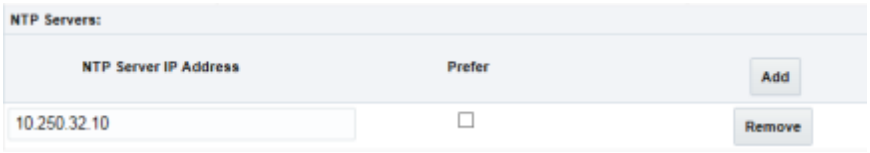
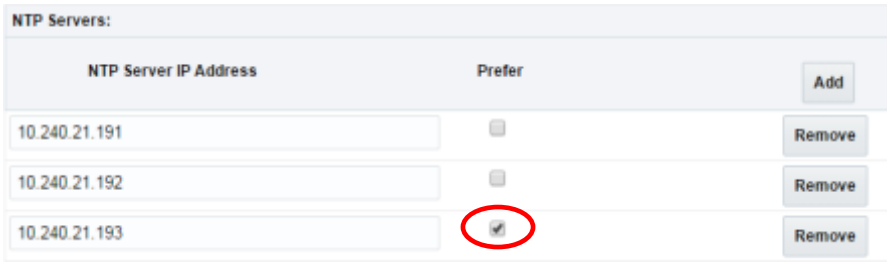
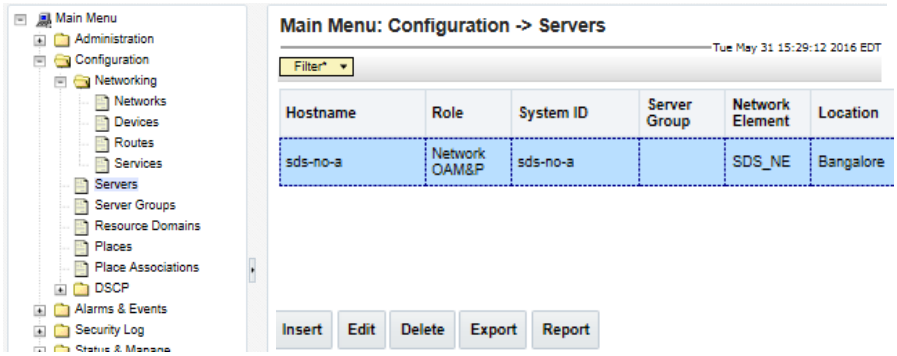
     or
   - For Layer 2, where VLAN tagging is used for XMI, select **bond0** as the Interface and mark the VLAN checkbox.

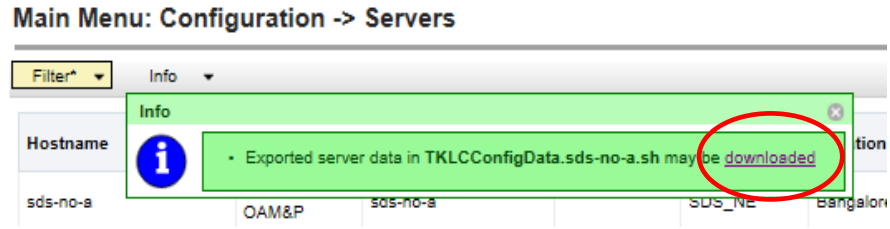
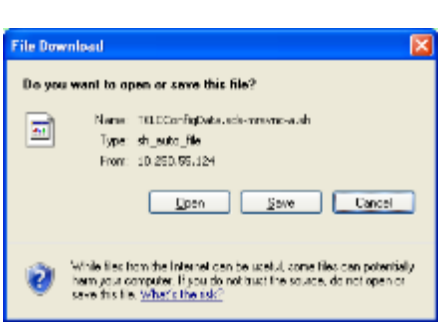
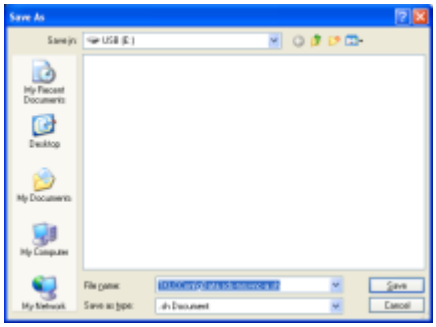


SDS (Primary NOAM)	Network	Interface	VLAN Checkbox
SDS NOAM Server (A or B)	XMI	bond1	✗
		bond0	✓

!!!CAUTION!!!

It is crucial the correct network configuration be selected in this step. Choosing an incorrect configuration results in the need to re-install the OS and restart the Query server installation procedure from the beginning.

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		
8. ☐	**SDS NOAM A or B**: Insert server	1. Click **Add** in the NTP Servers section.  2. Type the **NTP Server IP Address**.  3. Repeat to add 3 NTP server IP addresses. 4. Optionally, mark the **Prefer** checkbox to prefer one server over the other.  5. Click **OK** when you have completed entering all the server data.
9. ☐	**SDS NOAM A or B**: Export the server	From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created. 

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		
10. ☐	**SDS NOAM B**: Load the TKLCConfig file ***Note***: Steps 10. to 15. are skipped for the first server (server A) since the TKLCConfig file is already on server A.	1. Click **Info** to display the download link for the SDS configuration data. 2. Click on the word **downloaded**.  3. Save the configuration file tp a USB flash drive.  
11. ☐	**SDS NOAM B**: Access the server console	Connect to the SDS NOAM B console using one of the access methods described in Section 2.3.

12. ☐	**SDS NOAM B**: Login	Log into the HP server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

13. ☐	**SDS NOAM B**: Load file	1. Insert the USB drive containing the server configuration file into the server's USB port.
		
		Figure 6. HP DL380 Gen8, Front Panel (USB Port)
		
		Figure 7. HP DL380 Gen9, Front Panel (USB Port)
		Output similar to this displays as the USB flash drive is inserted into the **SDS** 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>`
		2. Press **Enter** to return to the command prompt.

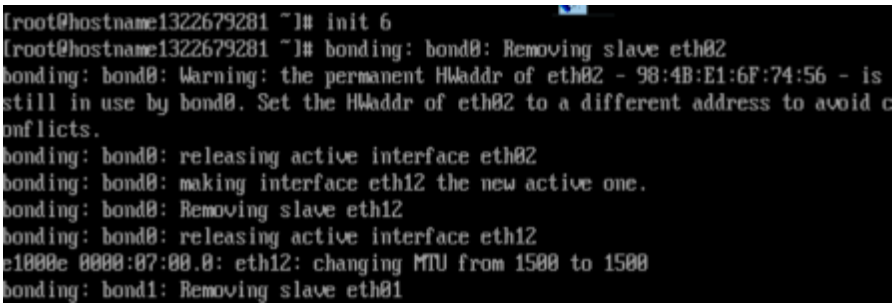
14. ☐	**SDS NOAM B**: Verify software directory	Verify the USB drive has been mounted under the /media directory.
		`$ df |grep sdb`
		`/dev/sdb1 2003076 8 2003068 1% /media/sdb1`

15. ☐	**SDS NOAM B**: Unmount USB	1. Unmount the USB drive partition. `$ sudo umount /media/sdb1` 2. Remove the USB drive from the server's front panel. ***Note:*** It is important to remove the USB drive before continuing.

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

16. ☐	**SDS NOAM A or B**: Copy the configuration file	1. 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. For example:
		TKLCConfigData<.server_hostname>.sh translates to TKLCConfigData.sh
		`$ sudo cp -p /var/TKLC/db/filemgmt/TKLCConfigData.sds-mrsvnc-a.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the presence of the configuration file and automatically executes it when found.
		After the script completes, a broadcast message is sent to the terminal.
		Note: It may take 3 to 20 minutes to complete this step depending on the server.
		`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.`
		2. Press **Enter**.

17. ☐	**SDS NOAM A or B**: Verify time zone	Verify the desired time zone is in use.
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2017`
		If the desired time zone is not displayed, set it with this command:
		`$ sudo set_ini_tz.pl <time_zone>`
		For example, to set the time to UTC (aka GMT):
		`$ sudo set_ini_tz.pl "Etc/UTC"`
		See Appendix G for a list of all valid time zones.
		Note: This is required to be for first server (NOAM). The rest of the servers get the TKLCconfig file generated on the active NOAM server and the TKLCconfig file sets the time zone.

18. ☐	**SDS NOAM A or B**: Reboot the SDS	`$ sudo init 6` ***Note:*** This may take approximately 9 minutes. 

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

19. ☐	**SDS NOAM A or B**: Login	After the server has completed the reboot, log into the server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

20. ☐	**SDS NOAM A or B**: Verify IP addresses	Verify the IMI and XMI IP addresses, and associated bond configurations, (from step 7.) have been correctly loaded.
		`$ 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`
		Note: The addresses can also be verified on the **Configuration > Server** screen.

21. ☐	**SDS NOAM A or B**: Verify connectivity	Execute the ntpq command to verify 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 contact the customer IT group to provide a network path from the SDS NOAM server XMI IP to the assigned NTP server IP addresses. Once network connectivity is established, repeat step 21.

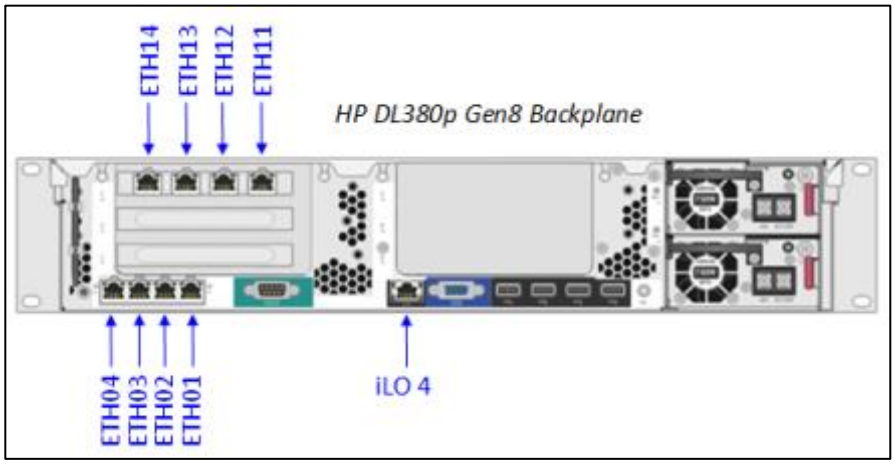
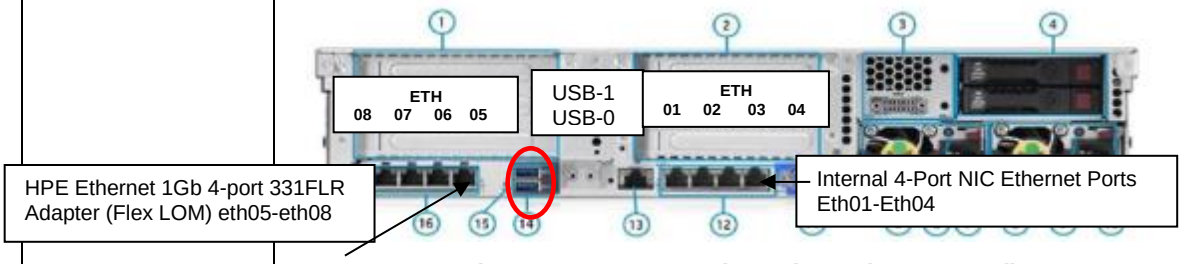
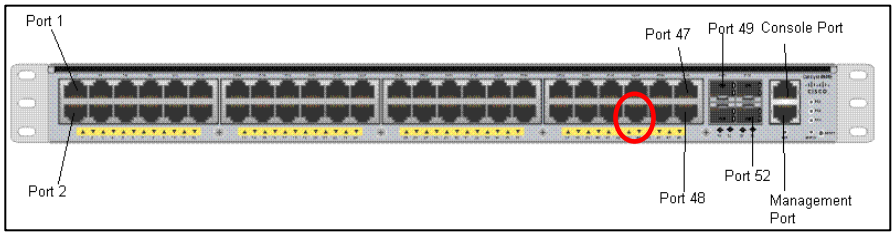
Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

22. ☐	**SDS NOAM A or B**: Verify system state	Execute the syscheck command to verify the state 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`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

23. ☐	**SDS NOAM A or B**: Exit	Exit to return to the server console to the login prompt. `$ exit`
24. ☐	Repeat	Configure SDS B by repeating steps 6. through 23. of this procedure.
		If aggregation switches are installed and 4948E-F switch configuration has not been completed before this step, stop and execute the following procedures: APPENDIX D.1 APPENDIX D.2 (Appendix D.2 references Appendix D.3, where applicable).

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

25. ☐	**SDS NOAM A or B**: Ping IMI and XMI addresses	1. From SDS NOAM A, ping the IMI IP address configured for SDS NOAM 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`
		2. From SDS NOAM A, ping the XMI IP address configured for on SDS NOAM 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`
		3. From SDS NOAM A, ping the 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`
		4. From SDS NOAM B, ping the 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. Configure SDSs A and B (1st SDS NOAM Site Only)		
26. ☐	**SDS NOAM A or B**: Disconnect laptop ***Note***: This step is only needed if referred from Appendix B, otherwise skip to the next step	For Gen8, disconnect the laptop from the server NOAM A, eth14 port.  **Figure 8. HP DL380 Gen8, Rear Panel (Ethernet)** For Gen9, disconnect the laptop from the server NOAM A, eth08 port.  **Figure 9. HP DL380 (Gen9), DC (Rear Panel)**
27. ☐	**Switch1A**: Connect laptop	Connect the laptop to port 44 on switch1A (bottom switch).  **Figure 10. Cisco 4948E-F Switch (Maintenance Access Port)**
28. ☐	**Laptop**: Set static IP	Set a static IP address and netmask within the management VLAN for the laptop's network interface card. 169.254.1.100 is suggested. Refer to Appendix C, steps 5. if assistance is needed to modify the laptop's network configuration.

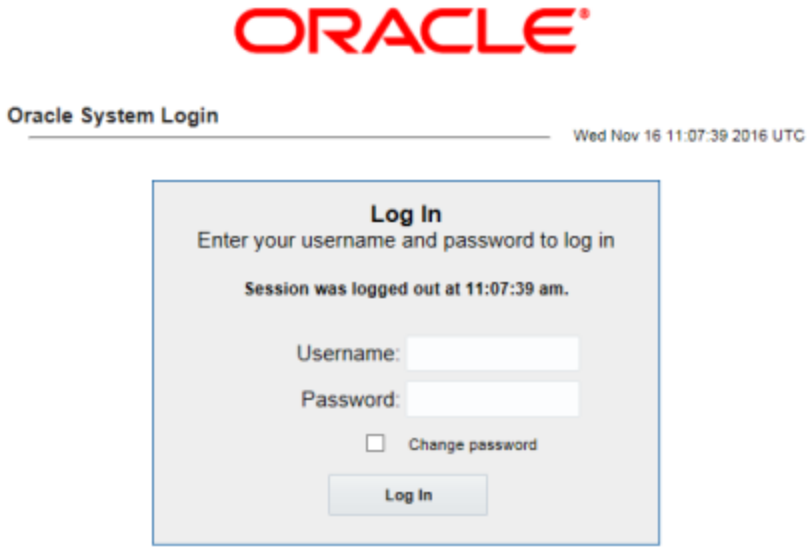
29. ☐	**SDS NOAM A**: Login	Log into the NOAM A server using the management VLAN IP address 169.254.1.11.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

Procedure 3. Configure SDSs A and B (1st SDS NOAM Site Only)		

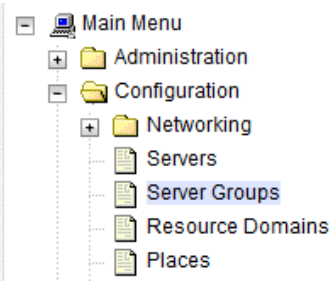
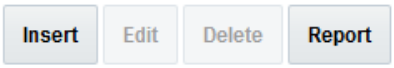
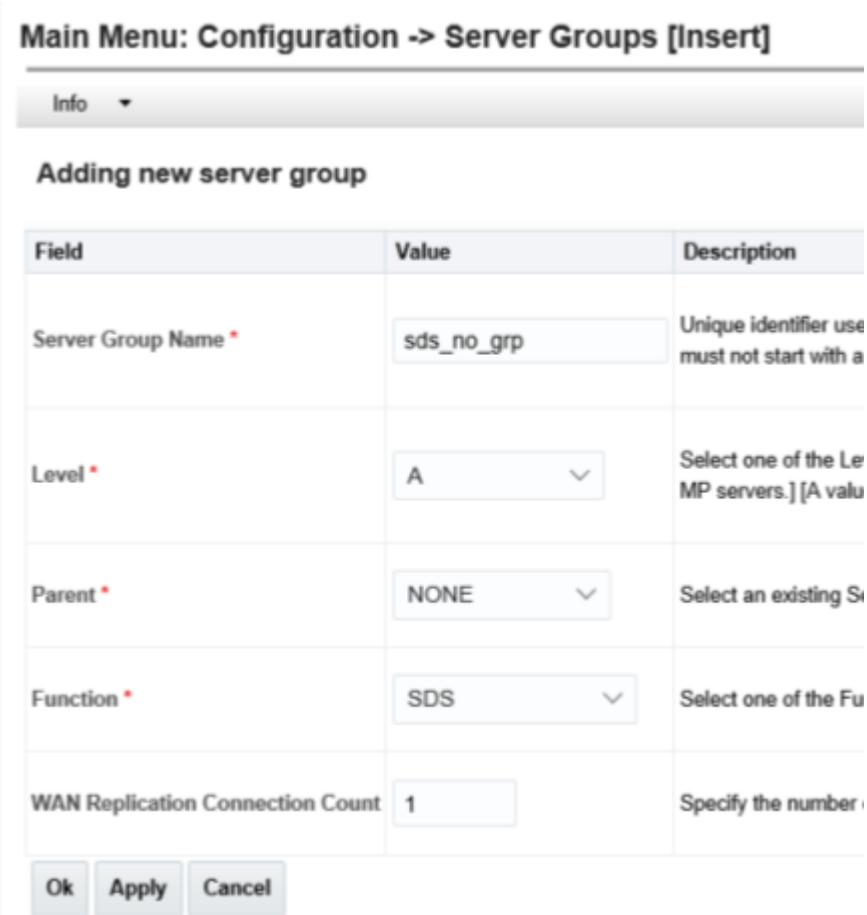
30. ☐	**SDS NOAM A**: Delete Ethernet connections	For Gen8, delete eth14:
		`$ sudo netAdm delete --device=eth14`
		`Interface eth14 removed`
		For Gen9, delete eth08:
		`$ sudo netAdm delete --device=eth08`
		`Interface eth08 removed`

5.2 OAM Pairing (1st SDS NOAM Site Only)

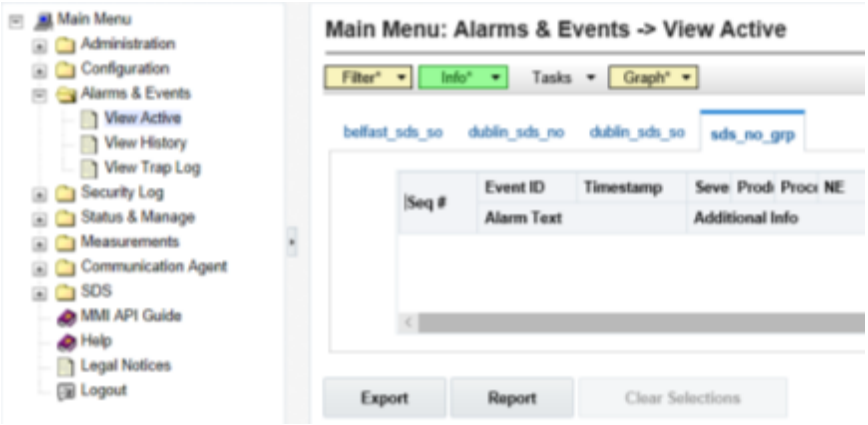
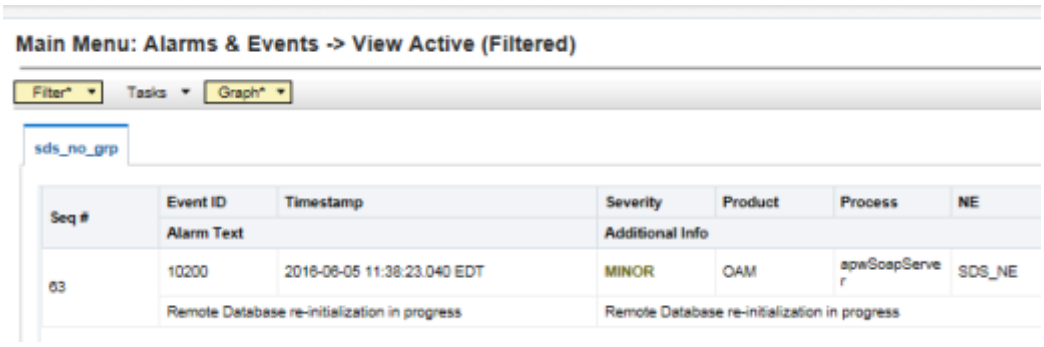
The user should be aware that during the OAM pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

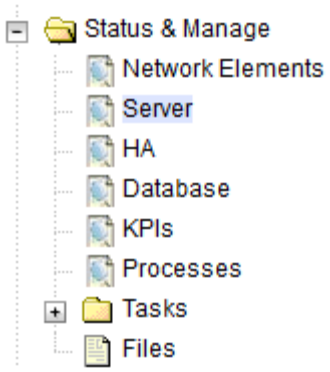
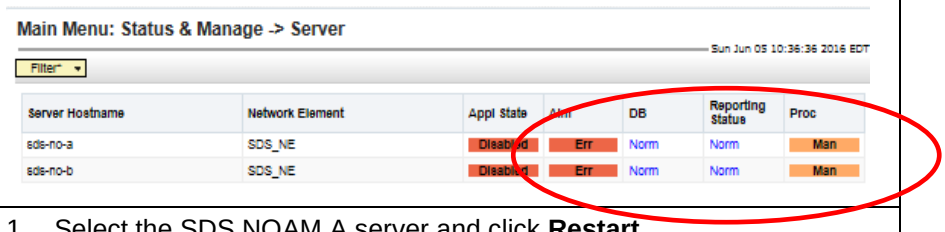
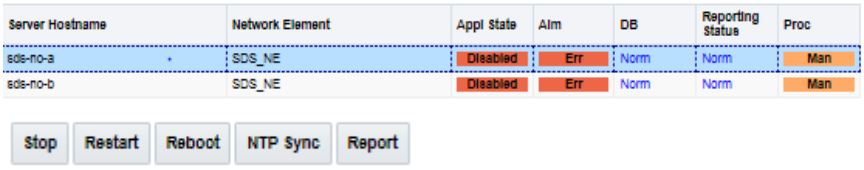
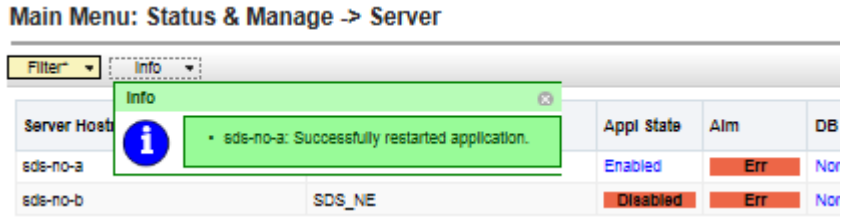
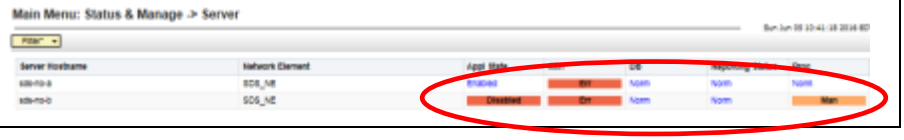
Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
1. ☐	**SDS NOAM A**: Login	Log into the active SDS site with the SDS NOAM A IP address using the default user and password. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**. 

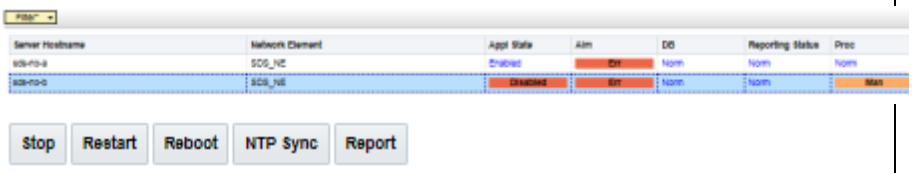
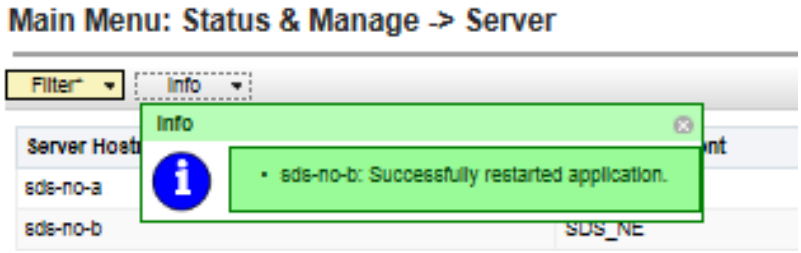
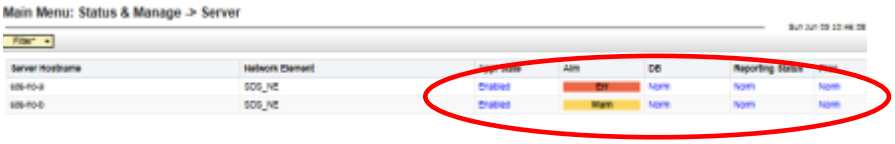
Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)

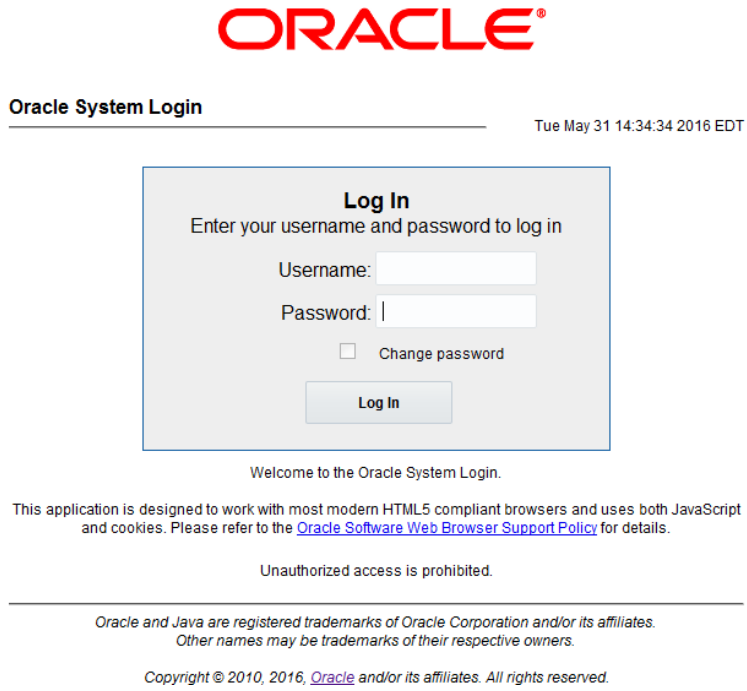
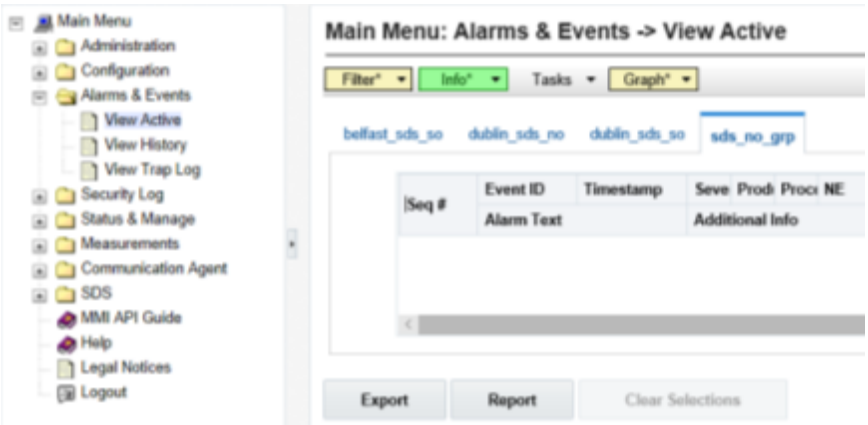
2. ☐	**SDS NOAM A**: Create a server group	1. Navigate to **Configuration > Server Groups**.  2. Click **Insert**.  3. Fill in the following fields: **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: SDS (Active/Standby Pair) **WAN Replication Connection Count**: Use Default Value (1)  4. Click **OK**.

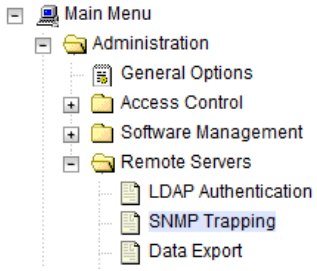
<table>
<tr><th colspan="3">Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)</th></tr>
<tr><td>3. ☐</td><td>SDS NOAM A: Add server to OAM Server Group</td><td>1. Select the new server group and click Edit.
Main Menu: Configuration -> Server Groups
Filter*
Server Group Name | Level | Parent | Function | Connection Count
NO_SG | A | NONE | SDS | 1
Insert | Edit | Delete | Report
2. Mark the Include in SG checkbox next to the A and B servers.
3. Click Apply.
4. Click Add next to VIP Address to add an IP.
5. Type the VIP Address and click OK.
VIP Assignment
VIP Address | Add
10.240.108.24 | Remove
Ok | Apply | Cancel</td></tr>
<tr><td>4. ☐</td><td>SDS NOAM A: Logout</td><td>Click Logout and wait at least 5 minutes before proceeding to the next step.
…se Updates | Help | Logged In Account guiadmin | Log Out
Important: 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.</td></tr>
</table>

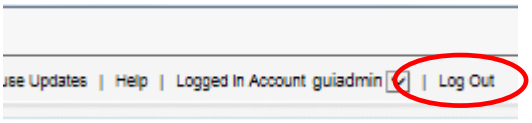
Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
5. ☐	**SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP (VIP) address using the default user and password. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.
6. ☐	**SDS VIP**: Make sure alarms clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 10200** does not display.
		If event ID 10200 (Remote Database re-initialization in progress) does display, do not proceed to the next step until the alarm clears. 

Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
7. ☐	**SDS VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify the DB status is **Norm** and the Proc status is **Man** for both servers. 
8. ☐	**SDS VIP**: Restart the SDS NOAM A server	1. Select the SDS NOAM A server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
9. ☐	**SDS VIP**: Verify status	Verify the Appl State is **Enabled**, DB status is **Norm**, and the Proc is **Man** for the SDS NOAM A server. 

Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
10. ☐	**SDS VIP**: Restart the SDS NOAM B server	1. Select the SDS NOAM B server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
11. ☐	**SDS VIP**: Verify status	1. Verify the Appl State is **Enabled**, and DB, Reporting Status, and Proc are **Norm** for both servers.  2. Wait at least **5 minutes** before proceeding to the next step. ***Important***: 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

Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
12. ☐	**SDS VIP**: Login	If necessary, login again to the GUI using the default user and password. 
13. ☐	**SDS VIP**: Wait for remote database alarm to clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 14101** (No remote provisioning clients are connected) is the only alarm present on the system at this time.

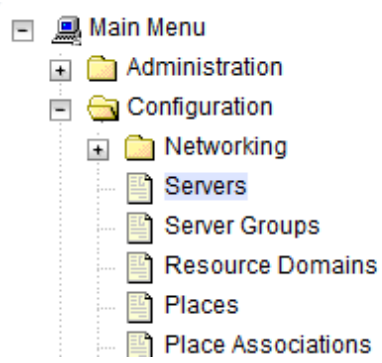
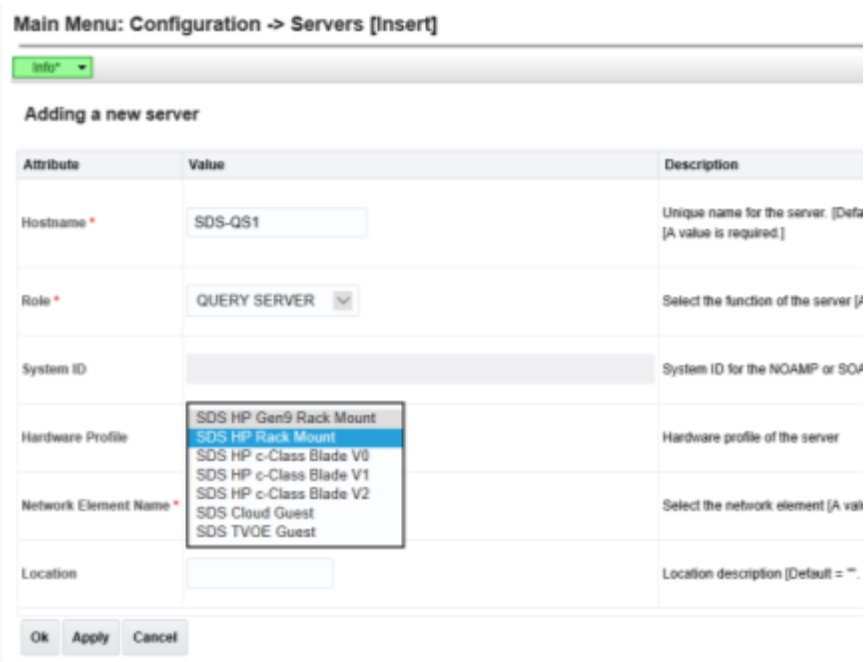
Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
14. ☐	**SDS VIP**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Click **Insert**. 3. Change the Enabled Versions to **SNMPv2c**. 4. Mark the Traps from Individual Servers checkbox as **Enabled**. 5. Provide **Community Names** for the SNMPv2c Read-Only and Read-Write fields. 6. Click **OK**.

Procedure 4. Pair the SDS NOAM Servers (1st SDS NOAM Site Only)		
15. ☐	**SDS VIP**: Logout	Click **Logout**. 

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.

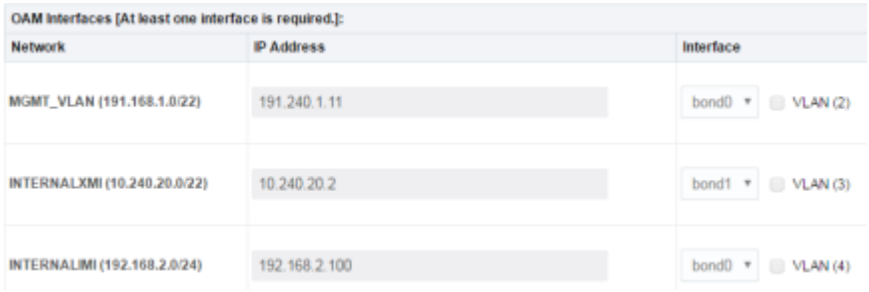
Procedure 5. Configure the Query Server (All SDS NOAM Sites)		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

Procedure 5. Configure the Query Server (All SDS NOAM Sites)		
2. ☐	**Primary SDS VIP**: Configure the Query server	1. Navigate to **Configuration > Servers**.  2. Click **Insert**. 3. Fill in the fields: **Hostname**: <Assigned Hostname> **Role**: Query Server **System ID**: Leave Blank **Hardware Profile**: Gen8: SDS HP Rack Mount Gen9: SDS HP Gen9 Rack Mount **Network Element Name**: [Select **NE** from list where Query server is physically located] Location: Optional 

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

3. ☐ **SDS NOAM A**: Insert the Query server

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



1. Type the Query server IP addresses for the MgmtVLAN network. Select **bond0** for the interface. Mark the **VLAN** checkbox.
2. Type the Query server IP addresses for the IMI network. Select **bond0** for the interface. Mark the **VLAN** checkbox.

Query Server	Network	IP Address	Interface	VLAN Checkbox
SDS-QS (Primary NE)	MgmtVLAN	169.254.1.13	bond0	✓
	IMI	169.254.100.13		
SDS-QS (DR NE)	MgmtVLAN	169.254.1.16	bond0	✓
	IMI	169.254.100.16		

Notes:

- These IP addresses are based on the information in the NAPD and the Network Element Config file.
- The **MgmtVLAN** only displays when 4948E-F Aggregation Switches are deployed with SDS NOAM/Query Server RMS. If the **MgmtVLAN** is not present, the **IMI** network values still apply.

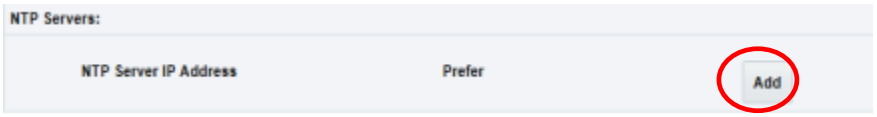
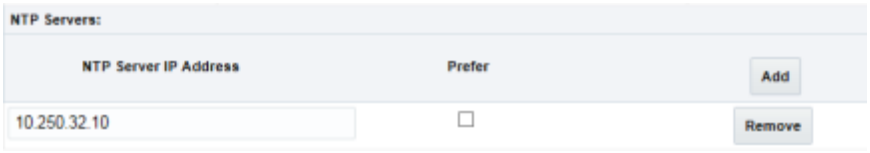
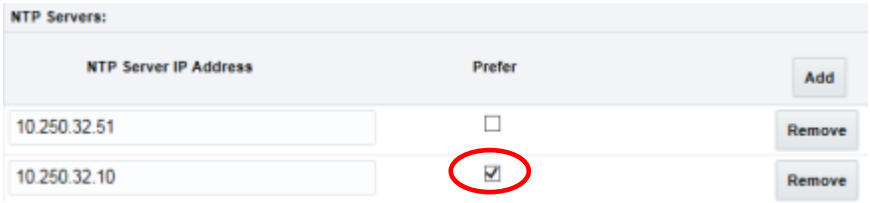
3. Type the Query server IP addresses for the XMI network.
   - For Layer 3, where no VLAN tagging is used for XMI, select **bond1** as the Interface and do NOT mark the VLAN checkbox.

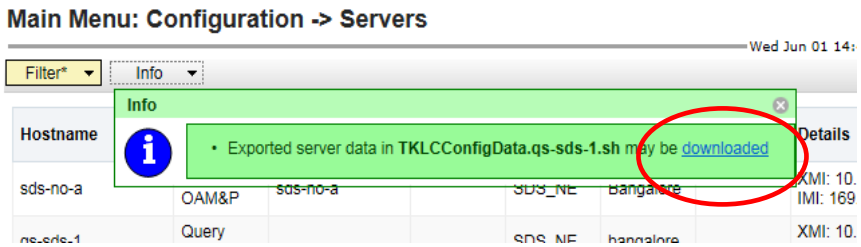
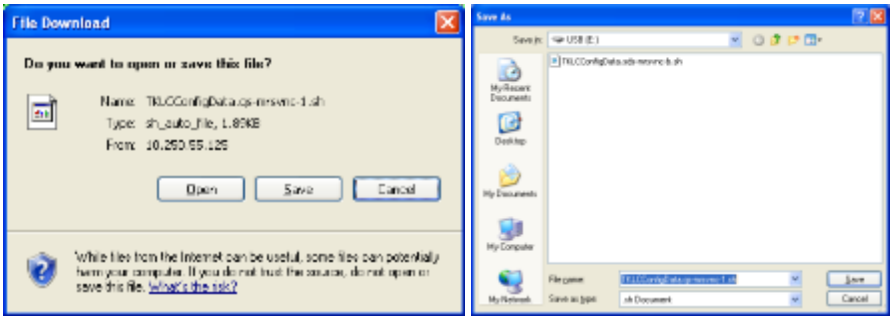
     or
   - For Layer 2, where VLAN tagging is used for XMI, select **bond0** as the Interface and mark the VLAN checkbox.

Query Server	Network	Interface	VLAN Checkbox
SDS-QS (Primary and DR)	XMI	bond1	✗
		bond0	✓

!!!CAUTION!!!

It is crucial the correct network configuration be selected in this step. Choosing an incorrect configuration results in the need to re-install the OS and restart the Query server installation procedure from the beginning.

Procedure 5. Configure the Query Server (All SDS NOAM Sites)		
4. ☐	**SDS NOAM A**: Insert the Query server	1. Click **Add** in the NTP Servers section.  2. Type the **NTP Server IP Address**.  3. Repeat to add 3 NTP server IP addresses. 4. Optionally, mark the **Prefer** checkbox to prefer one server over the other.  5. Click **OK** when you have completed entering all the server data.
5. ☐	**Active SDS VIP**: Export the initial configuration	From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.

Procedure 5. Configure the Query Server (All SDS NOAM Sites)		
6. ☐	**Primary SDS VIP**: Load the TKLCConfig file	1. Click **Info** to display the download link for the SDS configuration data. 2. Click on the word **downloaded**.  3. Save the configuration file tp a USB flash drive. 
7. ☐	**Query Server**: Access the server console	Connect to the Query Server console using one of the access methods described in section 2.3.

8. ☐	**Query Server**: Login	Log into the Query server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

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

9. ☐	**Query Server**: Load file	1. Insert the USB drive containing the server configuration file into the server's USB port.
		
		Figure 11. HP DL380 Gen8, Front Panel (USB Port)
		
		Figure 12. HP DL380 Gen9, Front Panel (USB Port)
		Output similar to this displays as the USB flash drive is inserted into the **SDS** 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>`
		2. Press **Enter** to return to the command prompt.

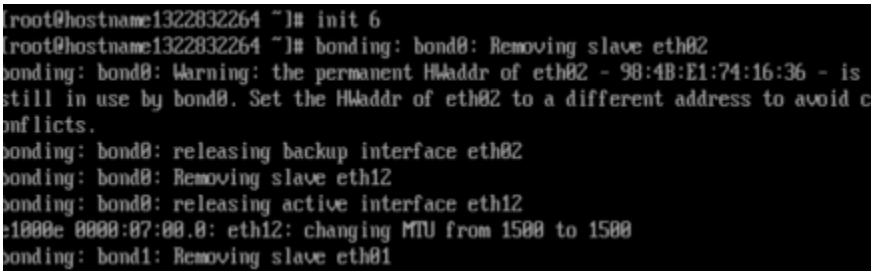
10. ☐	**Query Server**: Verify software directory	Verify the USB drive has been mounted under the /media directory.
		`$ df |grep sdb`
		`/dev/sdb1 2003076 8 2003068 1% /media/sdb1`
		Note: Search **df** for the device named in the output.

11. ☐	**Query Server**: Copy the configuration file	`$ sudo cp -p /media/sdb1/TKLCConfigData.qs-mrsvnc-1.sh /var/TKLC/db/filemgmt/`
12. ☐	**Query Server**: Unmount USB	1. Unmount the USB drive partition. `$ sudo umount /media/sdb1` 2. Remove the USB drive from the server's front panel. ***Note:*** It is important to remove the USB drive before continuing.

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

13. ☐	**Query Server**: Copy configuration file	1. 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. For example:
		TKLCConfigData<.server_hostname>.sh translates to TKLCConfigData.sh
		`$ sudo cp –p /var/TLKC/db/filemgmt/TKLCConfigData.qs-mrsvnc-1.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the presence of the configuration file and automatically executes it when found.
		After the script completes, a broadcast message is 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 2017):`
		`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.`
		2. Press **Enter**.

14. ☐	**SDS NOAM A or B**: Verify time zone	Verify the desired time zone is in use.
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2017`
		If the desired time zone is not displayed, set it with this command:
		`$ sudo set_ini_tz.pl <time_zone>`
		For example, to set the time to UTC (aka GMT):
		`$ sudo set_ini_tz.pl "Etc/UTC"`
		See Appendix G for a list of all valid time zones.

15. ☐	**Query Server**: Reboot the Query server	`$ sudo init 6` 

16. ☐	**Query Server**: Login	After the server has completed the reboot, log into the server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

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

17. ☐	**Query Server**: Accept upgrade	Accept upgrade to 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`

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

18. ☐	**Query Server**: Verify IP addresses	Verify the IMI and XMI IP addresses from step 3. have been correctly loaded.
		`$ 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`

19. ☐	**Query Server**: Ping IMI and XMI addresses	1. From the Query server, ping the IMI IP address for SDS 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`
		2. From the Query server, ping the 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`

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

20. ☐	**Query Server**: Verify connectivity	Execute the ntpq command to verify 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`

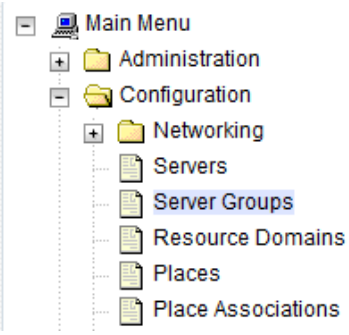
21. ☐	**Query Server**: Verify system state	Execute the syscheck command to verify the state of the server.
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

22. ☐	**Query Server**: Exit	Exit to return to the server console to the login prompt. `$ exit`

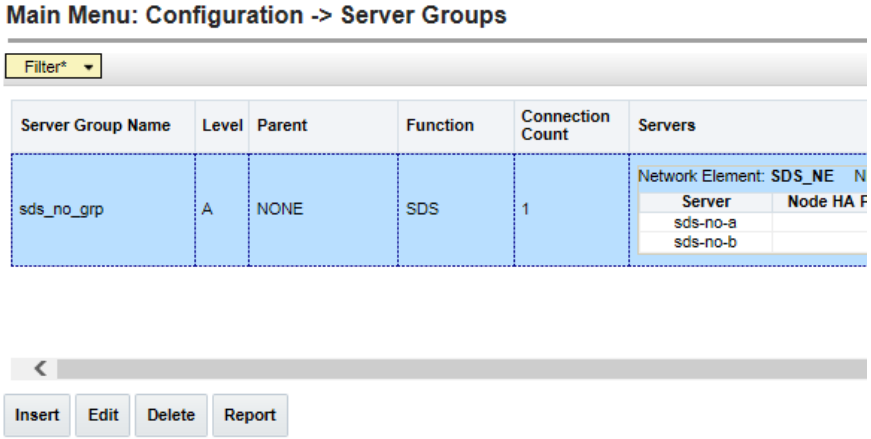
Procedure 5. Configure the Query Server (All SDS NOAM Sites)

23. ☐ **Primary SDS VIP**: Add server to OAM Server Group

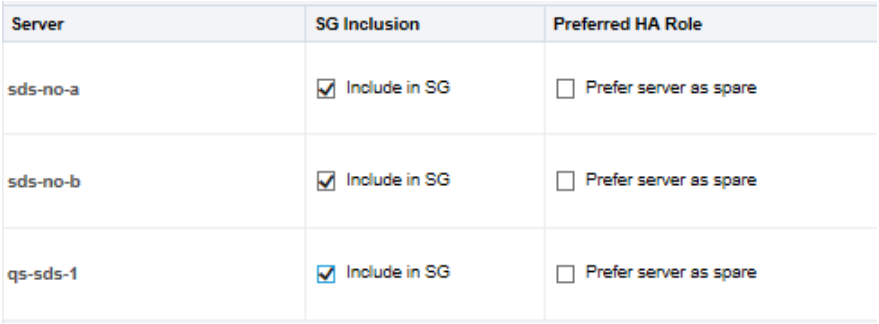
1. Navigate to **Configuration > Server Groups**.



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

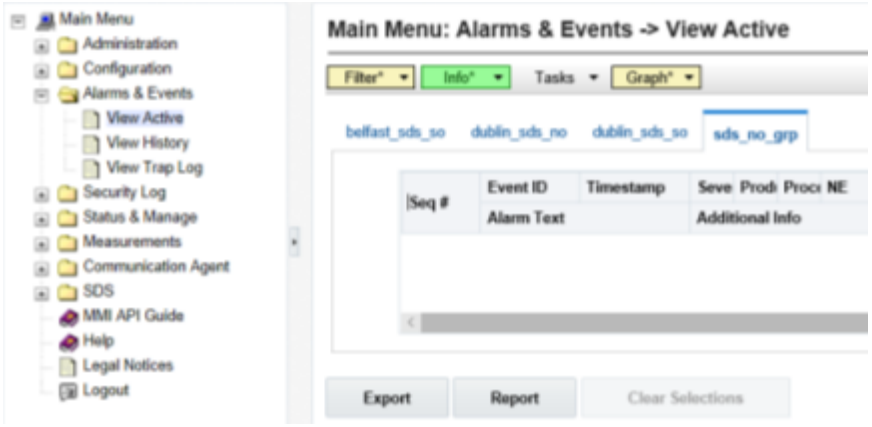
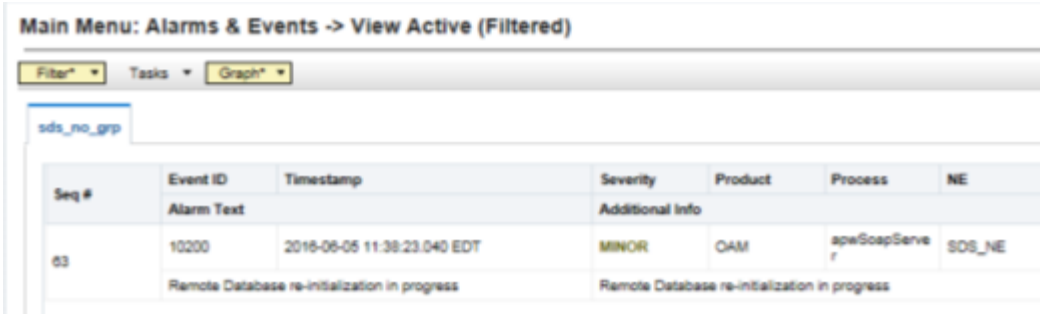
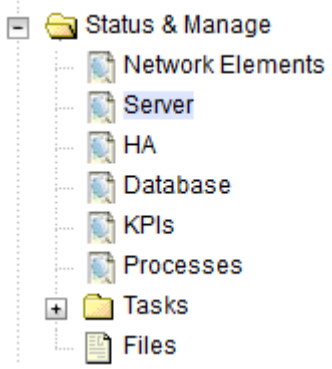
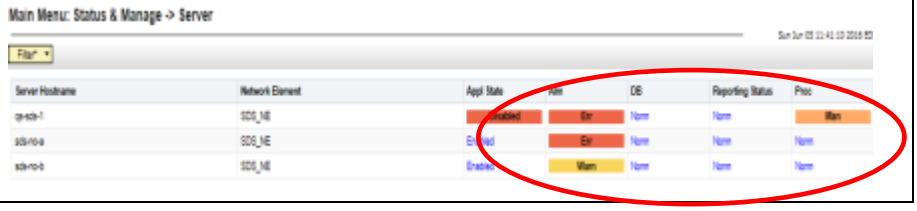


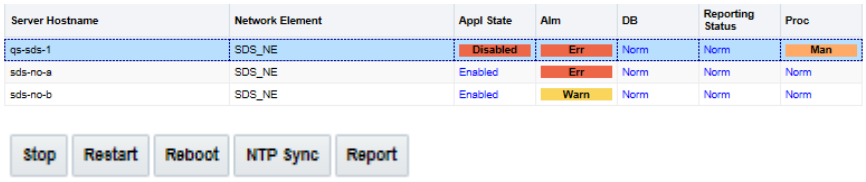
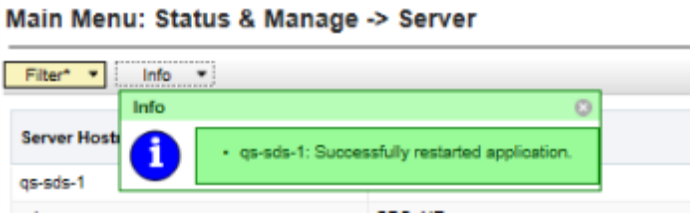
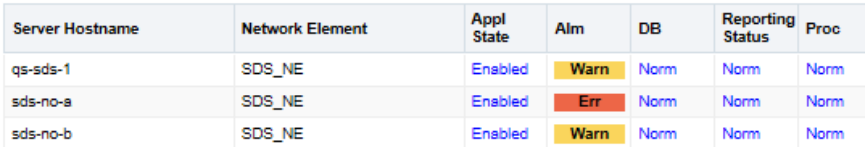
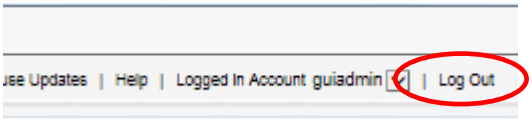
3. In the portion of the screen that lists the servers for the server group, find the Query server being configured. Mark the **Include in SG** checkbox.



4. Leave other boxes unchecked and click **OK**.

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

24. ☐	**Primary SDS VIP**: Make sure alarms clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 10200** displays 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 clears. 
25. ☐	**Primary SDS VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify the DB and Reporting Status is **Norm** and the Proc status is **Man** for the Query server. 

Procedure 5. Configure the Query Server (All SDS NOAM Sites)		
26. ☐	**Primary SDS VIP**: Restart the Query server	1. Select the Query server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
27. ☐	**Primary SDS VIP**: Verify status	Verify the Appl Ste is **Enabled**, the DB, Reporting Status, and Proc are **Norm** for the Query server. 
28. ☐	**Primary SDS VIP**: Logout	Click **Logout**. 

5.4 OAM Installation for the DR SDS NOAM Site

Assumptions:

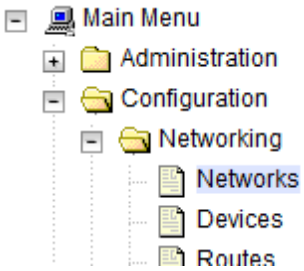
- The SDS network element XML file for the disaster recovery SDS provisioning site has been previously created as described in Appendix E.
- The network element XML files are either on a USB flash drive or the laptop's hard drive. This procedure is written for XML files on a USB flash drive, but the files can exist on any accessible drive.

Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only)		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

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

2. ☐ **Primary SDS VIP**: Create the SDS VIP network element using the XML file

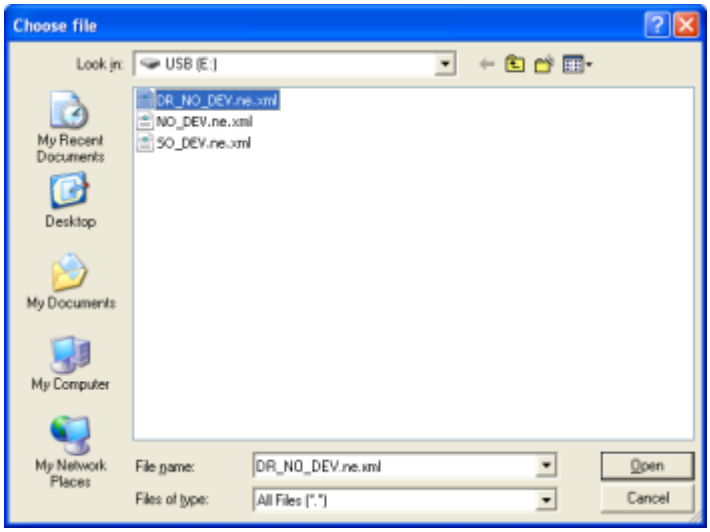
1. Navigate to **Configuration > Networking > Networks**.



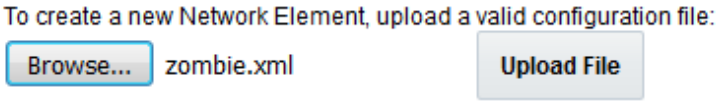
2. Click **Browse** and type the pathname of the NOAM network XML file.

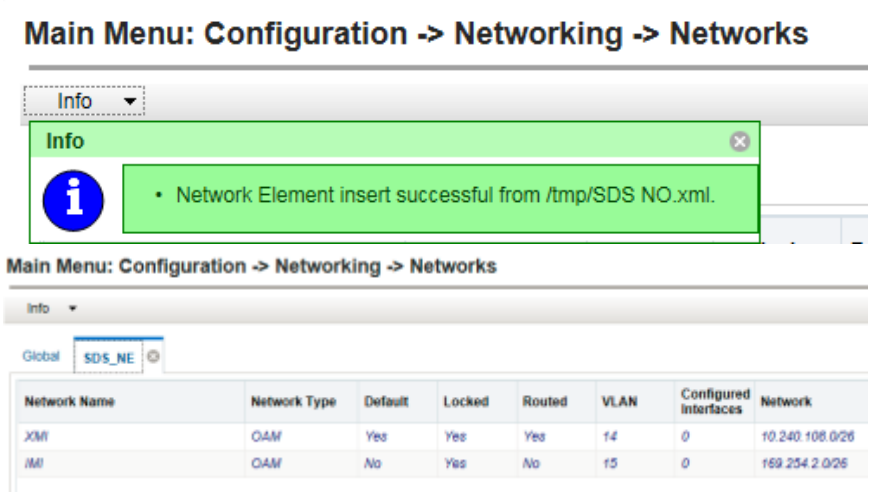
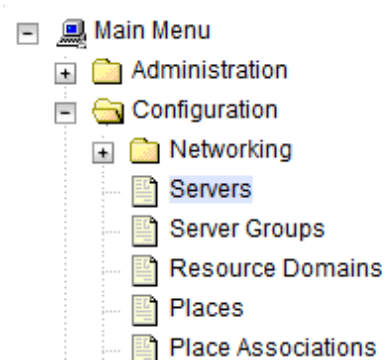
Note: This step assumes the **XML** files were previously prepared as described in Appendix E.

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

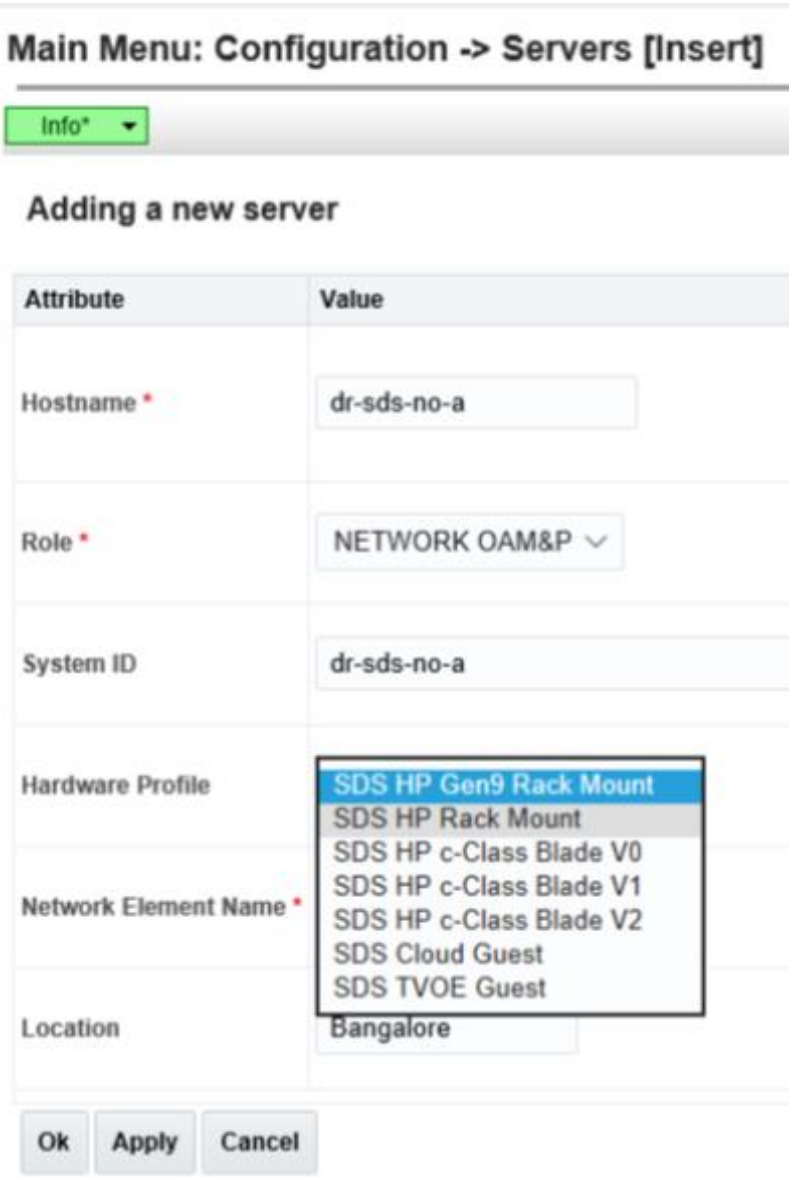


4. Click **Upload File** to upload the XML file.



<table>
<tr><th colspan="3">Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only)</th></tr>
<tr><td>3. ☐</td><td>Primary SDS VIP: Validate the file</td><td>Click Info to see the banner information showing that the data has been successfully validated and committed to the DB.
 
</td></tr>
<tr><td>4. ☐</td><td>Primary SDS VIP: Configure the DR NOAM server
Note: This step through to the last step of this procedure needs to be done for both the SDS DR NOAM A and SDS DR NOAM B servers.</td><td>1. Navigate to Configuration > Servers.
 

2. Click Insert.
3. Fill in the fields:
Hostname: <Assigned Hostname for DR NOAM server>
Role: Network OAM&P
System ID: <Assigned Hostname for DR NOAM server>
Hardware Profile: Gen8: SDS HP Rack Mount
Gen9: SDS HP Gen9 Rack Mount
Network Element Name: [Select NE from list where SDS DR (A or B) is physically located]
Location: (Optional) Enter the location of the server</td></tr>
</table>

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

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

5. ☐ **Primary SDS VIP**: Insert the VM server

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

1. Type the DR SDS IP addresses for the **MgmtVLAN** network, select **bond0** as the interface, and mark the **VLAN** checkbox.
2. Type the DSR SDS IP addresses for the IMI network, select **bond0** as the Interface, and mark the **VLAN** checkbox.

SDS (DR NOAM)	Network	IP Address	Interface	VLAN Checkbox
DR SDS-A	MgmtVLAN	169.254.1.14	bond0	✓
	IMI	169.254.100.14		
DR SDS-B	MgmtVLAN	169.254.1.15	bond0	✓
	IMI	169.254.100.15		

Notes:

- These IP addresses are based on the information in the NAPD and the Network Element Config file.
- The MgmtVLAN only displays when 4948E-F Aggregation Switches are deployed with SDS NOAM/Query Server RMS. If the MgmtVLAN is not present, the IMI network values still apply.

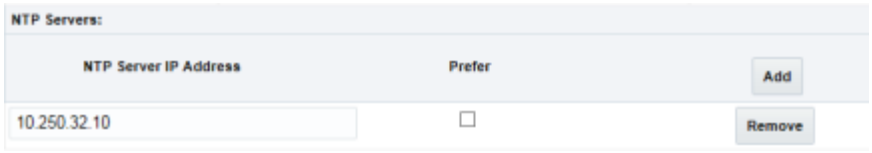
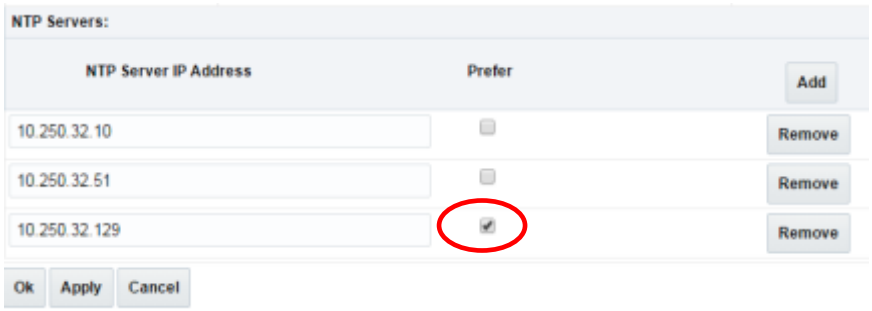
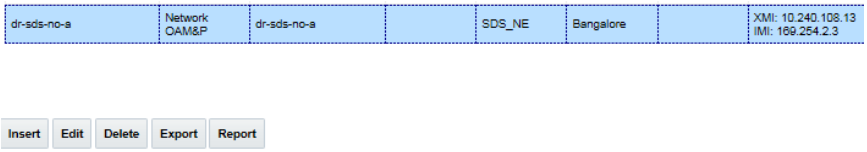
3. Type the DR SDS IP addresses for the **XMI** network.
   - For Layer 3, where no VLAN tagging is used for XMI, select **bond1** as the Interface and do NOT mark the VLAN checkbox.

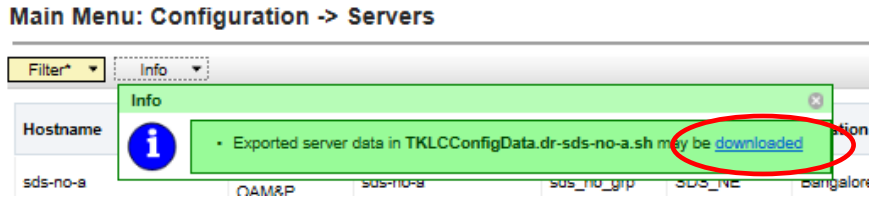
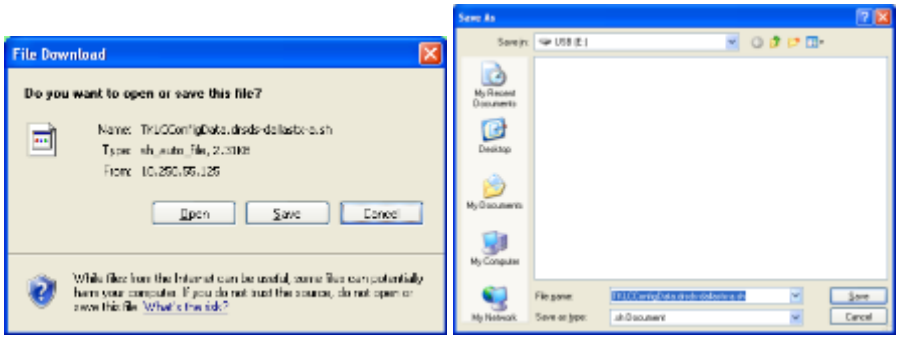
     or
   - For Layer 2, where VLAN tagging is used for XMI, select **bond0** as the Interface and mark the VLAN checkbox.

SDS (DR NOAM)	Network	Interface	VLAN Checkbox
DR SDS NOAM Server (A or B)	XMI	bond1	✗
		bond0	✓

!!!CAUTION!!!

It is crucial the correct network configuration be selected in this step. Choosing an incorrect configuration results in the need to re-install the OS and restart the Query server installation procedure from the beginning.

Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only)		
6. ☐	**SDS NOAM A**: Insert server	1. Click **Add** in the NTP Servers section. 2. Type the **NTP Server IP Address**.  3. Repeat to add 3 NTP server IP addresses. 4. Optionally, mark the **Prefer** checkbox to prefer one server over the other.  5. Click **OK** when you have completed entering all the server data.
7. ☐	**Primary SDS VIP**: Export the initial configuration	From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created. 

Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only)		
8. ☐	**Primary SDS VIP**: Load the TKLCConfig file	1. Click **Info** to display the download link for the SDS configuration data. 2. Click on the word **downloaded**.  3. Save the configuration file tp a USB flash drive. 
9. ☐	**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.

10. ☐	**SDS DR NOAM Server**: Login	Log into the DR NOAM as admusr
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

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

11. ☐	**SDS DR NOAM Server**: Load file	1. Insert the USB drive containing the server configuration file into the server's USB port.
		
		Figure 13. HP DL380 Gen8, Front Panel (USB Port)
		
		Figure 14. HP DL380 Gen9, Front Panel (USB Port)
		Output similar to this displays as the USB flash drive is inserted into the **SDS** 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>`
		2. Press **Enter** to return to the command prompt.

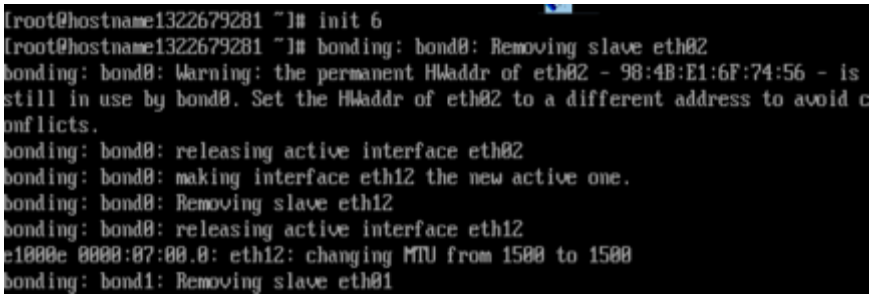
12. ☐	**SDS DR NOAM Server**: Verify software directory	Verify the USB drive has been mounted under the /media directory.
		`$ df |grep sdb`
		`/dev/sdb1 2003076 8 2003068 1% /media/sdb1`

13. ☐	**SDS DR NOAM Server**: Unmount USB	1. Unmount the USB drive partition. `$ sudo umount /media/sdb1` 2. Remove the USB drive from the server's front panel. ***Note:*** It is important to remove the USB drive before continuing.

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

14. ☐	**SDS DR NOAM Server**: Copy the configuration file	1. 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. For example:
		TKLCConfigData<.server_hostname>.sh translates to TKLCConfigData.sh
		`$ sudo cp –p /var/TLKC/db/filemgmt/TKLCConfigData.dr-sds-no-a.sh /var/tmp/TKLCConfigData.sh`
		Note: The server polls the /var/tmp directory for the presence of the configuration file and automatically executes it when found.
		After the script completes, a broadcast message is 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 2017):`
		`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.`
		2. Press **Enter**.

15. ☐	**SDS NOAM A or B**: Verify time zone	Verify the desired time zone is in use.
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2017`
		If the desired time zone is not displayed, set it with this command:
		`$ sudo set_ini_tz.pl <time_zone>`
		For example, to set the time to UTC (aka GMT):
		`$ sudo set_ini_tz.pl "Etc/UTC"`
		See Appendix G for a list of all valid time zones.

16. ☐	**Server NOAM A**: Reboot the OAM server	`$ sudo init 6` 

17. ☐	**SDS DR NOAM Server**: Login	After the server has completed the reboot, log into the server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

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

18. ☐	**SDS DR NOAM Server**: Verify IP addresses	Verify the IMI and XMI IP addresses from step 5. have been correctly loaded.
		`$ 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`

19. ☐	**SDS DR NOAM Server B**: Verify connectivity	Execute the ntpq command to verify 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`

		If connectivity to the NTP server(s) cannot be established, stop and contact the customer IT group to provide a network path from the SDS NOAM server XMI IP to the assigned NTP server IP addresses. Once network connectivity is established, repeat step 19.

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

20. ☐	**SDS DR NOAM Server**: Verify system state	Execute the syscheck command to verify the state 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`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

21. ☐	**SDS DR NOAM Server**: Exit	Exit to return to the server console to the login prompt. `$ exit`
22. ☐	Repeat	Configure SDS B by repeating steps 4. through 21. of this procedure.
		If aggregation switches are installed and 4948E-F switch configuration has not been completed before this step, stop and execute the following procedures: APPENDIX D.1 APPENDIX D.2 (Appendix D.2 references Appendix D.3, where applicable).

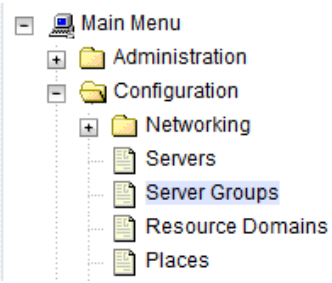
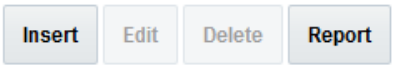
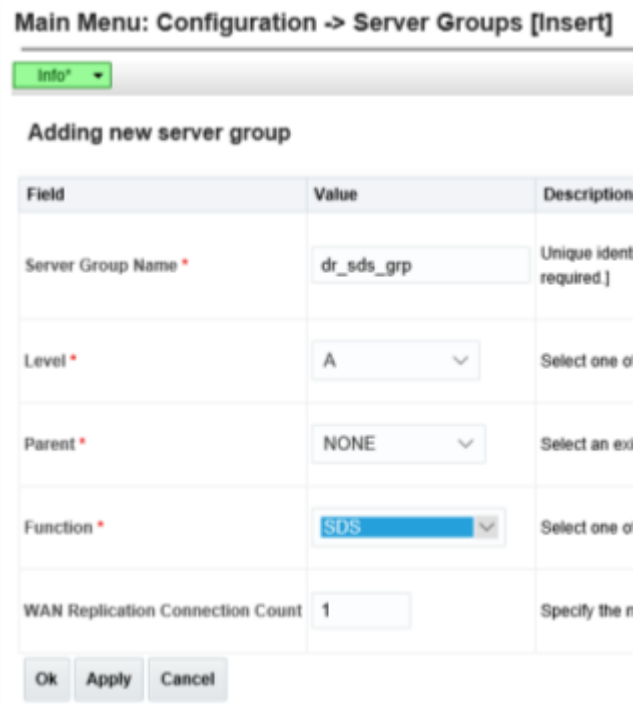
Procedure 6. Configure the DR NOAM Servers (DR SDS NOAM Site Only)		

23. ☐	**SDS DR NOAM**: Ping IMI and XMI addresses	1. From SDS DR NOAM A, ping the IMI IP address configured for SDS DR NOAM 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`
		2. From SDS DR NOAM, ping the 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`
		3. From SDS DR NOAM, ping 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`

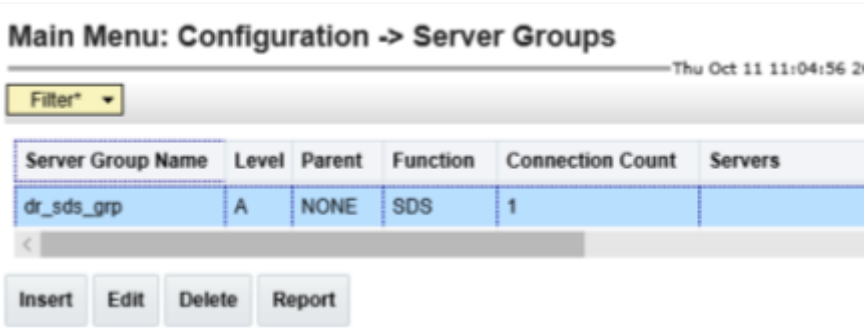
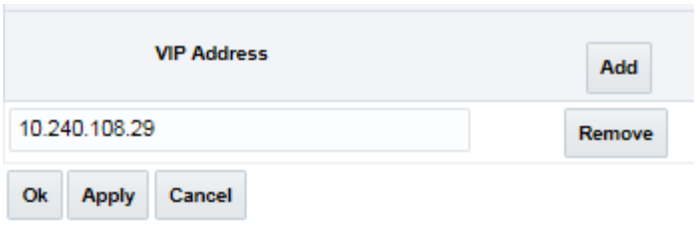
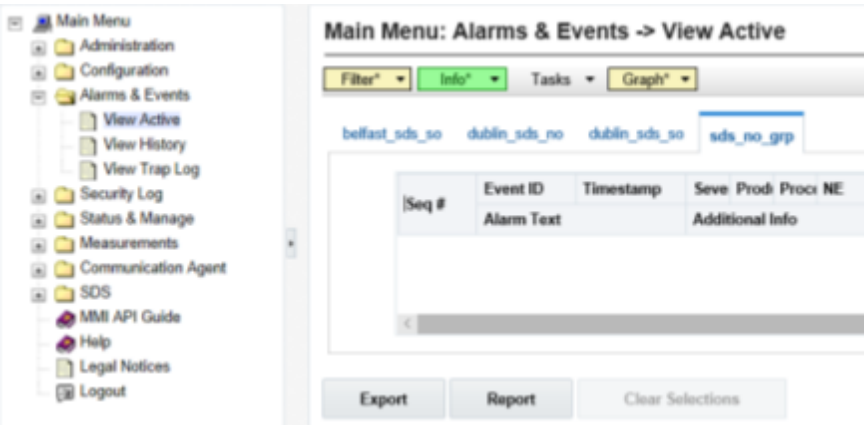
5.5 OAM Pairing for DR SDS NOAM Site

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. Pair the DR SDS NOAM Servers (DR SDS NOAM Site Only)		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

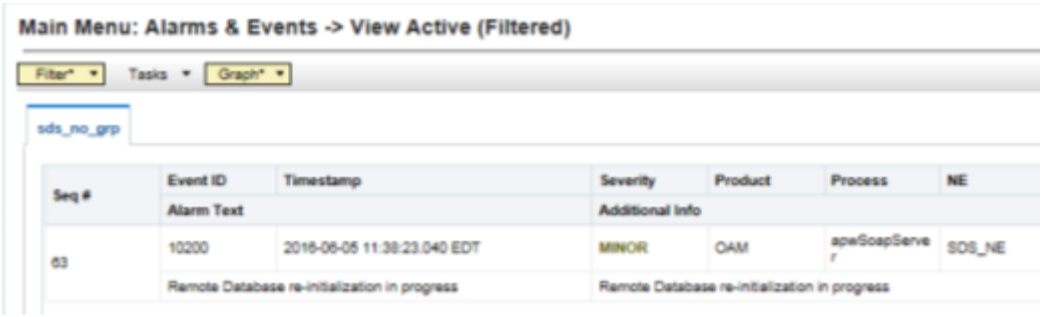
Procedure 7. Pair the DR SDS NOAM Servers (DR SDS NOAM Site Only)		
2. ☐	**Primary SDS VIP**: Create a server group	1. Navigate to **Configuration > Server Groups**.  2. Click **Insert**.  3. Fill in the following fields: **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: SDS (Active/Standby Pair) **WAN Replication Connection Count**: Use Default Value (1)  4. Click **OK**.

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

3. ☐	**Primary SDS VIP**: Add server to OAM Server Group	1. Select the new server group and click **Edit**.  2. Mark the **Include in SG** checkbox next to the A and B servers. 3. Click **Apply**. 4. Click **Add** next to VIP Address to add an IP. 5. Type the **VIP Address** and click **OK**. 
4. ☐	**Primary SDS NOAM VIP**: Make sure alarms clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 10200** displays with the DR SDS NOAM server hostname in the Instance field.

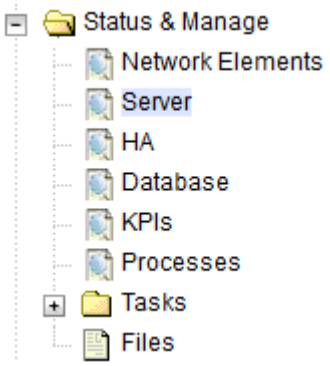
Procedure 7. Pair the DR SDS NOAM Servers (DR SDS NOAM Site Only)

Monitor event ID 10200 (Remote Database re-initialization in progress). Do not proceed to the next step until the alarm clears for both DR SDS NOAM servers.

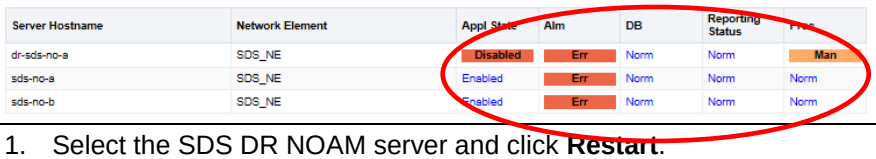


5. ☐ **Primary SDS NOAM VIP**: Verify status

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



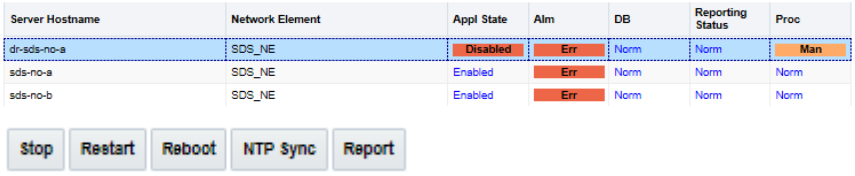
2. Verify the DB and Reporting Status is **Norm** and the Proc status is **Man** for both DR SDS NOAM servers.



Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
dr-sds-no-a	SDS_NE	Disabled	Err	Norm	Norm	Man
sds-no-a	SDS_NE	Enabled	Err	Norm	Norm	Norm
sds-no-b	SDS_NE	Enabled	Err	Norm	Norm	Norm

6. ☐ **Primary SDS NOAM VIP**: Restart the SDS DR NOAM server

1. Select the SDS DR NOAM server and click **Restart**.

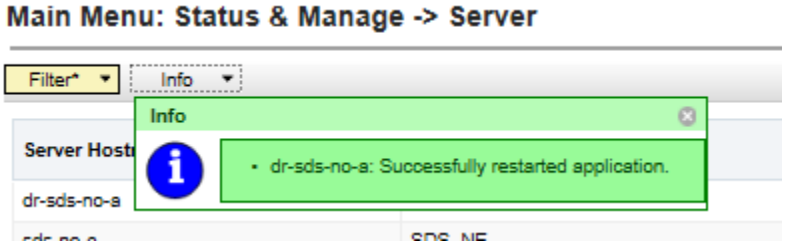


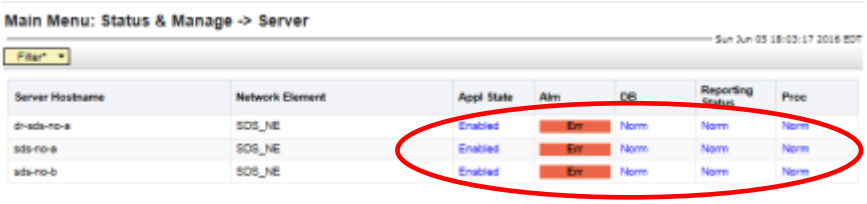
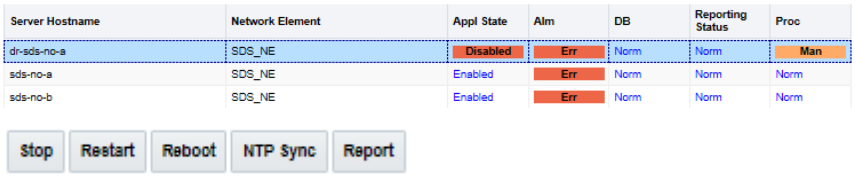
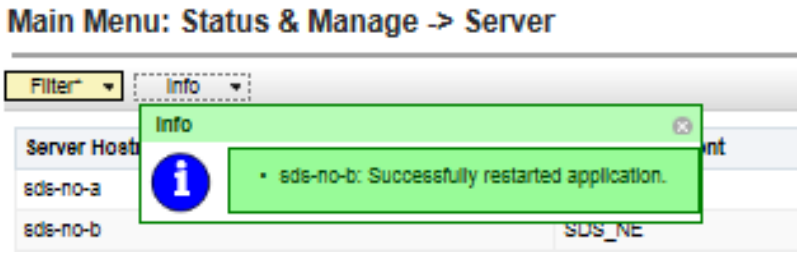
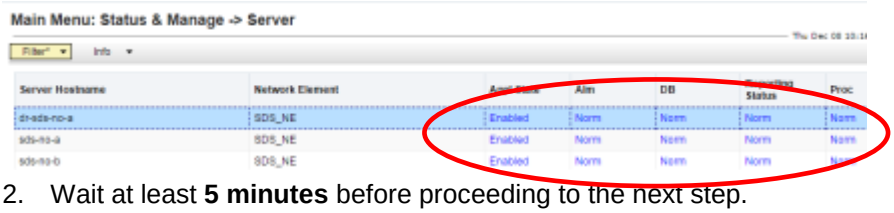
Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
dr-sds-no-a	SDS_NE	Disabled	Err	Norm	Norm	Man
sds-no-a	SDS_NE	Enabled	Err	Norm	Norm	Norm
sds-no-b	SDS_NE	Enabled	Err	Norm	Norm	Norm

Stop | Restart | Reboot | NTP Sync | Report

2. Click **OK** to confirm.

The Info banner displays a success message.



Procedure 7. Pair the DR SDS NOAM Servers (DR SDS NOAM Site Only)		
7. ☐	**Primary SDS NOAM VIP**: Verify status	Verify the Appl Ste is **Enabled**, the DB, Reporting Status, and Proc are **Norm** for the SDS NOAM A server. 
8. ☐	**Primary SDS NOAM VIP**: Restart the SDS NOAM B server	1. Select the SDS DR NOAM B server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
9. ☐	**Primary SDS NOAM VIP**: Verify status	1. Verify the Appl State is **Enabled**, and DB, Reporting Status, and Proc are **Norm** for both servers.  2. Wait at least **5 minutes** before proceeding to the next step. ***Important***: 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.
10. ☐	**Primary SDS VIP**: Add the Query server for the DR SDS	Repeat all steps listed in Procedure 5 except use the DR SDS NOAM NE and Server Group instead of the Primary SDS NOAM NE (1st SDS NOAM site) and Server Group.

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 a SDS SOAM site.

This procedure assumes the PMAC server has already been installed as described in [3].

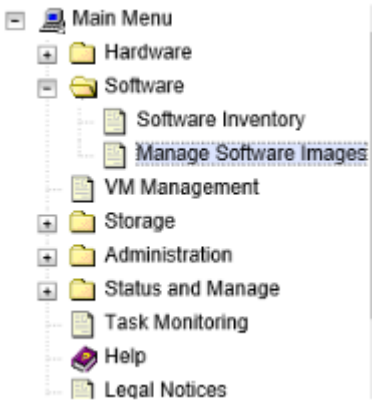
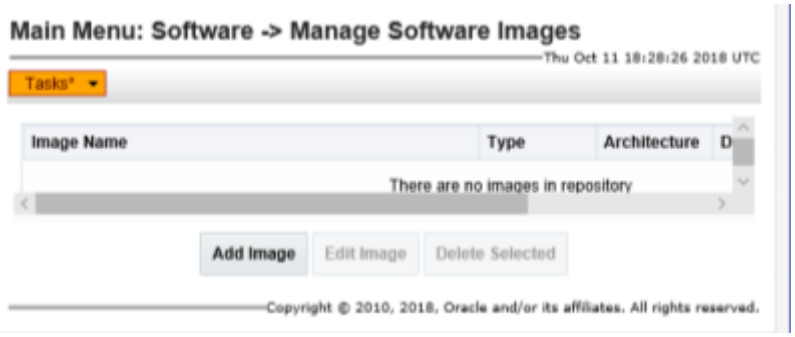
Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites		

1. ☐	**Active SDS VIP (CLI)**: Login	Log into the HP server as the admusr:
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

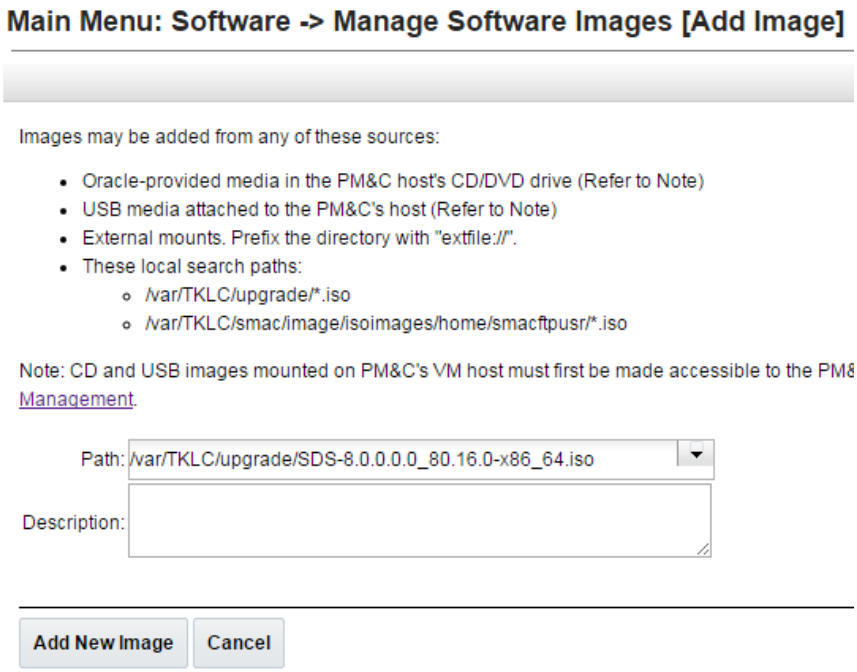
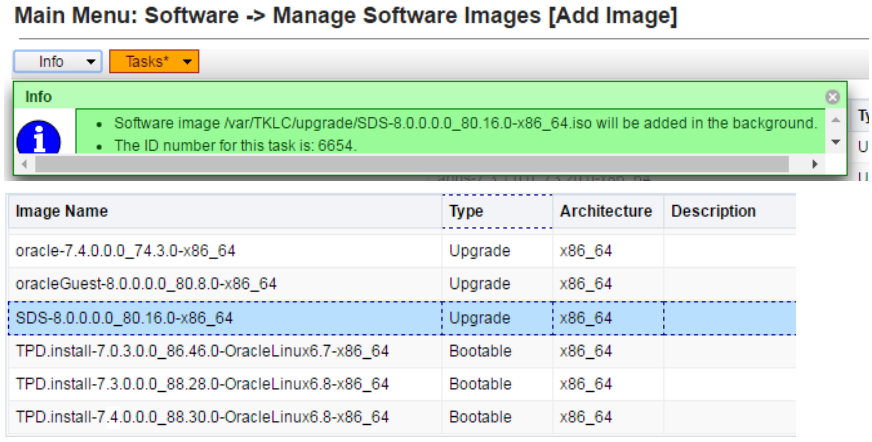
2. ☐	**Active SDS VIP (CLI)**: Change directory	Navigate to the /var/TKLC/upgrade/ directory. `$ cd /var/TKLC/upgrade/`

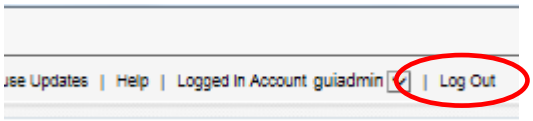
3. ☐	**Active SDS VIP (CLI)**: Verify ISO file is present	Verify the **SDS ISO** file is present.
		`$ ls`
		`SDS-8.1.0.0.0_80.16.0-x86_64.iso`

4. ☐	**Active SDS VIP (CLI)**: Trransfer ISO file	sftp the SDS ISO file to the PMAC server.
		`$ 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`
		Note: After the ISO has been transferred to PMAC server, the file can be removed from /var/TKLC/upgrade directory from this server.

Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites		
5. ☐	**PMAC Server GUI**: Login	Log into the active PMAC Guest server with the Mgmt IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.
6. ☐	**PMAC Server GUI**: Add the ISO image	1. Navigate to **Software > Manage Software Images**.  2. Click **Add Image**. 

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

7. ☐	**PMAC Server GUI**: Add the ISO image	1. Select the Path for the SDS ISO file from the /var/TKLC/upgrade directory. 2. Optionally add a Description. 3. Click **Add New Image**.  4. Click **OK** to confirum removing the source image. 5. Monitor progress on the screen and on the Tasks screen. 

Procedure 8. Add SDS Software Images to PMAC Servers for DSR Signaling Sites		
8. ☐	**PMAC Server GUI**: Logout	Click **Logout**. 

9. ☐	**PMACServer GUI**: Load TPD ISO	If the TPD ISO has not been loaded onto the PMAC already, add the TPD ISO image to the PMAC. This can be done in one of three ways:
		• Insert the Application CD required by the application into the removable media drive.
		• Attach the USB device containing the ISO image to a USB port.
		• Copy the application ISO file to the PMAC server into the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
		cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server).
		Using sftp, connect to the PMAC server
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		After the image transfer is 100% complete, close the connection:
		`$ quit`

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.

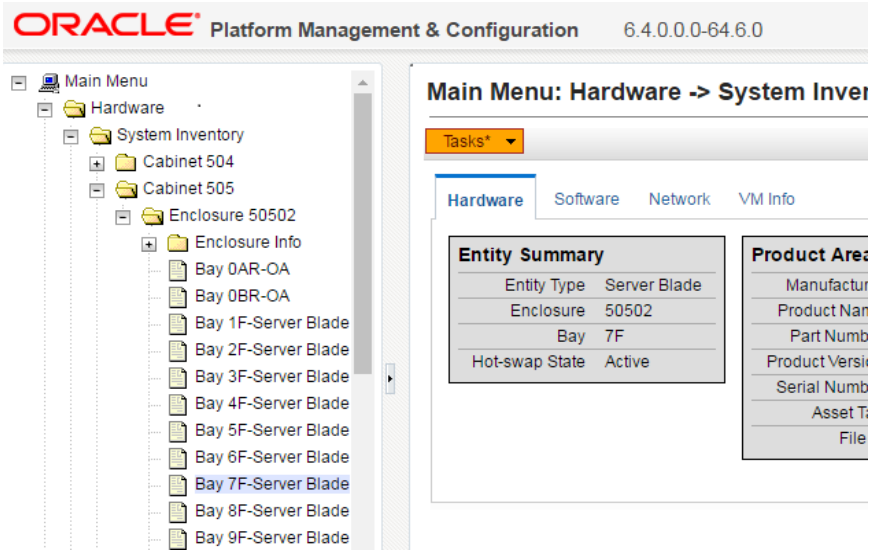
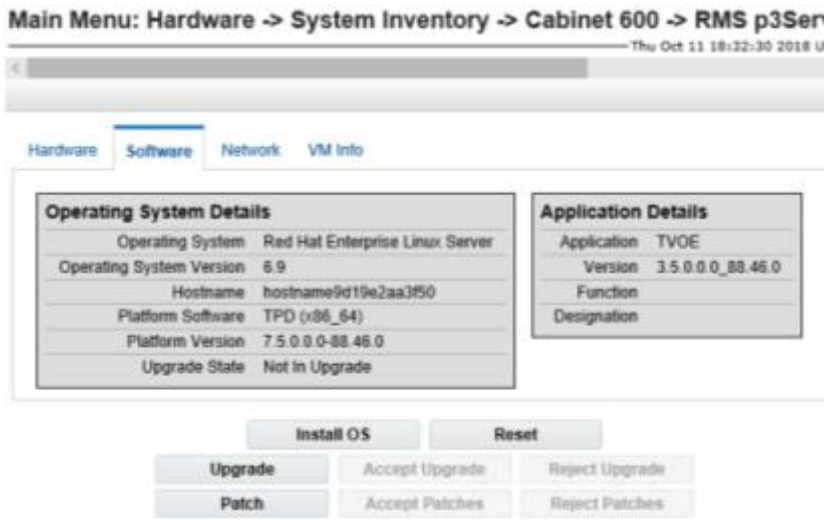
This procedure is for installing the SOAM software on the OAM server blades located at each DSR Signaling Site. The SOAM and DSR OAM servers run in two virtual machines on the same HP C-Class blade.

This procedure assumes DSR 8.2 or later OAM has already been installed in a virtual environment on the server blade, as described in as described in [3].

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. Configure the SDS SOAM Servers (All SOAM Sites)		
1. ☐	**PMAC Server GUI**: Login	Log into the active PMAC Guest server with the Mgmt IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

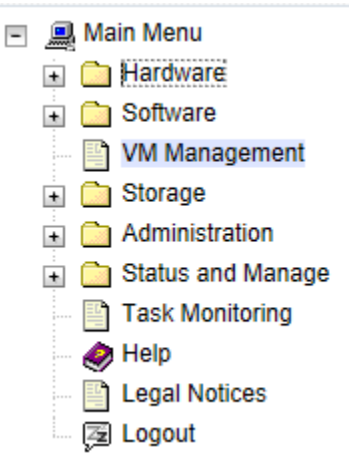
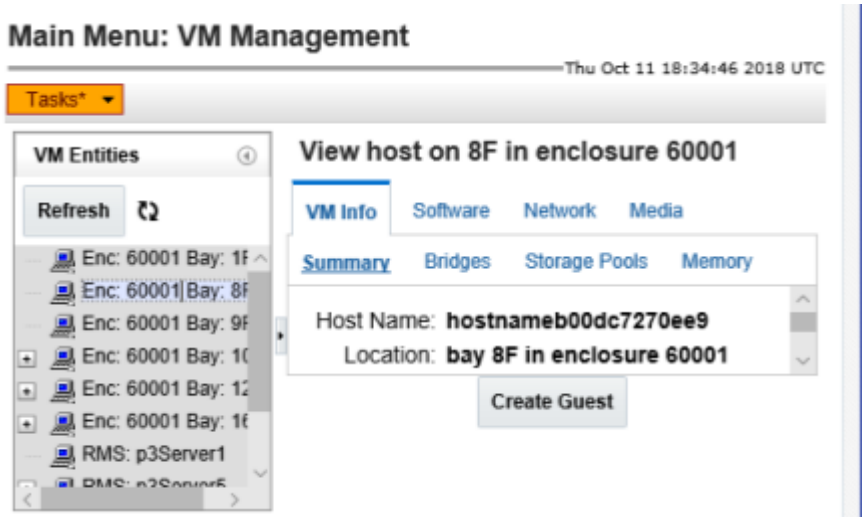
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)

2. ☐	**PMAC Server GUI**: Verify TVOE installation	1. Navigate to **Hardware > System Inventory > <Cabinet> > <Enclosure> > <Server Blade>**.  2. Select the Software tab and verify the TVOE application has been installed. 

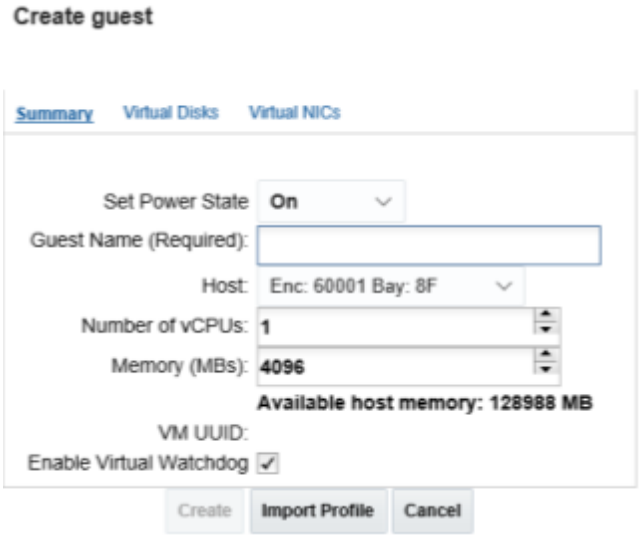
If TVOE was not installed or is the incorrect version on the blade server, stop and execute these steps:

- Verify the enclosure and bay number are correct.
- Refer to [1] for TVOE installation or contact DSR installation engineer to confirm the location of the OAM blade and status of TVOE installation.
- Restart this procedure.

Note: It is assumed the TVOE version corresponds with the correct DSR and SDS installation guidelines. This can be checked by executing **appRev**.

Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
3. ☐	**PMAC Server GUI**: Create a guest account	1. Navigate to **VM Management**.  2. In the VM Entitites box, select the desired server. 3. Click **Create Guest**.  4. Click **Import Profile**.

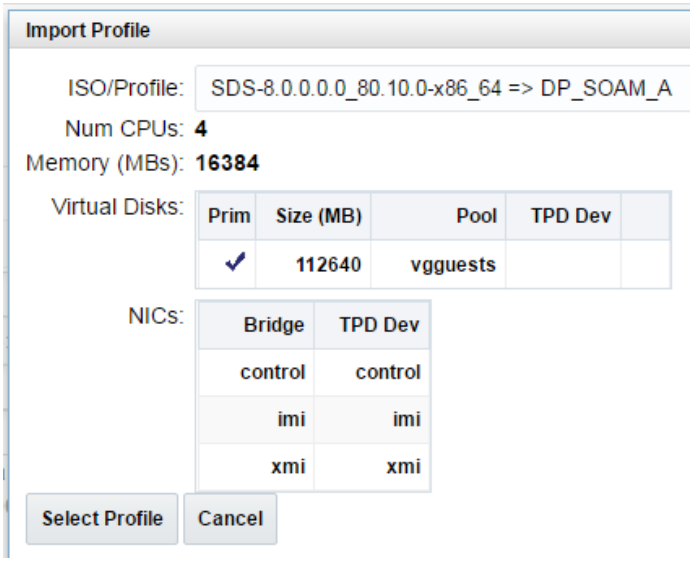
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)



5. Select ISO/Profile option that matches the hardware for the SOAM VM TVOE server and click **Select Profile**.

SDS Release	TVOE HW Type (BL460 Blade Server)	Role	Choose Profile (<Application ISO NAME>) >
8.2	Gen8/Gen9 Blade (if 1 Billion subscribers support is not needed)	SOAM-A	DP_SOAM_A
		SOAM-B	DP_SOAM_B
8.2	Gen8/Gen9 Blade (if 1 Billion subscribers support is needed)	SOAM-A SOAM-B	DP_SOAM_1B_RE

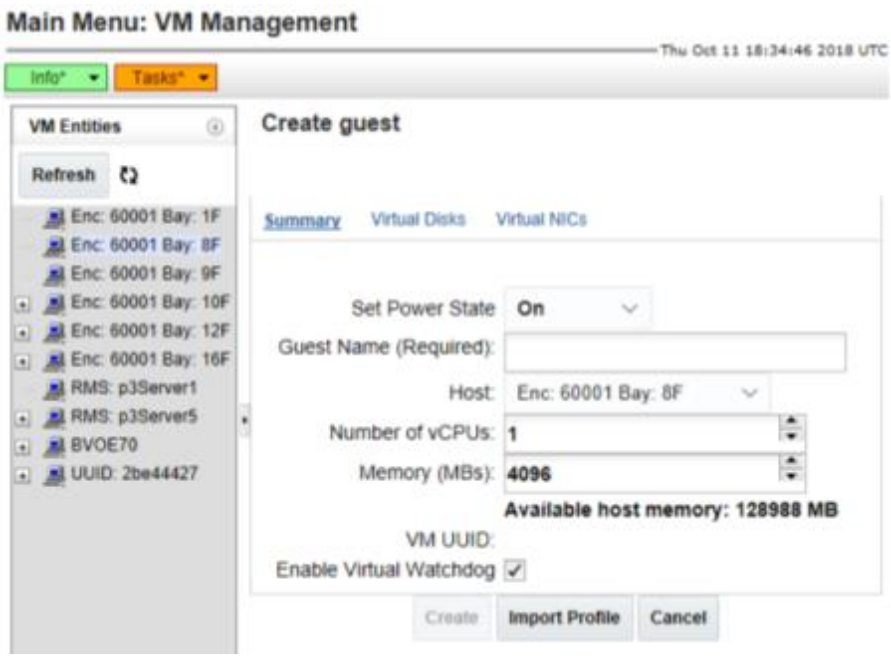
Note: Application_ISO_NAME is the name of the SDS application ISO to be installed on this SOAM.



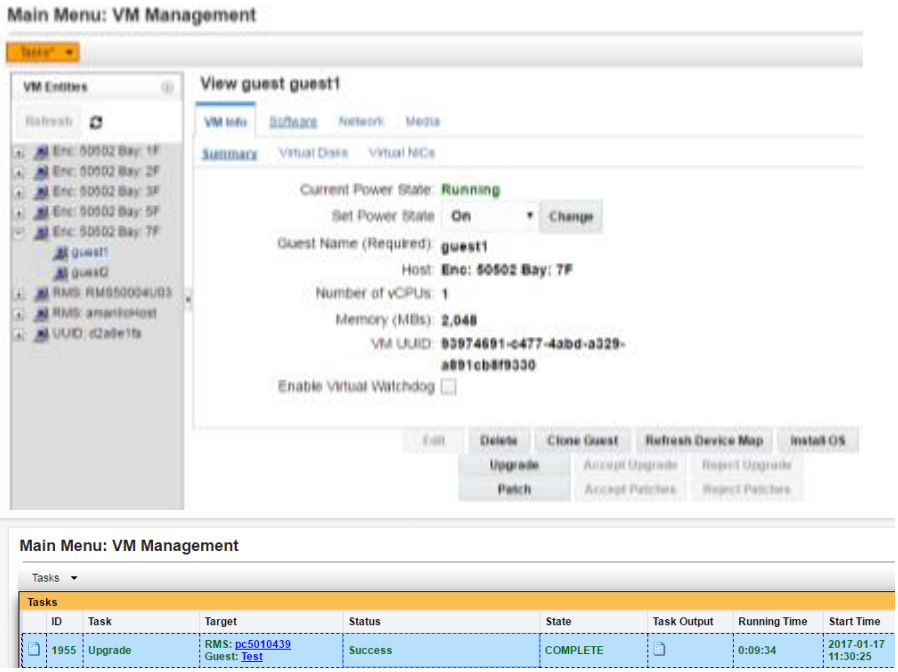
6. Overwrite the **Name** with the server host name (for example, so-mrsvnc-a).

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

7. Click **Create**.



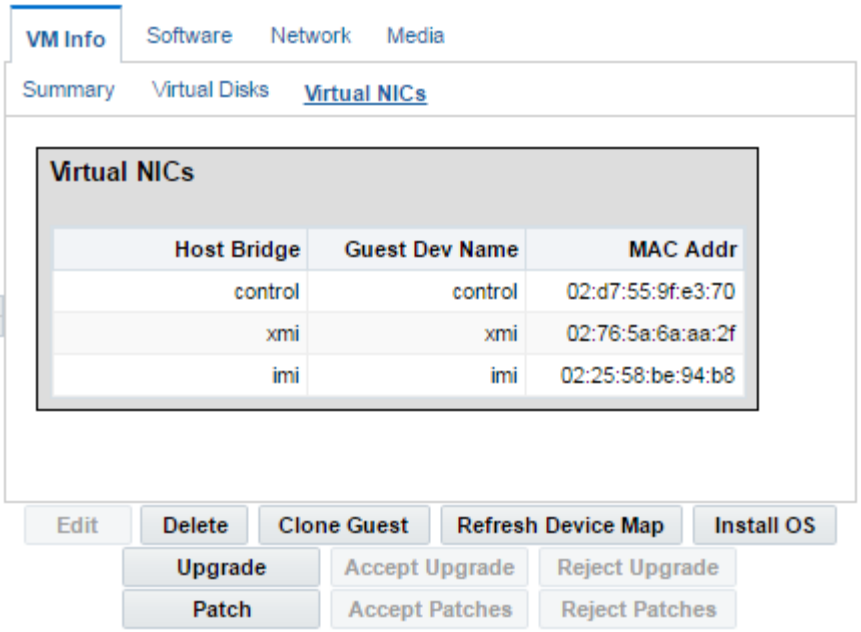
8. Verify that task successfully completes by monitoring progress on the screen and under the Tasks tab.



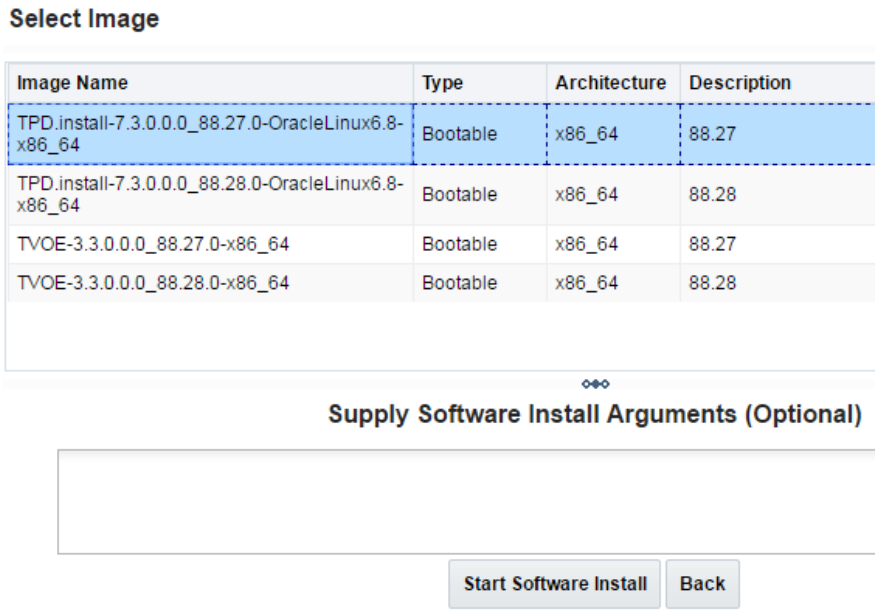
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)

4. ☐ **PMAC Server GUI**: Install the operating system

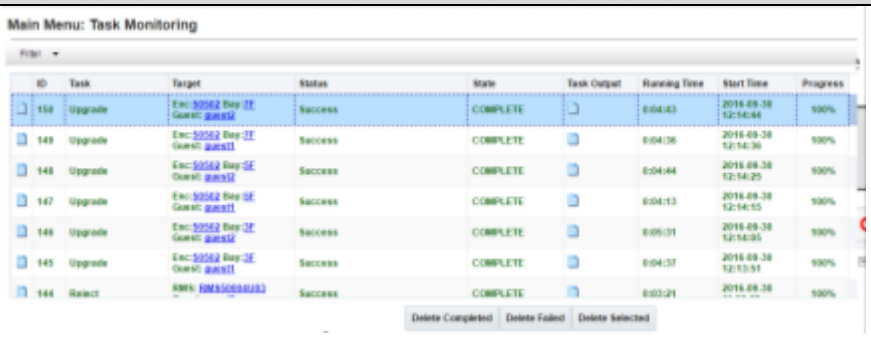
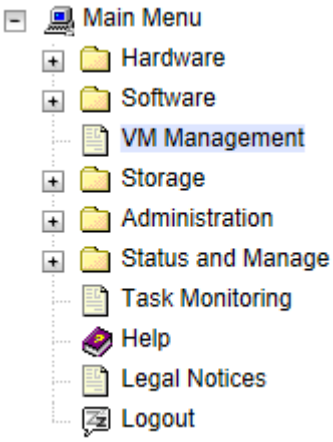
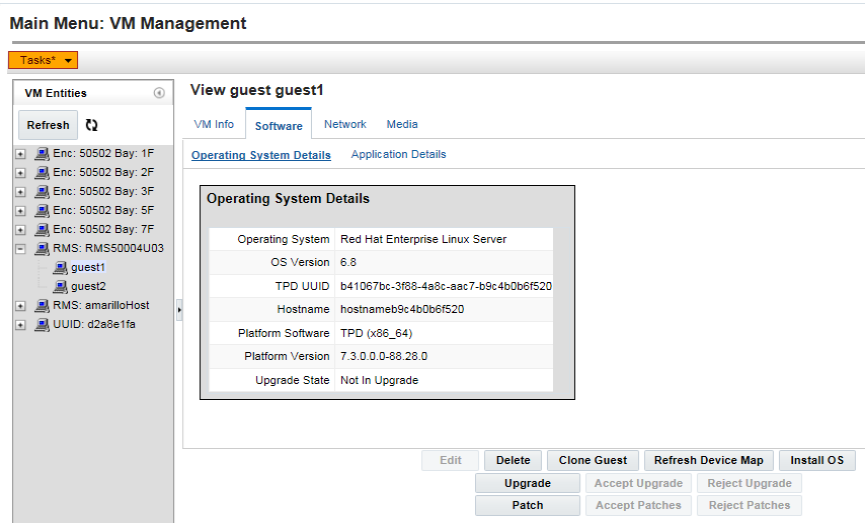
1. Click **Install OS**.



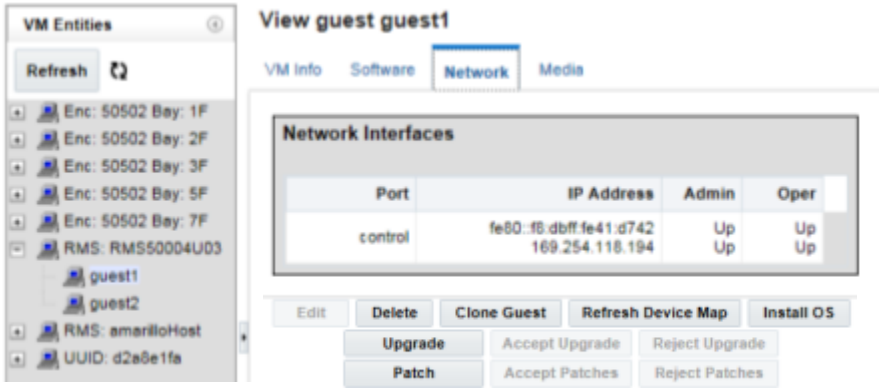
2. Select the desired TPD image and click **Start Install**.



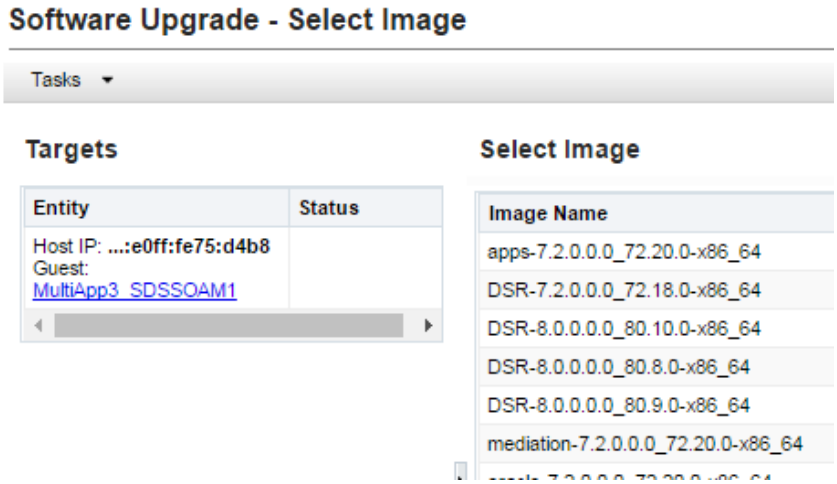
3. Click **OK** to confirm.
4. Monitor the task by navigating to **Task Monitoring**. It takes about 11 minutes to complete. Progress displays as 100%, Status shows Success, and State displays as Complete.

Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
		
5. ☐	**PMAC Server GUI**: Upgrade the network	1. Navigate to **VM Management**.  2. Under VM Entities column, expand (+) plus sign on the Host server containing the newly created VM Guest. 3. Select the Software tab and verify the OS has been installed.  4. Select the Application Details heading and verify the table is blank. 5. Select the Network tab and note the control IP address for this SOAM VM. It is referenced later. 6. Click **Upgrade**.

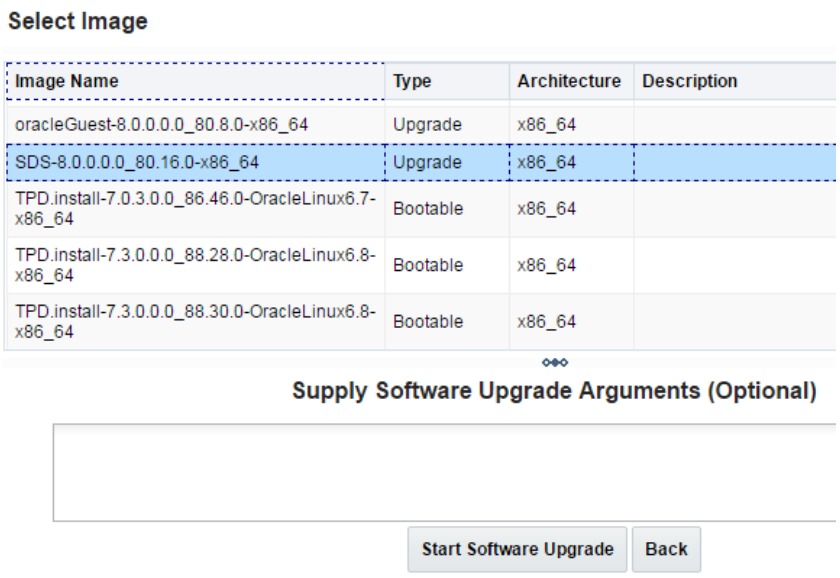
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)



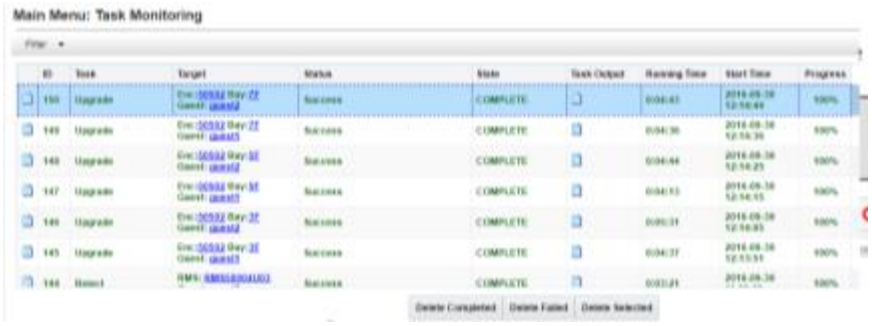
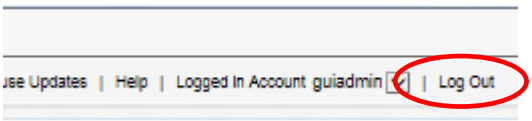
7. Select the correct SDS version from the Image Name list.

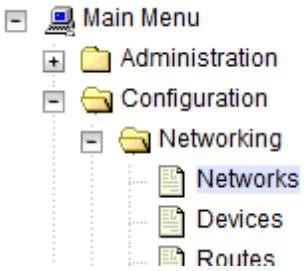
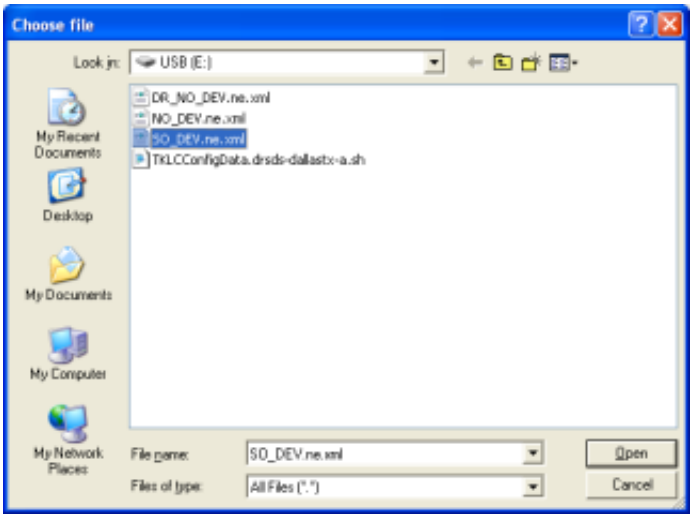
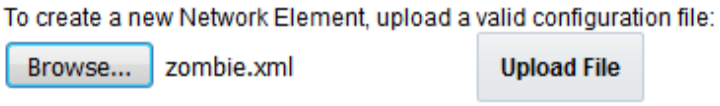


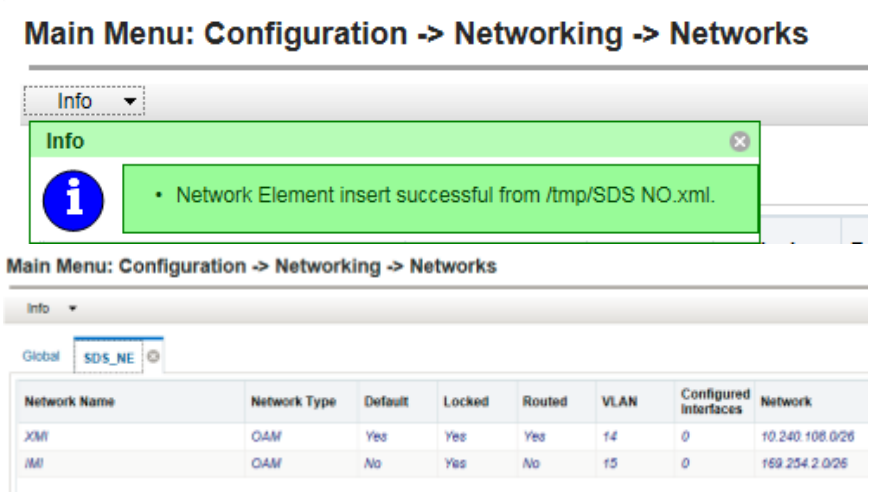
8. Click **Start Software Upgrade**.



9. Click **OK** to confirm.
10. Monitor the task by navigating to **Task Monitoring**. It takes about 8 minutes to complete. Progress displays as 100%, Status shows

Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
		Success, and State displays as Complete. 
6. ☐	Repeat	Repeat steps 2. through 5. of this procedure for the SOAM B server.
7. ☐	**PMAC Server GUI**: Logout	Click **Logout**. 
8. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
9. ☐	**Primary SDS VIP**: Create the SDS VIP network element using the XML file	1. Navigate to **Configuration > Networking > Networks**.  2. Click **Browse** and type the pathname of the NOAM network XML file. ***Note:*** This step assumes the **XML** files were previously prepared as described in Appendix E. 3. Select the location of the **XML** file and click **Open**.  4. Click **Upload File** to upload the XML file. 

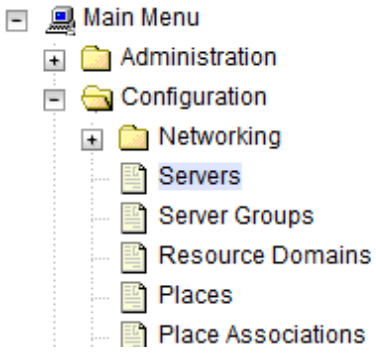
Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
10. ☐	**Primary SDS VIP**: Validate the file	Click **Info** to see the banner information showing that the data has been successfully validated and committed to the DB. 

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

11. ☐ **Primary SDS VIP**: Configure the SOAM server

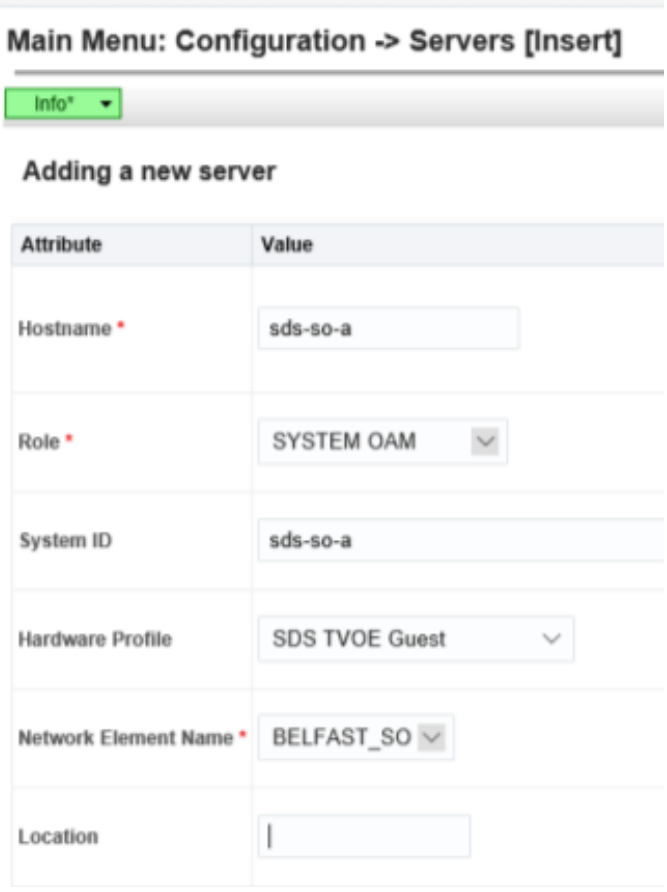
Note: This step through to step 14. of this procedure needs to be done for both the SDS SOAM A and SDS SOAM B servers.

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



2. Click **Insert**.
3. Fill in the fields:

Hostname:	<Assigned Hostname for SOAM server>
Role:	System OAM&P
System ID:	<Assigned Hostname for SOAM server>
Hardware Profile:	SDS TVOE Guest
Network Element Name:	[Select NE from list where SOAM (A or B) server is physically located]
Location:	(Optional) Enter the location of the server

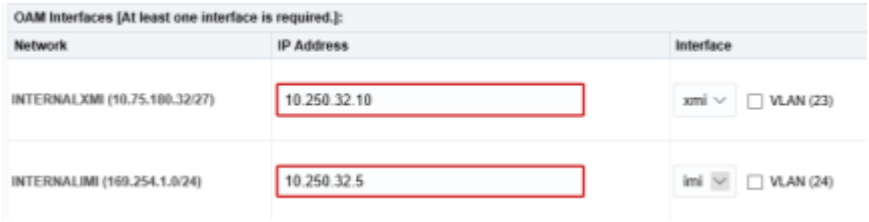


Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)

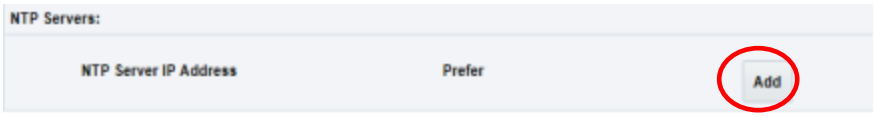
12. ☐ **Primary SDS VIP**: Insert the server

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

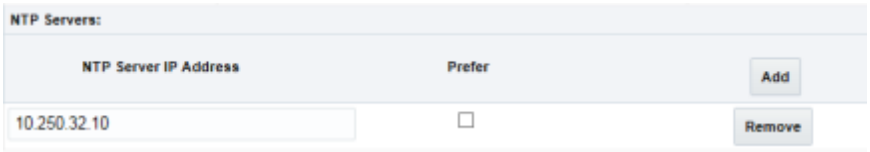
1. Type the XMI IP addresses for the SDS SOAM server, set the Interface to XMI, and do NOT mark the VLAN checkbox.
2. Type the IMI IP addresses for the SDS SOAM server, set the Interface to IMI, and do NOT mark the VLAN checkbox.



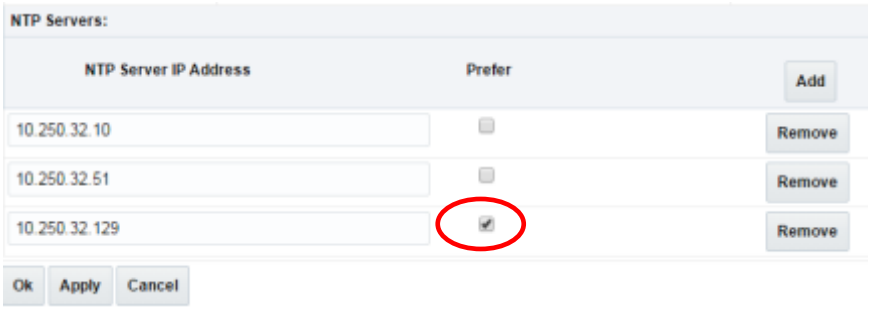
3. Click **Add** in the NTP Servers section.



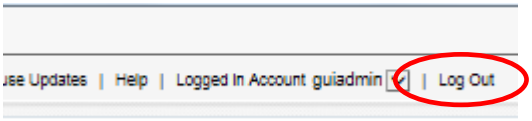
4. Type the **NTP Server IP Address**.



5. Repeat to add 3 NTP server IP addresses.
6. Optionally, mark the **Prefer** checkbox to prefer one server over the other.



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

Procedure 9. Configure the SDS SOAM Servers (All SOAM Sites)		
13. ☐	**Primary SDS VIP**: Export the initial configuration	From the GUI screen, select the SDS server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.
14. ☐	Repeat	Repeat steps 11. through 13. of this procedure to configure SDS SOAM B.
15. ☐	**Primary SDS VIP**: Logout	Click **Logout**. 
16. ☐	**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.

17. ☐	**Primary SDS VIP**: Login	Log into the HP server as admusr.
		`login: admusr`
		`Using keyboard-interactive authentication`
		`Password: <admusr_password>`

18. ☐	**Primary SDS VIP**: Change directory	Change directory to the file management space. `$ sudo cd /var/TKLC/db/filemgmt`

19. ☐	**Primary SDS VIP**: Find SOAM files	List the files to find the configuration files with the SOAM server A and B names.
		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`

20. ☐	**Primary SDS VIP**: Copy files	Copy the configuration files 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`

21. ☐	**Primary SDS VIP**: Logout	Exit the Primary SDS CLI. `$ exit`

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

22. ☐	**PMAC Server CLI**: Login	ssh to the PMAC Guest VM server as admusr.
		`login: admusr`
		`Password: <admusr_password>`

23. ☐	**PMAC Guest VM**: Key exchange	Keyexchange with SOAM control IP.
		`$ keyexchange admusr@<SOAM_Control_IP>`
		`[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.`

24. ☐	**PMAC Guest VM**: Copy file	Copy the server configuration file to the control IP for the SOAM.
		Note: The Control IP for each SOAM is obtained in step 5. of this procedure.
		`$ 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`

25. ☐	**PMAC Guest VM**: Connect to console	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>`

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

26. ☐	**SOAM Guest VM**: Copy the configuration file	1. 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. For example:
		TKLCConfigData<.server_hostname>.sh translates to TKLCConfigData.sh
		`$ sudo cp –p /var/TLKC/db/filemgmt/TKLCConfigData.dr-sds-no-a.sh /var/tmp/TKLCConfigData.sh`
		2. The server polls the /var/tmp directory for the presence of the configuration file and automatically executes it when found.
		After the script completes, a broadcast message is sent to the terminal.
		3. 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 2017):`
		`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.`
		4. Press **Enter**.

27. ☐	**SOAM Guest VM**: Verify time zone	Verify the time zone displayed matches value set in Procedure 3, step 17. .
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2017`

28. ☐	**SOAM Guest VM**: Reboot the SOAM server	`$ sudo init 6`
		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.`

29. ☐	**PMAC Guest VM**: Reconnect	After the SOAM server has rebooted, reconnect to the SOAM server console from the PMAC server console.
		`$ sudo ssh <SOAM_Control_IP>`
		`admusr@192.168.1.199's password: <admusr_password>`

30. ☐	**SOAM Guest VM**: Verify IP addresses	Verify the IMI and XMI IP addresses from step 12. have been correctly loaded.
		`$ 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`

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

31. ☐	**SOAM Guest VM**: Verify system state	Execute the syscheck command to verify the state 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`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

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

32. ☐	**SOAM Guest VM**: Accept upgrade to the application software	1. Run the accept script from the command line to start a screen session on blades and VM guest.
		2. Press **q** 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]`

33. ☐	Repeat	Repeat steps 22. through 32. of this procedure to configure SDS SOAM B.

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

34. ☐	**SOAM Guest B**: Ping IMI and XMI addresses	1. 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`
		2. 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`
		3. 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`

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

35. ☐	**SOAM Guest VM**: Verify connectivity	Execute the ntpq command to verify 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 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`

		If connectivity to the NTP server(s) cannot be established, stop and contact the customer IT group to verify the IP addresses for the NTP server(s) are correct. 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, repeat step 35.
36. ☐	**SOAM Guest VM**: Exit	Exit from the SOAM command line to return to the PMAC server console prompt. `$ exit`
37. ☐	**PMAC Guest VM**: Exit	Exit from the PMAC server. `$ exit`

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

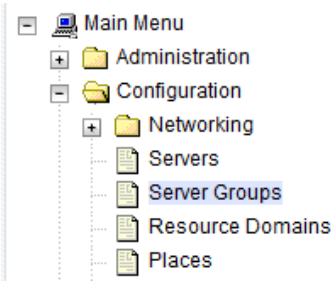
The user should be aware that during the OAM Pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 10. Pair the SDS SOAM Servers (All SOAM Sites)		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

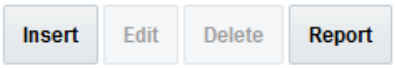
Procedure 10. Pair the SDS SOAM Servers (All SOAM Sites)

2. ☐ **Primary SDS VIP**: Create a server group

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

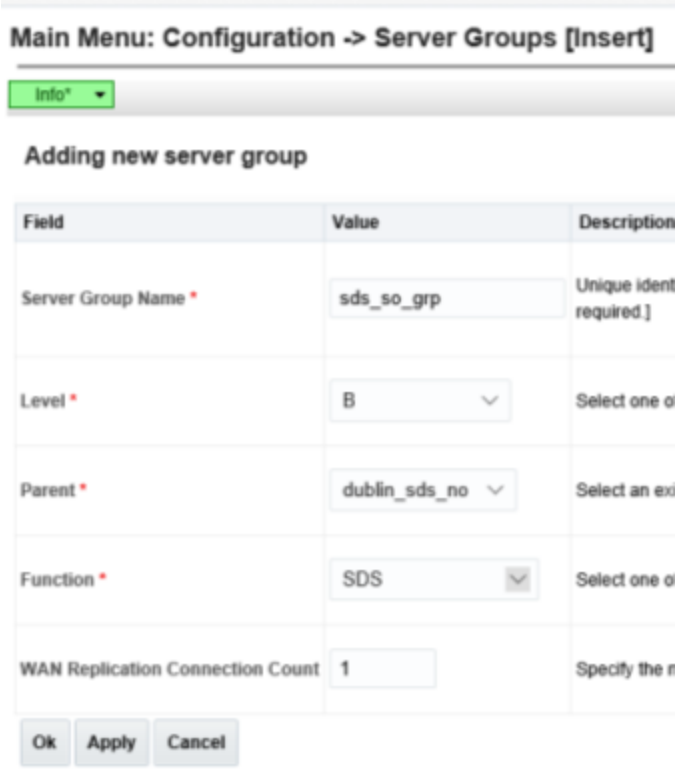


2. Click **Insert**.



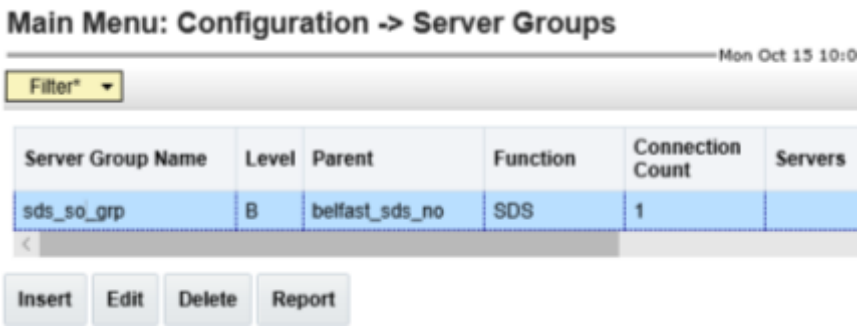
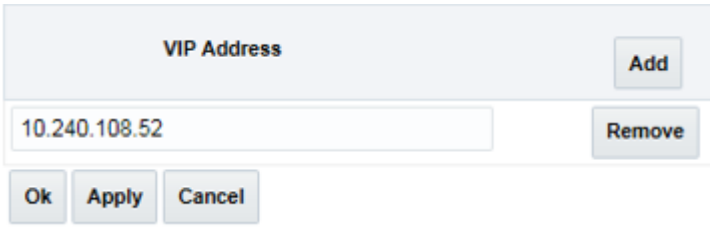
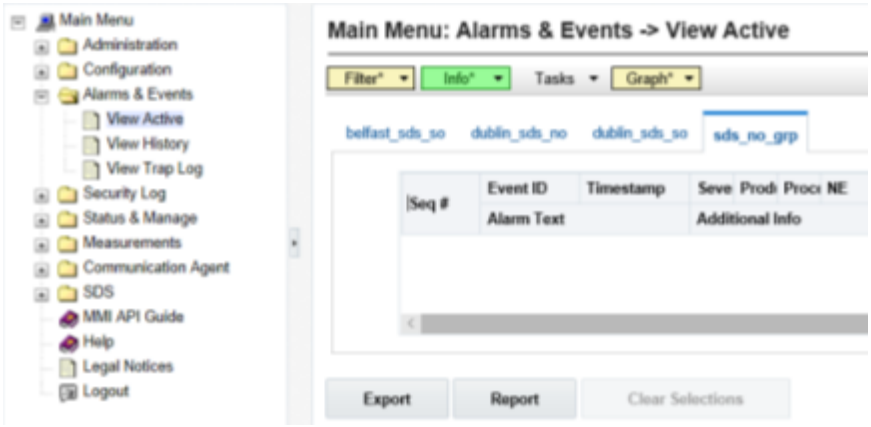
3. Fill in the following fields:

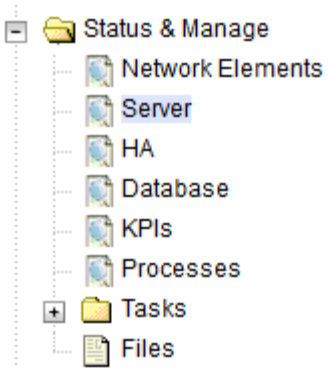
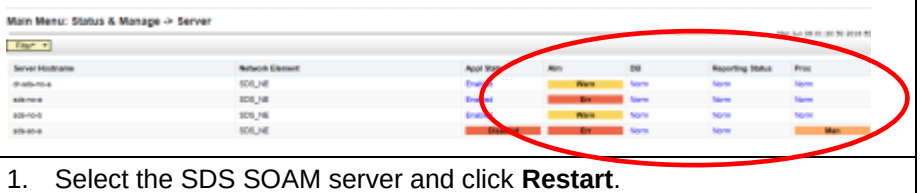
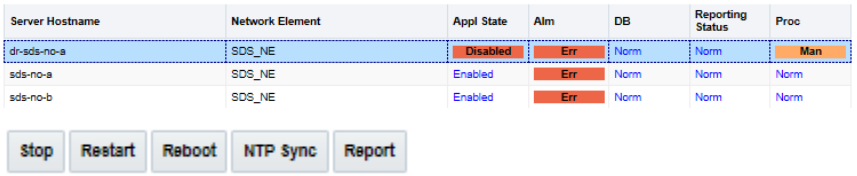
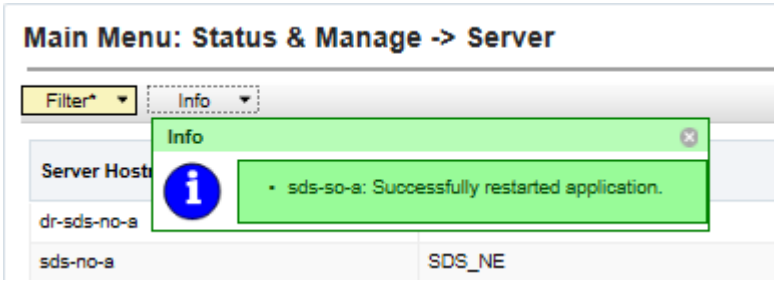
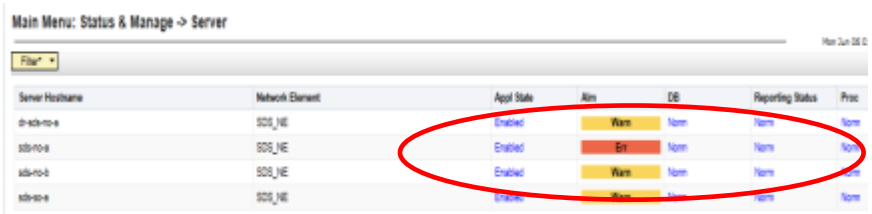
Server Group Name:	<Server Group Name>
Level:	B
Parent:	First site's server group
Function:	SDS (Active/Standby Pair)
WAN Replication Connection Count:	Use Default Value (1)

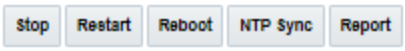
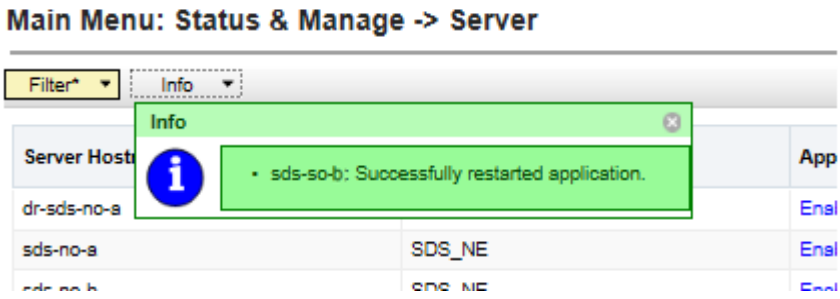
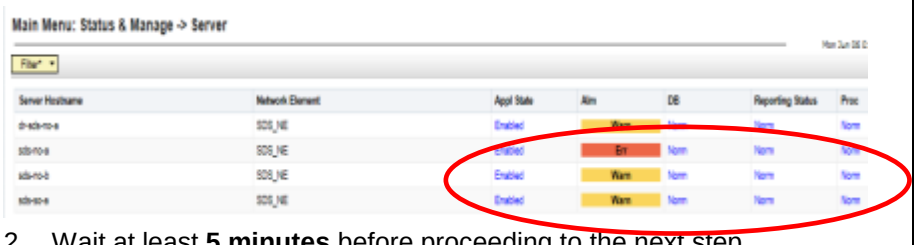
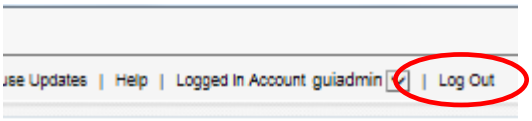


4. Click **OK**.

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

3. ☐	**Primary SDS VIP**: Add server to OAM Server Group	1. Select the new server group and click **Edit**.  2. Mark the **Include in SG** checkbox next to the A and B servers. 3. Click **Apply**. 4. Click **Add** next to VIP Address to add an IP. 5. Type the **VIP Address** and click **OK**. 
4. ☐	**Primary SDS VIP**: Make sure alarms clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 10200** displays with the SDS SOAM 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 clears for both SDS SOAM servers.

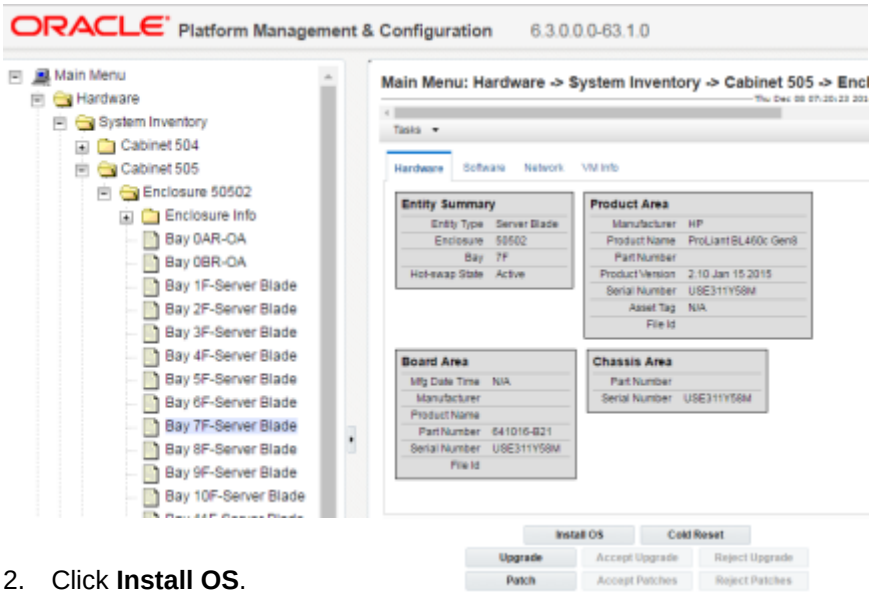
Procedure 10. Pair the SDS SOAM Servers (All SOAM Sites)		
5. ☐	**Primary SDS VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify the DB is **Norm** and the Proc status is **Man** for both servers. 
6. ☐	**Primary SDS VIP**: Restart the SDS SOAM server	1. Select the SDS SOAM server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
7. ☐	**Primary SDS VIP**: Verify status	Verify the Appl Ste is **Enabled**, the DB, Reporting Status, and Proc are **Norm** for the SDS SOAM A server. 

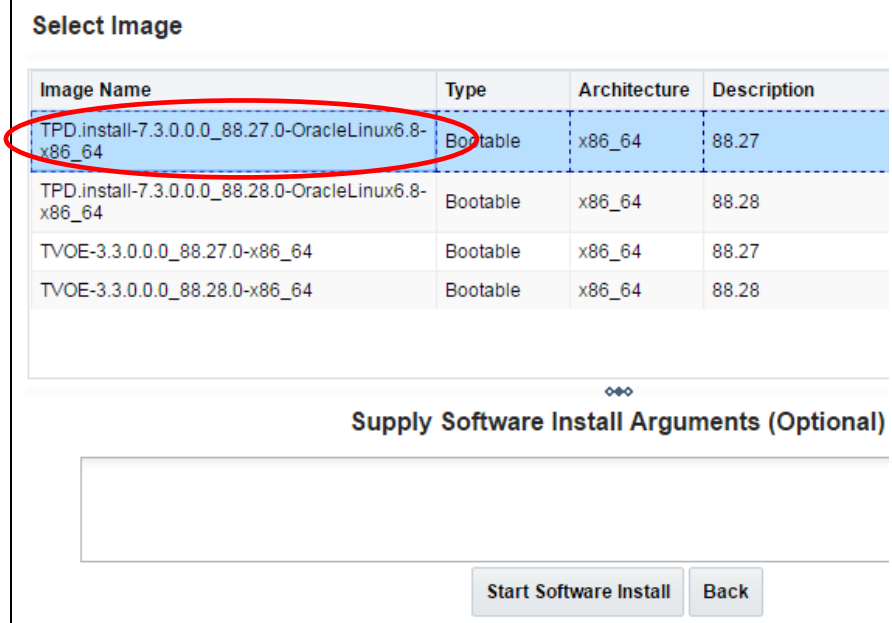
Procedure 10. Pair the SDS SOAM Servers (All SOAM Sites)		
8. ☐	**Primary SDS VIP**: Restart the SDS SOAM B server	1. Select the SDS SOAM B server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 
9. ☐	**Primary SDS VIP**: Verify status	1. Verify the Appl State is **Enabled**, and DB, Reporting Status, and Proc are **Norm** for both servers.  2. Wait at least **5 minutes** before proceeding to the next step. ***Important***: To refresh the status screen, navigate to **Status & Manage > Server** again from the main menu.
10. ☐	**Primary SDS VIP**: Logout	Click **Logout**. 

5.9 DP Installation (All SOAM Sites)

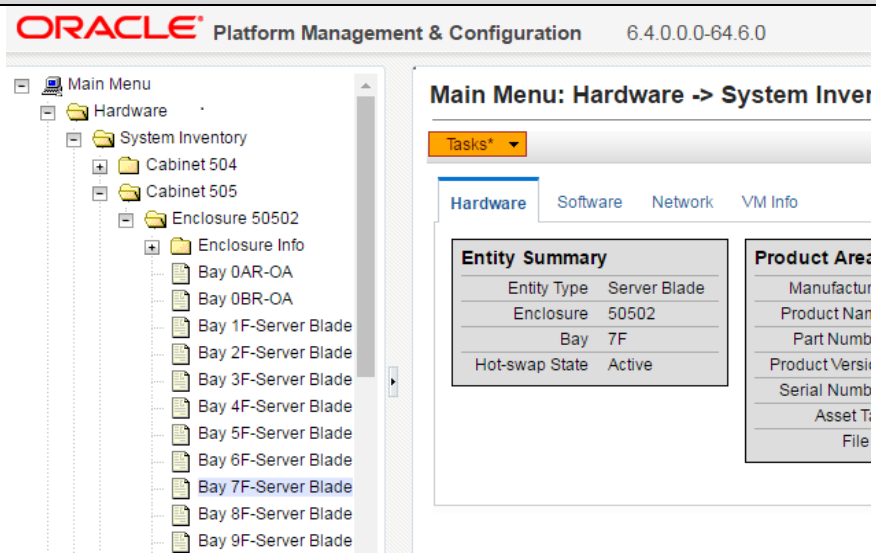
During the Data Processor (DP) installation, various errors may display at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
		Execute Appendix I Disable Hyperthreading for Gen8 and Gen9 (DP Only) on each DP blade after this procedure.
1. ☐	**PMAC Guest VM**: Login	Log into the active PMAC Guest SOAM server with the XMI IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.

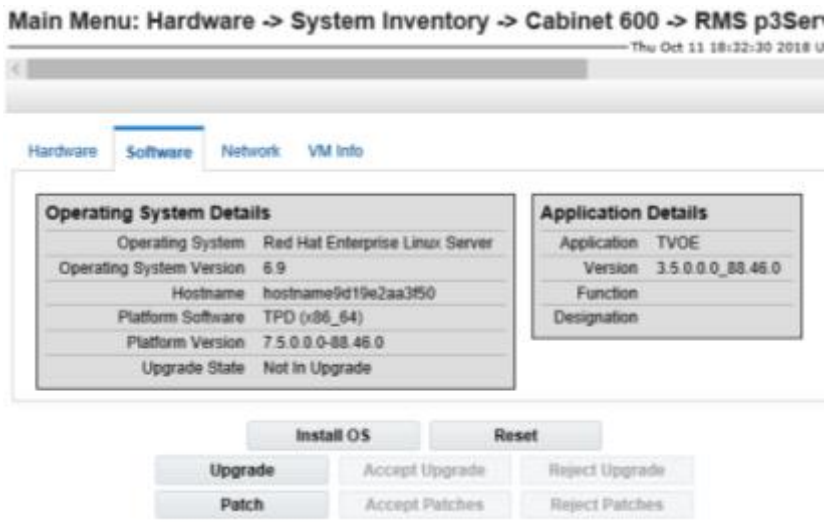
Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
2. ☐	**PMAC Guest VM**: Install OS	1. Navigate to **Hardware > System Inventory > <Cabinet> > <Enclosure> > <Server Blade>**.  2. Click **Install OS**.

Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
3. ☐	**PMAC Guest VM**: Upgrade the server	1. Select the **TPD Image** from the Image Name list and click **Start Software Install**.  2. Click **OK** to confirm. 3. Monitor the task by navigating to **Task Monitoring**. It takes about 25 minutes to complete. Progress displays as 100%, Status shows Success, and State displays as Complete. 4. Note the task number assigned to SDS Application upgrade. This number is used to track its progress.
4. ☐	Repeat	Repeat steps 2. and 3. of this procedure for each additional DP server blade in the SOAM enclosure.
5. ☐	**PMAC Guest VM**: Verify TPD installation	1. Navigate to **Hardware > System Inventory > <Cabinet> > <Enclosure> > <Server Blade>**.

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

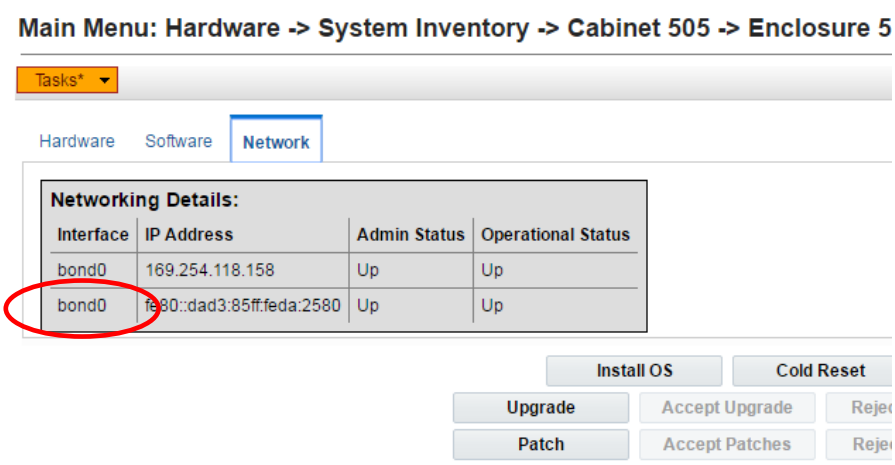


2. Select the Software tab and verify the TPD application has been installed.

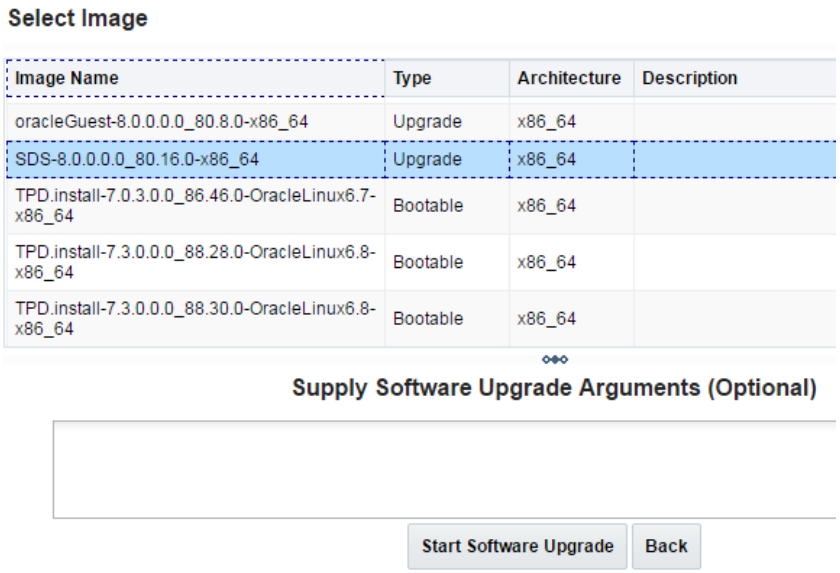


3. Select the Network tab and note the control IP address for the DR called **bond0**. It is referenced later.
4. Click **Upgrade**.

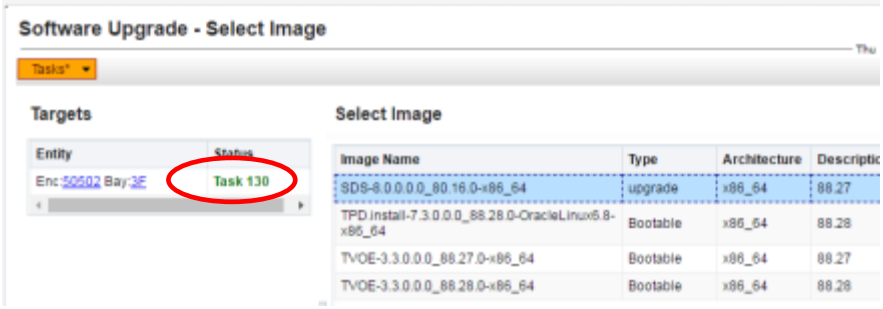
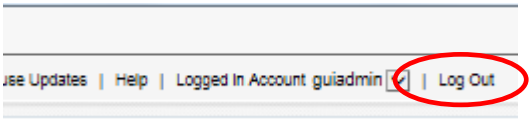
Procedure 11. Install the Data Processor Blade (All SOAM Sites)



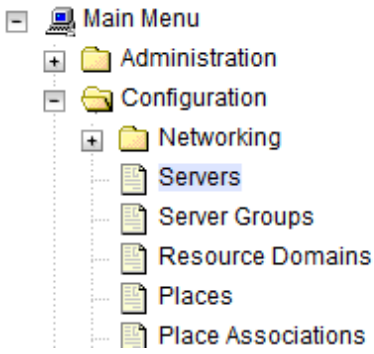
5. Select the correct SDS version from the Image Name list.
6. Click **Start Software Upgrade**.



7. Click **OK** to confirm.
8. Monitor the task by navigating to **Task Monitoring**. It takes about 20 minutes to complete. Progress displays as 100%, Status shows Success, and State displays as Complete.
9. Note the task number assigned to the SDS application upgrade. This number is used to track its progress.

Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
		
6. ☐	Repeat	Repeat step 5. of this procedure for each additional DP server blade.
7. ☐	**PMAC Guest VM**: Logout	Click **Logout**. 
8. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP address as the **default** user. If the Security Certificate Warning screen displays, click **Continue to this website (not recommended)**.
9. ☐	**Primary SDS VIP**: Configure the DP server ***Note***: This step through to step 13. of this procedure needs for each DP server.	1. Navigate to **Configuration > Servers**.

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



2. Click **Insert**.
3. Fill in the fields:

Hostname: <Assigned Hostname for DP server>
Role: MP
System ID: <Assigned Hostname for DP server>
Hardware Profile: Use table to select appropriate profile

DP HW Profile	Network	Bonded Interfaces	Comments
SDS HP c-Class Blade V0	IMI	Bond0 (eth01, eth02)	Use when both XMI and IMI are to be VLAN tagged.
	XMI		
SDS HP c-Class Blade V1	IMI	Bond0 (eth01, eth02)	Use when XMI enclosure switches are connected to DP blade mezzanine card ports eth23 / eth24.
	XMI	bond1 (eth23, eth24)	
SDS HP c-Class Blade V2	IMI	Bond0 (eth01, eth02)	Use when XMI enclosure switches are connected to DP blade mezzanine card ports eth21 / eth22.
	XMI	bond1 (eth21, eth22)	

Network Element Name: [Select NE from list where DP server is physically located]
Location: (Optional) Enter the location of the server

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

10. **Primary SDS VIP**: Insert the server

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

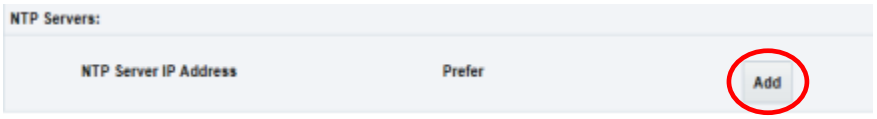
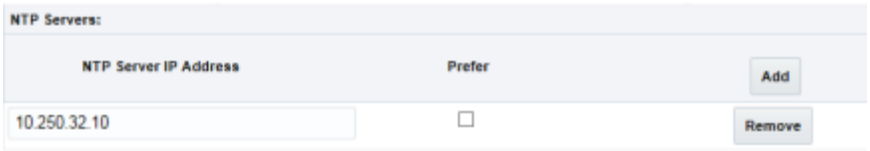
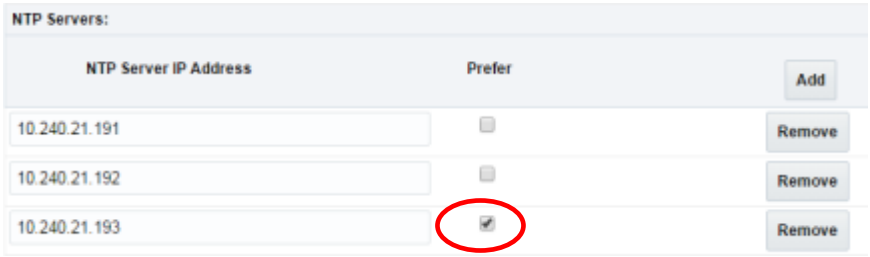
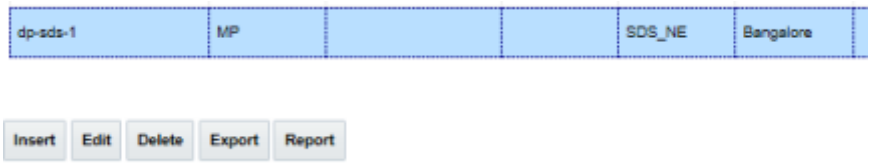
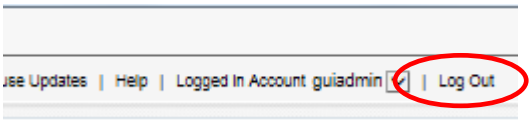
1. Type the IMI IP addresses for the **DP** server, select **bond0** as the interface, and mark the **VLAN** checkbox.
2. Type the XMI IP addresses for the **DP** server.
   - For Layer 3, where no VLAN tagging is used for XMI, select **bond1** as the Interface and do NOT mark the VLAN checkbox.

     or
   - For Layer 2, where VLAN tagging is used for XMI, select **bond0** as the Interface and mark the VLAN checkbox.

DP Server	Network	Interface	VLAN Checkbox
DP Server	XMI	bond1	✗
		bond0	✓

!!!CAUTION!!!

3. It is crucial the correct network configuration be selected in this step. Choosing an incorrect configuration results in the need to re-install the OS and restart the Query server installation procedure from the beginning.

Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
11.	**Primary SDS VIP**: Insert server	1. Click **Add** in the NTP Servers section.  2. Type the **NTP Server IP Address**.  3. Repeat to add 3 NTP server IP addresses. 4. Optionally, mark the **Prefer** checkbox to prefer one server over the other.  5. Click **OK** when you have completed entering all the server data.
12. ☐	**Primary SDS VIP**: Insert server	From the GUI screen, select the DP server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created. 
13. ☐	Repeat	Repeat steps 9. through 13. of this procedure for each DP server installed in the SOAM cabinet.
14. ☐	**Primary SDS VIP**: Logout	Click **Logout**. 

15. ☐	**Primary SDS VIP**: Login	ssh to the Primary SDS NOAM VIP as admusr.
		`login: admusr`
		`Password: <admusr_password>`

16. ☐	**Primary SDS VIP**: Change directory	Change directory to the file management space. `$ sudo cd /var/TKLC/db/filemgmt`

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

17. ☐	Primary SDS VIP: Find DP files	List the files to find the configuration files with the DP server names.
		Note: These should appear toward the bottom of the listing.
		`$ 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`

18. ☐	**Primary SDS VIP**: Copy files	Copy the configuration files to the PMAC.
		`$ 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`

19. ☐	**Primary SDS VIP**: Logout	Exit the Primary SDS CLI. `$ exit`

20. ☐	**PMAC Server CLI**: Login	ssh to the PMAC Guest VM server as admusr.
		`login: admusr`
		`Password: <admusr_password>`

21. ☐	**PMAC Guest VM**: Key exchange	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.`

22. ☐	**PMAC Guest VM**: Copy file	Copy the server configuration file to the control IP for the DP server.
		Note: The Control IP for each DP server is obtained in step 5. (3) of this procedure.
		`$ 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`

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

23. ☐	**PMAC Guest VM**: Connect to console	Connect to the DP server console from the PMAC server console.
		`$ ssh <DP_Control_IP>`
		`Password: <admusr_password>`

24. ☐	DP Server: Copy the configuration file	1. 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 from the file name. For example:
		TKLCConfigData<.server_hostname>.sh translates to TKLCConfigData.sh
		`$ sudo cp –p /var/TKLC/db/filemgmt/TKLCConfigData.dp-carync-1.sh /var/tmp/TKLCConfigData.sh`
		2. The server polls the /var/tmp directory for the presence of the configuration file and automatically executes it when found.
		After the script completes, a broadcast message is sent to the terminal.
		3. 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 2017):`
		`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.`
		4. Press **Enter**.

25. ☐	**DP Server**: Verify time zone	Verify that the desired time zone is currently in use.
		`$ date`
		`Mon Aug 10 19:34:51 UTC 2015`

26. ☐	**DP Server**: Reboot the DP server	`$ sudo init 6`
		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.`

27. ☐	**PMAC Guest VM**: Reconnect	After the DP server has rebooted, reconnect to the DP server console from the PMAC server console.
		`$ sudo ssh <DP_Control_IP>`
		`Password: <admusr_password>`

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

28. ☐	**DP Server**: Verify IP addresses	Verify the IMI and XMI IP addresses from step 10. have been correctly loaded to bond1 and bond0.4.
		`$ 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`

29. ☐	**SOAM Guest VM**: Verify system state	Execute the syscheck command to verify the state 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`
		Note: Stop and resolve any errors returned from syscheck before continuing with the next step.

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

30. ☐	**DP Server**: Accept upgrade to the application software	1. Run the accept script from the command line to start a screen session on blades and VM guest.
		2. Press **q** 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]`

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

31. ☐	**DP Server**: Ping IMI and XMI addresses	1. 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`
		2. From the DP server, ping the 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`

32. ☐	**DP Server**: Verify connectivity	Execute the ntpq command to verify 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 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`

33. ☐	**DP Server**: Disable hyper threading	Execute Appendix I: Disable Hyper threading (DP Only) on server.

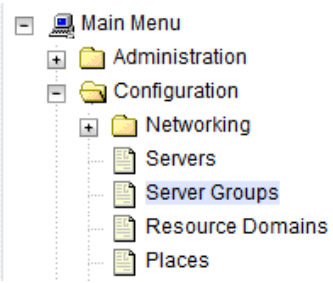
34. ☐	**DP Server**: Exit	Exit from the command line to return to the server console prompt.
		`$ exit`
		`Connection to 192.168.1.199 closed.`

35. ☐	Repeat	Repeat steps 22. through 34. of this procedure for each DP server installed in the same SOAM enclosure.
36. ☐	**PMAC Guest VM**: Exit	Exit from the PMAC server. `$ exit`

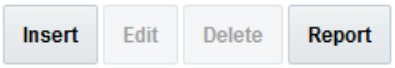
Procedure 11. Install the Data Processor Blade (All SOAM Sites)

37. ☐ **Primary SDS VIP**: Create a server group

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

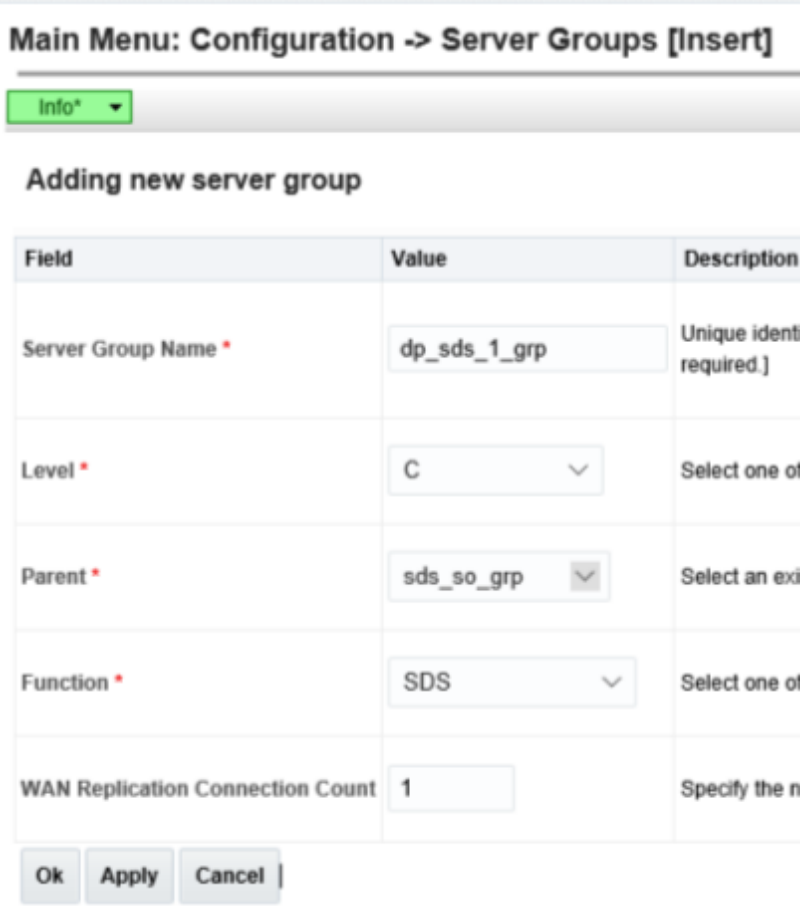


2. Click **Insert**.



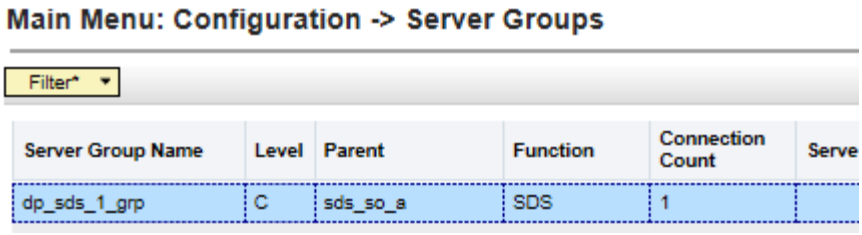
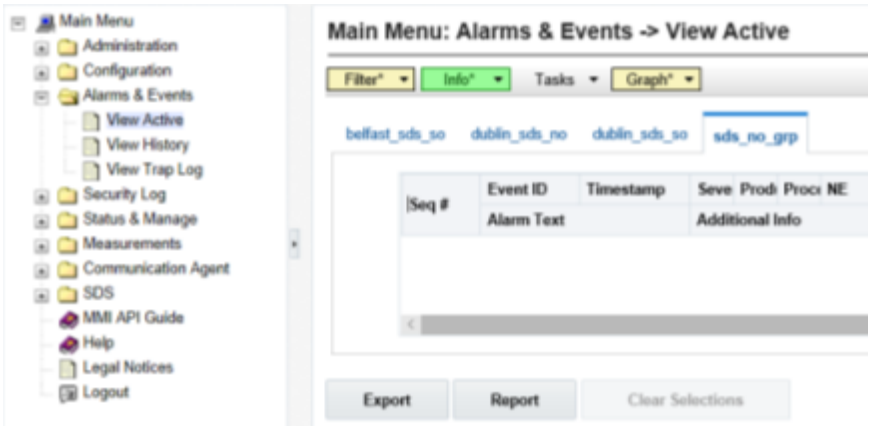
3. Fill in the following fields:

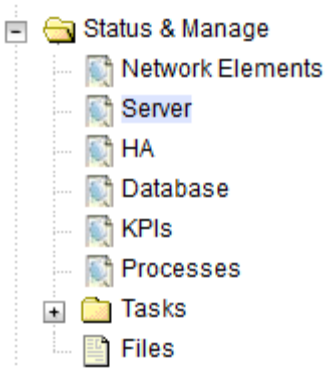
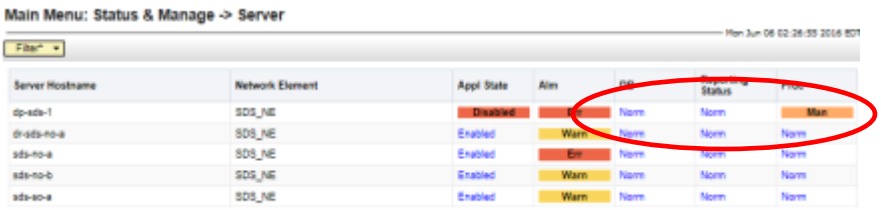
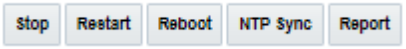
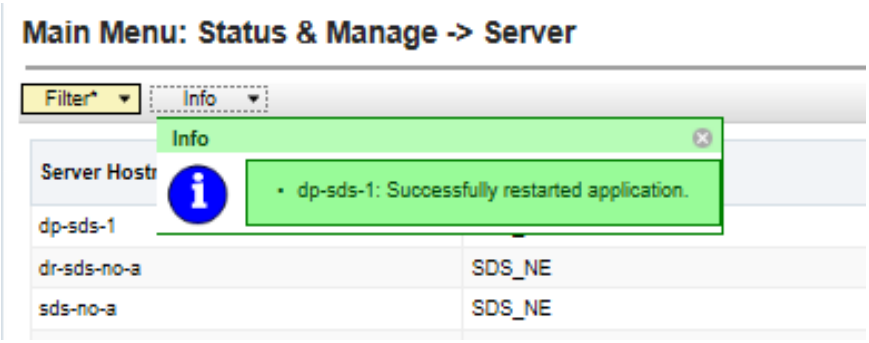
Server Group Name:	<Server Group Name>
Level:	C
Parent:	System OAM group
Function:	SDS (Active/Standby Pair)
WAN Replication Connection Count:	Use Default Value (1)

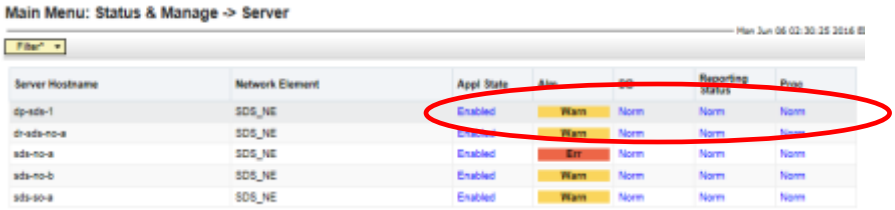


4. Click **OK**.

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

38. ☐	**Primary SDS VIP**: Add server to OAM Server Group	1. Select the new server group and click **Edit**.  2. Mark the **Include in SG** checkbox next to the A and B servers. 3. Click **OK**.
39. ☐	Repeat	Repeat steps 37. And 38. of this procedure for each DP server installed in the same SOAM enclosure, using a unique group name for each DP.
40. ☐	**Primary SDS VIP**: Make sure alarms clear	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID 10200** displays with the SDS SOAM 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 clears for all DP servers.

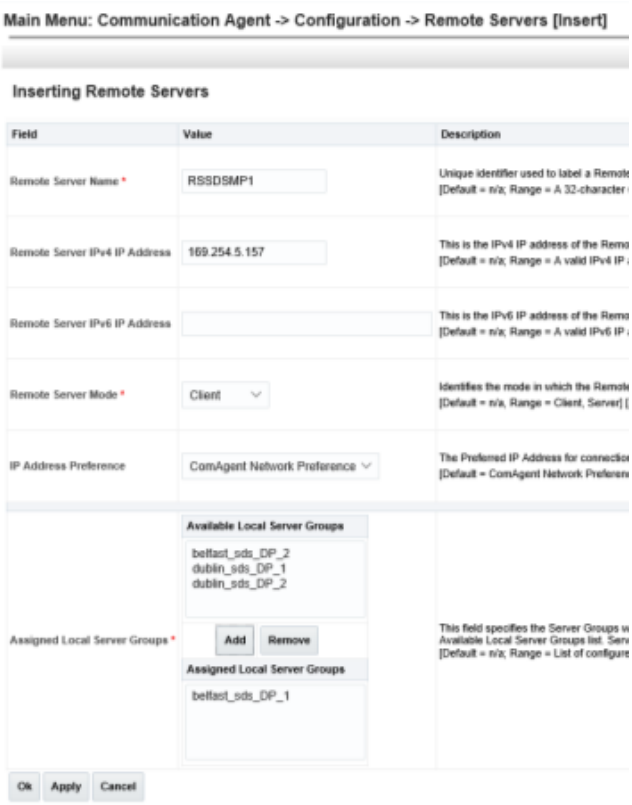
Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
41. ☐	**Primary SDS VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify the DB is **Norm** and the Proc status is **Man** for the DP server. 
42. ☐	**Primary SDS VIP**: Restart the SDS SOAM B server	1. Select the DP server and click **Restart**.  2. Click **OK** to confirm. The Info banner displays a success message. 

Procedure 11. Install the Data Processor Blade (All SOAM Sites)		
43. ☐	**Primary SDS VIP**: Verify status	1. Verify the Appl State is **Enabled**, and DB, Reporting Status, and Proc are **Norm** for the DP server.  2. Wait at least **5 minutes** before proceeding to the next step. ***Important***: To refresh the status screen, navigate to **Status & Manage > Server** again from the main menu.
44. ☐	Repeat	Repeat steps 41. through 43. of this procedure for each additional DP server installed in the SOAM cabinet.

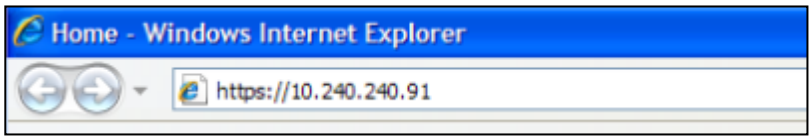
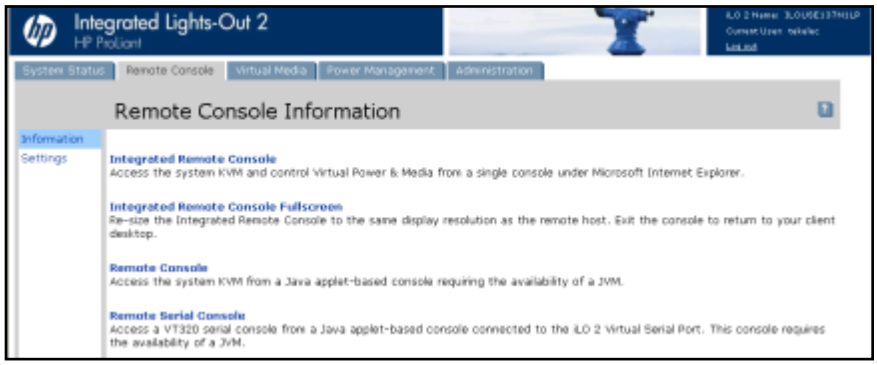
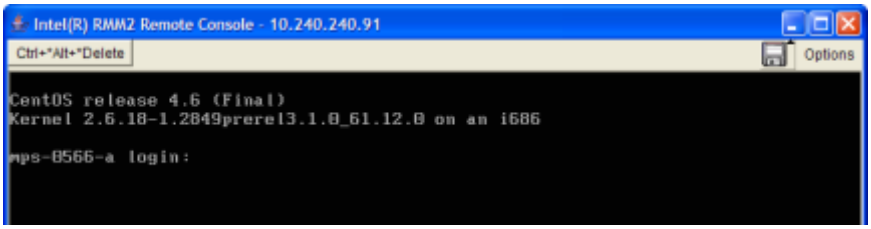
5.10 Configure ComAgent

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. Configure ComAgent (All SOAM Sites)		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI virtual IP (VIP) address using the default user and password. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.

Procedure 12. Configure ComAgent (All SOAM Sites)		
2. ☐	**Primary SDS VIP**: Add a message processor server	1. Navigate to **Communication Agent > Configuration > Remote Servers**. 2. Click **Insert**. 3. Type a **Remote Server Name** for the DSR message processor server. 4. Use either the **IPv4** or **IPv6** line to enter the IMI IP address for the MP blade. 5. Select the **IP Address Preference**. 6. Select **Client** as the Remote Server Mode. 7. Select the **Local Server Group** and click **Add** to assign it. 8. Click **OK**. 
3. ☐	Repeat	Repeat this procedure for each additional remote DA-MP in the associated DSR SOAM NE.

Appendix A. Access the iLO VGA Redirection Window

Procedure 13. Access the iLO VGA Redirection Window		
1. ☐	Login	Log into the iLO console as the administrator using the https:// access.  ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.
2. ☐	Access the Remote Console	From the Remote Console tab, click **Integrated Remote Console**.  The iLO Console window displays. The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer. 

Appendix B. Create a Temporary External IP Address to Access SDS GUI

This procedure creates a temporary external IP address to access the SDS A GUI before configuring the first SDS. This procedure assumes the user has access to the iLO and can access an external (XMI) network at the customer site. Use this IP address in a web browser to access the GUI to configure the first SDS.

Note: If this method is used, then the Ethernet port (for Gen8, eth02; for Gen9, eth03) must be unconfigured in step 1. of Procedure 3 in Section 5.1 Configure SDS A and B (1st SDS NOAM Site Only).

Procedure 14. Create a Temporary External IP Address to Access SDS GUI		

1. ☐	Login	Log into the SDS NOAM A ILO as indicated in Appendix A.
		`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. ☐	Delete bond0, if present	For Gen8:
		`$ 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	For Gen8, use eth02:
		`$ sudo netAdm set --device=eth02`
		`--onboot=yes --netmask=255.255.255.0`
		`--address=<XMI_IP_Address_for_SDS_A>`
		`Interface eth02 updated`
		For Gen9, use eth03:
		`$ 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. ☐	Ping gateway	Wait a few minutes and then ping the default gateway to ensure connectivity. `$ ping <XMI_IP_Address_for_default_gateway>`
6. ☐	Log off the ILO	`$ exit`

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

This procedure connects a laptop to the SDS NOAM A server using 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 before configuring the first SDS.

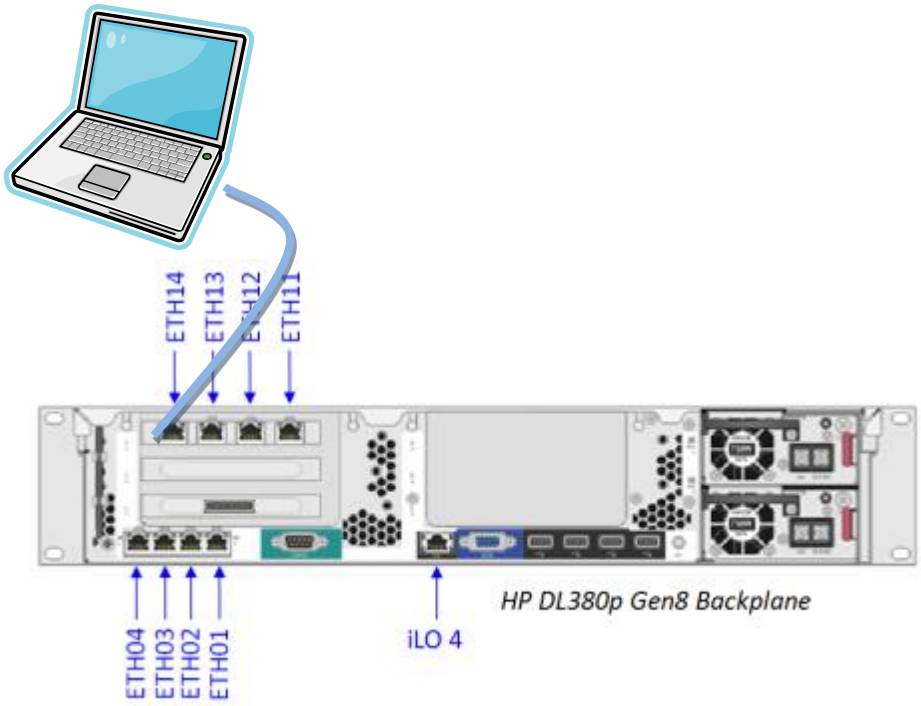
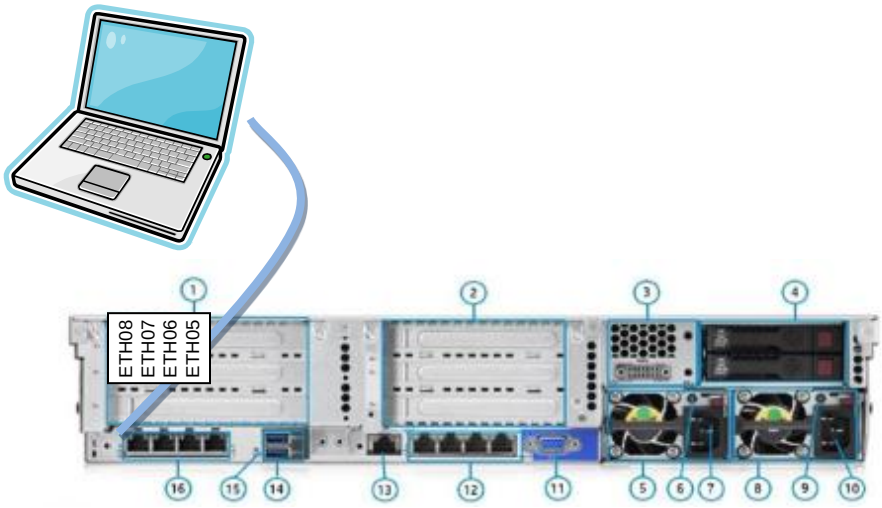
This procedure configures a temporary external IP address for SDS NOAM A for the 1st SDS site. Use this IP address in a web browser to access the GUI to configure the first SDS.

When this procedure is complete, the user can 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.

Procedure 15. Establish a Local Connection for Accessing the SDS GUI		
1. ☐	Access the server's console	Connect to the SDS NOAM A server's console using one of the access methods described in Section 2.3.

2. ☐	Login	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. ☐	Configure static IP 192.168.100.11 for SDS NOAM A server	For Gen8, configure on eth14 port.
		`$ sudo netAdm set --device=eth14 --address=192.168.100.11 --netmask=255.255.255.0 --onboot=yes`
		For Gen9, configure on eith08 port
		`$ sudo netAdm set --device=eth08 --address=192.168.100.11 --netmask=255.255.255.0 --onboot=yes`

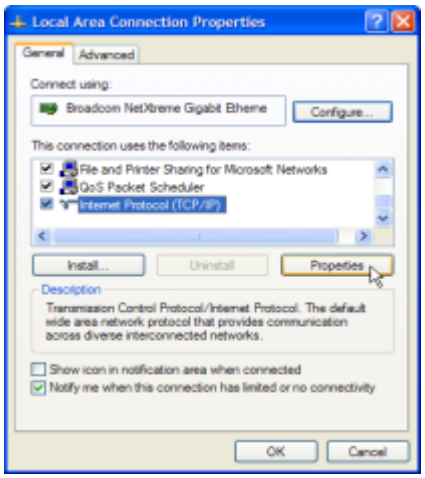
Procedure 15. Establish a Local Connection for Accessing the SDS GUI		
4. ☐	Physically connect the laptop to the server	For Gen8: 1. Plug in one end of the Ethernet cable (straight-thru) into the back of SDS NOAM A server ETH14 (top left port). 2. Plug the other end of the Ethernet cable into the laptop's Ethernet jack  **Figure 15. HP DL380p Gen8 Backplane** For 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.  **Figure 16. HP DL380 (Gen9), DC (Rear Panel)**

Procedure 15. Establish a Local Connection for Accessing the SDS GUI

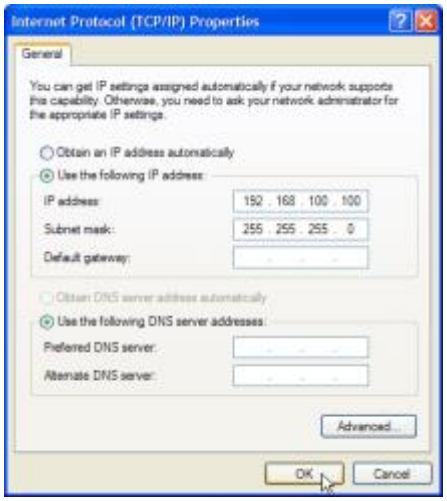
5. ☐ Set the IP address and netmask

For Windows XP:

1. From the Control Panel, double-click on **Network Connections**.
2. Right-click on the wired **Ethernet Interface** icon and click **Properties**.
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.

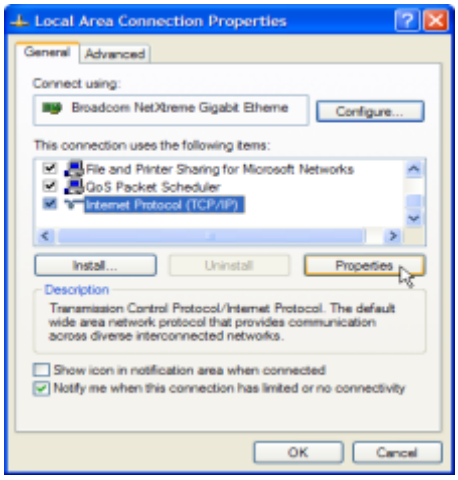


4. Set the IP address and netmask of the laptop's network interface card to an IP address within the same network subnet as the statically assigned IP address used in step 3. (192.168.100.100 is suggested).
5. Click **OK**.
6. Click **Close**.

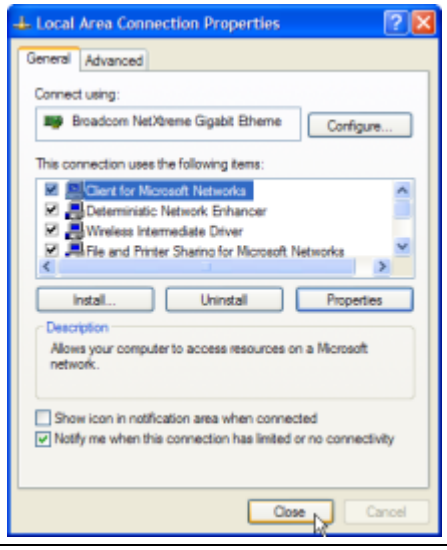


For Windows Vista/Win 7:

1. From the Control Panel, double-click on **Network and Sharing Center**.
2. Select **Manage Network Connections** (left menu).
3. Right-click the wired **Ethernet Interface** icon and Click **Properties**.
4. Select **Internet Protocol Version 4 (TCP/IPv4)**.



5. 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. (192.168.100.100 is suggested).
6. Click **OK**.
7. Click **Close**.



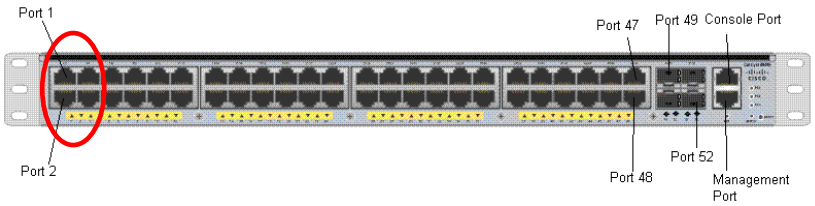
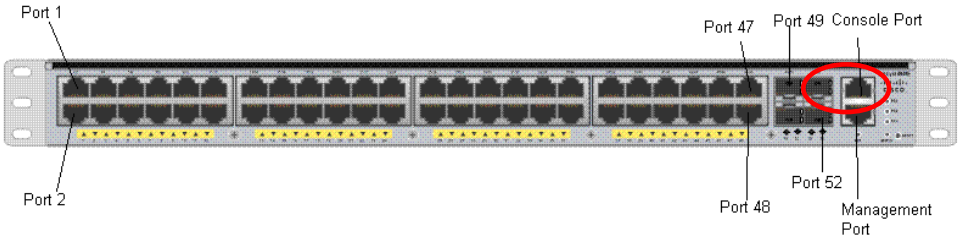
Appendix D. Configure Cisco 4948E-F Aggregation Switches

These switch configuration procedures require the SDS hardware (servers and switches) be installed in a frame as indicated in Figure 17.

DL380 Gen8/Gen9		
U	SDS - DC - Seismic	
44	PDP-A	PWR
43		
42		
41	OPEN	
40	FILLER PANEL	
39	FILLER PANEL	
38	FILLER PANEL	
37	FILLER PANEL	
36	FILLER PANEL	
35	FILLER PANEL	
34	FILLER PANEL	
33	FILLER PANEL	
32	FILLER PANEL	
31	SWITCH B (Cisco 4948E-F)	SW
30	FILLER PANEL	
29	SWITCH A (Cisco 4948E-F)	
28	FILLER PANEL	
27	FILLER PANEL	
26	FILLER PANEL	
25	FILLER PANEL	
24	FILLER PANEL	
23	FILLER PANEL	
22	FILLER PANEL	
21	FILLER PANEL	
20	FILLER PANEL	
19	FILLER PANEL	
18	FILLER PANEL	
17	FILLER PANEL	
16	FILLER PANEL	
15	FILLER PANEL	
14	FILLER PANEL	
13	FILLER PANEL	
12	FILLER PANEL	
11	FILLER PANEL	
10	FILLER PANEL	
9	SERVER C - QUERY (HP DL380 Gen8/Gen9)	Servers
8		
7	SERVER B - SDS NOAM (HP DL380 Gen8/Gen9)	
6		
5	SERVER A - SDS NOAM (HP DL380 Gen8/Gen9)	
4		
3	FILLER PANEL	
2	FILLER PANEL	
1	FILLER PANEL	

Figure 17. SDS Frame Layout

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

Procedure 16. Verify Cisco Switch Wiring		
1. ☐	Set/Verify the cable configuration at the Cisco 4948E-F switches	1. Verify the ISL switch1A, Port 1 to switch1B, Port 1 is connected. 2. Verify the ISL switch1A, Port 2 to switch1B, Port 2 is connected. 3. Verify the ISL switch1A, Port 3 to switch1B, Port 3 is connected. 4. Verify the ISL switch1A, Port 4 to switch1B, Port 4 is connected.  **Figure 18. Cisco 4948E-F Switch ISL Connections – Switch 1B (Top) to Switch 1A (Bottom)**
2. ☐	Verify server A has the Quad-Serial card interface ports connected to the console port of each switch port	For Gen8: 1. Verify the switch 1A console port is connected to server A Quad-Serial port S1 using cable 830-1229-xx. 2. Verify the switch 1B console port is connected to server A Quad-Serial port S2 using cable 830-1229-xx.  **Figure 19. Cisco 4948E-F Switch (Console Port)** 3. Verify switch 1A, port 5, is connected to server A eth01. 4. Verify switch 1B, port 5, is connected to server A eth11. 5. Verify switch 1A, port 6, is connected to server B eth01. 6. Verify switch 1B, port 6, is connected to server B eth11. 7. Verify switch 1A, port 7, is connected to server C eth01. 8. Verify switch 1B, port 7, is connected to server C eth11.

Procedure 16. Verify Cisco Switch Wiring

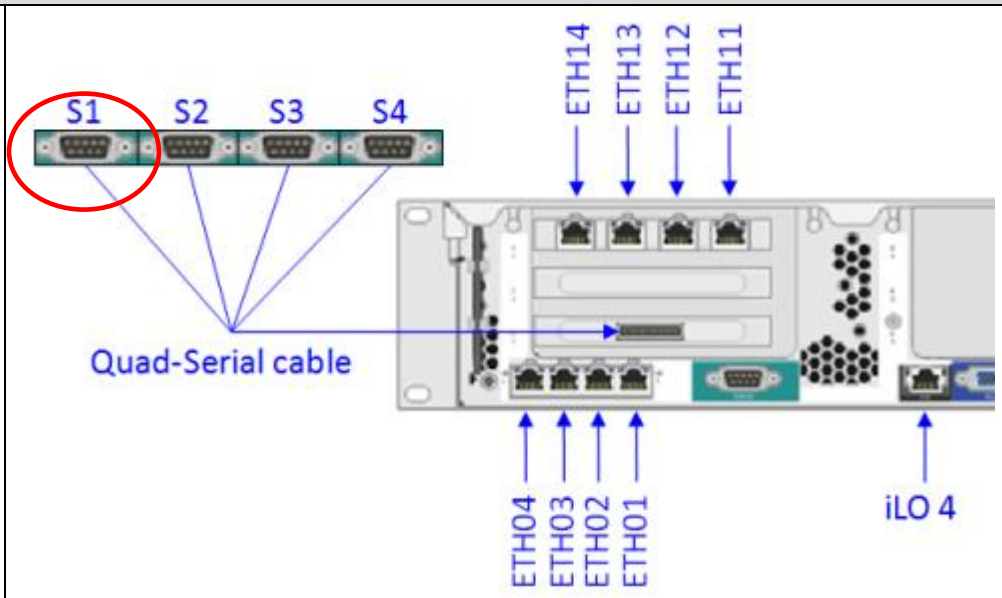


Figure 20. HP DL380 Gen8, Rear Panel (Quad-Serial Ports)

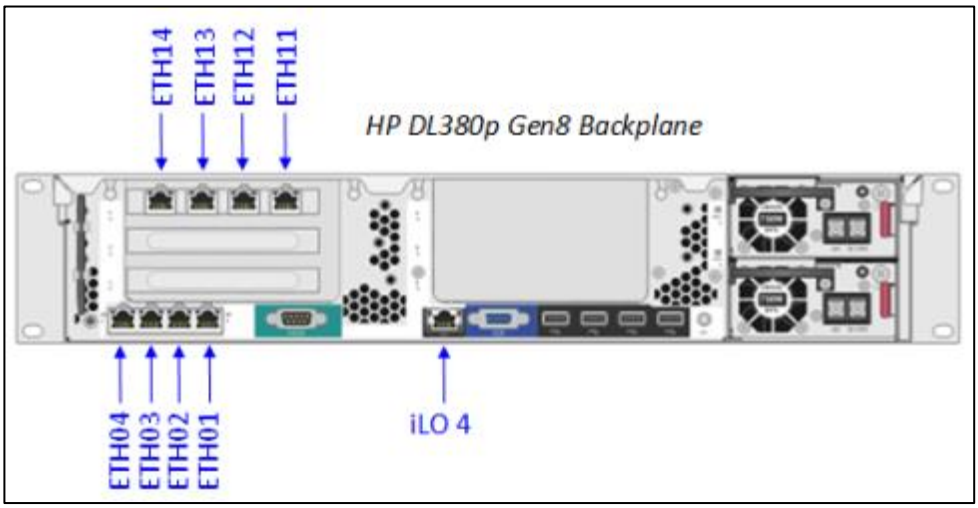


Figure 21. HP DL380 Gen8, Rear Panel (Ethernet)

For Gen9:

1. Verify the switch 1A console port is connected to server A USB port USB0.
2. Verify the switch 1B console port is connected to server A USB port USB1.

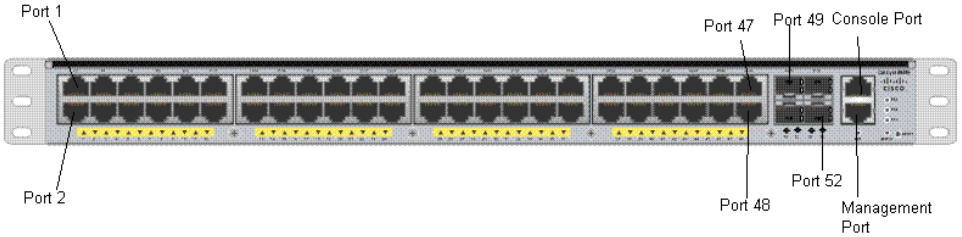
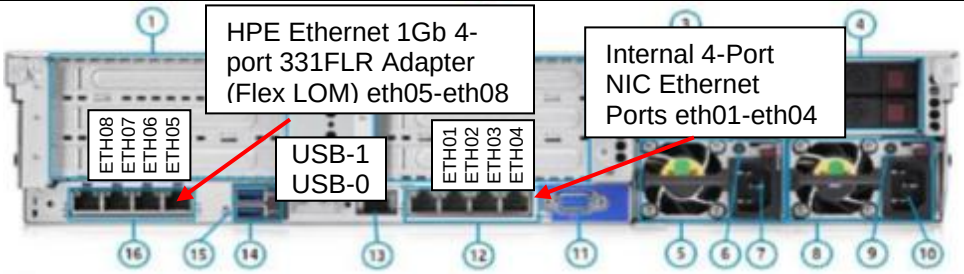


Figure 22. Cisco 4948E-F Switch (Console Port)

Procedure 16. Verify Cisco Switch Wiring		
		 **Figure 23. HP DL380 (Gen9), DC (Rear Panel)** 3. Verify switch 1A, port 5, is connected to server A eth01. 4. Verify switch 1B, port 5, is connected to server A eth02. 5. Verify switch 1A, port 6, is connected to server B eth01. 6. Verify switch 1B, port 6, is connected to server B eth02. 7. Verify switch 1A, port 7, is connected to server C eth01. 8. Verify switch 1B, port 7, is connected to server C eth02.

D.2 Configure Cisco 4948E-F Aggregation Switches

This procedure may refer to variable data indicated by text within <>. Refer to Table 4 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 inject bad characters if you backspace! Press **Ctrl-C** to exit netConfig if you make a mistake on any field and re-run that command.

Table 4. 4948-F Aggregation Switch Variables

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 [4]: _____

Variable	Value
<switch_platform_username>	Contact My Oracle Support (MOS)
<switch_platform_password>	Contact My Oracle Support (MOS)
<switch_console_password>	Contact My Oracle Support (MOS)
<switch_enable_password>	Contact My Oracle Support (MOS)
<Server A_mgmt VLAN_IP_address >	Primary SDS: 169.254.1.11 DR SDS: 169.254.1.14

Variable	Value
<Server B_mgmt VLAN_IP_address>	Primary SDS: 169.254.1.12 DR SDS: 169.254.1.15
<switch_mgmt VLAN_ID>	2
<switch1A_mgmt VLAN_IP_address>	169.254.1.1
<netmask>	255.255.255.0
<switch1B_mgmtVLAN_IP_address>	169.254.1.2
<management_server_mgmt interface>	bond0.2
<Server A_iLO_IP> (See NAPD documentation for IP address)	
<Server B_iLO_IP> (See NAPD documentation for IP address)	

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 My Oracle Support (MOS)
<management_server_mgmtInterface>	bond0.2
<switch_backup_user>	Contact My Oracle Support (MOS)
<switch_backup_user_password>	Contact My Oracle Support (MOS)

Uplinks, if present, must be disconnected from the customer network before executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Refer to Section 0 for determining which cables are used for customer uplink.

Needed Material:

- HP Misc. Firmware DVD
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- 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 My Oracle Support (MOS).

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
1. ☐	**Server A**: Access the server console	Connect to the Server A console using one of the access methods described in Section 2.3.

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

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

3. ☐	**Server A**: Verify files exist	1. Verify the switch1A initialization file exists.
		`$ 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`
		2. Verify the switch1B initialization file exists.
		`$ 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`
		3. Verify the switch configuration files exist.
		`$ 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 My Oracle Support (MOS) for assistance.

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

4. ☐	**Server A**: For serial ports	For Gen8, 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`
		If output does not match the example, contact My Oracle Support (MOS) for assistance.
		For Gen9, 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`

5. ☐	**Server A**: Set up conserver serial console access for switch1A	For Gen8:
		`$ 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:`

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

		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: <PRESS ENTER KEY HERE>
		...No entry provided for bond. Resorting to default.
		Slave interfaces for bond0:
		bond0 interface: eth01
		bond0 interface: eth11
		For Gen9:
		$ 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

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
		(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: [PRESS ENTER KEY] ...No entry provided for bond. Resorting to default. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02

6. ☐	**Server A**: Set up conserver serial console access for switch1B	For Gen8:
		$ 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

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
		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
		For Gen9: $ 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

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

7. ☐	**Server A**: Add a repository for SSH service	1. 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`
		2. 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`

8. ☐	**Server A**: Add a repository for TFTP service	1. 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`
		2. Verify 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/`

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

9. ☐	**Server A**: Create console service for switch1A	1. 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`
		2. 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`

10. ☐	**Server A**: Add repository for switch1B console service	1. 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`
		2. 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`

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

11. ☐	**Server A**: Verify and remove 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 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...`

12. ☐	**Server A**: Add repository for switches	***Note:*** Remember to copy the firmware file to this server.
		1. 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.`

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
		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. 2. 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.

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

```
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.
```

3. 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
```

<table>
<tr><th colspan="3">Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)</th></tr>
<tr><td>13. ☐</td><td>Server A: Log into switch 1A</td><td>Example:
console -M <SERVER A_mgmtVLAN_IP_address> -l platcfg switch1A_console
<pre>$ /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></pre></td></tr>
<tr><td>14. ☐</td><td>Switch 1A: Note the image version for comparison in a following step.</td><td><pre>Switch> show version | include image
System image file is "bootflash:cat4500e-entservicesk9-mz.122-54.XO.bin"</pre></td></tr>
<tr><td colspan="3">
If the switch 1A (4948E-F) IOS does not display the correct version, then stop and execute these following steps:
• Appendix D.3 Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)
• Return to this procedure and continue with the next step.
Notes:
• For each switch, compare the IOS version from previous steps with the IOS version specified in the Firmware Upgrade Pack Release Notes [3] 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.</td></tr>
<tr><td>15. ☐</td><td>Switch 1A: Verify bootflash</td><td>1. Execute show bootflash to verify that only the correct bootflash is present.
<pre>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)</pre>2. Note the image version for comparison in a following step.</td></tr>
</table>

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
16. ☐	**Switch 1A**: 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
17. ☐	**Switch 1A**: Reload the switch	1. Reload the switch Switch#reload System configuration has been modified. Save? [yes/no]: no Proceed with reload? [confirm] <ENTER> 2. 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>
18. ☐	**Switch 1A**: Enter enable mode	Switch#enable

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

19. ☐	**Switch 1A**: Verify you see the correct IOS version listed inthe bootflash and note the image version for comparison in a following step and then exit	`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)`

20. ☐	**Switch 1A**: Close connection to switch	`Switch#quit`
		`Switch con0 is now available`
		`Press RETURN to get started.`

21. ☐	**Switch 1A**: Exit from switch	Exit from console by pressing **Ctrl+e+c+.** (press Control and e, followed by c and a period). You are returned to the server prompt.
22. ☐	**Server A**: Log into switch 1B	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>`

23. ☐	**Switch 1B**: 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 switch 1B IOS does not display the correct version, then stop and execute these following steps: • Appendix D.3 Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites) beginning with step 25. • Return to this procedure and continue with the next step. ***Notes***: • For each switch, compare the IOS version from previous steps with the IOS version specified in the Firmware Upgrade Pack Release Notes [3] 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 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		

24. ☐	**Switch 1B**: Verify bootflash	1. 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)`
		2. Note the image version for comparison in a following step.

25. ☐	**Switch 1B**: 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`

26. ☐	**Switch 1B**: Reload the switch	1. Reload the switch
		`Switch#reload`
		`System configuration has been modified. Save? [yes/no]: no`
		`Proceed with reload? [confirm] <ENTER>`
		2. 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>`

Procedure 17. Configure Cisco 4948E-F Switches (All SDS NOAM Sites)		
27. ☐	**Switch 1B**: Enter enable mode	`Switch#enable`

28. ☐	**Switch 1B**: Verify you see the correct IOS version listed inthe bootflash and note the image version for comparison in a following step and then exit	`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)`

29. ☐	**Switch 1B**: Close connection to switch	`Switch#quit`
		`Switch con0 is now available`
		`Press RETURN to get started.`

30. ☐	**Switch 1B**: Exit from switch	Exit from console by pressing **Ctrl+e+c+.** (press Control and e, followed by c and a period). You are returned to the server prompt.

31. ☐	**Server A**: Open firewall	1. Open firewall.
		`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`
		2. Turn on tftp.
		`$ tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`

32. ☐	**Server A**: Initialize switches	1. 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`
		2. 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

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

33. ☐	**Server A**: Ping switches	***Note:*** VIP addresses are not yet available.
		1. Ping switch 1A's SVI (router interface) addresses to verify switch initialization.
		`$ 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 14006 ms`
		`rtt min/avg/max/mdev = 0.381/0.592/3.097/0.669 ms`
		2. Ping switch 1B's SVI (router interface) addresses to verify switch initialization.
		`$ 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 14003 ms`
		`rtt min/avg/max/mdev = 0.378/0.747/2.769/0.825 ms, pipe 3`
		!!WARNING!!
		Verify the pings are successful before continuing to the next step. If the ping continues to receive "Destination Host Unreachable," then stop this procedure and contact My Oracle Support (MOS).

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

34. ☐	**Server A**: Configure switches	1. 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`
		2. 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

35. ☐	**Server A**: Undo the temporary changes.
	(If netconfig is used to update the firmware, then this is not needed)
		`$ tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`

36. ☐	**Server A**: Close firewall. (If netconfig is used to update the firmware, then this is not needed)	`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`

37. ☐	**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`

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

38. ☐	**Server A**: Execute the **service network restart** to restore Server A networking to the original state	`$ 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 ]`

39. ☐	**Server A**: Ping switches	***Note:*** VIP addresses are not yet available.
		1. Ping switch 1A's SVI (router interface) addresses to verify switch configuration.
		`$ 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 4003 ms`
		`rtt min/avg/max/mdev = 0.426/0.428/0.431/0.002 ms`
		2. Ping switch 1B's SVI (router interface) addresses to verify switch configuration.
		`$ 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 3999 ms`
		`rtt min/avg/max/mdev = 0.393/0.399/0.407/0.013 ms`

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

40. ☐	**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>`

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

42. ☐	**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>`

43. ☐	**Server A**: Close SSH connection to switch 1B	`$ quit` `Connection to 169.254.1.2 closed.`

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

44. ☐	**Server B**: Ping switches	***Note:*** VIP addresses are not yet available.
		1. Ping switch 1A's SVI (router interface) addresses to verify switch configuration.
		`$ 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 4003 ms`
		`rtt min/avg/max/mdev = 0.426/0.428/0.431/0.002 ms`
		2. Ping switch 1B's SVI (router interface) addresses to verify switch configuration.
		`$ 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 3999 ms`
		`rtt min/avg/max/mdev = 0.393/0.399/0.407/0.013 ms`

45. ☐	**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>`

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

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

47. ☐	**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>`

48. ☐	**Server B**: Close SSH connection to switch 1B	`switch1B> quit` `Connection to 169.254.1.2 closed.`

49. ☐	**Server B**: 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`

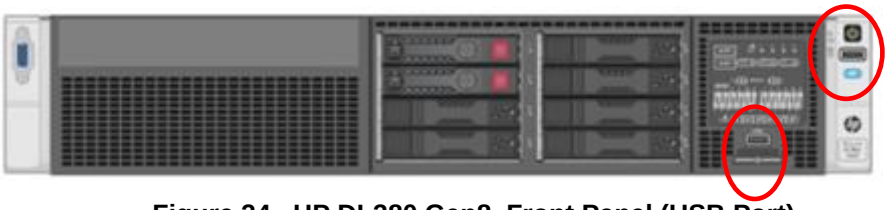
D.3 Cisco 4948E-F IOS Upgrade (All SDS NOAM Sites)

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		
1. ☐	**Server A**: Access the console	Connect to the Server A console using one of the access methods described in Section 2.3.

2. ☐	**Server A**: Login	1. Access the command prompt.
		2. Log into the 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>`
		*** 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`

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

3. ☐	**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 7.

4. ☐	**Server A**: Load software	Insert the USB drive containing the HP Misc Firmware image with the correct 4948E-F IOS version into the server's USB port.  **Figure 24. HP DL380 Gen8, Front Panel (USB Port)** **Figure 25. HP DL380 Gen9, Front Panel (USB Port)**

5. ☐	**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`

6. ☐	**Server A**: Open firewall	`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`

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

8. ☐	**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 and bond0.2 are both present, skip to step 10. If only bond0 is present, continue with the next step.

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

9. ☐	**Server A**: Create bond0.2	For Gen8, create the bond0.2 and add interfaces eth01 and eth11 to it.
		`$ 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, create the bond0.2 and add interfaces eth01 and eth02 to it.
		`$ 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 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

10. ☐	**Server A**: Disable the bond0.2 interface to switch1B and verify the bond0.2 IP address.	On Server A, ensure the interface connected to switch1A is the only interface available and obtain the IP address of <Server A_mgmtVLAN_Interface>.
		For Gen8:
		`$ 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:169.254.1.255 Mask: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)`
		For Gen 9:
		`$ 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:169.254.1.255 Mask: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)`
		The IP address of the <SERVER A_mgmtVLAN_IP_address> is highlighted.

11. ☐	**Server A**: Connect to switch1A console	`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>`
12. ☐	**Switch 1A**: Enter enable mode	`Switch> enable`

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

13. ☐	**Switch 1A**: 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`

14. ☐	**Switch 1A**: 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 the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact My Oracle Support (MOS).

15. ☐	**Switch 1A**: 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):`
		`!!!!!

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		
17. ☐	**Switch 1A**: Remove old IOS image	`Switch# delete /force /recursive bootflash:<OLD_IOS_image>`

18. ☐	**Switch 1A**: 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: You should see only the IOS version you uploaded.

19. ☐	**Switch 1A**: Reset switch 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`

20. ☐	**Switch 1A**: 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 Save option.

21. ☐	**Switch 1A**: 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"`
		Note: You should see only the IOS version you uploaded. If the IOS version is not the correct version, stop here and contact My Oracle Support (MOS).

22. ☐	**Switch 1A**: After the reload, enter enable mode	`Switch> enable`

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

23. ☐	**Switch 1A**: 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: You should see only the IOS version you uploaded.

24. ☐	**Switch 1A**: Exit the switch1A console session	`Switch# <CTRL-e><c><.>` Hot Key sequence: Ctrl-E, C, period

25. ☐	**Server A**: Disable the bond0.2 interface to switch1A	On Server A ensure 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>.

26. ☐	**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>`
27. ☐	**Switch 1B**: Enter enable mode	`Switch> enable`

28. ☐	**Switch 1B**: 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 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

29. ☐	**Switch 1B**: 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 the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact My Oracle Support (MOS).

30. ☐	**Switch 1B**: 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):`
		`!!!!!

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

34. ☐	**Switch 1B**: 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`

35. ☐	**Switch 1B**: 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 Save option.

36. ☐	**Switch 1B**: 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"`
		Note: You should see only the IOS version you uploaded. If the IOS version is not the correct version, stop here and contact My Oracle Support (MOS).

37. ☐	**Switch 1B**: Enter enable mode	`Switch> enable`

38. ☐	**Switch 1B**: 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: You should see only the IOS version you uploaded.

39. ☐	**Switch 1B**: Exit the switch1B console session	`Switch# <CTRL-e><c><.>` Hot Key sequence: Ctrl-E, C, period

Procedure 18. Cisco 4948E-F IOS Upgrade (SDS sites)		

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

41. ☐	**Server A**: 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`

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

Appendix E. Create 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 in the **/usr/TKLC/sds/vlan** directory.

The customer is required to create individual XML files for each of their SDS network elements (NOAM and SOAM). The format for each of these XML files is identical. Table 5 shows an example of the **SDS_NO_NE.xml** file in IPv4 and Table 6 shows an example in IPv6 format.

The highlighted values in each table must be updated for each network element (site).

Notes:

1. The **Description** column includes comments for this document only. **Do not include** the Description column in the actual XML file used during installation.
2. The **MgmtVLAN** network should only be implemented when two dedicated aggregation switches (typically Cisco 4948E-F) are used exclusively for the SDS NOAM and Query server (RMS) IMI network. The MgmtVLAN network should be **removed** from the network element XML file when SDS aggregation switches are not part of the implementation.
3. When installing **IPv6** for the XMI or IMI networks, note that the **MgmtVLAN** (if implemented) should remain in the **IPv4** format only.
4. When creating the SDS **SOAM NE XML** file, 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 5. 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>**MgmtVLAN**</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.

XML File Text	Description
<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 6. 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>**MgmtVLAN**</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.

XML File Text	Description
<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. Install NetBackup Client

Procedure 19. Install NetBackup Client		

1. ☐	Install NetBackup client software	Execute Section 3.10.5 Application NetBackup Client Install/Upgrade Procedures in reference [6] to complete this step.
		Note: If installing NetBackup client software, it must be installed and configured on all SDSs (primary SDS and DR SDSs only).
		Locate the **bpstart_notify** and **bpend_notify** scripts to execute this step. These scripts are located in:
		`/usr/TKLC/appworks/sbin/bpstart_notify`
		`/usr/TKLC/appworks/sbin/bpend_notify`
		The NetBackup client software must be installed on each SDS NOAM server.

2. ☐	Link notify scripts to known path stated in step 1	`ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify` `ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify`

Procedure 19. Install NetBackup Client		

3. ☐	Verify the NetBackup 1556 port is open for IPv4 protocol	`iptables -L 60sds-INPUT -n | grep 1556`
		If there is no output, then enable the 1556 port 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 the NetBackup 1556 port is open for IPv6 protocol	`ip6tables -L 60sds -INPUT -n | grep 1556`
		If there is no output, then enable the 1556 port for NetBackup on IPv6:
		`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 time zone strings that can be used for the time zone setting in a CSV file, or as the time zone parameter when manually setting a DSR time zone.

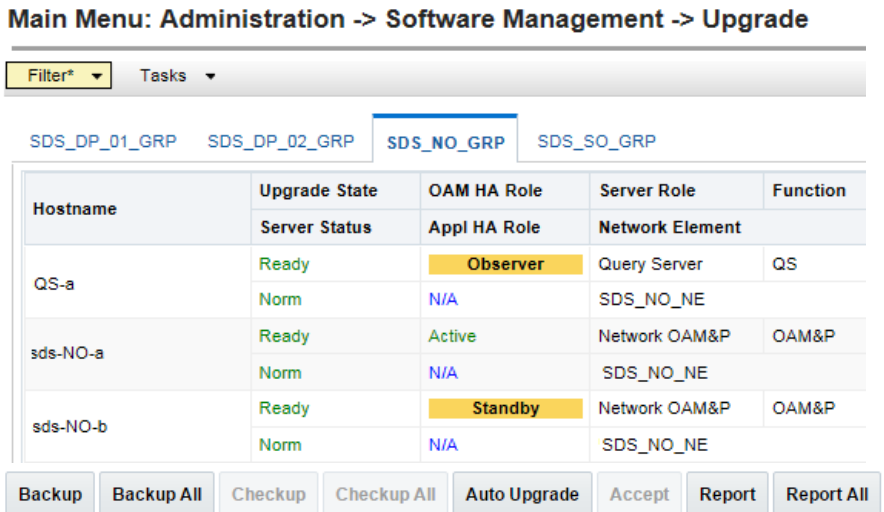
Table 7. List of Selected Time Zone Values

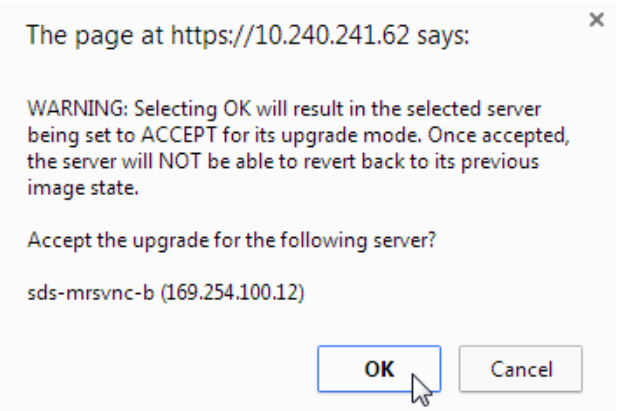
Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08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

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

Appendix H. Accept Installation from SDS NOAM GUI

This procedure accepts an application installation through SDS NOAM GUI.

Procedure 20. Accept Installation from SDS NOAM GUI		
1. ☐	**Primary SDS VIP**: Login	Log into the active SDS site with the XMI Virtual IP (VIP) address using the default user and password. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.
2. ☐	**Primary SDS VIP**: Accept the upgrade	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the row containing the server and click **Accept**. 

Procedure 20. Accept Installation from SDS NOAM GUI		
3. ☐	**Primary SDS VIP**: Accept the upgrade	Click **OK** to accept the upgrade. 

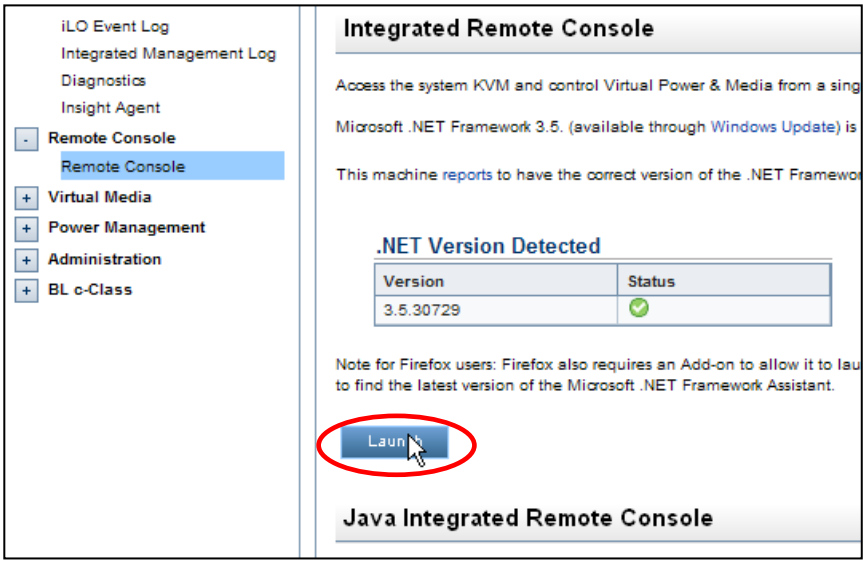
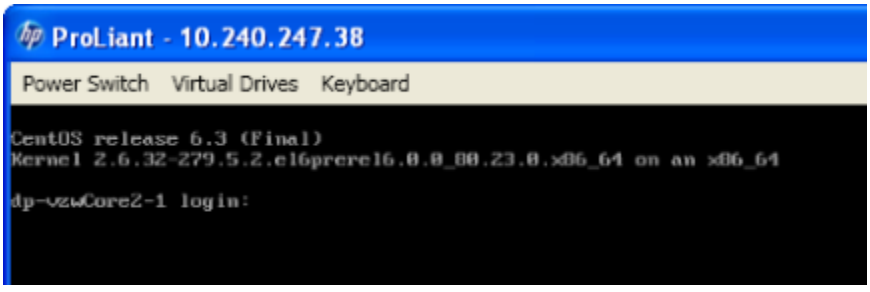
Appendix I. Disable Hyperthreading for Gen8 and Gen9 (DP Only)

Procedure 21. Gen8: Disable Hyperthreading		

1. ☐	**DP Server XMI IP (SSH)**: Login	1. Access the command prompt using the DP blade's XMI IP address.
		2. Login as admusr.
		`login: admusr`
		`Password: <admusr_password>`

2. ☐	**DP Server XMI IP (SSH)**: Determine hyperthreading status	Execute hpasmcli command to determine the status of hyperthreading for the DP blade.
		`$ sudo hpasmcli -s "show ht"`
		`Processor hyper-threading is currently enabled.`
		Output returned may state either **enabled** or **disabled**.

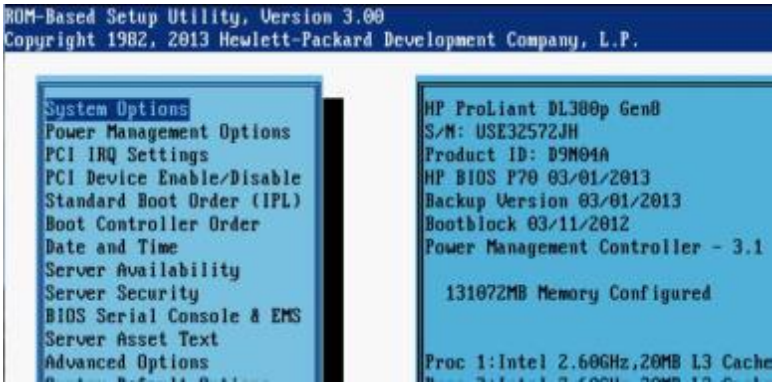
		If output from step 2. shows that hyperthreading is currently **enabled**, then continue with step 3. of this procedure. If output from step 2. shows that hyperthreading is currently **disabled**, then **STOP** and restart Appendix I on the next installed DP blade.

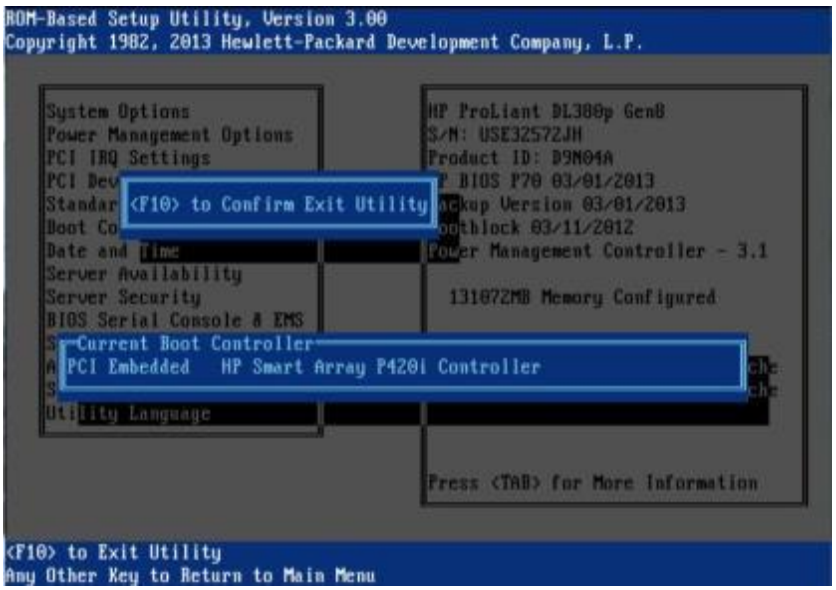
Procedure 21. Gen8: Disable Hyperthreading		
3. ☐	Login	Log into the iLO console as the administrator using the https:// access. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.
4. ☐	Access the iLO Console screen	1. Under the Integrated Remote Console section, click **Launch**.  2. Answer **Yes/OK** to any screens that need confirmation.  ***Note:*** The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.

Procedure 21. Gen8: Disable Hyperthreading		

1. ☐	**DP Server XMI IP (SSH)**: Login	1. Access the command prompt using the DP blade's XMI IP address.
		2. Login as admusr.
		`login: admusr`
		`Password: <admusr_password>`

2. ☐	Reboot the server	Login and execute the init 6 command at 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 displays.
3. ☐	Reboot the server to access the setup utility	1. Press and hold the power button until the server turns off. 2. After approximately 5-10 seconds, power the server on. 3. 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 need to press **F9** 2-3 times. The F9=Setup changes to **F9 Pressed** once it is accepted. The ROM-Based Setup Utility menu displays. ***Note:*** It is normal for 2 minutes or more to occur between pressing **F9** and entering the Blade BIOS screen.

Procedure 21. Gen8: Disable Hyperthreading		
4. ☐	Select System Options	Select **System Options** and press **Enter**. 
5. ☐	Select Processor Options	Select **Processor Options** and press **Enter**.
6. ☐	Select Hyperthreading	Select **Intel® Hyperthreading** and press **Enter**.

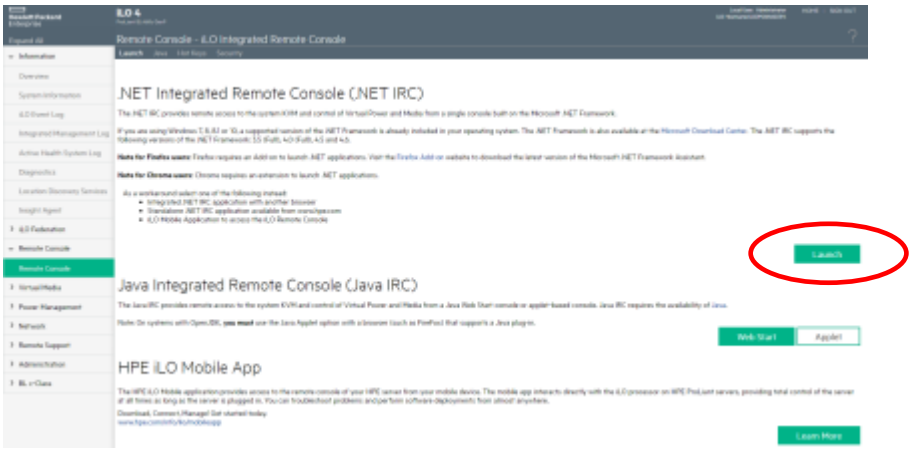
Procedure 21. Gen8: Disable Hyperthreading		
7. ☐	Disable hyperthreading	Select **Disabled** and press **Enter**.
8. ☐	Save the configuration and exit	Press **F10** to save the configuration and exit. The server reboots.  ***Note:*** It is normal for the Remote Console window to stay blank for up to 3 minutes before initial output appears.
9. ☐	Wait for the login prompt	Continue to monitor the server boot process until the screen returns to the login prompt and then close the window.

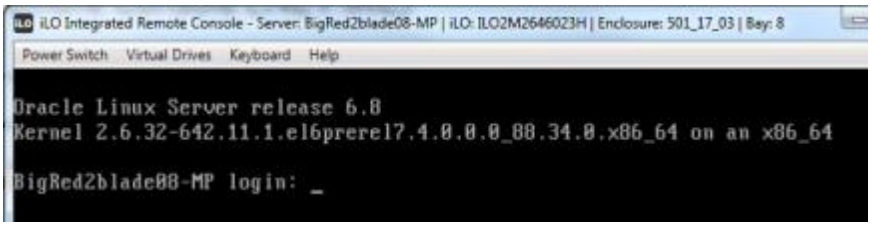
Procedure 22. Gen9: Disable Hyperthreading		

1. ☐	**DP Server XMI IP (SSH)**: Login	1. Access the command prompt using the DP blade's XMI IP address.
		2. Login as admusr.
		`login: admusr`
		`Password: <admusr_password>`

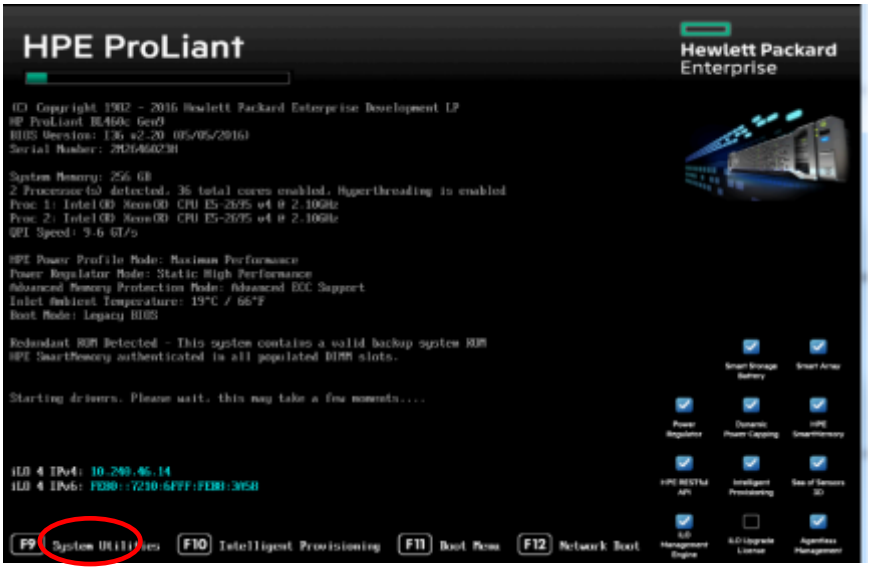
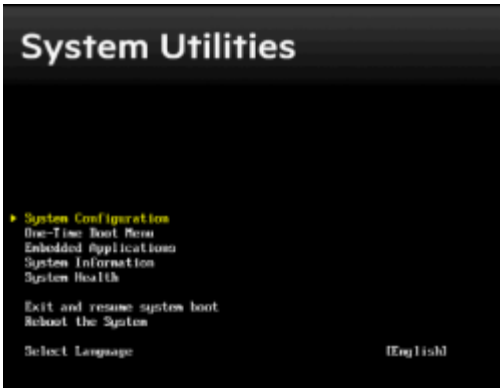
2. ☐	**DP Server XMI IP (SSH)**: Determine hyperthreading status	Execute hpasmcli command to determine the status of hyperthreading for the DP blade.
		`$ sudo hpasmcli -s "show ht"`
		`Processor hyper-threading is currently enabled.`
		Output returned may state either **enabled** or **disabled**.

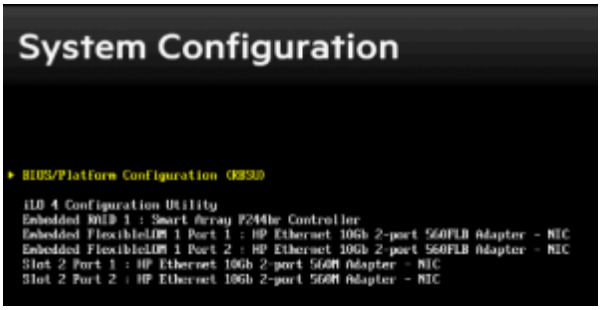
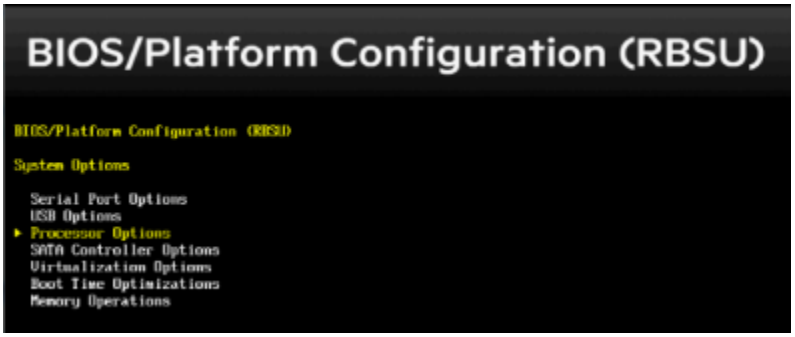
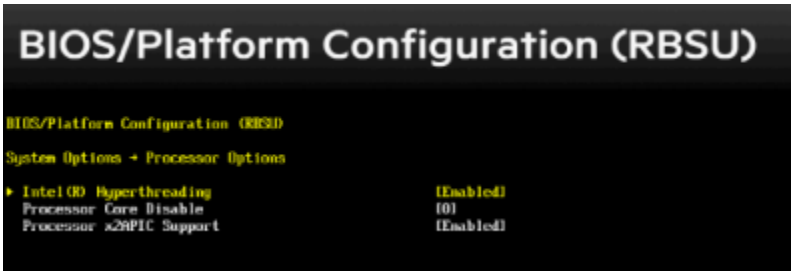
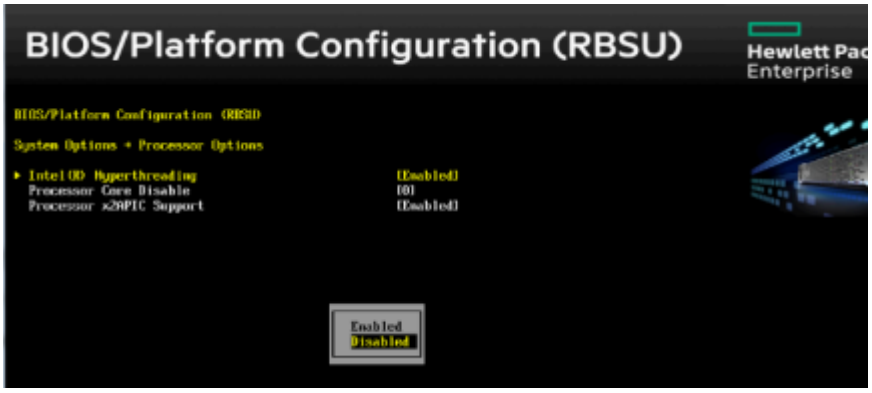
		If output from step 2. shows that hyperthreading is currently **enabled**, then continue with the next step of this procedure. If output from step 2. shows that hyperthreading is currently **disabled**, then **STOP** and restart Appendix I on the next installed DP blade.
3.	Login	Log into the iLO console as the administrator using the https:// access. ***Note:*** If the Security Certificate screen displays, select **Continue to this website (not recommended)**.

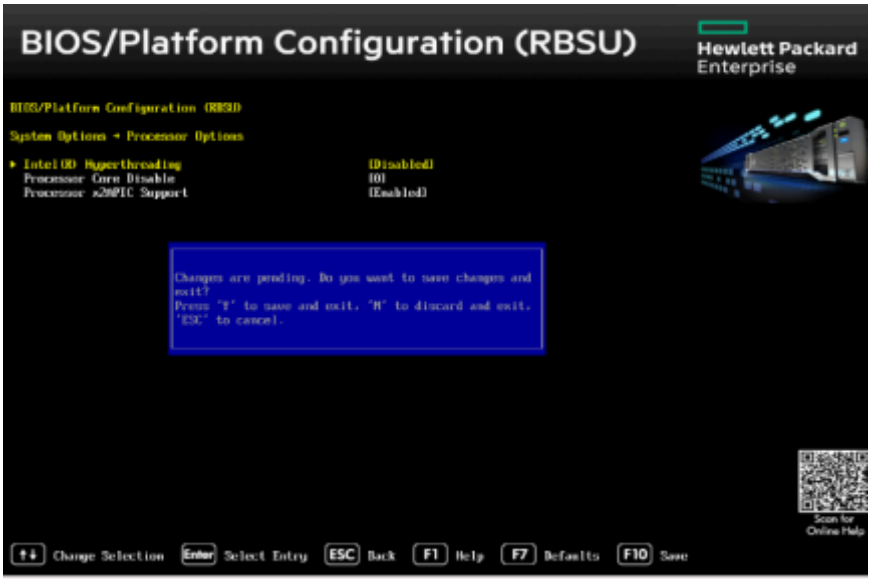
<table>
<tr><th colspan="3">Procedure 22. Gen9: Disable Hyperthreading</th></tr>
<tr><td>4. ☐</td><td>Access the iLO Console screen</td><td>1. Under the Integrated Remote Console section, click Launch.
 

2. Answer Yes/OK to any screens that need confirmation.
 

Note: The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.</td></tr>
<tr><td>5. ☐</td><td>DP Server XMI IP (SSH): Login</td><td>1. Access the command prompt using the DP blade's XMI IP address.
2. Login as admusr.
<pre>login: admusr
Password: <admusr_password></pre></td></tr>
<tr><td>6. ☐</td><td>Reboot the server</td><td>Login and execute the init 6 command at the command prompt.
<pre>$ sudo init 6</pre>Note: It is normal for the Remote Console window to stay blank for up to 3 minutes before initial output displays.</td></tr>
</table>

Procedure 22. Gen9: Disable Hyperthreading		
7. ☐	Reboot the server to access the setup utility	1. Press and hold the power button until the server turns off. 2. After approximately 5-10 seconds, power the server on. 3. 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 need to press **F9** 2-3 times. The F9=Setup changes to **F9 Pressed** once it is accepted.  The ROM-Based Setup Utility menu displays. ***Note:*** It is normal for 2 minutes or more to occur between pressing **F9** and entering the Blade BIOS screen.
8. ☐	Select System Configuration	Select **System Configuration** and press **Enter**. 

Procedure 22. Gen9: Disable Hyperthreading		
9. ☐	Select BIOS/Platform Configuration	Select **BIOS/Platform Configuration** and press **Enter**. 
10. ☐	Select Processor Options	Select **Processor Options** and press **Enter**. 
11. ☐	Select Hyperthreading	Select **Intel® Hyperthreading** and press **Enter**. 
12. ☐	Disable hyperthreading	Select **Disabled** and press **Enter**. 

Procedure 22. Gen9: Disable Hyperthreading		
13. ☐	Save the configuration and exit	Press **F10** to save the configuration and exit. The server reboots.  ***Note:*** It is normal for the Remote Console window to stay blank for up to 3 minutes before initial output displays.
14. ☐	Wait for the login prompt	Continue to monitor the server boot process until the screen returns to the login prompt and then close the window.

Appendix J. Configure the HP DL380 (GEN8 and GEN9) Server CMOS Clock/BIOS Settings

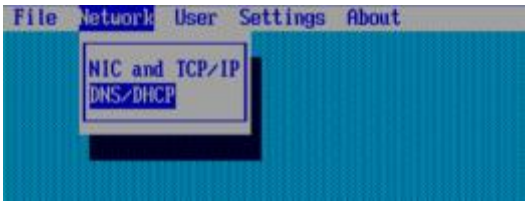
J.1 Gen8: Configure the ILO for Rack Mount Server

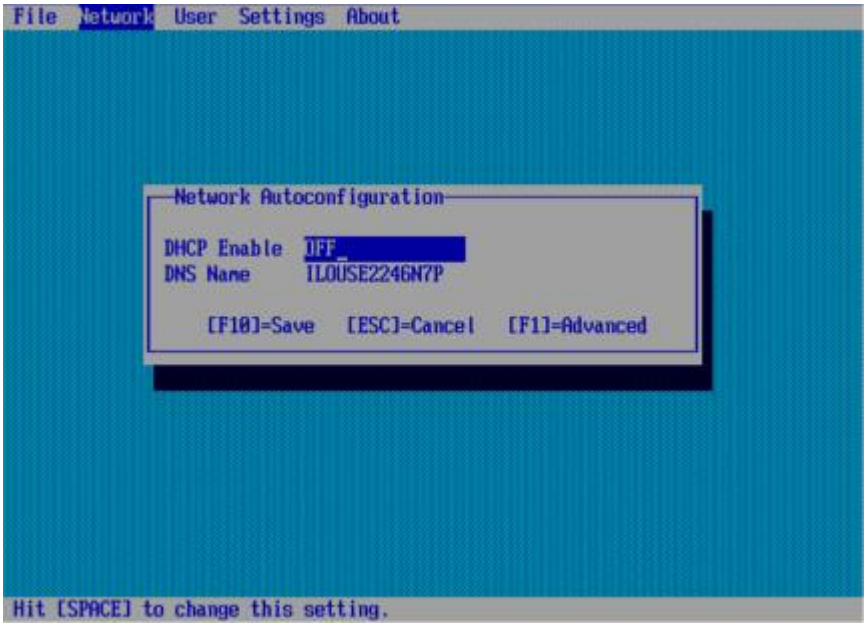
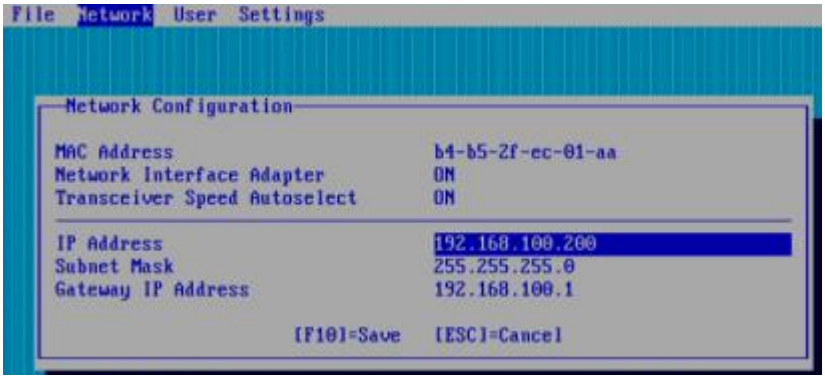
J.1.1 RMS: Configure iLO

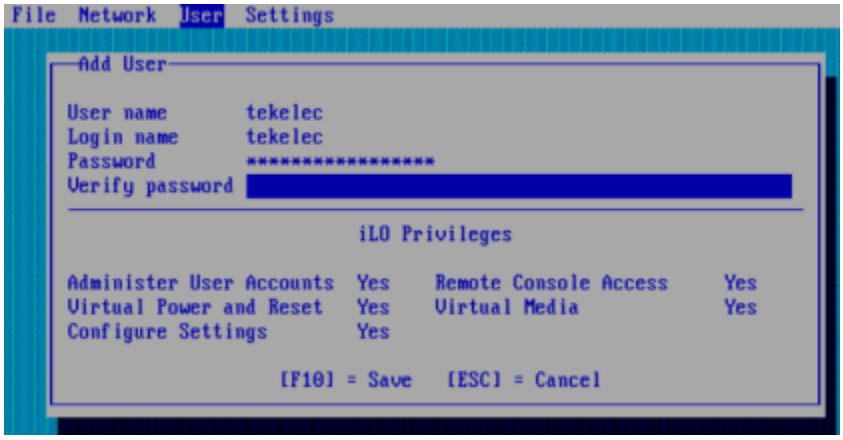
This procedure configures Integrated Lights Out (iLO) for RMS. It configures the NIC and TCP/IP, DNS/DHCP parameters, and adds a new iLO user.

Prerequisites and Requirements:

- Server powered on
- Server booting up or rebooted

Procedure 23. Gen8: Configure the Integrated Lights Out (iLO) for Rack Mount Server		
1. ☐	Configure iLO for RMS	For HP Gen8 DL380 servers: 1. Reboot the server. 2. When **iLO 4 Standard press [F8] to configure** displays, press **F8**. 3. Wait for the iLO Configuration screen to display.
2. ☐	Access DNS/DHCP	Use the arrow keys to navigate to **Network > DNS/DHCP**. 

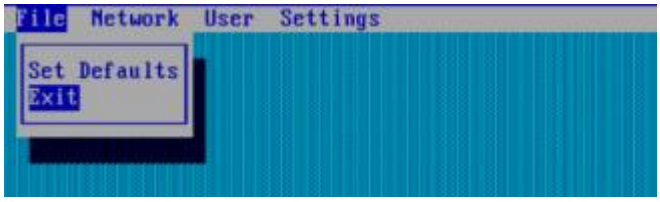
Procedure 23. Gen8: Configure the Integrated Lights Out (iLO) for Rack Mount Server		
3. ☐	Verify DHCP is set to off	Verify **DNS/DHCP** is set to **OFF**.  If not set to **OFF**: Use the **Spacebar** to toggle the setting to **OFF**. Press **F10** to save the changes.
4. ☐	Access NIC and TCP/IP	Use the arrow keys to navigate to **Network > NIC and TCP/IP**. 
5. ☐	Set the IP address	1. Use the arrow keys to set the **IP Address** based on the information in the NAPD. 2. Press **F10** to save the changes.
6. ☐	Access the User menu	Use the arrow keys to navigate to **User > Add**.

Procedure 23. Gen8: Configure the Integrated Lights Out (iLO) for Rack Mount Server		
7. ☐	Set the tekelec user	1. Use the arrow keys to add the tekelec user and password. Username: tekelec Password: tekelec1 2. Press **F10** to save the changes. 
8. ☐	Repeat	Repeat this procedure for other servers.

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

Prerequisites and Requirements:

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

Procedure 24. Enter the ROM-Based Setup Utility (RBSU)		
1. ☐	Access RBSU	1. Reboot the server. 2. Press **F9** when prompted for setup.
2. ☐	Access the initial iLO Configuration Utility screen	Use the arrow keys to navigate to **Network**. 

This procedure verifies/configures the serial port options for the embedded and virtual serial ports.

Prerequisites and Requirements:

- Server rebooted and in RBSU mode

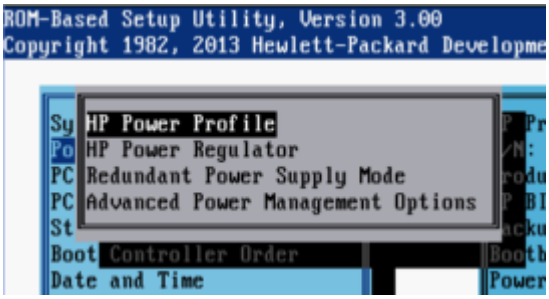
Procedure 25. Verify/Configure Serial Port Options		
1. ☐	**RBSU**: Access the embedded serial port settings	Navigate to **System Options > Serial Port Options > Embedded Serial Port** and press **Enter**.
2. ☐	**RBSU**: Verify the embedded serial port settings	Verify the **Embedded Serial Port** is set for **COM 2**. If it is not set to **COM 2**: Press **Enter** and select **COM 2**. Press **Enter**.

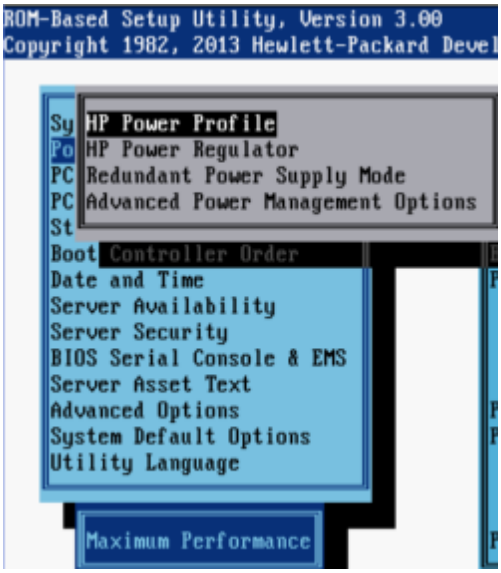
Procedure 25. Verify/Configure Serial Port Options		
3. ☐	**RBSU**: Verify the virtual serial port settings	1. Use the arrow keys to select **Virtual Serial Port**. 2. Verify **Virtual Serial Port** is set for **COM 1**. If it is not set to **COM 1**: Press **Enter** and select **COM 1**. Press **Enter**.

This procedure configures power management options. The server HP power profile is verified or set to maximum performance.

Prerequisites and Requirements:

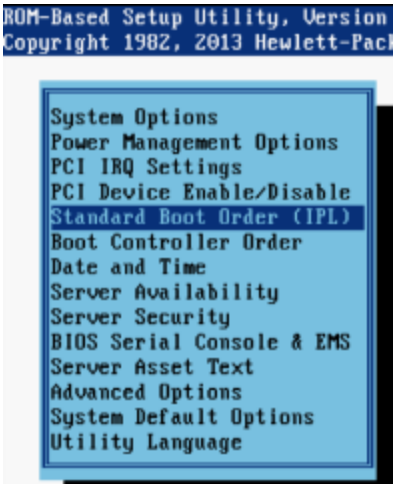
- Server rebooted and in RBSU

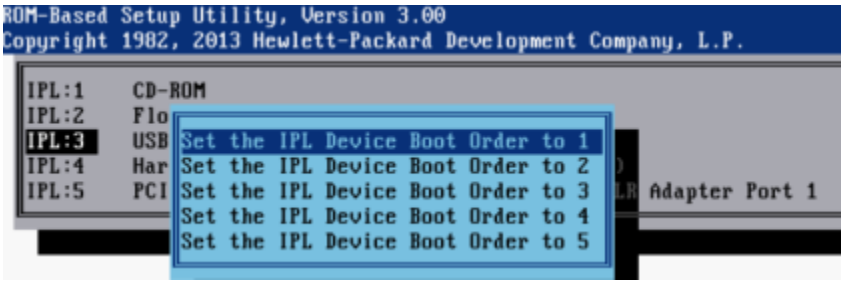
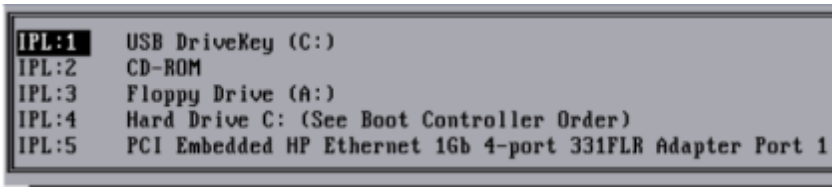
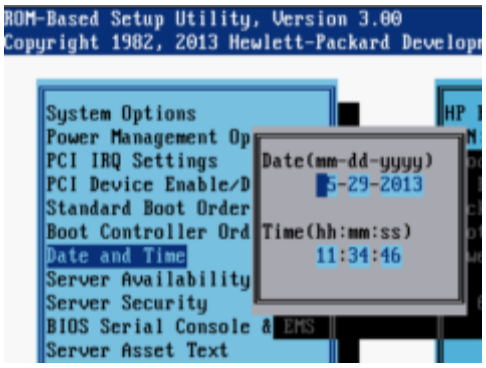
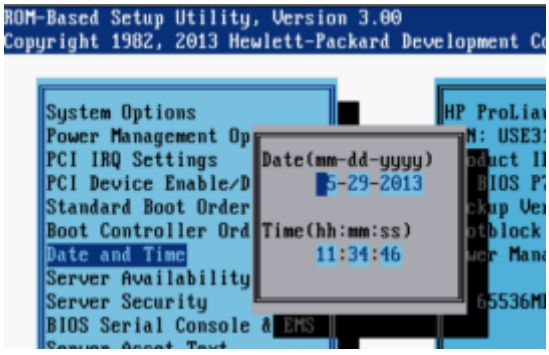
Procedure 26. Verify/Set Power Management		
1. ☐	**RBSU**: Access the HP power profile	Navigate **Power Management Options > HP Power Profile** and press **Enter**.  ***Note:*** Press **Esc**, if needed, to access previous menus.

Procedure 26. Verify/Set Power Management		
2. ☐	**RBSU**: Verify the HP power profile	Verify the **HP Power Profile** is set to **Maximum Performance**.  If not set to **Maximum Performance**: Press **Enter** and select **Maximum Performance**. Press **Enter**.

Prerequisites and Requirements:

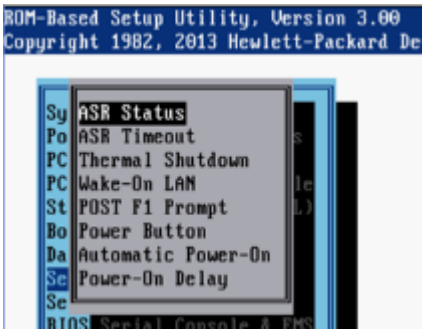
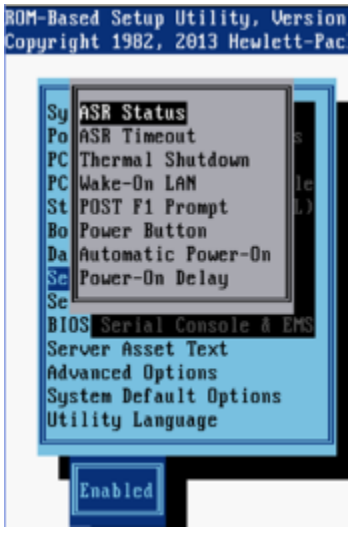
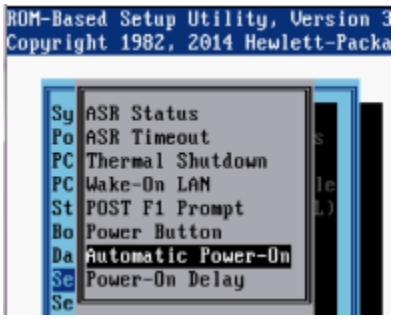
- Server rebooted and in RBSU

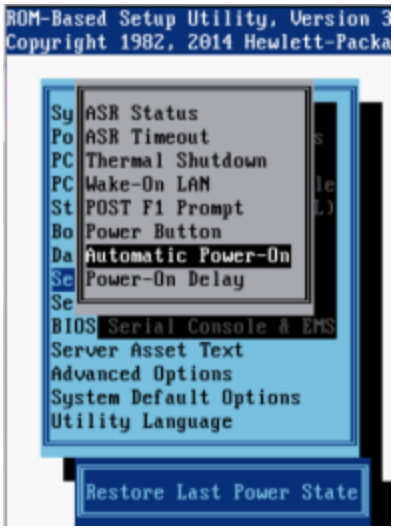
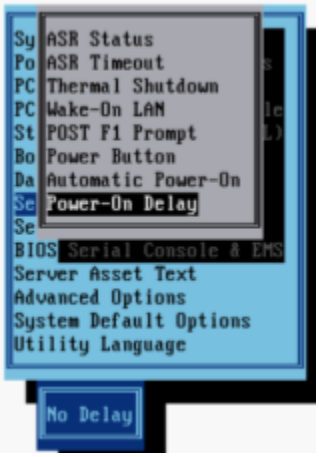
Procedure 27. Verify/Set Standard Boot Order (IPL)		
1. ☐	**RBSU**: Verify or set the standard boot order	Navigate **Standard Boot Order (IPL)** and press **Enter**.  ***Note:*** Press **Esc**, if needed, to access previous menus.

Procedure 27. Verify/Set Standard Boot Order (IPL)		
2. ☐	**RBSU**: Verify the IPL:1 setting	Select **Set the IP Device Boot Order to 1** and verify it is set to **USB DriveKey (C:)**.  If **IPL:1** is not **USB DriveKey:** Select **USB DriveKey** and press **Enter**. Select **Set the IPL Device Boot Order to 1** and press **Enter**. Verify that IPL:1 is set to USB DriveKey (C:) 
3. ☐	**RBSU**: Access the Date and Time menu	Navigate to **Date and Time** and press **Enter**.  ***Note:*** Press **Esc**, if needed, to access previous menus.
4. ☐	**RBSU**: Set the current date and time	1. Use the arrow keys to set the current **Date** and **Time**. Use **UTC** for the time settings. 2. Press **Enter** to confirm the settings. 

Prerequisites and Requirements:

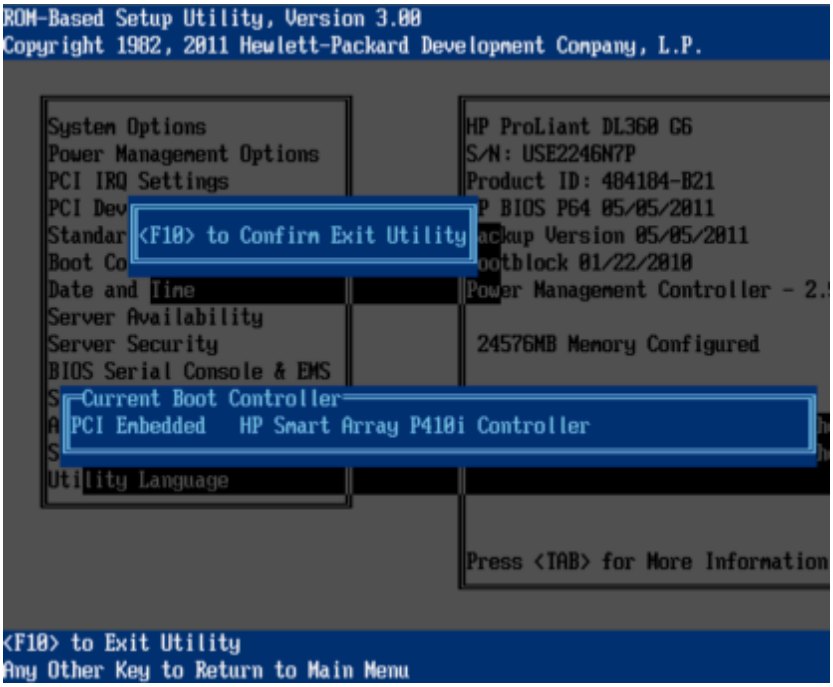
- Server rebooted and in RBSU

Procedure 28. Verify/Set Server Availability		
1. ☐	**RBSU**: Verify server availability	Navigate **Server Availability > ASR Status** and press **Enter**.  ***Note:*** Press **Esc**, if needed, to access previous menus,
2. ☐	**RBSU**: Verify the ASR status setting	Verify the **ASR Status** is set to **Enabled**.  If not set to **Enabled**: Press **Enter** and select **Enabled**. Press **Enter**.
3. ☐	**RBSU**: Access Automatic Power-On menu	Navigate to **Automatic Power-On** and press **Enter**.  ***Note:*** Press **Esc**, if needed, to access previous menus.

Procedure 28. Verify/Set Server Availability		
4. ☐	**RBSU**: Verify the automatic power-on setting	Verify the **Automatic Power-On** is set to **Restore Last Power State**.  If not set to **Restore Last Power State**: Press **Enter** and select **Restore Last Power State**. Press **Enter**.
5. ☐	**RBSU**: Access Power-On Delay menu	Navigate to **Power-On Delay** and press **Enter**. ***Note:*** Press **Esc**, if needed, to access previous menus.
6. ☐	**RBSU**: Verify the power-on delay setting	Verify the **Power-On Delay** is set to **No Delay**.  If not set to **No Delay**: Press **Enter** and select **No Delay**. Press **Enter**.

Prerequisites and Requirements:

- Tasks within the RBSU have been completed

Procedure 29. Exit the RBSU		
1. ☐	**RBSU**: Exit RBSU	To exit RBSU, press **Esc** and press **F10** to confirm. 

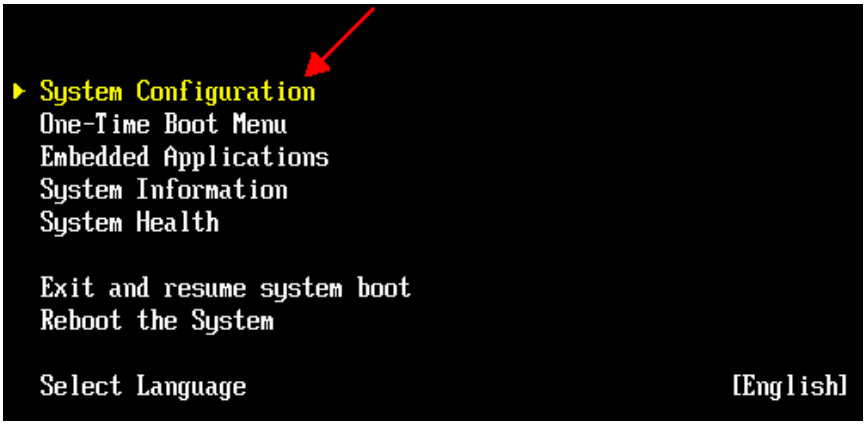
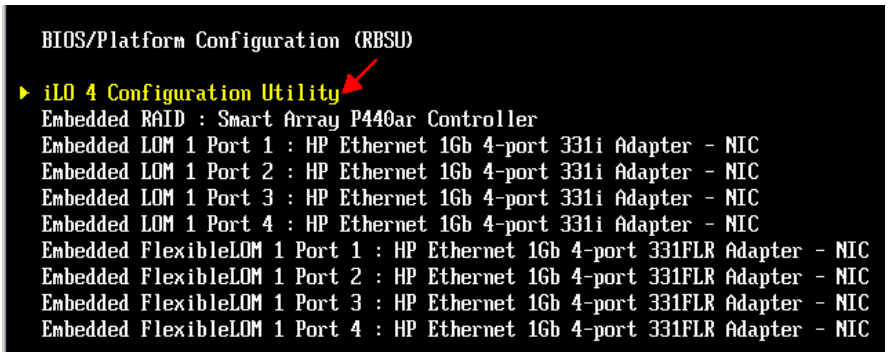
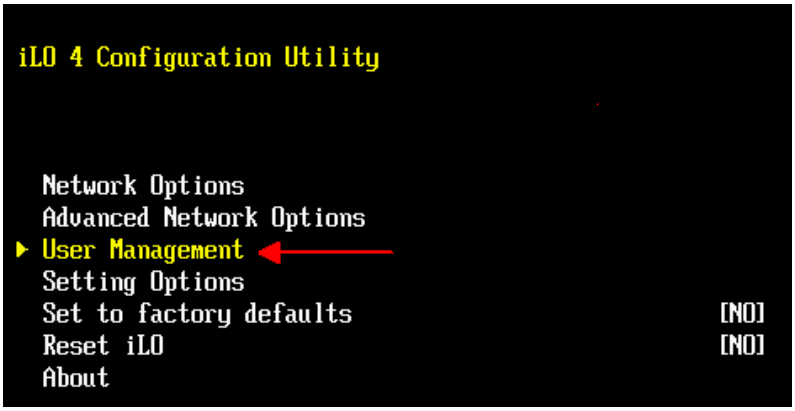
J.2 Gen9: RMS Configure ILO

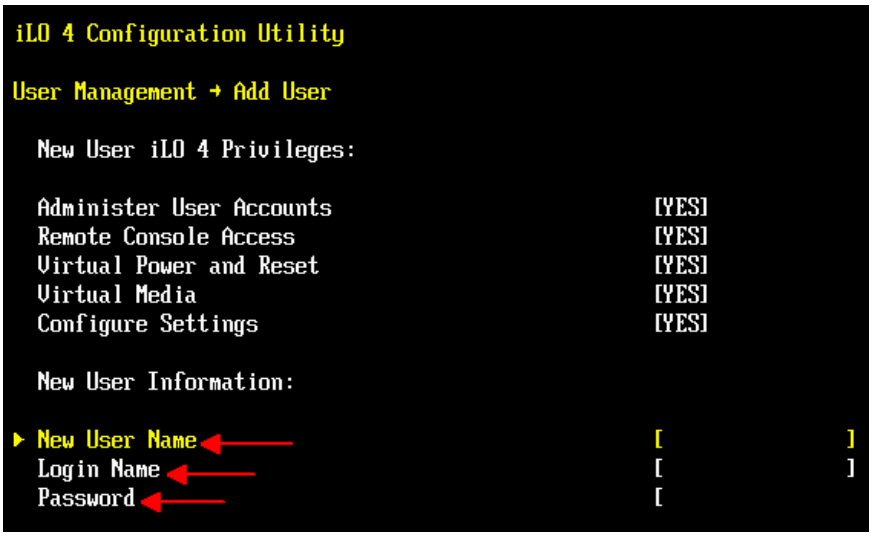
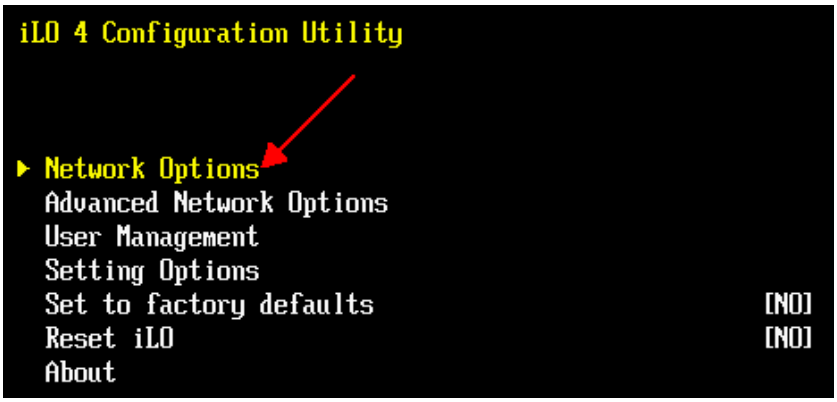
J.2.1 RMS: Configure iLO

Prerequisites and Requirements:

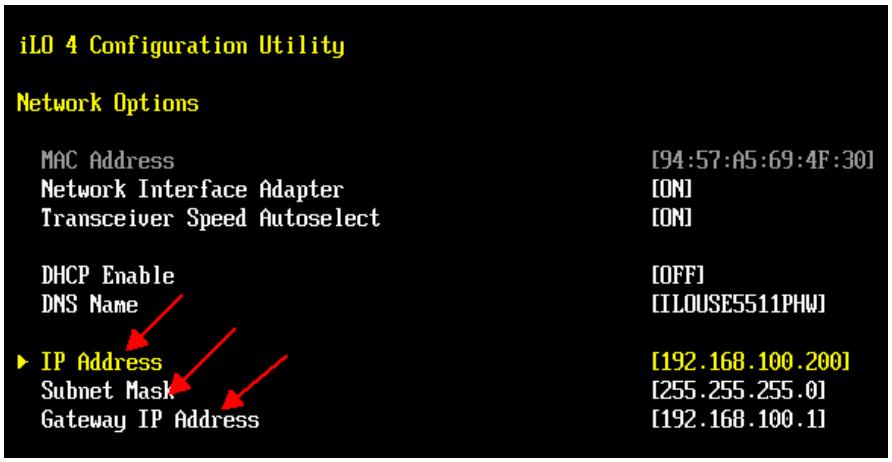
- Server powered on

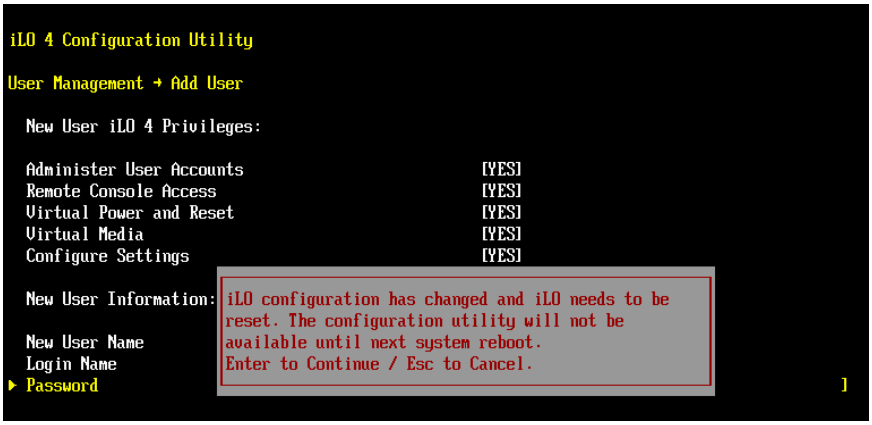
Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS)		
1. ☐	Access system utilities	1. Reboot the server. 2. Press **F9** for System Utilities when prompted with the option.

Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS)		
2. ☐	**System Utilities**: Access iLO 4 configuration utility	1. Press **Enter** to select the **System Configuration** menu.  2. Press **Enter** to select the **iLO 4 Configuration Utility** menu. 
3. ☐	Access user management	Press **Enter** to select the **User Management** menu. 

Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS)		
4. ☐	Access the Add User menu	Press **Enter** to select the **Add User** menu.
5. ☐	Add admusr	Enter the **New User Name**, **Login Name**, and **Password** for tekelec: New User Name: tekelec Login Name: tekelec Password: tekelec1 
6. ☐	Access Network options	1. Press **Esc** to go back to the iLO 4 Configuration Utility menu. 2. Press **Enter** to select **Network Options**. 

<table>
<tr><th colspan="3">Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS)</th></tr>
<tr><td>7. ☐</td><td>Verify the DHCP enable setting</td><td>Verify the DHCP Enable is set to OFF.

If it is not set to OFF:
Press Enter and arrow down to select OFF.
Press Enter.</td></tr>
<tr><td>8. ☐</td><td>Set the IP address, subnet mask, and gateway IP address</td><td>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
 
</td></tr>
</table>

Procedure 30. Gen9: Configure Integrated Lights Out (iLO) for Rack Mount Servers (RMS)		
9. ☐	Exit the iLO Configuration Utility	1. Press **F10** to save changes. 2. Press **Y** to confirm. 3. Reboot the server. 
10. ☐	Repeat	Repeat this procedure for other servers.

J.2.2 Gen9: RMS BIOS Configuration, Verify Processor and Memory

These procedures configure the BIOS on the rack mount server and verify the processor and memory configuration.

J.2.2.1 Gen9: Enter the ROM-Based Setup Utility (RBSU)

Prerequisites and Requirements:

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

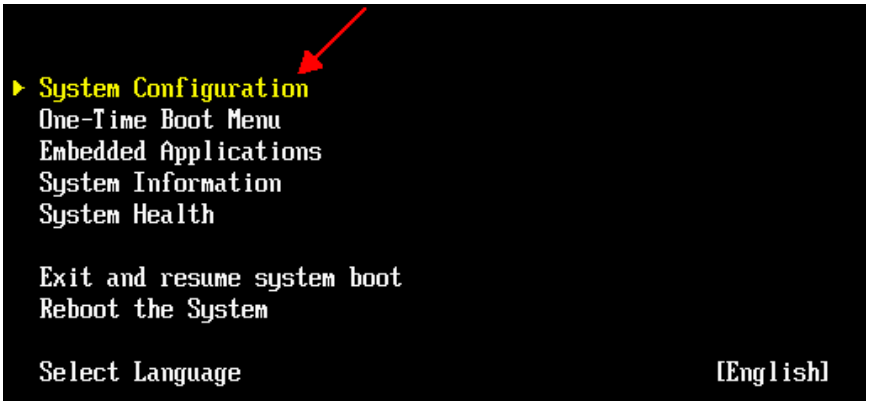
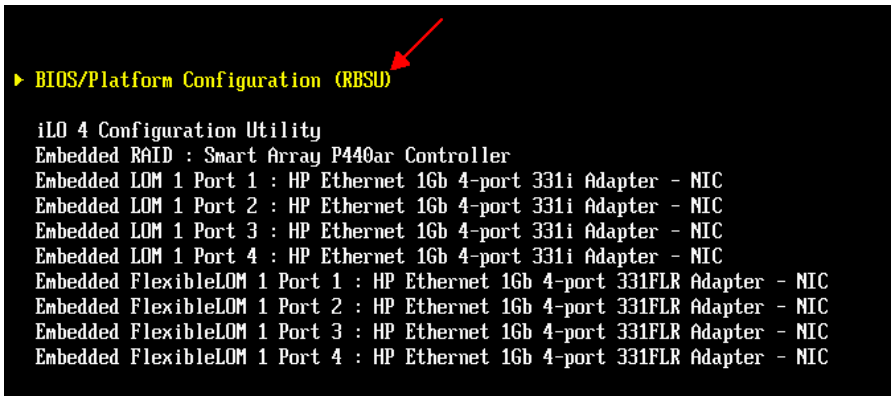
Procedure 31. Verify/Configure BIOS Settings and Verify Configured Memory		
1. ☐	Access system utilities	1. Reboot the server. 2. Press **F9** for System Utilities when prompted with the option.

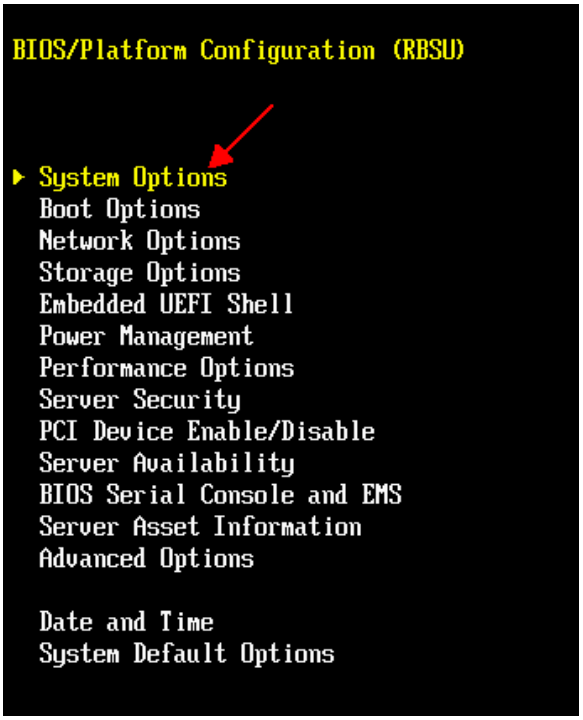
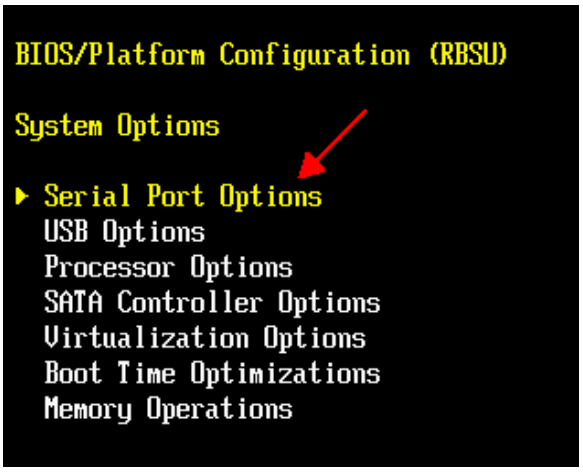
J.2.2.2 Gen9: Verify/Configure Serial Port Options

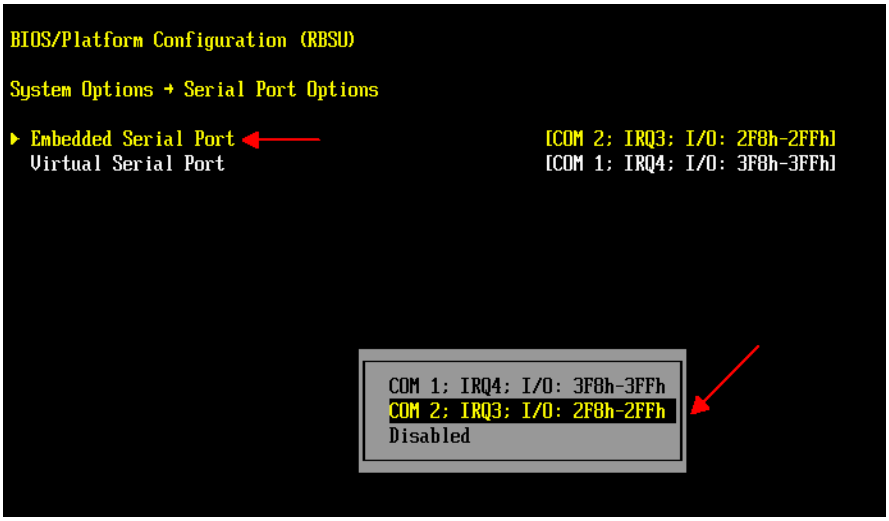
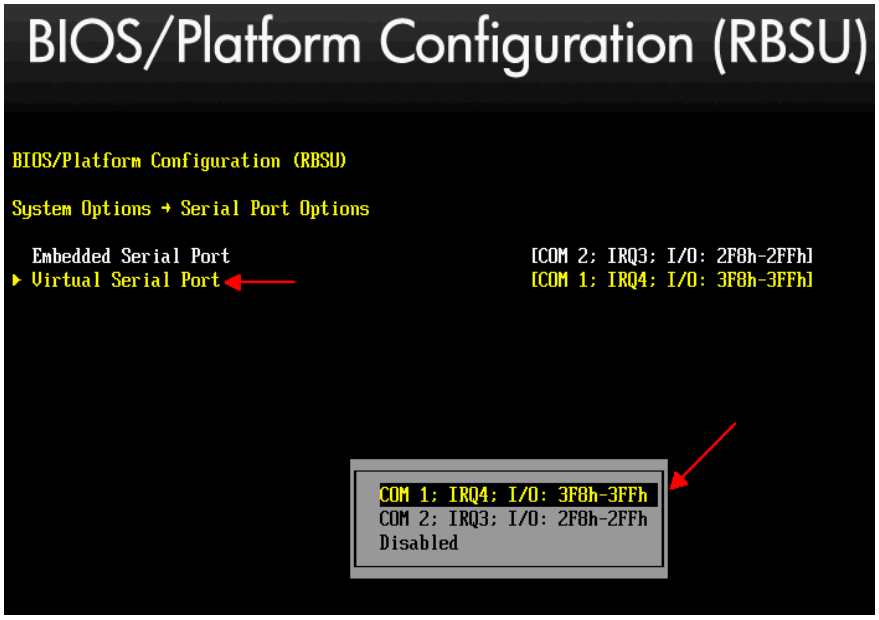
This procedure verifies/configures the serial port options for the embedded and virtual serial ports.

Prerequisites and Requirements:

- Server rebooted and in RBSU mode

Procedure 32. Verify/Configure Serial Port Options		
1. ☐	**System Utilities**: Access RBSU	1. Press **Enter** to select the **System Configuration** menu.  2. Select **BIOS/Platform Configuration (RBSU)**. 

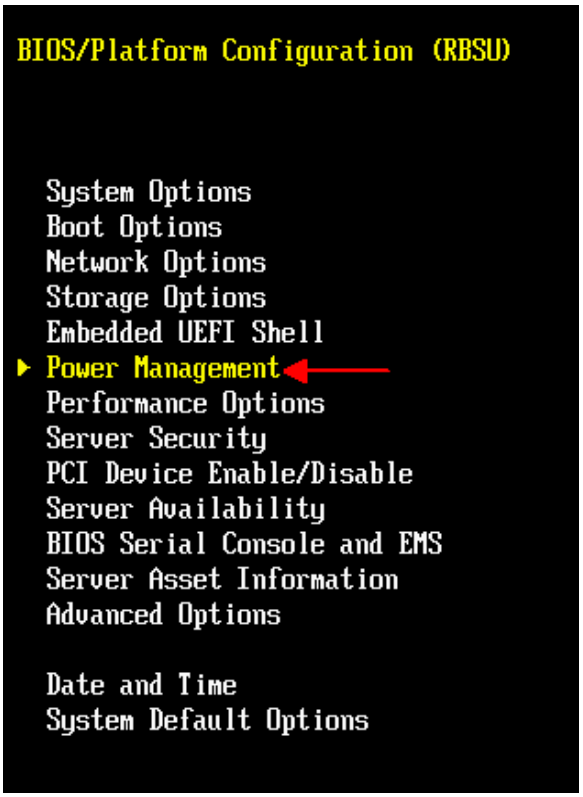
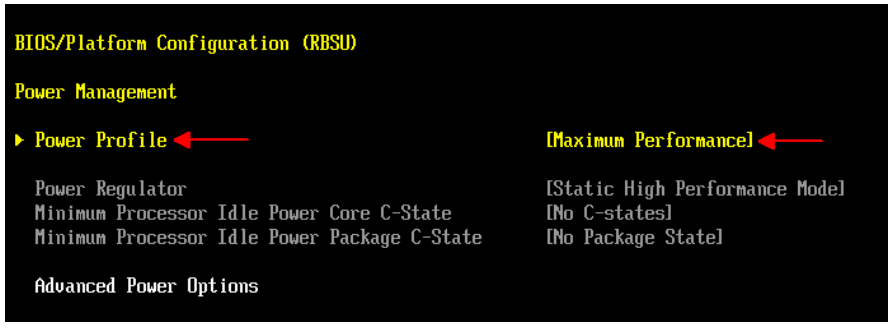
Procedure 32. Verify/Configure Serial Port Options		
2. ☐	**RBSU**: Serial port options	1. Select **System Options**.  2. Select **Serial Port Options**. 

Procedure 32. Verify/Configure Serial Port Options		
3. ☐	**RBSU**: Verify the embedded serial port settings	Select **Embedded Serial Port** and verify it is set for **COM 2**.  If it is not set to **COM 2**: Press **Enter** and select **COM 2**. Press **Enter**.
4. ☐	**RBSU**: Verify the virtual serial port settings	Select **Virtual Serial Port** and verify it is set for **COM 1**.  If it is not set to **COM 1**: Press **Enter** and select **COM 1**. Press **Enter**.

This procedure configures power management options. The server HP power profile is verified/set to maximum performance.

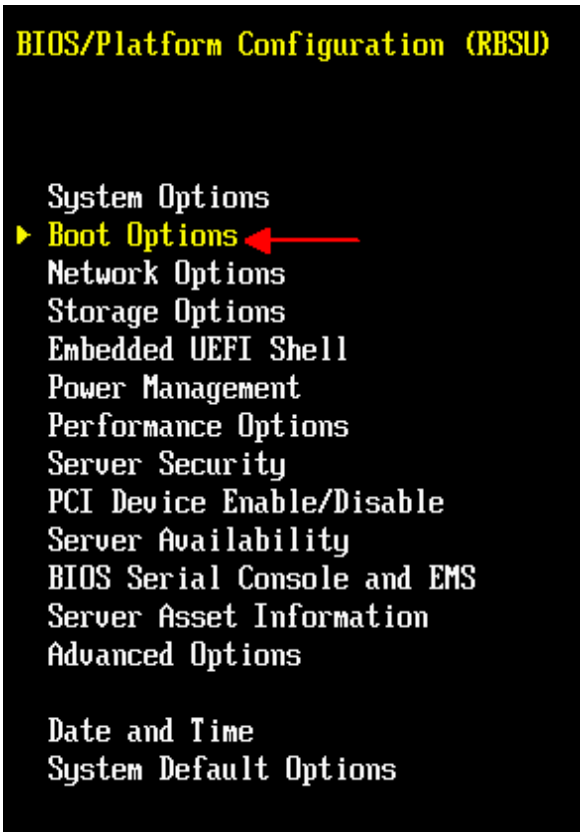
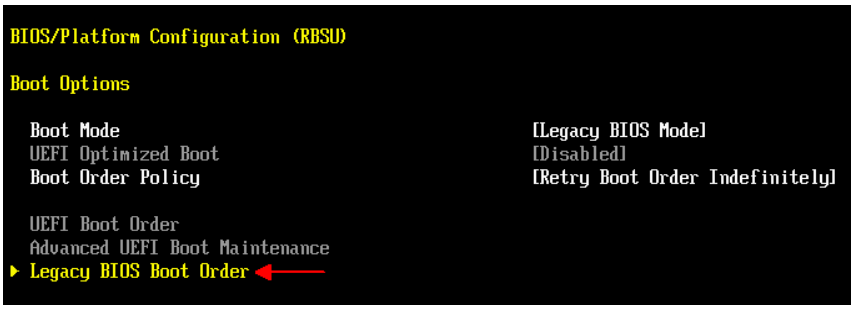
Prerequisites and Requirements:

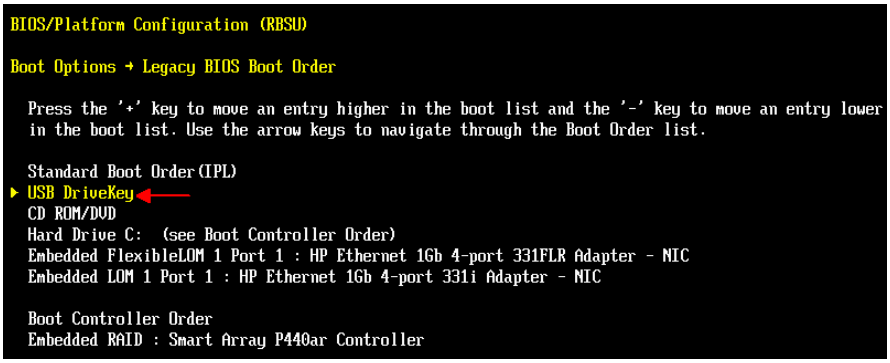
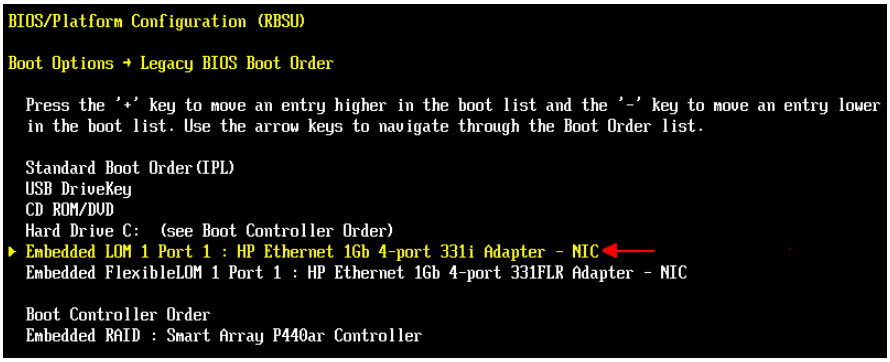
- Server rebooted and in RBSU

Procedure 33. Gen9: Verify/Set Power Management		
1. ☐	**RBSU**: Verify/set the HP power profile	1. Select **Power Management**. 2. Press **Enter**. 
2. ☐	**RBSU**: Verify power management options	Select **Power Profile** and **Maximum Performance**. 
3. ☐	Select power profile	Verify it is set to **Maximum Performance**. If not set to **Maximum Performance**: Press **Enter** and select **Maximum Performance**. Press **Enter**.

Prerequisites and Requirements:

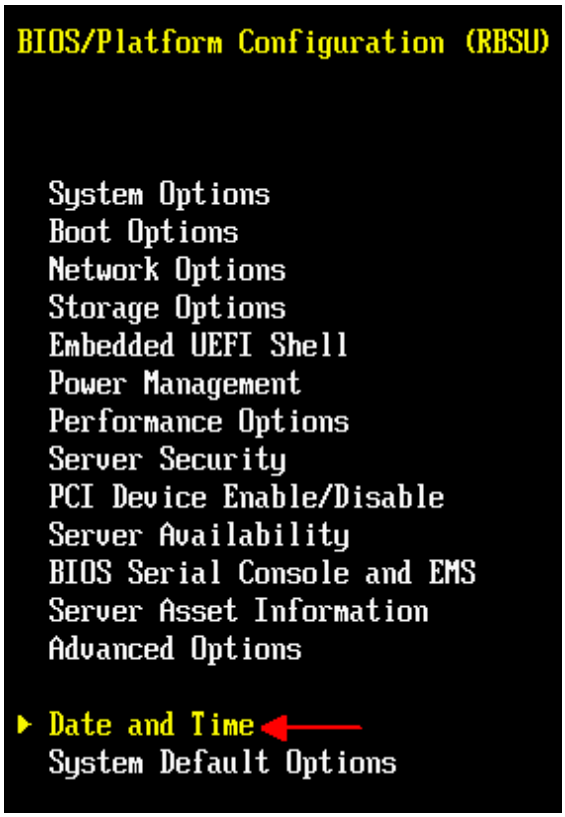
- Server rebooted and in RBSU

Procedure 34. Gen9: Verify/Set Standard Boot Order (IPL)		
1. ☐	**RBSU**: Verify or set the legacy boot order	1. Select **Boot Options**. 2. Press **Enter**.  3. Select **Legacy BIOS Boot Order**. 4. Press **Enter**. 

Procedure 34. Gen9: Verify/Set Standard Boot Order (IPL)		
2. ☐	**RBSU**: Verify USB DriveKey	Under the Standard boot order (IPL) heading, verify **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  

Prerequisites and Requirements:

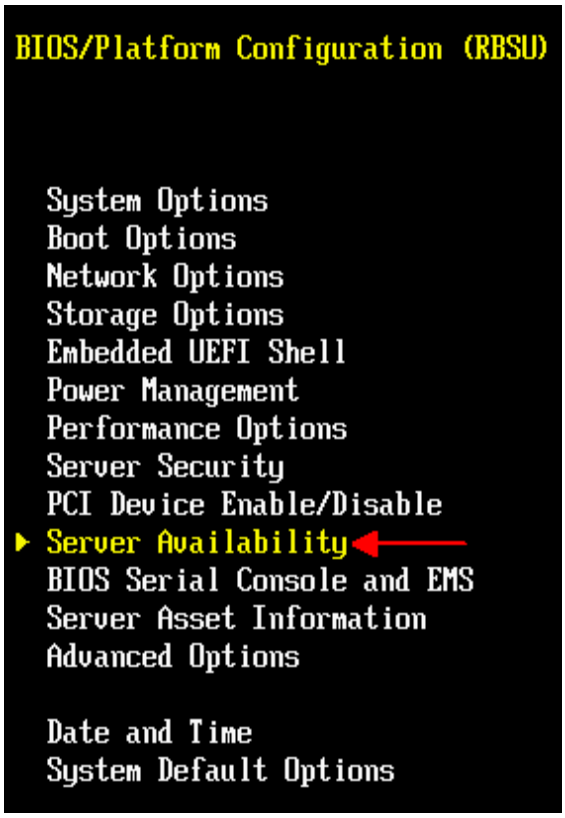
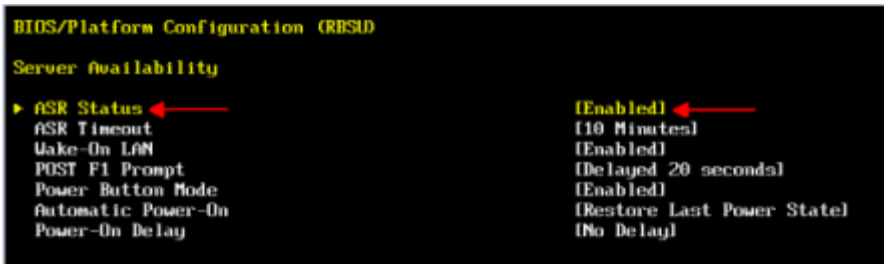
- Server rebooted and in RBSU

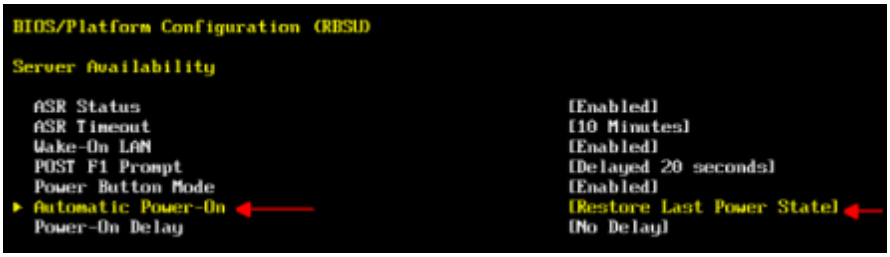
Procedure 35. Gen9: Verify/Set System Date and Time		
1. ☐	**RBSU**: Set the system date and time	1. Select **Date and Time**. 2. Press **Enter**. 
2. ☐	**RBSU**: Set the current date and time	1. Set th **Date** and **Time** (UTC). Use **UTC** for the time settings. 2. Press **Enter** to confirm the settings.

This procedure configures server availability, which determines how the server behaves following a power loss and recovery. The server is set to restore last power state following a power outage and recovery, and set to power on with no delay.

Prerequisites and Requirements:

- Server rebooted and in RBSU

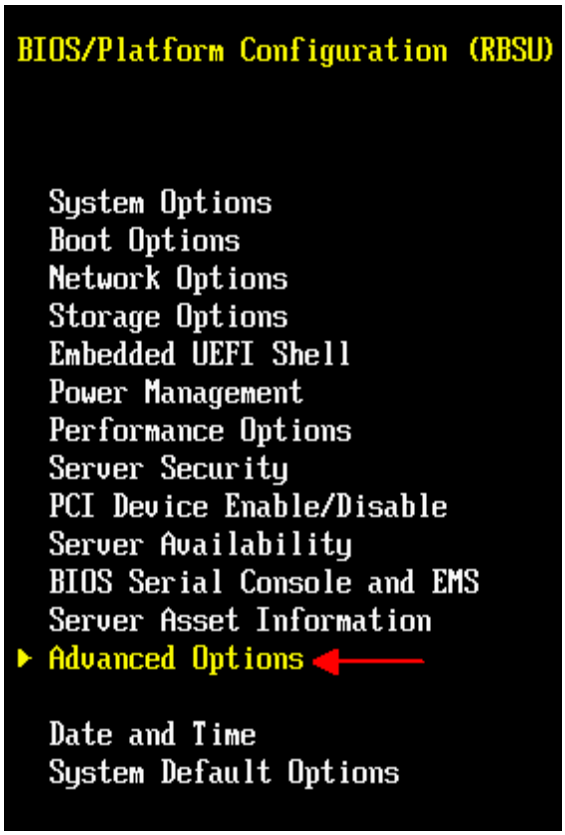
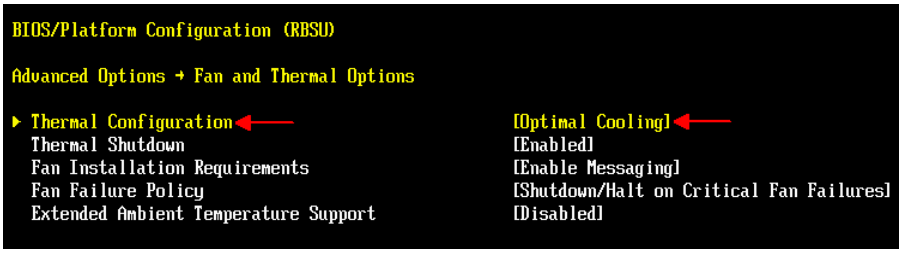
Procedure 36. Gen9: Verify/Set Server Availability		
1. ☐	**RBSU**: Verify server availability options	1. Select **Server Availability**. 2. Press **Enter**. 
2. ☐	**RBSU**: Verify ASR status	Verify the **ASR Status** is set to **Enabled**.  If not set to **Enabled**: Press **Enter** and select **Enabled**. Press **Enter**.

Procedure 36. Gen9: Verify/Set Server Availability		
3. ☐	**RBSU**: Verify automatic power-on	Verify **Automatic Power-On** is set to **Restore Last Power State**.  If not set to **Restore Last Power State**: Press **Enter** and select **Restore Last Power State**. Press **Enter**.
4. ☐	**RBSU**: Verify power-on delay	Verify **Power-On Delay** is set to **No Delay**. If not set to **No Delay**: Press **Enter** and select **No Delay**. Press **Enter**.
5. ☐	**RBSU**: Verify post F1 prompt	Verify **POST F1 Prompt** is set to **Delayed 20 seconds**. If not set to **Delayed 20 seconds**: Press **Enter** and select **Delayed 20 seconds**. Press **Enter**.

This procedure configures advanced options. The fan and thermal options are verified/set to optimal cooling.

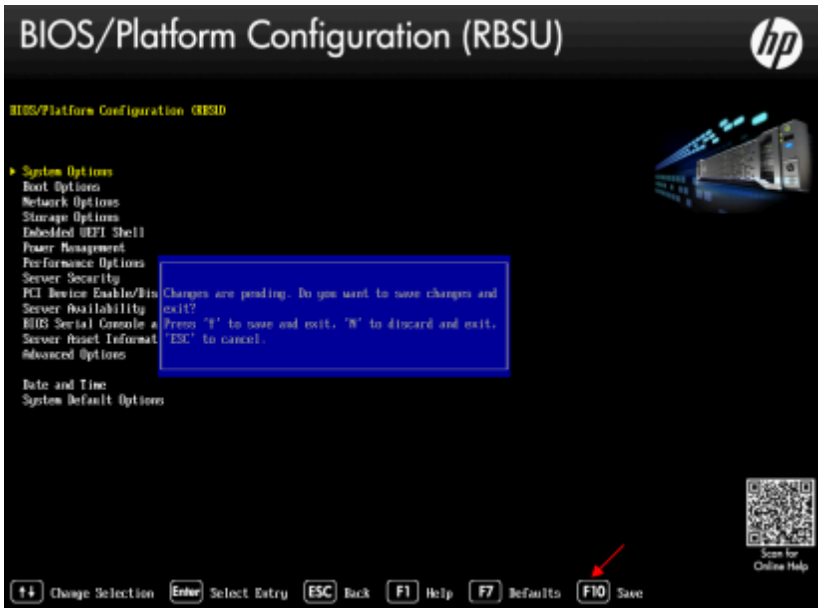
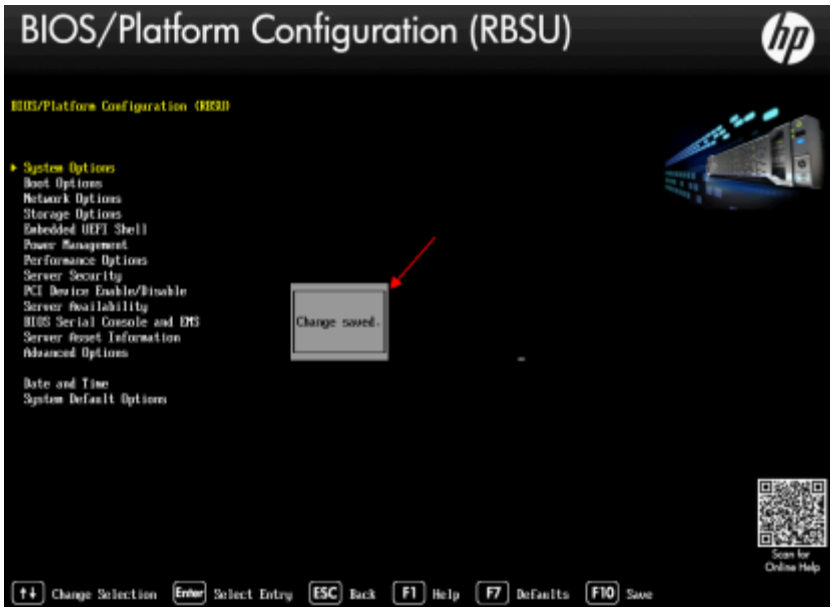
Prerequisites and Requirements:

- Server rebooted and in RBSU

Procedure 37. Gen9: Verify/Advanced Options		
1. ☐	**RBSU**: Verify advance options	1. Select **Advanced Options**. 2. Press **Enter**. 
2. ☐	**RBSU**: Verify Thermal Configuration is set for Optimal Cooling	1. Select **Fan and Thermal Options**. 2. Verify **Thermal Configuration** is set to **Optimal Cooling**.  If not set to **Optimal Cooling**: Press **Enter** and select **Optimal Cooling**. Press **Enter**.

Prerequisites and Requirements:

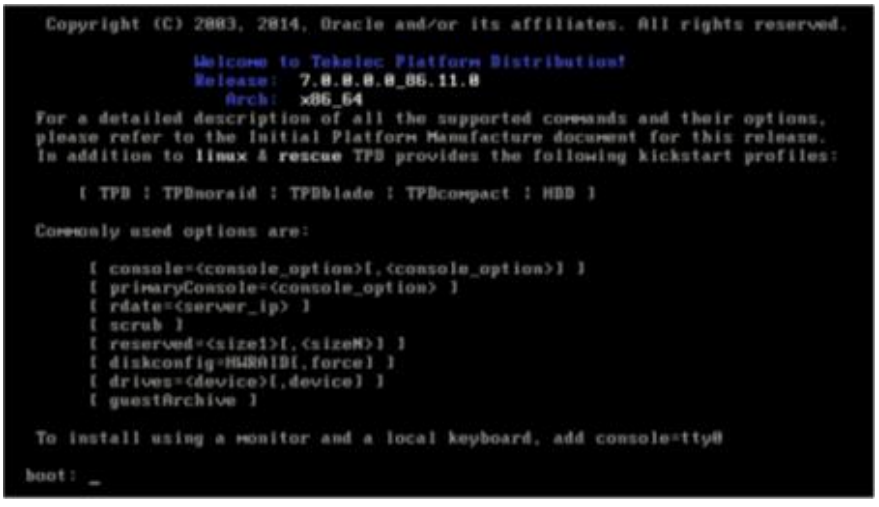
Tasks within the RBSU have been completed.

Procedure 38. Gen9: Save and Exit RBSU		
1. ☐	Save and exit RBSU	1. Press **F10** to save changes 2. Enter **Y** to confirm changes  3. Press **Esc**. 4. Press **F10** to confirm exit utility. 

Procedure 38. Gen9: Save and Exit RBSU		
2. ☐	**RBSU**: Exit RBSU and system utilities	1. Press **Esc**. 2. Press **Enter** to confirm.

Appendix K. Install OS IPM on Servers

This procedure installs the OS IPM.

Procedure 39. Install OS IPM on Servers		
1. ☐	Enter TPD command	Figure 26 shows a sample output screen indicating the initial boot from the install media was successful. The information in this screen output is representative of TPD 7.0.0.0.0.  **Figure 26. Boot from Media Screen, TPD 7.0.0.0.0** Based on the deployment type, either TPD or TVOE can be installed.

Procedure 39. Install OS IPM on Servers

The command to start the installation is dependent upon several factors, including the type of system, knowledge of whether an application has previously been installed or a prior IPM install failed, and what application will be installed.

Text case is important and the command must be typed exactly.

IPM the server by entering the TPD command at the boot prompt. An example command to enter is:

```
TPDnoraid console=tty0 diskconfig=HWRAID,force
```

The Linux kernel loads as shown in Figure 27.

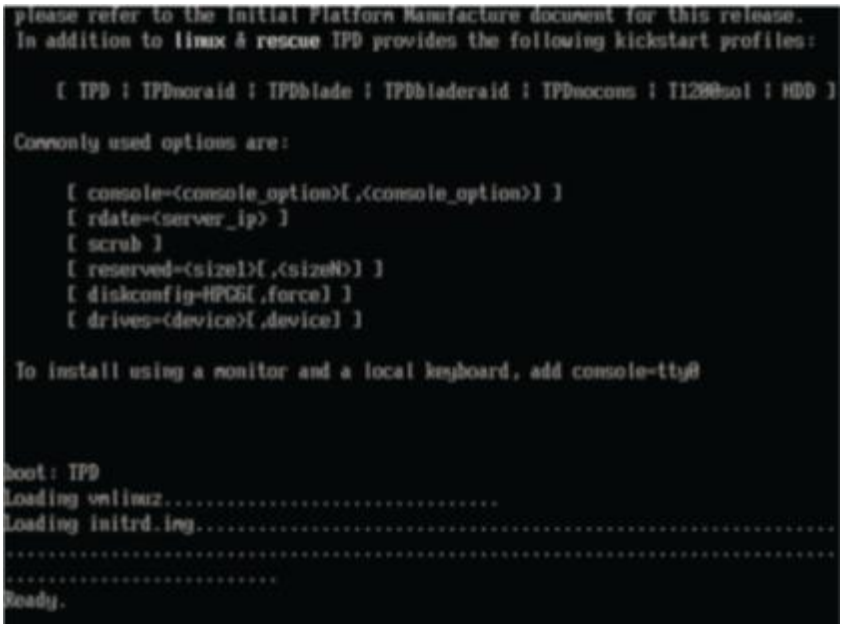


Figure 27. Kernel Loading Output

After a few seconds, additional messages begin scrolling on the screen as the Linux kernel boots, and then the drive formatting and file system creation steps begin:

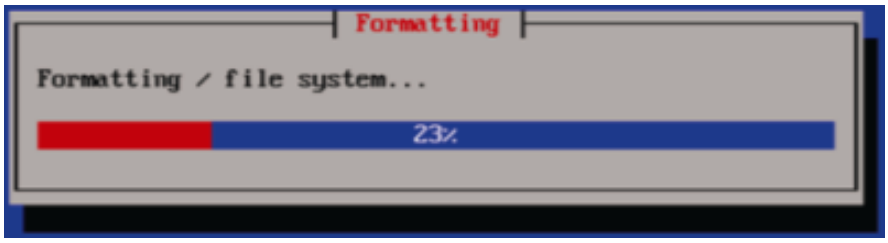


Figure 28. File System Creation Screen

Once the drive formatting and file system creation steps are complete, a screen similar to Figure 29 displays indicating the package installation step is about to begin.

Procedure 39. Install OS IPM on Servers

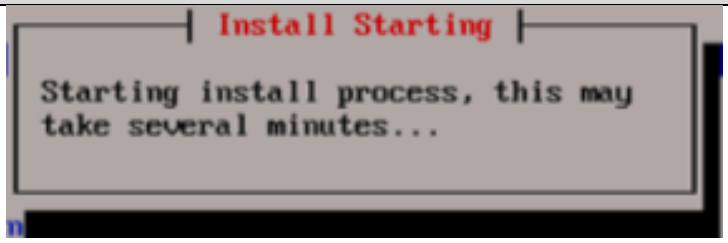


Figure 29. Package Installation Screen

Once Figure 29 displays, it may take several minutes before anything changes. After a few minutes, a screen similar to Figure 30 displays showing the status of the package installation step. For each package, there is a status bar at the top indicating how much of the package has been installed, with a cumulative status bar at the bottom indicating how many packages remain. In the middle, the text statistics indicate the total number of packages, the number of packages installed, the number remaining, and current and projected time estimates.

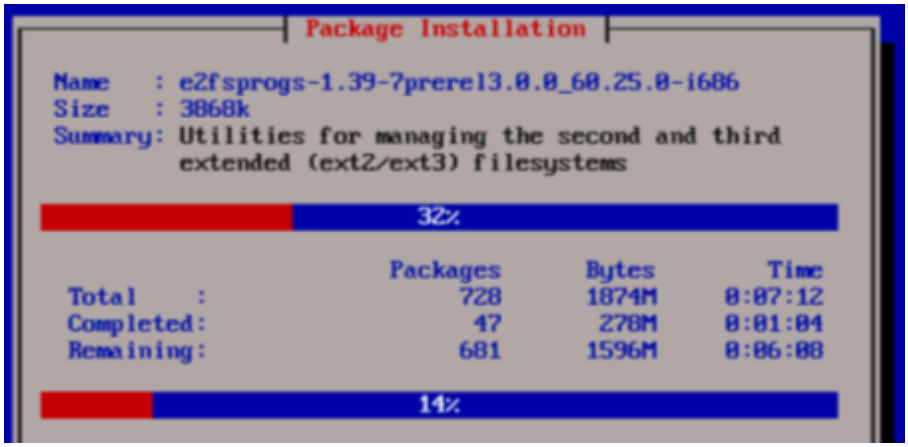
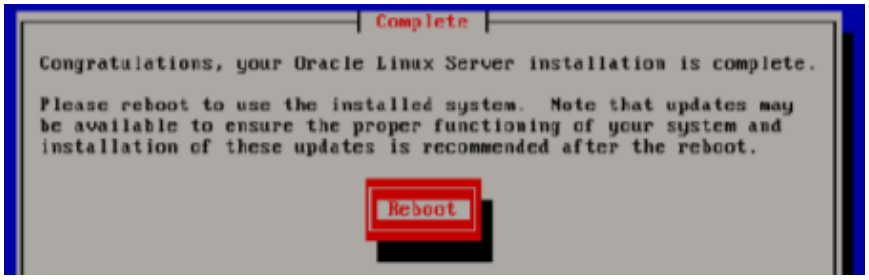
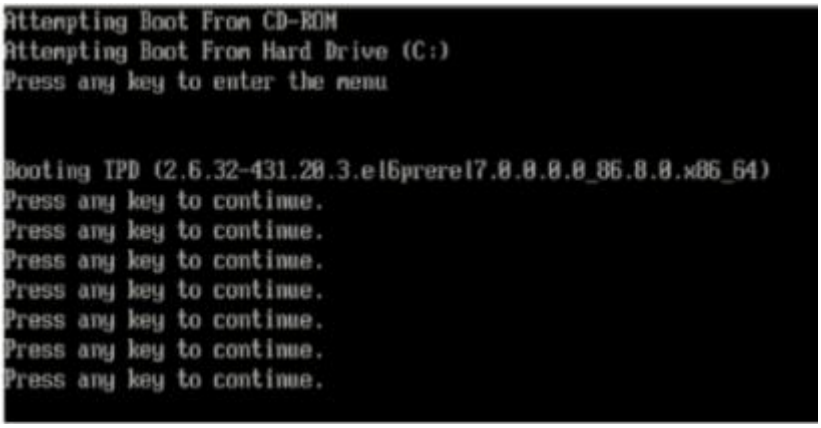


Figure 30. Installation Statistics Screen

Procedure 39. Install OS IPM on Servers		
2. ☐	Reboot the system	Once all the packages have been successfully installed, a screen similar to Figure 31 displays, letting you know the installation process is complete. Remove the installation media (DVD or USB key) and press **Enter** to reboot the system. The system may reboot several times during the IPM process. No user input is required if this occurs.  **Figure 31. Installation Complete Screen** After a few minutes, the server boot sequence starts and displays the new IPM load booting.  **Figure 32. Boot Loader Output** A successful IPM platform installation process results in a user login prompt.

Appendix L. 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:

3. Select **2** for New Service Request.
4. Select **3** for Hardware, Networking and Solaris Operating System Support.
5. 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 will be 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, and 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.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link. The Communications Documentation page displays. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or Platforms.
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays.
5. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.