Oracle® Communications

Diameter Signaling Router

SDS Software Upgrade Guide

Release 8.2

E88971-01

March 2018

ORACLE

Oracle® Communications DSR, SDS Software Upgrade Guide, Release 8.2

Copyright © 2011, 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.

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

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

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

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

See more information on My Oracle Support (MOS).

Table of Contents

1. Introduction 8
1.1 References 8
1.2 Acronyms 8
1.3 Terminology 9
1.4 How to Use this Document 10
1.5 Activity Logging 10
1.6 Use of Health Checks 11
1.7 Large Installation Support 11
1.8 Warnings, Cautions, and Notes 11
1.8.1 Netbackup 7.7 Support 11
1.8.2 Upgrade Scenario 11
2. General Description 11
2.1 SDS 8.2 Supported Upgrade Paths 12
3. Upgrade Overview 13
3.1 Upgrade Requirements 13
3.1.1 ISO Image File 14
3.1.2 Logins, Passwords, and Site Information 14
3.2 Upgrade Maintenance Windows 15
3.3 Upgrade Preparation Overview 17
3.4 Primary SDS Site/DR SDS Site Upgrade Execution Overview 18
3.5 SOAM Upgrade Execution Overview 18
3.6 Post Upgrade Execution Overview 18
3.7 Recovery Procedures Overview 19
4. SDS Upgrade Matrix 19
5. Upgrade Preparation 20
5.1 Requirements Check 20
5.2 Review Release Notes 20
5.3 Perform Firmware Verification (Upgrade Preparation) 21
5.4 Perform Health Check (Upgrade Preparation) 21
5.5 ISO Administration 21
5.6 Back Up TKLCConfigData File 26
5.7 Perform Health Check (Post ISO Administration) 26
5.8 Full Database Backup (PROV & COMCOL ENV for All Servers) 26
6. Automated Site Upgrade 32
6.1 Site Upgrade Execution 32
6.2 Minimum Server Availability 36

6.3 Site Upgrade Options 36
6.4 Cancel and Restart Auto Site Upgrade 37
7. Automated Server Group Upgrade 39
7.1 Cancel and Restart Automated Server Group Upgrade 39
7.2 Site Accept 40
8. Primary/DR SDS NOAM Upgrade Execution 41
8.1 Perform Health Check (Primary/DR NOAM Pre-Upgrade) 41
8.2 Upgrade the Primary SDS NOAM 42
8.3 Upgrade DR SDS NOAM 54
8.4 Perform Health Check (Primary/DR NOAM Post Upgrade) 56
8.5 SNMP Configuration Update (Post Primary/DR NOAM Upgrade) 56
9. Site Upgrade Execution 56
9.1 Automated Site Upgrade 56
9.1.1 Perform Health Check (Pre-Upgrade) 57
9.1.2 Upgrade SOAM 57
9.1.3 Rearrange Automate Site Upgrade Cycles 62
9.1.4 Perform Health Check (Post Upgrade) 65
9.2 SOAM Upgrade Execution (Manual and Automated Server Group) 66
9.2.1 Perform Health Check (SOAM Pre-Upgrade) 66
9.2.2 Upgrade SOAM 67
9.2.3 Perform Health Check (SOAM Post Upgrade) 69
9.3 Post Upgrade Procedures 69
9.3.1 Accept the Upgrade 69
9.3.2 SOAM VM Profile Update 73
10. Recovery Procedures 73
10.1 Backout Setup 73
10.2 Perform Backout 74
10.2.1 Back Out the SOAM 74
10.2.2 Back Out the DR SDS NOAM 77
10.2.3 Back Out the Primary SDS NOAM 79
Appendix A Access the OAM GUI Using the VIP (NOAM/SOAM) 83
Appendix B Health Check Procedures 84
Appendix C Upgrade Server Administration on SDS 7.x 99
Appendix D Upgrade Server Administration on SDS 8.x 105
Appendix E Back Out a Single Server 111
Appendix F Manually Perform ISO Validation 119
Appendix G Undeploy an ISO File (Post Upgrade Acceptance) 123

Appendix H Add the SDS ISO to the PMAC Software Repository 125
Appendix I Recover from a Failed Upgrade 131
Appendix J Add New SOAM Profile on Existing VM 137
Appendix K Manual Completion of Server Upgrade 166
Appendix L ISO Link Correction 169
Appendix M Increase Maximum Number of Open Files 171
Appendix N Advanced Health Check 174
Appendix O Workaround to Resolve Server HA Failover Issue 177
Appendix P Workaround for SNMP Configuration 177
Appendix Q Workaround to Resolve Syscheck Error for CPU Failure 180
Appendix R Workaround to Fix cmsoapa Restart 181
Appendix S Workaround to Fix DNS Issue 182
Appendix T My Oracle Support (MOS) 183

List of Tables

Table 1. Acronyms 8
Table 2. Terminology 9
Table 3. Logins, Passwords, and Site Information 14
Table 4. Upgrade Maintenance Windows 15
Table 5. Upgrade Preparation Procedures 17
Table 6. Primary SDS/DR SDS Upgrade Procedures Strategy 18
Table 7. SOAM Upgrade Procedures 18
Table 8. Post Upgrade Procedures 18
Table 9. Backout Procedures 19
Table 10. SDS Upgrade Matrix 19
Table 11. SDS Upgrade – List of Procedures 20
Table 12. Site Upgrade Planning — Automed vs. Manual Upgrade 56

List of Figures

Figure 1. Example Procedure Steps Used in This Document 10
Figure 2. SDS 8.0 Supported Upgrade Paths 13
Figure 3. Upgrade Perspective of SDS Site Topology 32
Figure 4. Site Upgrade — NOAM View 33
Figure 5. Site Upgrade — Entire Site View 33
Figure 6. Site Upgrade — Site Initiate Screen 34
Figure 7. Site Upgrade Monitoring 35

Figure 8. Server Group Upgrade Monitoring 35
Figure 9. Server Group Upgrade Monitoring 35
Figure 10. Auto Site Upgrade General Options 36
Figure 11. Site Upgrade Active Tasks 37
Figure 12. User Cancelled the Site Upgrade Tasks 37
Figure 13. Partially Upgraded Site 38
Figure 14. Restarting Site Upgrade. 38
Figure 15. Server Group Upgrade Active Tasks 39
Figure 16. Site Accept Button 40
Figure 17. Site Accept Screen 40

List of Procedures

Procedure 1. Required Materials Check 20
Procedure 2. ISO Administration 21
Procedure 3. TKLCConfigData Backup 26
Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers 27
Procedure 5. Upgrade the Primary SDS NOAM 42
Procedure 6. Upgrade DR SDS NOAM 54
Procedure 7. Upgrade SOAM 58
Procedure 8. Rearrange Automated Site Upgrade Cycles 62
Procedure 9. Upgrade SOAM 67
Procedure 10. Accept the Upgrade 69
Procedure 11. Back Out the SOAM 74
Procedure 12. Back Out the DR SDS NOAM 77
Procedure 13. Back Out Primary SDS NOAM 79
Procedure 14. Access the OAM GUI Using the VIP (NOAM/SOAM) 83
Procedure 15. Health Check Procedure 85
Procedure 16. Upgrade Server Administration on SDS 7.x 99
Procedure 17. Upgrade Server Administration on SDS 8.x 105
Procedure 18. Back Out a Single Server 111
Procedure 19. Manually Perform ISO Validation 119
Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance 123
Procedure 21. Add the SDS ISO to the PMAC Software Repository 125
Procedure 22. Recover from a Failed Upgrade 131
Procedure 23. Add SDS Software Images to PMAC Server 137
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group 142
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile 146

Procedure 26. Place the SDS SOAM VM into the SOAM Server Group 160
Procedure 27. Manual Completion of Server Upgrade 167
Procedure 28. ISO Link Correction 169
Procedure 29. Increase Maximum Number of Open Files 171
Procedure 30. Advanced Health Check 174
Procedure 31. Workaround to Resolve Server HA Failover Issue 177
Procedure 32. Workaround for SNMP Configuration 177
Procedure 33. Workaround to Resolve Syscheck Error for CPU Failure 180
Procedure 34. Workaround to Fix the cmsoapa Restart 181
Procedure 35. Workaround to Fix DNS Issue 182

1. Introduction

This document describes methods used and procedures executed to perform an application software upgrade on in-service SDS servers and SDS DP blades in an SDS network. The supported paths are:

- Major upgrade from SDS 7.x to SDS 8.2
- Minor upgrade from SDS release 8.2.x to a later 8.2.y release

The audience for this document includes Oracle customers and the Global Software Delivery SDS group.

This document provides instructions to execute any SDS 8.2 software upgrade.

The SDS software includes all Tekelec Platform Distribution (TPD) software. Any TPD upgrade necessary is included automatically as part of the SDS software upgrade. The execution of this procedure assumes the SDS software load (ISO file, CD-ROM, or other form of media) has already been delivered to the customer's premises. This includes delivery of the software load to the local workstation being used to perform this upgrade.

Note: The distribution of the SDS software load is outside the scope of this procedure.

1.1 References

[1] SDS 8.2 Initial Installation and Configuration Guide

[2] Database Management: Backup and System Restoration

[3] SDS 8.2 Disaster Recovery Guide

[4] HP Solutions Firmware Upgrade Pack Release Notes, v2.1.5 (or latest 2.1 version)

[5] Platform 7.2 Configuration Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Meaning
CLI	Command Line Interface
CSV	Comma-separated Values
DP	Database Processor
DR	Disaster Recovery
GA	General Availability
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IPM	Initial Product Manufacture
ISO	ISO 9660 file system
LA	Limited Availability
MOP	Method of Procedure

Acronym	Meaning
MP	Message Processing or Message Processor
NE	Network Element
NO (or NOAM)	Network OAM&P
OAM&P	Operations, Administration, Maintenance and Provisioning
SDS	Subscriber Database Server
SO (or SOAM)	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
XSI	External Signaling Interface

1.3 Terminology

This section describes terminology as it is used within this document.

Table 2. Terminology

Term	Meaning
Upgrade	The process of converting an application from its current release on a system to a newer release.
Major upgrade	An upgrade from a current major release to a newer major release. An example of a major upgrade is SDS 7.1 to SDS 8.2.
Incremental upgrade	An upgrade from a current build to a newer build within the same major release. An example of an incremental upgrade is SDS 8.2.0.0.0_82.3.0 to 8.2.0.0.0_82.4.0.
Software only upgrade	An upgrade that does not require a database schema change; only the software is changed.
Single server upgrade	The process of converting an SDS server from its current release on a single server to a newer release.
Backout	The process of reverting a single SDS server to a prior version. This could be performed due to failure in single server upgrade.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.
Source release	Software release to upgrade from.
Target release	Software release to upgrade to.

Term	Meaning
Upgrade ready	State that allows for graceful upgrade of a server without degradation of service. It is a state that a server is required to be in before it can be upgraded. The state is defined by the following attributes: • Server is forced standby • Server is application disabled (signaling servers do not process any traffic)

1.4 How to Use this Document

When executing the procedures in this document, there are a few key points to help ensure the user understands procedure convention. These points are:

1. Before beginning a procedure, completely read the instructional text (it displays 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.
3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix T before attempting to continue.

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

- Each step has a checkbox the user should mark to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- The title box describes the operations to be performed during that step.
- 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.
- Each command the user enters, as well as any response output, is formatted in `10-point Courier` font.

	Title/Instructions	Directive/Result Steps
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify network element data	View the network elements configuration data; verify the data; save and print report. 1. Navigate to **Configuration > Network Elements**.

Figure 1. Example Procedure Steps Used in This Document

1.5 Activity Logging

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

1.6 Use of Health Checks

The user may execute the **Perform Health Check** or **View Logs** steps freely or repeat as many times as desired in between procedures during the upgrade process. It is not recommended to do this in between steps within a procedure, unless there is a failure to troubleshoot.

1.7 Large Installation Support

For large systems containing multiple signaling network elements, it may not be feasible to apply the software upgrade to every network element within a single maintenance window; however, whenever possible, primary SDS site and DR SDS site network elements should be upgraded within the same maintenance window.

1.8 Warnings, Cautions, and Notes

This section presents notices of warnings and cautions that directly relate to the success of the upgrade. It is imperative that each of these notices be read and understood before continuing with the upgrade. If there are any conflicts, issues, or questions related to these notices, it is recommended to contact My Oracle Support (MOS) as directed in Appendix T before starting the upgrade

1.8.1 Netbackup 7.7 Support

Netbackup 7.7 requires additional disk space that is not available before SDS release 8.0. Thus, SDS must be upgraded to release 8.0 or higher before upgrading to Netbackup 7.7. But, while upgrading from SDS 8.0 to 8.1, Netbackup 7.7 is already be supported.

WARNING Upgrade DSR to release 8.2 before upgrading to NetBackup 7.7.

1.8.2 Upgrade Scenario

Caution

SDS Upgrade

If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes.

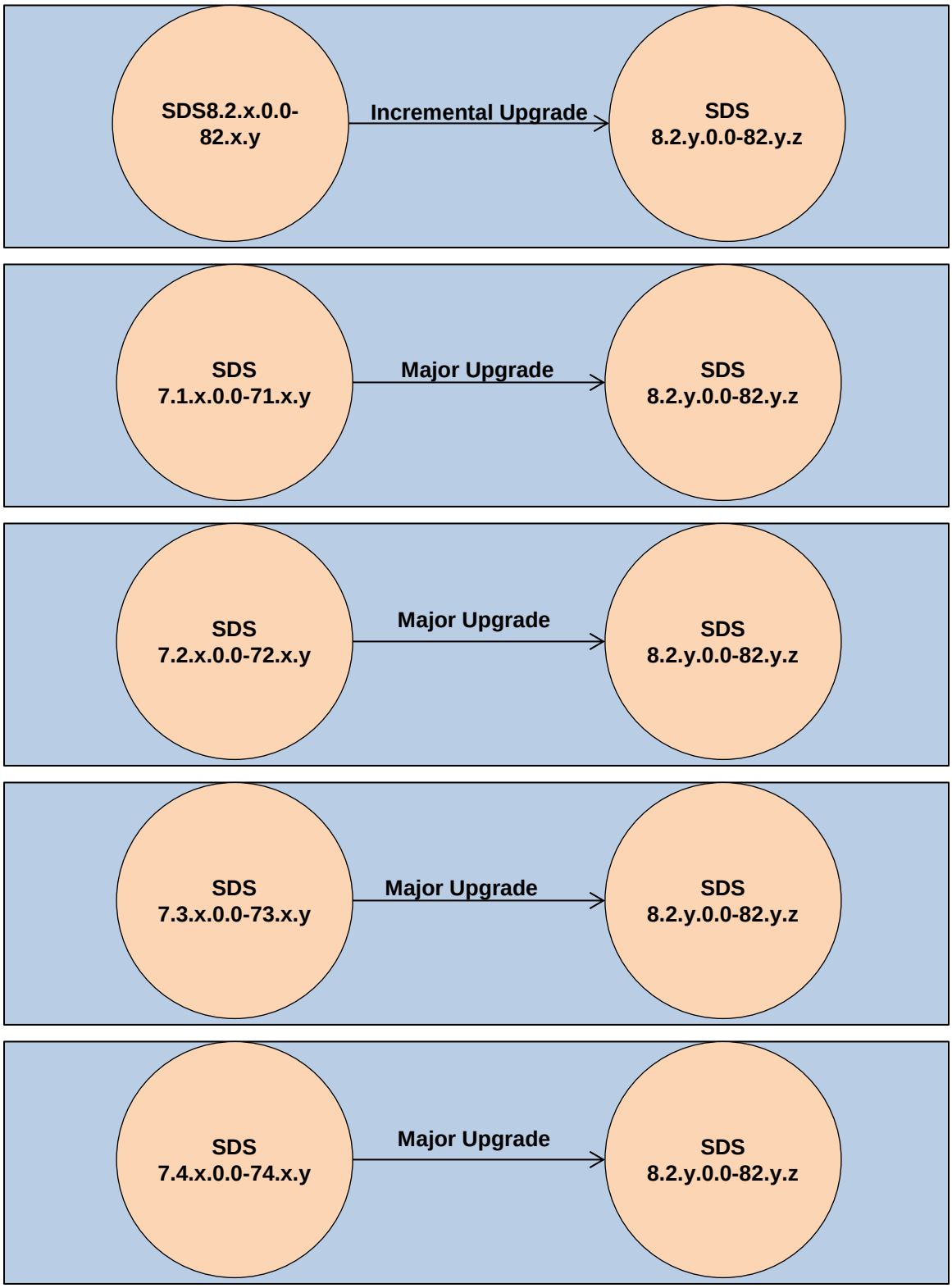
2. General Description

This document defines the step-by-step actions performed to execute a software upgrade of an in-service SDS from the source release to the target release.

Note: Initial Installation is not within the scope of this upgrade document. See [1] SDS 8.2 Initial Installation and Configuration Guide for more information.

2.1 SDS 8.2 Supported Upgrade Paths

The supported SDS 8.2 upgrade paths are shown in the Figure 2.



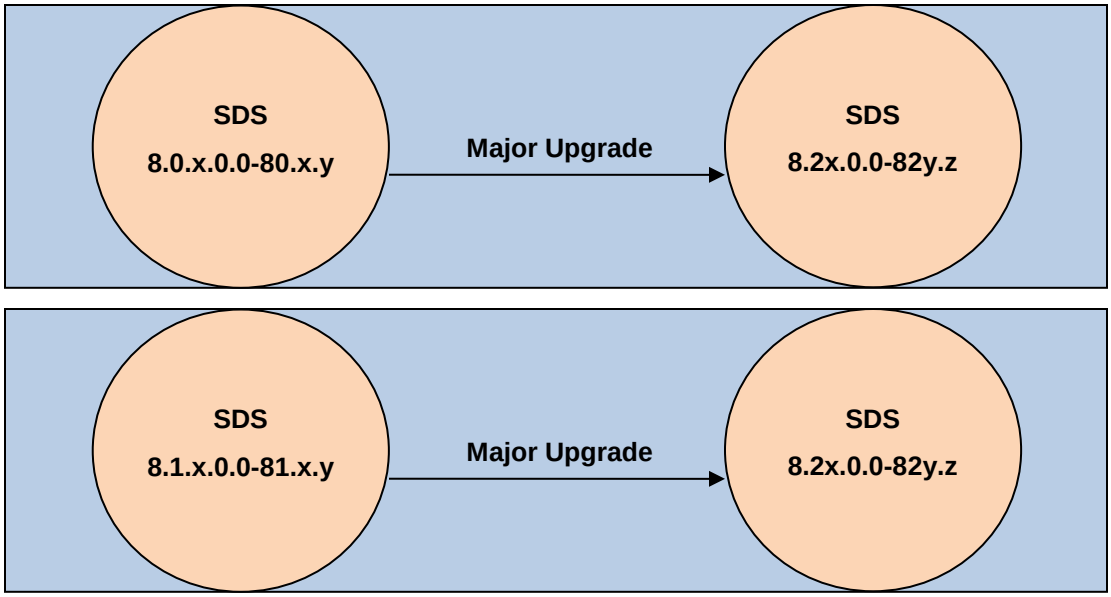


Figure 2. SDS 8.0 Supported Upgrade Paths

3. Upgrade Overview

This section lists the required materials and information needed to execute an upgrade. It also provides a brief timing overview of the activities needed to upgrade the source release software that is installed and running on an SDS server to the target release software. The approximate time required is outlined in sections 3.3 through 3.7. These tables are used to plan and estimate the time necessary to complete the upgrade.

Timing values are estimates only. They estimate the completion time of a step or group of steps for an experienced user. These tables are not to be used to execute procedures. Detailed steps for each procedure are provided in section 5.

3.1 Upgrade Requirements

The following levels of access, materials and information are needed to execute an upgrade:

- Target-release ISO image file

  Example: SDS-8.2.0.0.0_82.4.0-x86_64.iso

- VPN access to the customer's network.
- GUI access to the SDS network OAM&P VIP with administrator's privileges.
- SSH/SFTP access to the SDS network OAM&P XMI VIP as the **admusr** user.

  Note: All logins into the SDS active and DR site servers are made using the external management (XMI) VIP unless otherwise stated.

- User logins, passwords, IP addresses and other administration information. See section 3.1.2.
- Direct access to server IMI IP addresses from the user's local workstation is preferable in the case of a backout.

  Note: If direct access to the IMI IP addresses is not available, then access to target server can be made using a tandem connection through the active primary SDS (that is, an SSH connection is made to the active primary SDS XMI first, then from the active primary SDS, an 2nd SSH connection can be made to the target server's IMI IP address).

3.1.1 ISO Image File

Obtain a copy of the target release ISO image file. This file is necessary to perform the upgrade. The SDS ISO image filename is in the following format:

Example: SDS-8.2.0.0.0_82.4.0-x86_64.iso

Note: Actual number values vary between releases.

Before executing this upgrade procedure, it is assumed the SDS ISO image file has already been delivered to the customer's system. The delivery of the ISO image requires the file be placed on the disk of a workstation with GUI access to the SDS XMI VIP. If the user performing the upgrade is at a remote location, it is assumed the ISO file is has already been transferred to the active primary SDS server before starting the upgrade procedure.

3.1.2 Logins, Passwords, and Site Information

Obtain all the information requested in the following table. This ensures the necessary administration information is available before an upgrade. Consider the confidential nature of the information recorded in this table. While all of the information in the table is required to complete the upgrade, there may be security policies in place that require secure disposal once the upgrade has been completed.

Table 3. Logins, Passwords, and Site Information

NE Type	NE Name
Primary SDS site	
DR SDS site	
SOAM 1 site	
SOAM 2 site	
SOAM 3 site	
SOAM 4 site	

Software	Value
Source release level	
Target release level	
Target release ISO filename	

Access Information	Value
Primary site XMI VIP (GUI)	
DR site XMI VIP	
SDS GUI admin username and password	
SDS root user password	
SDS admusr user password	
SDS platcfg user password	
Blade's iLO admin username and password	
PMAC GUI admin username and password*	

Access Information	Value
PMAC user root password*	
PMAC user admusr password*	
PMAC user PMACftpusr password*	
Onboard administrator GUI admin username and password	

* Not applicable for cloud deployments

3.2 Upgrade Maintenance Windows

WARNING It is recommended that SOAM NE sites containing mated Database Processors (DPs) be upgraded in separate maintenance windows, if possible.

Table 4. Upgrade Maintenance Windows

Maintenance Window 1 Date: _____	1. Record the names of the primary SDS NE site, DR SDS NE site, and server's hostnames to be upgraded during Maintenance Window 1 in the space provided. 2. Mark the associated checkbox as each server upgrade is completed. Primary SDS NE site name: _____ ☐ Primary SDS active server: _____ ☐ Primary SDS standby server: _____ ☐ Primary SDS query server: _____ DR SDS NE site name: _____ ☐ DR SDS active server: _____ ☐ DR SDS standby server: _____ ☐ DR SDS query server: _____
Maintenance Window 2 Date: _____	1. Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. 2. Mark the associated checkbox as each server upgrade is completed. SOAM NE site name: _____ ☐ Active SOAM Server: _____ ☐ Standby SOAM Server: _____ ☐ DP 1 Server: _____ ☐ DP 6 Server: _____ ☐ DP 2 Server: _____ ☐ DP 7 Server: _____ ☐ DP 3 Server: _____ ☐ DP 8 Server: _____ ☐ DP 4 Server: _____ ☐ DP 9 Server: _____ ☐ DP 5 Server: _____ ☐ DP 10 Server: _____

Maintenance Window 2 Date: _____	1. Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. 2. Mark the associated checkbox as each server upgrade is completed. SOAM NE site name: _____ ☐ Active SOAM Server: _____ ☐ Standby SOAM Server: _____ ☐ DP 1 Server: _____ ☐ DP 6 Server: _____ ☐ DP 2 Server: _____ ☐ DP 7 Server: _____ ☐ DP 3 Server: _____ ☐ DP 8 Server: _____ ☐ DP 4 Server: _____ ☐ DP 9 Server: _____ ☐ DP 5 Server: _____ ☐ DP 10 Server: _____
Maintenance Window 2 Date: _____	1. Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. 2. Mark the associated checkbox as each server upgrade is completed. SOAM NE site name: _____ ☐ Active SOAM Server: _____ ☐ Standby SOAM Server: _____ ☐ DP 1 Server: _____ ☐ DP 6 Server: _____ ☐ DP 2 Server: _____ ☐ DP 7 Server: _____ ☐ DP 3 Server: _____ ☐ DP 8 Server: _____ ☐ DP 4 Server: _____ ☐ DP 9 Server: _____ ☐ DP 5 Server: _____ ☐ DP 10 Server: _____
Maintenance Window 2 Date: _____	1. Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. 2. Mark the associated checkbox as each server upgrade is completed. SOAM NE site name: _____ ☐ Active SOAM Server: _____ ☐ Standby SOAM Server: _____ ☐ DP 1 Server: _____ ☐ DP 6 Server: _____ ☐ DP 2 Server: _____ ☐ DP 7 Server: _____ ☐ DP 3 Server: _____ ☐ DP 8 Server: _____ ☐ DP 4 Server: _____ ☐ DP 9 Server: _____ ☐ DP 5 Server: _____ ☐ DP 10 Server: _____

Note: Make copies of this sheet as needed for more additional SOAM NE sites.

3.3 Upgrade Preparation Overview

The pre-upgrade procedures shown in the following table should be executed before the upgrade maintenance window and may be executed outside a maintenance window if desired.

CAUTION

If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes.

WARNING

In 8.2, Ext ID/MTC-HSS features are introduced in SDS.

Provisioning these features is not allowed until all the servers are upgraded and the upgrade is accepted.

Table 5. Upgrade Preparation Procedures

Procedure Number	Procedure Title	Elapsed Time (Hrs:Min)	
		This Step	Cumulative
Procedure 1	Required Materials Check	00:15	00:15
Procedure 2	ISO Administration	*	*
Procedure 4	Full Database Backup (PROV and COMCOL Env for All Servers	01:00	01:15

*__Note__: ISO transfers to the target systems cannot be estimated since times vary significantly depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed before the scheduled maintenance window. The user should schedule the required maintenance windows accordingly.

3.4 Primary SDS Site/DR SDS Site Upgrade Execution Overview

The procedures shown in the following table are executed inside a maintenance window.

WARNING

The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 6.

Note: During the upgrade of servers, there are steps to check the replication status before going to the next server backout. Follow those steps to execute; otherwise, data loss is possible.

Note: During upgrade some alarms/events may be raised that can be ignored. Alarms are mentioned in step 4 of Appendix B.

Table 6. Primary SDS/DR SDS Upgrade Procedures Strategy

Procedure Number	Procedure Title	Elapsed Time (Hrs:Min)	
		This Step	Cumulative
Procedure 5	Upgrade the Primary SDS NOAM	01:00	02:15
Procedure 6	Upgrade DR SDS NOAM	01:00	03:15

3.5 SOAM Upgrade Execution Overview

The procedures shown in the following table should be executed inside a separate maintenance window.

Table 7. SOAM Upgrade Procedures

Procedure Number	Procedure Title	Elapsed Time (Hrs:Min)	
		This Step	Cumulative
Procedure 9	Upgrade SOAM	01:30	01:30

3.6 Post Upgrade Execution Overview

These procedures are performed only after all sites on network have been upgraded.

Table 8. Post Upgrade Procedures

Procedure Number	Procedure Title	Elapsed Time (Hrs:Min)	
		This Step	Cumulative
Procedure 10	Accept the Upgrade	*	*

3.7 Recovery Procedures Overview

These procedures are customized to the specific situation encountered and therefore do not have well-established timeframes.

WARNING

The order of the backout for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 9.

Note: During backout of servers, there are steps to check the replication status before going to the next server backout. Follow those steps to execute; otherwise, data loss is possible.

Note: During the backout some alarms/events may be raised that can be ignored. Alarms are mentioned in step 4 of Appendix B.

Table 9. Backout Procedures

Procedure Number	Procedure Title	Elapsed Time (Hrs:Min)	
		This Step	Cumulative
Procedure 11	Back Out the SOAM	*	*
Procedure 12	Back Out the DR SDS NOAM	*	*
Procedure 13	Back Out the Primary SDS NOAM	*	*

4. SDS Upgrade Matrix

Upgrading SDS in the customer network is a task that requires multiple procedures of varying types.

The matrix shown below provides a guide to the user as to which procedures are to be performed on which site types.

As always, it is recommended to contact MOS for assistance if having trouble with the interpretation or execution of any of the procedures listed.

STOP

Primary SDS NOAM and DR SDS NOAM sites must be upgraded in the same maintenance window.

Replication between Primary and DR SDS NOAM sites will be down till DR SDS NOAM is upgraded completely.

Table 10. SDS Upgrade Matrix

Network Element Type	Procedures						
	1	2	3	4*	5†	7	8
Primary NOAM NE DR NOAM NE (SDS/Query Server)	Yes	Yes	Yes	Yes	Yes	No	Yes
SOAM NE (SOAM/DP)	Yes	No	No	No	No	Yes	Yes

* Appendix A Health Check Procedures is executed before starting this procedure.

† Appendix A Health Check Procedures is executed after completing this procedure.

Table 11. SDS Upgrade – List of Procedures

Procedure Number	Title	Page
Procedure 1	Required Materials Check	20
Procedure 2	ISO Administration	21
Procedure 3	Back Up TKLCConfigData File	26
Procedure 4	Full Database Backup (PROV and COMCOL Env for All Servers	27
Procedure 5	Upgrade Primary SDS NOAM	42
Procedure 6	Upgrade DR SDS NOAM	54
Procedure 7	Upgrade SOAM with ASU	58
Procedure 9	Upgrade SOAM manually	67
Procedure 32	Workaround for SNMP Configuration	177
Procedure 10	Accept the Upgrade	69

5. Upgrade Preparation

This section provides detailed procedures to prepare a system for upgrade execution. These procedures may be executed outside of a maintenance window.

5.1 Requirements Check

This procedure verifies all required materials needed to perform an upgrade have been collected and recorded.

Procedure 1. Required Materials Check

1. ☐	Verify all upgrade requirements have been met.	Requirements are listed in section 3.1 Upgrade Requirements. Verify all upgrade requirements have been met.
2. ☐	Verify all administration data needed during upgrade.	Verify all information in section 3.1.2 Logins, Passwords, and Site Information has been entered and is accurate.

5.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the SDS 8.x release to understand the functional differences (if any) and possible impacts to the upgrade. When upgrading SDS to the target release, the following alarms may be reported on the GUI during the period when the primary SDS site NE is at the new software level and the DR SDS site NE is at the old software level:

- 31124: A DB replication audit command detected errors
- 31105: The DB merge process (inetmerge) is impaired by a s/w fault
- 31232: High availability server has not received a message on specified path within the configured interval
- 31283: Lost Communication with server (cmha)
- 31109: Topology Config Error (cmha)

These alarms, if present, exist for the active and standby DR SDS site servers. They should clear automatically within 5 minutes, and cease to be raised once the DR provisioning site NE is upgraded to the same software level as the primary SDS site. To avoid seeing these alarms altogether, the upgrade

of the primary SDS Site and DR SDS site NEs should be performed within the same maintenance window.

5.3 Perform Firmware Verification (Upgrade Preparation)

This section is not applicable to a software-centric upgrade.

This procedure is part of software upgrade preparation and is necessary to determine if a firmware update is required. If [4] has been provided with the upgrade material, follow the provided instructions to verify the firmware on SDS rack mount servers and DP blades. Execute firmware upgrade procedures if required by [4]:

☐ Execute the **Upgrade DL360 or DL380 Server Firmware** section for SDS rack mount servers.

☐ Execute the **Upgrade Blade Server Firmware** section for SDS DP blades.

5.4 Perform Health Check (Upgrade Preparation)

This procedure is part of software upgrade preparation and is used to determine the health and status of the SDS network and servers. This procedure may be executed multiple times, but must also be executed at least once 24-36 hours before starting a maintenance window.

☐ Execute SDS health check procedures as specified in Appendix A.

5.5 ISO Administration

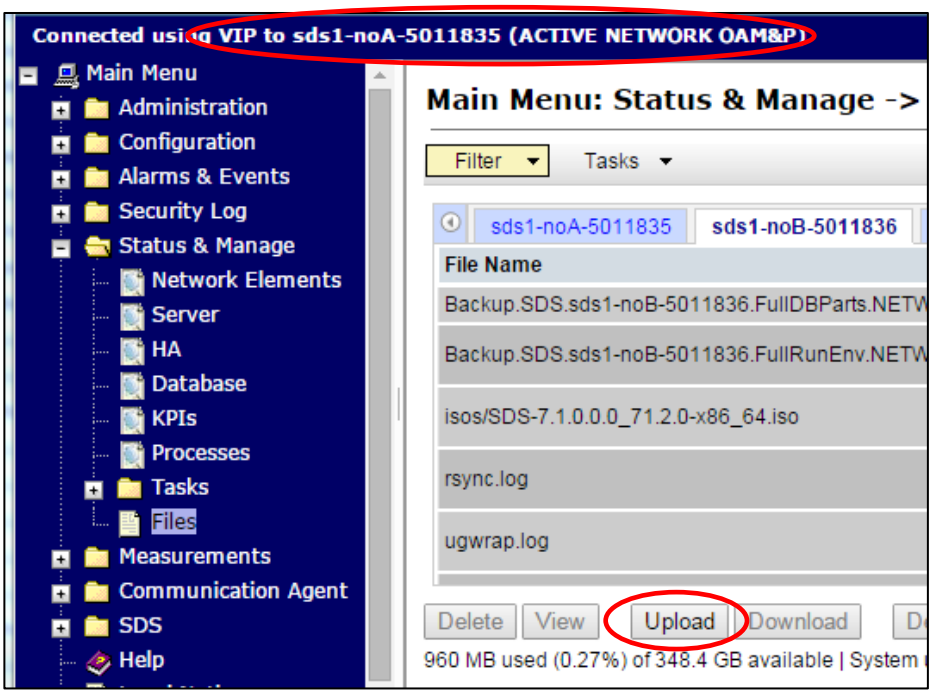
ISO transfers to the target servers may require a significant amount of time depending on the number of systems and the speed of the network. Therefore, it is highly reccommended that the ISO transfers to the target servers be completed before the first scheduled maintenance window.

Note: Appendix H Add the SDS ISO to the PMAC Software Repository may be executed at anytime after Procedure 2 ISO Administration has been completed.

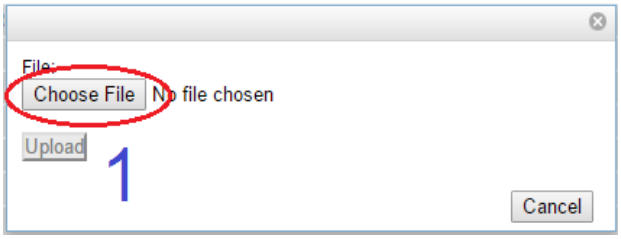
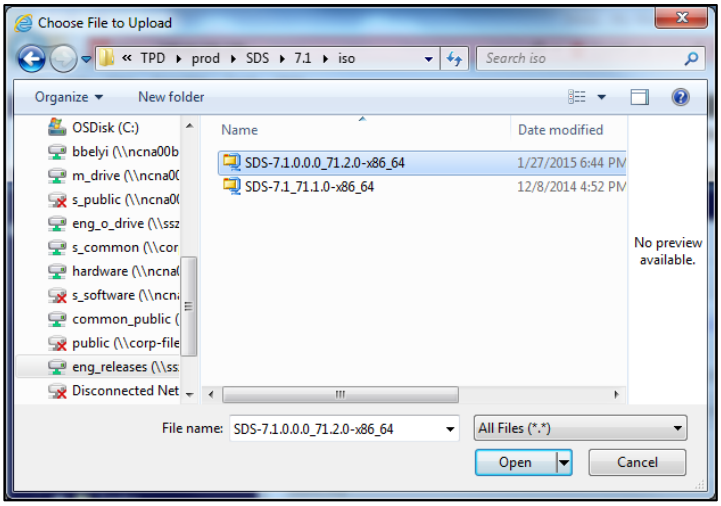
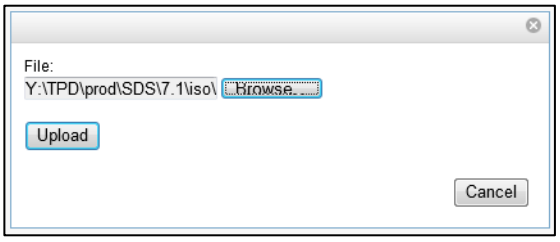
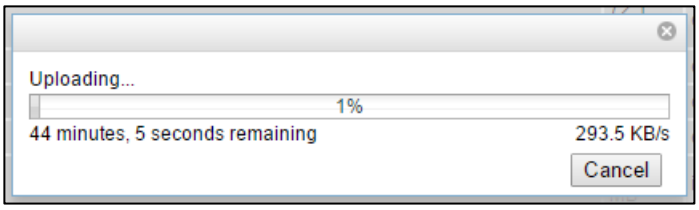
Procedure 2. ISO Administration

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

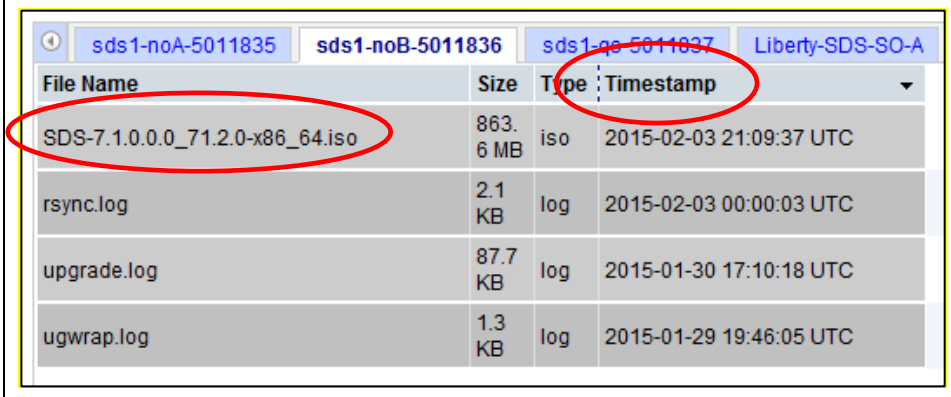
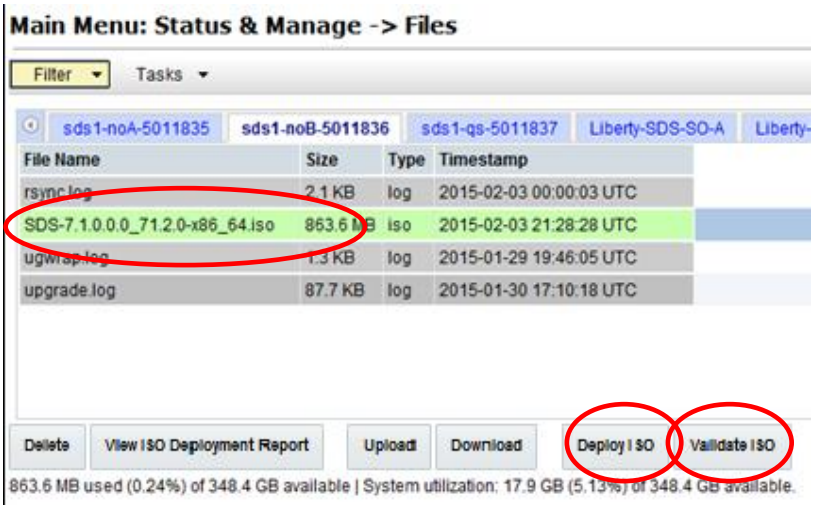
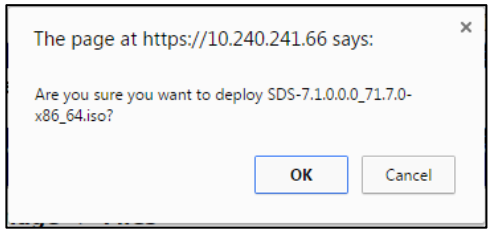
Procedure 2. ISO Administration

2. ☐	**Primary SDS NOAM VIP (GUI)**: Connect to the SDS server	1. Navigate to **Status & Manage > Files**. 2. Select the hostname of the **active** primary SDS server from the list of tabs. 3. Click **Upload**.  ***Note***: The active primary SDS server displays in the GUI banner as connected to the VIP with a state of **ACTIVE NETWORK OAM&P**.

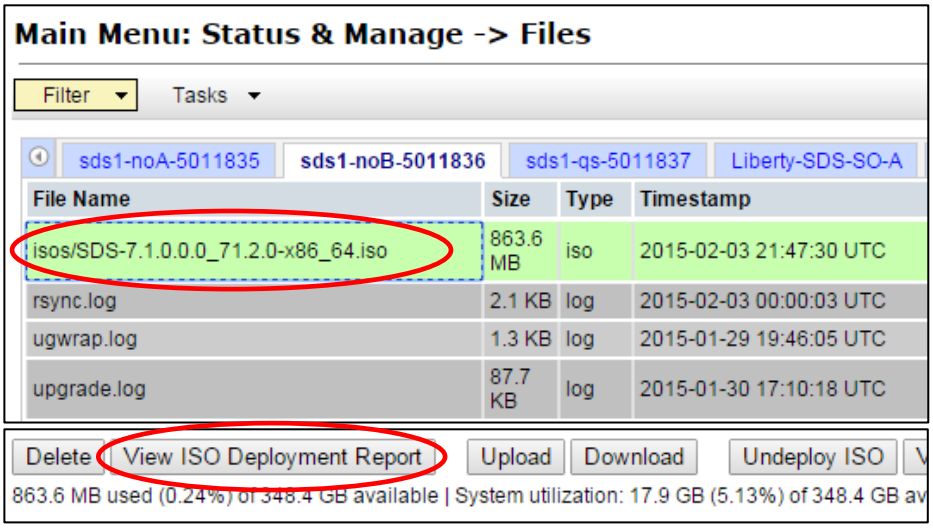
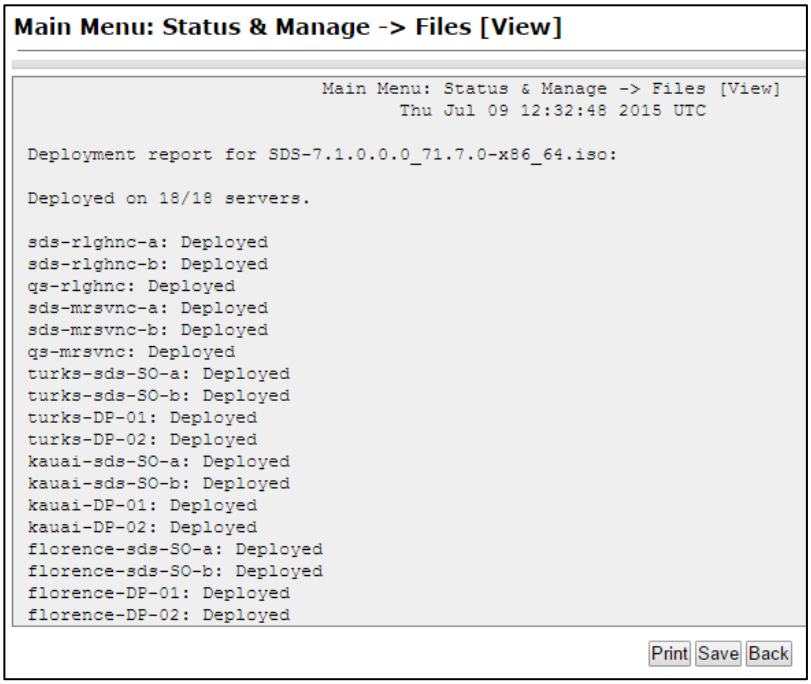
Procedure 2. ISO Administration

3. ☐	**Primary SDS NOAM VIP**: Upload the ISO file	1. Click **Choose File**.  2. Locate the ISO file for the target release and click **Open**.  3. Click **Upload**.  4. Monitor the upload until the file transfer completes.  ***Note***: If transfering the ISO file to the server manually (using secure copy (scp)), the iso must be placed in the **/var/TKLC/db/filemgmt/** directory with **664** permissions and **awadmin:awadm** ownership.

Procedure 2. ISO Administration

4. ☐	**Primary SDS NOAM VIP**	Click the **Timestamp** heading twice to sort the column by most recent files.  The ISO file displays at the top of the list.
5. ☐	**Primary SDS NOAM VIP**: Deploy the ISO file to all SDS server in the network	1. Select the ISO file. 2. Click **Validate ISO**. 3. Wait for validatin to pass. 4. Click **Deploy ISO**.  5. Click **OK**. 

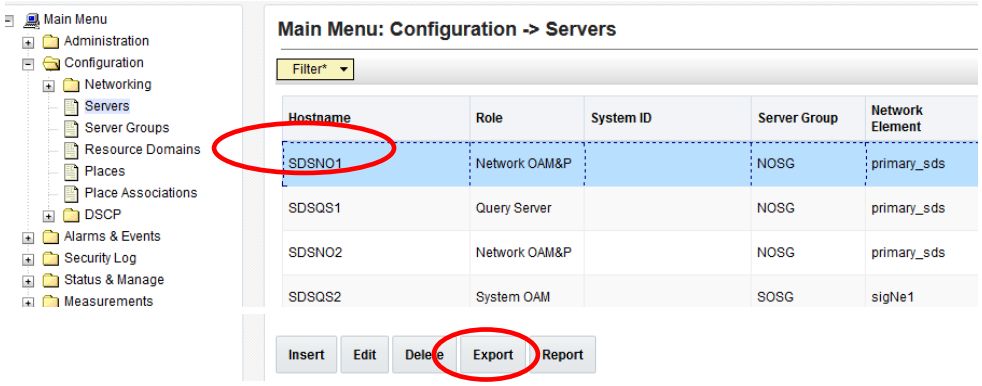
Procedure 2. ISO Administration

6. ☐	**Primary SDS NOAM VIP**: Monitor the ISO deployment status	1. Select the ISO file. 2. Click **View ISO Deployment Report**. 
7. ☐	**Primary SDS NOAM VIP**: View the report	The ISO Deployment Report shows the status of deployment to all servers in the topology. Refresh the report by clicking **Back** and repeating step 6 of this procedure until the **ISO** has been **Deployed** to all servers.  ***Note***: This completes the ISO administration procedure for source release 7.x and later, skip the remaining steps.
8. ☐		Perform Appendix L ISO Link Correction if upgrading from release 7.1, 7.2, 7.3, or 7.4 to SDS 8.2.

5.6 Back Up TKLCConfigData File

This section backs up the TKLCConfigData file on all the servers. This helps to restore networking and server-related information in some cases. For example, for disaster recovery if a server is lost during an upgrade.

Procedure 3. TKLCConfigData Backup

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP GUI**: Export servers	1. Navigate to **Configuration > Servers**. 2. Select each server in the topology and click **Export**.  ***Note***: The active primary SDS server displays in the GUI banner as it is connected to the VIP with a state **Active Network OAM&P**.

3. ☐	**Primary SDS NOAM Server**: Back up TKLCConfig data and access the CLI of the primary SDS NOAM	1. Access the primary SDS NOAM server command line using ssh or a console.
		`ssh admusr@<NOAM_VIP>`
		2. Transfer the **TKLCConfigData** files for all servers in the **/var/TKLC/db/filemgmt** directory to a remote location.
		`$ cd /var/TKLC/db/filemgmt`
		`$ scp TKLCConfigData.<Sever Hostname>.sh <username>@<remote-server>:<directory>`
		Example:
		`scp TKLCConfigData.SDSDRNO1.sh <username>@<remote-server>:<directory>`
		Remember to back up the TKLCConfig data file for **all** servers.

5.7 Perform Health Check (Post ISO Administration)

This procedure is part of Software Upgrade Preparation and is used to determine the health and status of the entire SDS network and servers. This may be executed multiple times but must also be executed at least once within the period of 24-36 hours before the start of a maintenance window.

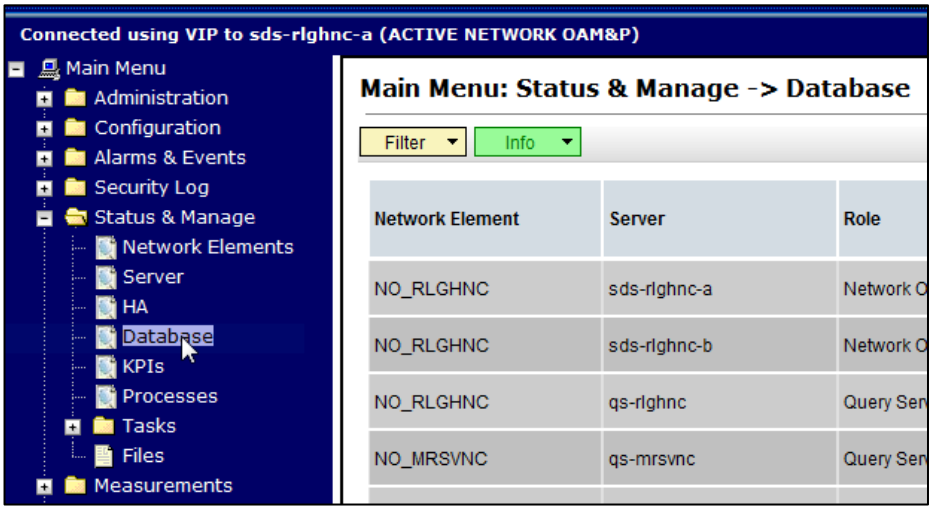
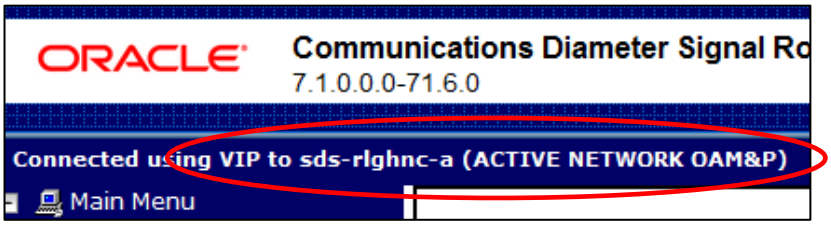
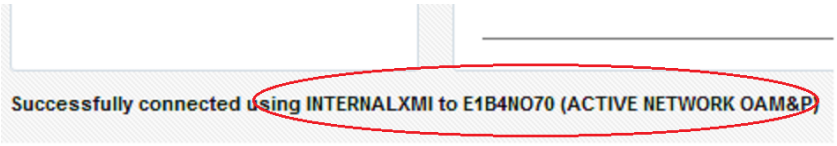
☐ Execute SDS Health Check procedures as specified in Appendix A.

5.8 Full Database Backup (PROV & COMCOL ENV for All Servers)

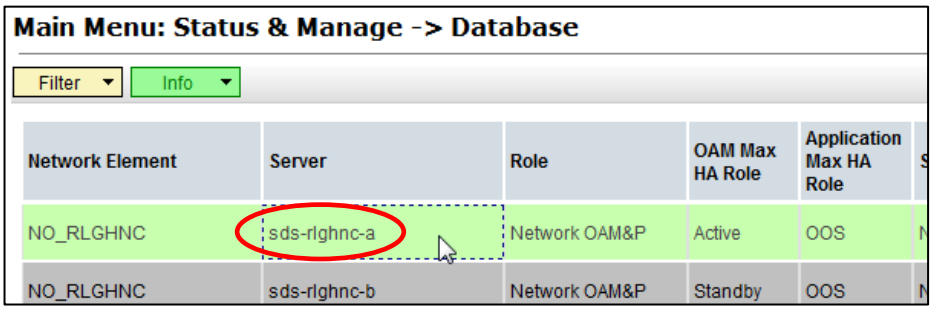
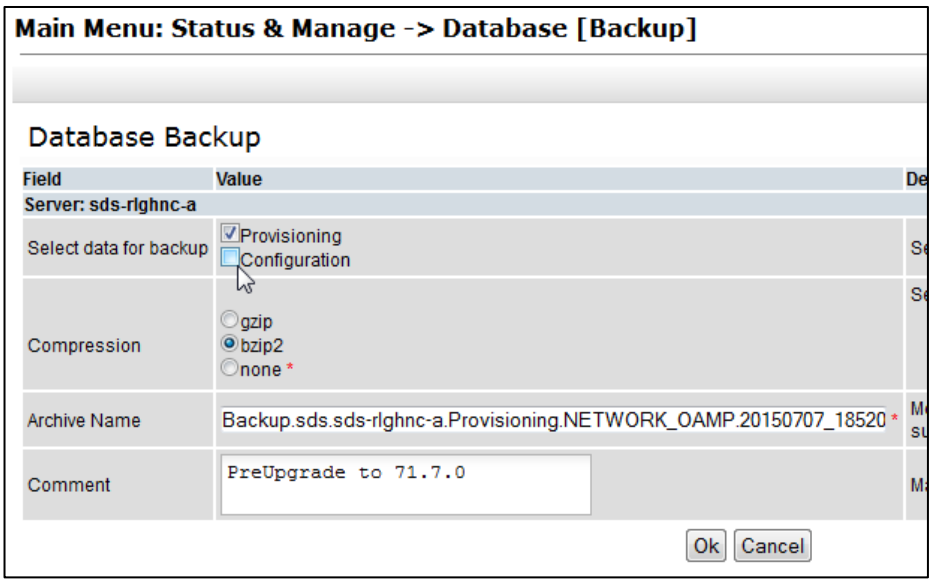
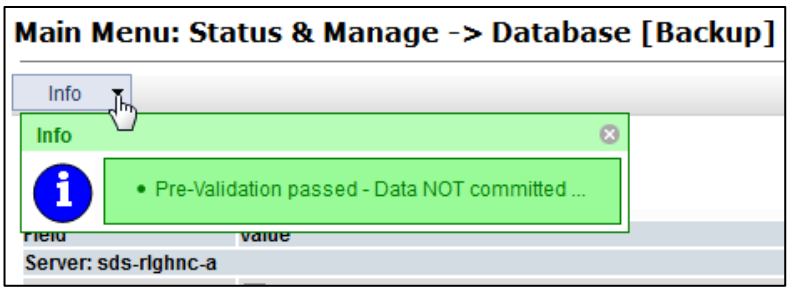
This procedure is part of software upgrade preparation and is used to conduct a full backup of the COMCOL run environment on every server, to be used in the event of a backout/rollback of the new software release.

Note: Do not perform this procedure until the ISO deployment is completed to all servers in the topology. Partial backout (that is, back out of one site) may fail in the event of incomplete ISO deployment/undeployment.

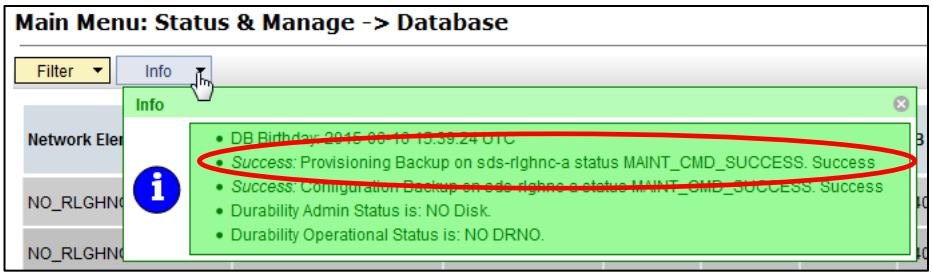
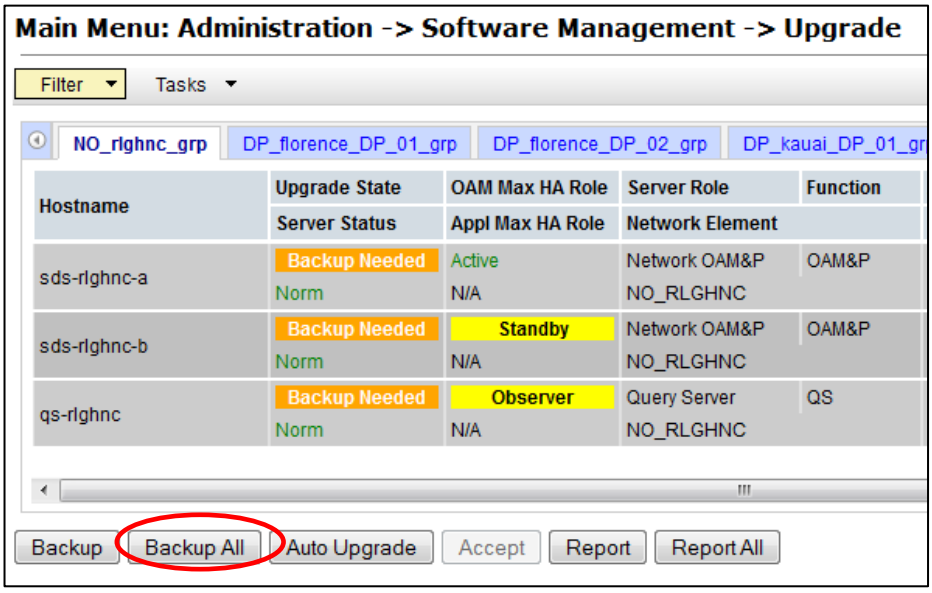
Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP (GUI)**: Verify the name of the primary active network OAM&P SDS server	1. Navigate to **Status & Manage > Database**.  2. Verify the hostname of the **active** primary OAM&P SDS server from the GUI banner.  ***Note***: If source release is 8.x, the banner is at the bottom of the screen. 

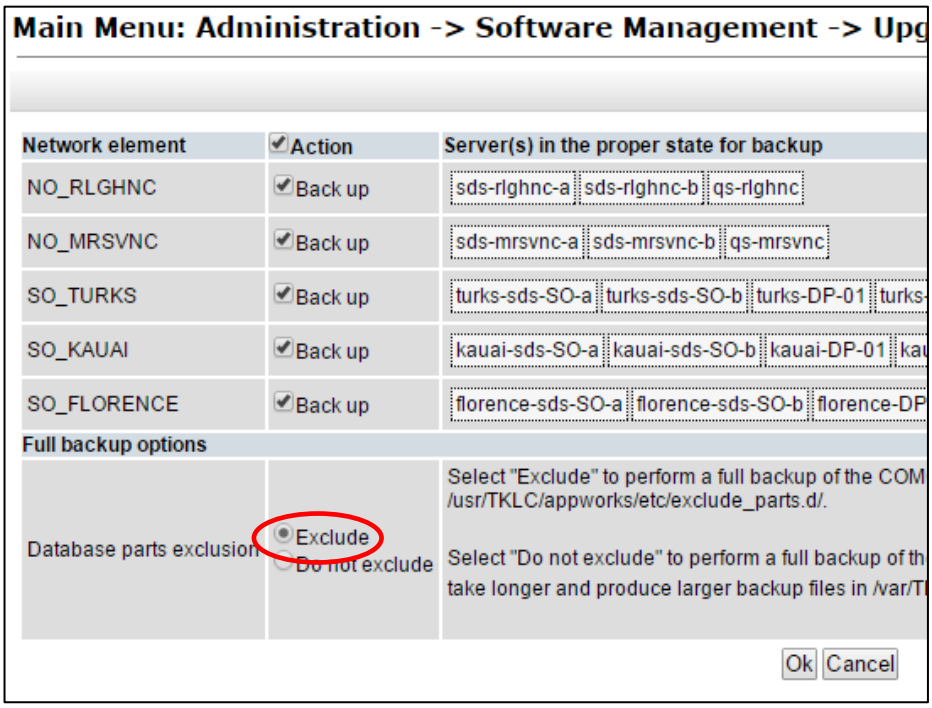
Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers

3. ☐	**Primary SDS NOAM VIP**: Back up the server	1. Select the SDS server.  2. Click **Backup**.
4. ☐	**Primary SDS NOAM VIP**: Back up the provisioning data	1. Unmark the **Configuration** checkbox. 2. Type a **Comment**.  ***Note***: The comment is a required field. Left click the mouse to make sure the cursor is outside the comment field. 3. Click **Info** to verify the changes have passed pre-validation.  4. Click **OK**.

Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers

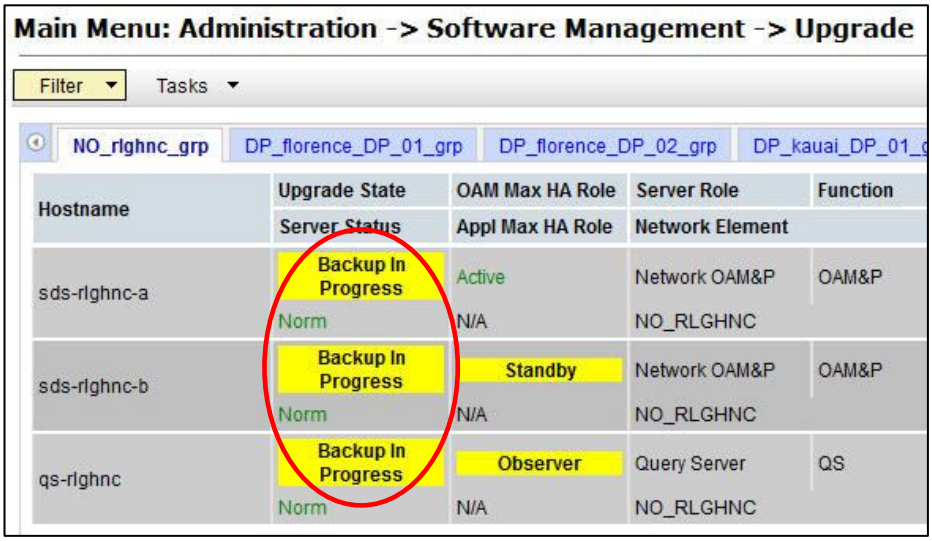
5. ☐	**Primary SDS NOAM VIP**: Verify status	1. Wait for the screen to refresh (about 1-2 minutes). 2. Click the **Info** tab to verify the **Provisioning Backup** shows a status of **MAINT_CMD_SUCCESS**.  If a status of **MAINT_IN_PROGRESS** is received, then **refresh** the Info message by navigating to **Status & Manage > Database** and clicking on the **Info** tab again. ***Note***: Depending on the size of the SDS provisioning database, the backup could take a couple of hours to complete. This completes the backup of the SDS provisioning database
6. ☐	**Primary SDS NOAM VIP**: Back up servers	1. Navigate to **Administration > Software Management > Upgrade**. 2. Click **Backup All**. 

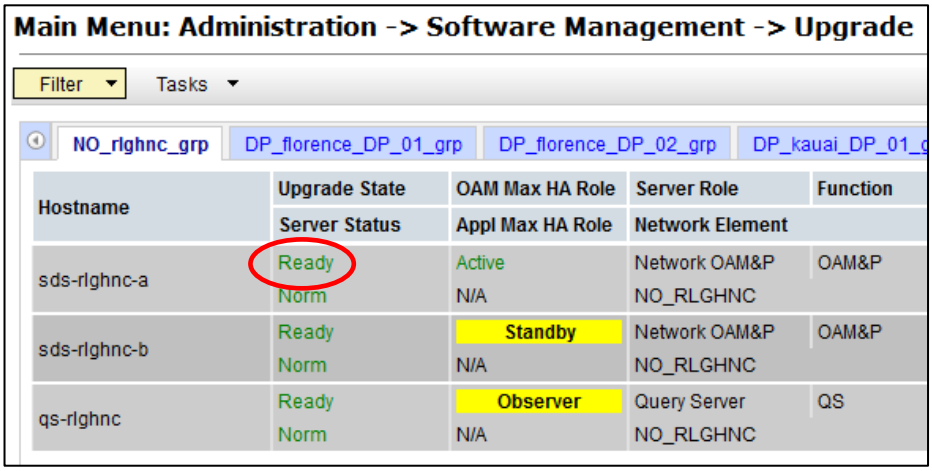
Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers

7. ☐	**Primary SDS NOAM VIP**: Back up servers	***Note***: All servers in an Upgrade state display on the screen. Servers in a **Forced Standby** or **OOS** state do not display. 1. Verify the **Exclude** option is selected. 2. Click **OK**. 

Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers

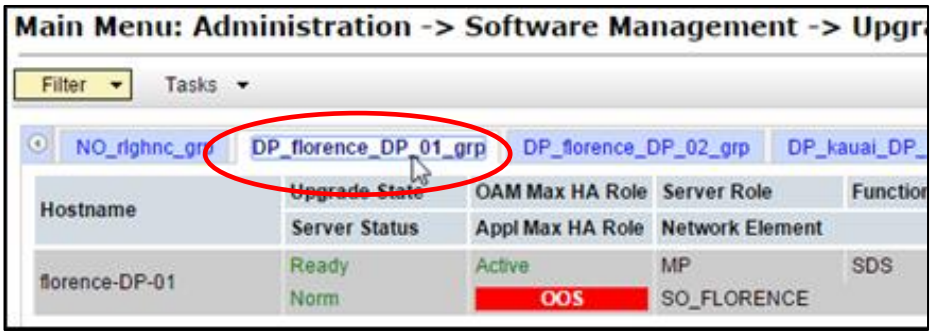
8. ☐	**Primary SDS NOAM VIP**: Monitor progress	1. Verify the **Upgrade State** of the servers goes from a **Backup in Progress** state to a **Ready** state.





Note: It can take up to 15 minutes for COMCOL backup to complete as the screen automatically refreshes.

2. Click on **each server tab** and monitor the backups until the server **Upgrade State** shows **Ready** for all servers on the tab.



Note: Starting with SDS 7.x, the **Appl Max HA Role** displays on this screen. This state is expected to be **OOS** for SDS DP servers.

6. Automated Site Upgrade

There are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature upgrades an entire site (SOAMs and DP servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade automatically prepares the server(s), performs the upgrade, and sequences to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity.

Automated Site Upgrade can be used to upgrade the SOAM and DP servers. However, Auto Site Upgrade cannot be used to upgrade PMAC or TVOE at a site.

With this feature, a site upgrade can be initiated on SO-A SG and all of its children (in this example, DP1 SG) using a minimum of GUI selections. The upgrade performs the following actions:

1. Upgrade SOA-1 and SOA-2
2. Upgrade the servers in DP1 SG
3. Immediately begin the upgrade of any other server groups, which are also children of SO-A SG (not shown). These upgrades begin in parallel with step 2.

Note: Auto Site Upgrade does not automatically initiate the upgrade of TSite 2 in parallel with TSite 1. However, the feature allows the user to initiate Auto Site Upgrade of multiple sites in parallel manually.

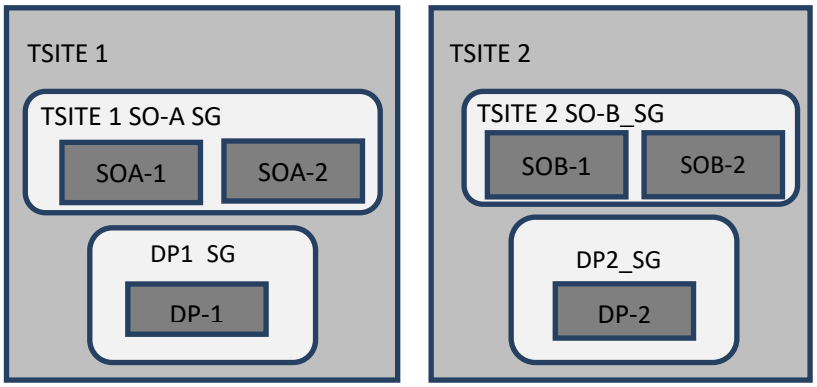


Figure 3. Upgrade Perspective of SDS Site Topology

6.1 Site Upgrade Execution

With Auto Site Upgrade, the upgrade is initiated from the **Administration > Software Management > Upgrade** screen. Upon initial entry to this screen, the user is presented with a tabbed display of the NOAM server group and SOAM sites (Figure 4). When the NOAM server group tab is selected (as shown in Figure 4), this screen is largely unchanged from the upgrade screen of previous releases. The NOAM server group servers are displayed with the usual assortment of buttons. On this screen, the **Auto Upgrade** button refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature becomes available once a SOAM server group tab is selected. The SOAM server group tabs correspond to the topological sites (TSites).

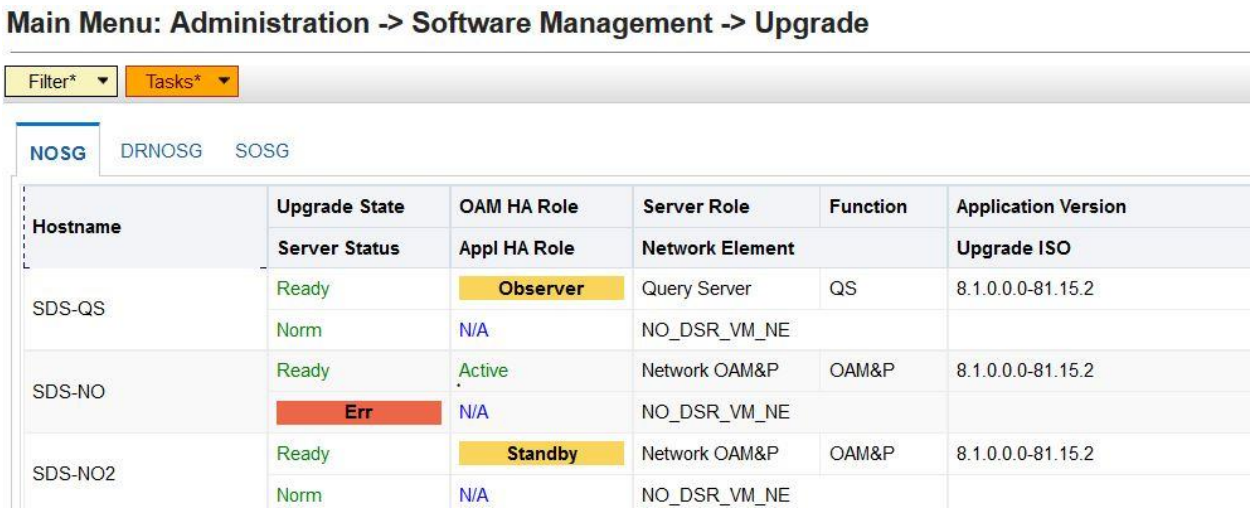


Figure 4. Site Upgrade — NOAM View

Upon selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen displays (Figure 5). Just below the row of NOAM and SOAM tabs is a row of links related to the selected SOAM site. The first link on the site summary screen displays the **Entire Site** view. In the entire site view, all of the server groups for the site are displayed in table form, with each server group populating one row. An upgrade summary of the server groups is provided in the table columns:

- The **Upgrade Method** column shows how the server group is upgraded. The upgrade method is derived from the server group function and the bulk availability option (see section 7.3 for additional details on bulk availability).
- The **Server Upgrade States** column groups the servers by state, indicating the number of servers in the server group that are in each state.
- The **Server Application Versions** column indicates the current application version, indicating the number of servers in the server group that are at each version.

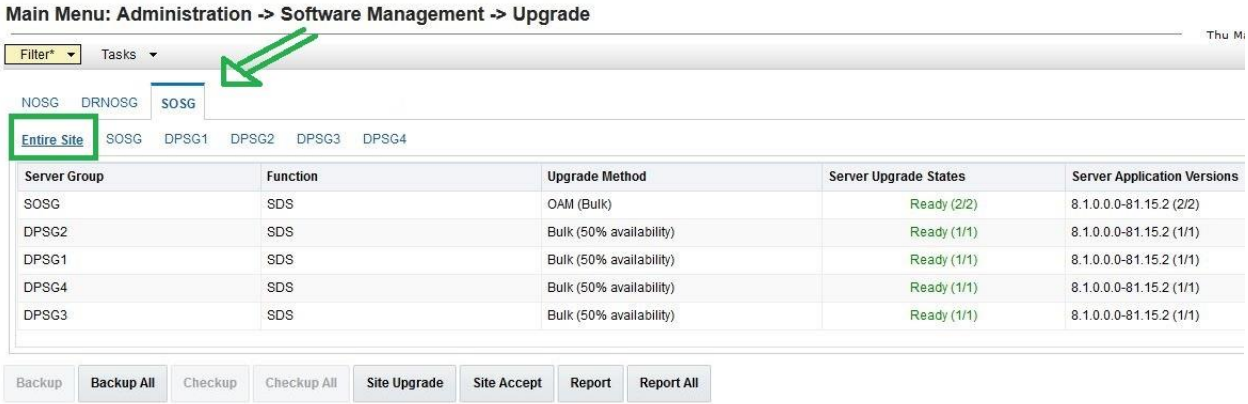


Figure 5. Site Upgrade — Entire Site View

For a server to be considered **Ready** for upgrade, the following conditions must hold true:

- Server has not been upgraded yet
- The FullDBParts and FullRunEnv backup files exist in the filemgmt area

A site is eligible for Auto Site Upgrade when at least one server in the site is upgrade-ready.

Click **Site Upgrade** from the **Entire Site** view to display the Upgrade Site Initiate screen (Figure 6). The Site Initiate screen shows the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 6, Cycle 1 upgrades the spare and standby SOAMs in parallel.

Note: This scenario assumes default settings for the site upgrade options. These options are described in section 7.3.

The specific servers to be upgraded in each cycle are identified in the **Servers** column on the Site Initiate screen. Cycle 1 is an atomic operation, meaning Cycle 2 cannot begin until Cycle 1 is complete. Once the standby SOAM are in the **Accept or Reject** state, the upgrade sequences to Cycle 2 to upgrade the active SOAM. Cycle 2 is also atomic - Cycle 3 does not begin until Cycle 2 is complete.

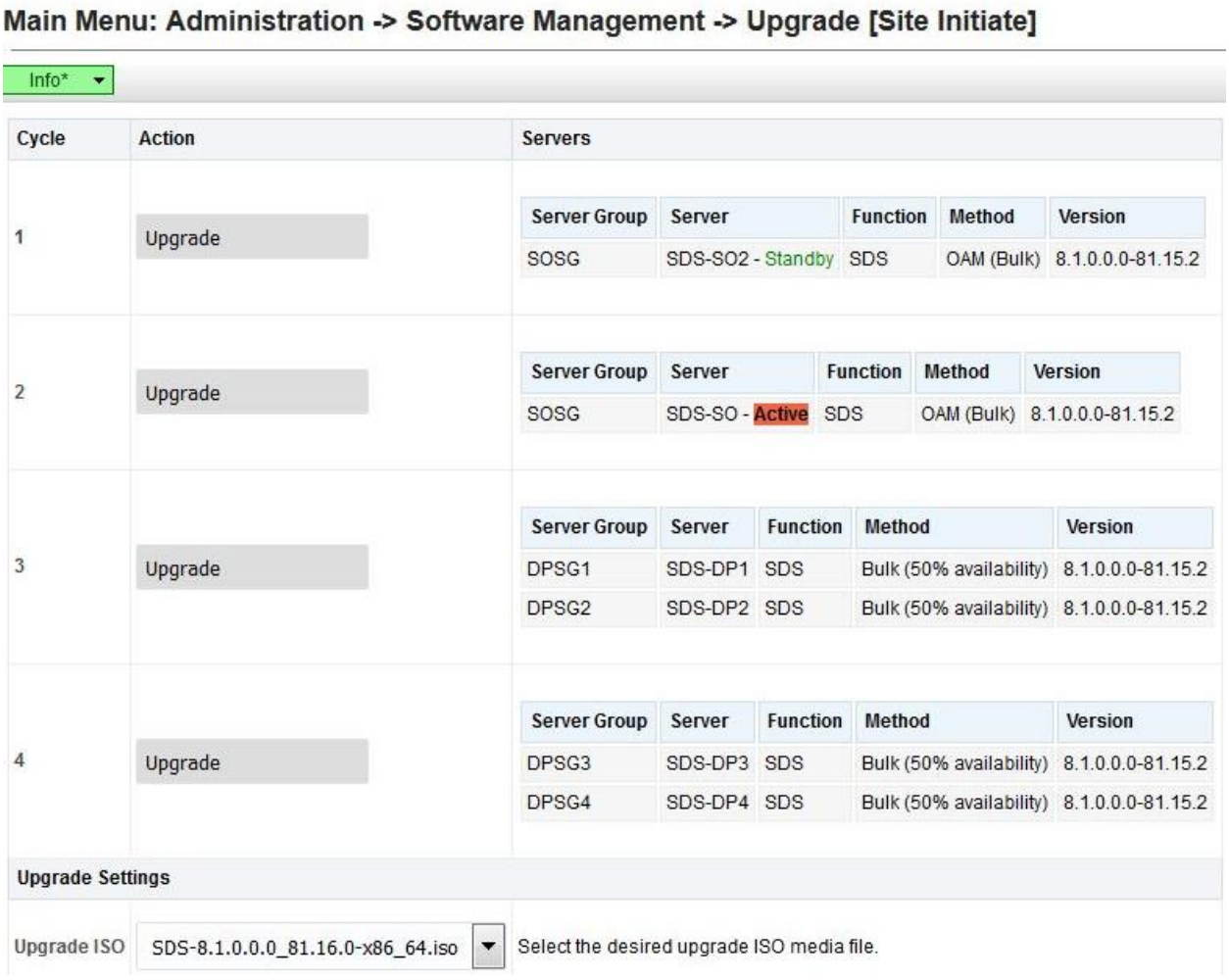


Figure 6. Site Upgrade — Site Initiate Screen

Cycles 3 through 4 upgrade all of the C-level servers for the site. These cycles are **not** atomic.

In Figure 6, Cycle 3 consists of SDS-DP1 and SDS-DP2 and Cycle 4 consists of SDS-DP3 and SDS-DP4.

The site upgrade is complete when every server in the site is in the **Accept or Reject** state.

In selecting the servers that will be included with each upgrade cycle, particularly the C-level, consideration is given to the server group function, the upgrade availability option, and the HA designation.

Note: The minimum availability option is a central component of the server selections for site upgrade. The effect of this option on server availability is described in detail in section 6.2.

To initiate the site upgrade, a target ISO is selected from the ISO picklist in the **Upgrade Settings** section of the Site Initiate screen (Figure 6). Once the **OK** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 7). With the **Entire Site** link selected, a summary of the upgrade status for the selected site displays. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. This view can be used to monitor the upgrade status of the overall site. More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.

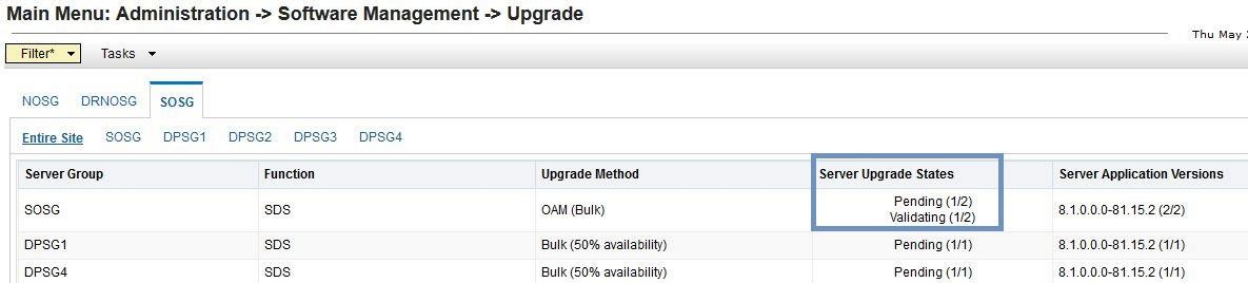


Figure 7. Site Upgrade Monitoring

When a server group link is selected on the Upgrade Administration screen, the table rows are populated with the upgrade details of the individual servers within that server group (Figure 8).

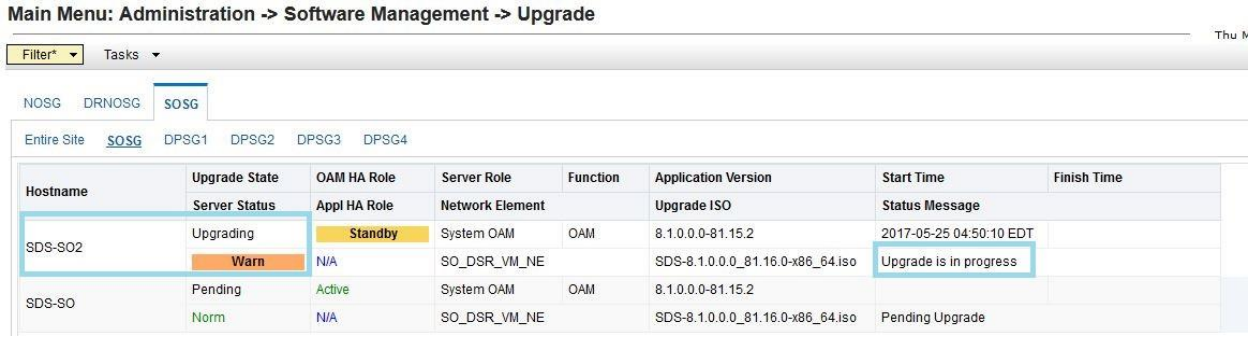


Figure 8. Server Group Upgrade Monitoring

Upon completion of a successful upgrade, every server in the site is in the **Accept or Reject** state (Figure 9).

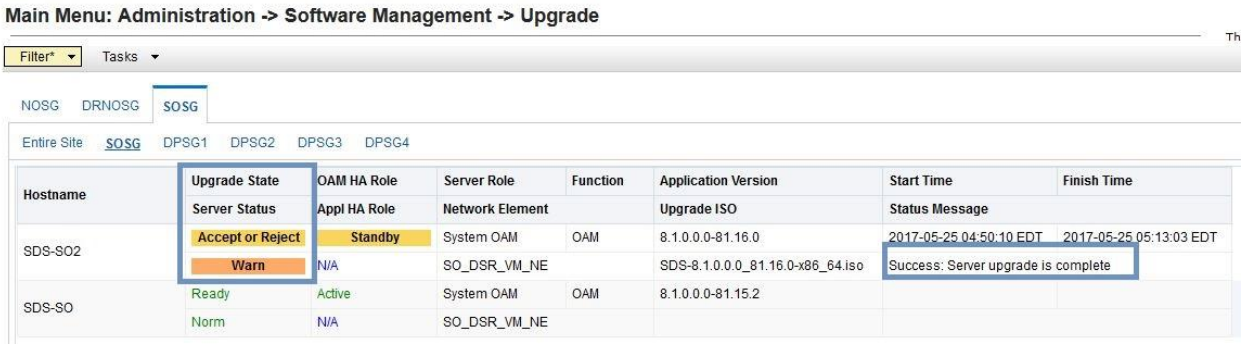


Figure 9. Server Group Upgrade Monitoring

See section 7.4 for a description of cancelling and restarting the Auto Site Upgrade.

6.2 Minimum Server Availability

The concept of Minimum Server Availability plays a key role during an upgrade using Automated Site Upgrade. The goal of server availability is to ensure that at least a specified percentage of servers (of any given type) remain in service to process traffic and handle administrative functions while other servers are upgrading.

For example, if the specified minimum availability is 50% and there are eight servers of type **X**, then four remain in service while four upgrade. However, if there are nine server of type **X**, then the minimum availability requires that five remain in service while four upgrade. The minimum availability calculation automatically rounds up in the event of a non-zero fractional remainder.

To meet the needs of a wide-ranging customer base, the minimum availability percentage is a user-configurable option. The option allows for settings of 50%, 66%, and 75% minimum availability. There is also a setting of 0% for lab upgrade support. This option is described in detail in section 6.3.

6.3 Site Upgrade Options

To minimize user interactions, the automated site upgrade makes use of a pair of pre-set options to control certain aspects of the sequence. These options control how many servers remain in service while others are upgrading and are located on the **Administration > General Options** screen. The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

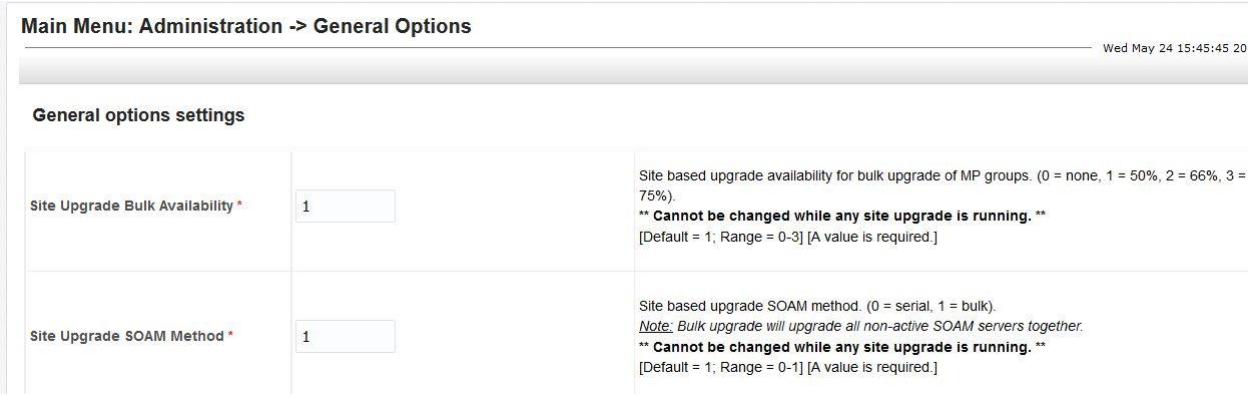


Figure 10. Auto Site Upgrade General Options

The first option that affects the upgrade sequence is the **Site Upgrade Bulk Availability** setting. This setting determines the number of C-level servers that remain in service during the upgrade. The default setting of **1** equates to 50% availability, meaning a minimum of one-half of the servers stay in service during the upgrade. The default setting is the most aggressive setting for upgrading the site, requiring the minimum number of cycles, thus the least amount of time. The settings of 66% and 75% increase the number of servers that remain in service during the upgrade. Note that increasing the availability percentage may increase the overall length of the upgrade.

A setting of **0** for the bulk availability option allows all of the DPs to be upgraded at once. This setting is not recommended for live production systems.

The Site Upgrade General Options cannot be changed while a site upgrade is in progress. Attempting to change either option while a site upgrade is in progress results in:

[Error Code xxx] - Option cannot be changed because one or more automated site upgrades are in progress

The second option that affects the upgrade sequence is the **Site Upgrade SOAM Method**. This option determines the sequence in which the SOAMs are upgraded. The default value of **1** considers the OAM

HA role of the SOAMs to determine the upgrade order. In this mode, all non-active SOAM servers are upgraded first (in parallel), followed by the active SOAM.

Changing the Site Upgrade SOAM Method setting to **0** causes the standby SOAM and the spare SOAM(s) to be upgraded serially. With this mode, the SOAM upgrade could take as many as four cycles to complete (that is, Spare - Spare - Standby - Active). As for SDS, there are no spare SOAMs, so this setting has no impact on the SOAM upgrade order.

Regardless of the SOAM upgrade method, the active SOAM are always upgraded after the standby SOAM.

6.4 Cancel and Restart Auto Site Upgrade

When an Auto Site Upgrade is initiated, several tasks are created to manage the upgrade of the individual server groups as well as the servers within the server groups. These tasks can be monitored and managed using the **Status & Manage > Tasks > Active Tasks** screen.

The main site upgrade controller task is identified by the naming convention **<site_name> Site Upgrade**. In Figure 7, the main task is task ID 1.

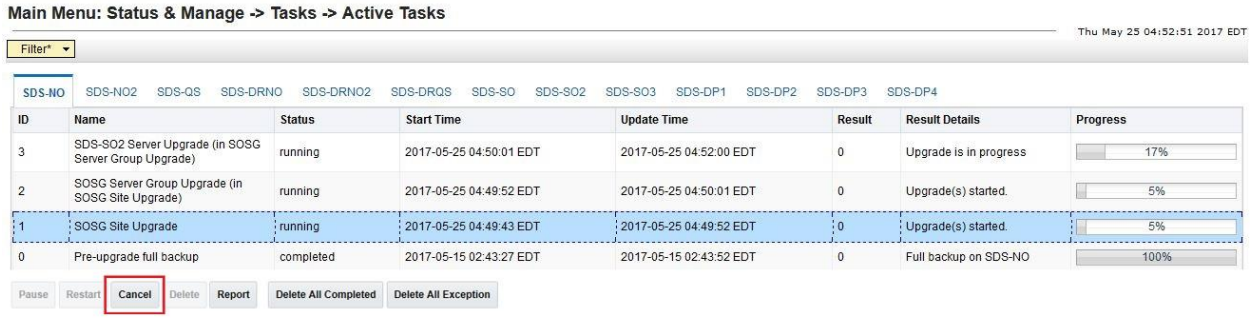


Figure 11. Site Upgrade Active Tasks

To cancel the site upgrade, select the site upgrade task and click **Cancel**. A screen asks you to confirm the cancel operation. The status changes from **running** to **completed**. The **Results Details** column updates to display **Site upgrade task cancelled by user**. All server group upgrade tasks, which are under the control of the main site upgrade task, immediately transition to **completed** state. However the site upgrade cancellation has no effect on the individual server upgrade tasks that are in progress. These tasks continue to completion. Figure 12 shows the Active Task screen after a site upgrade has been cancelled.

Once the site upgrade task is cancelled, it cannot be restarted. However, a new site upgrade can be started using the Upgrade Administration screen.

After user has cancelled the task. The servers, which were in progress when the upgrade was cancelled, continued to upgrade to the target release.

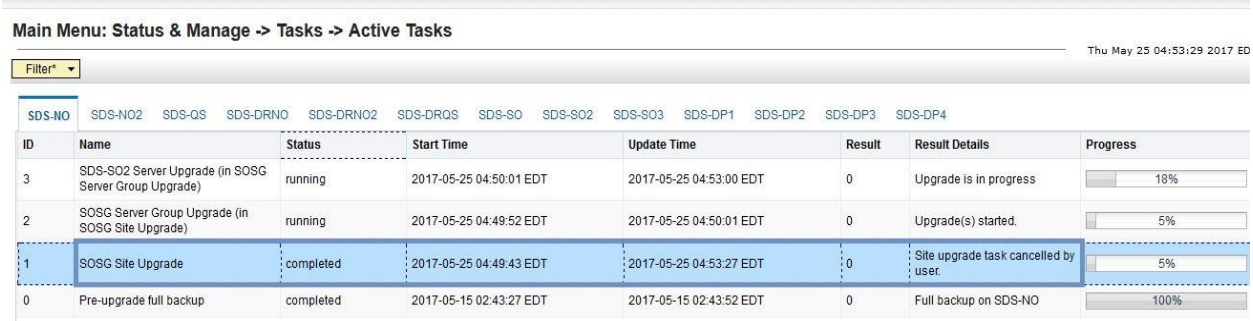


Figure 12. User Cancelled the Site Upgrade Tasks

Figure 12 represents a site upgrade that was cancelled before the site was completely upgraded. The servers that were in progress when the upgrade was cancelled continued to upgrade to the target release. These servers are now in the **Accept or Reject** state. The servers that were pending when the upgrade was cancelled are now in the **Ready** state, ready to be upgraded.

To restart the upgrade, verify the **Entire Site** link is selected and click **Site Upgrade**. The Upgrade Site Initiate screen displays.

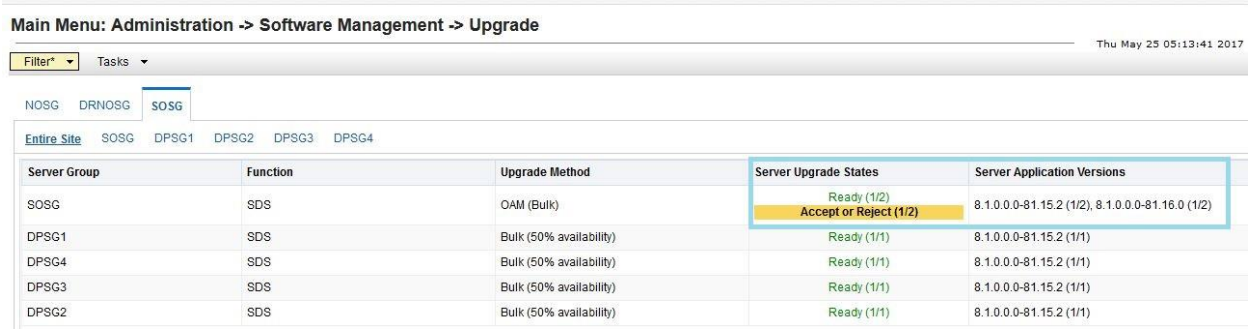


Figure 13. Partially Upgraded Site

On the Upgrade Site Initiate screen, the servers that have not yet been upgraded are grouped into the number of cycles that are required to complete the site upgrade. As an example, Figure 13 shows the upgrade that was cancelled and only three cycles are needed since the availability requirements can be met by the servers that have already been upgraded. Once an ISO is selected and the **OK** button is clicked, the site upgrade continues normally.

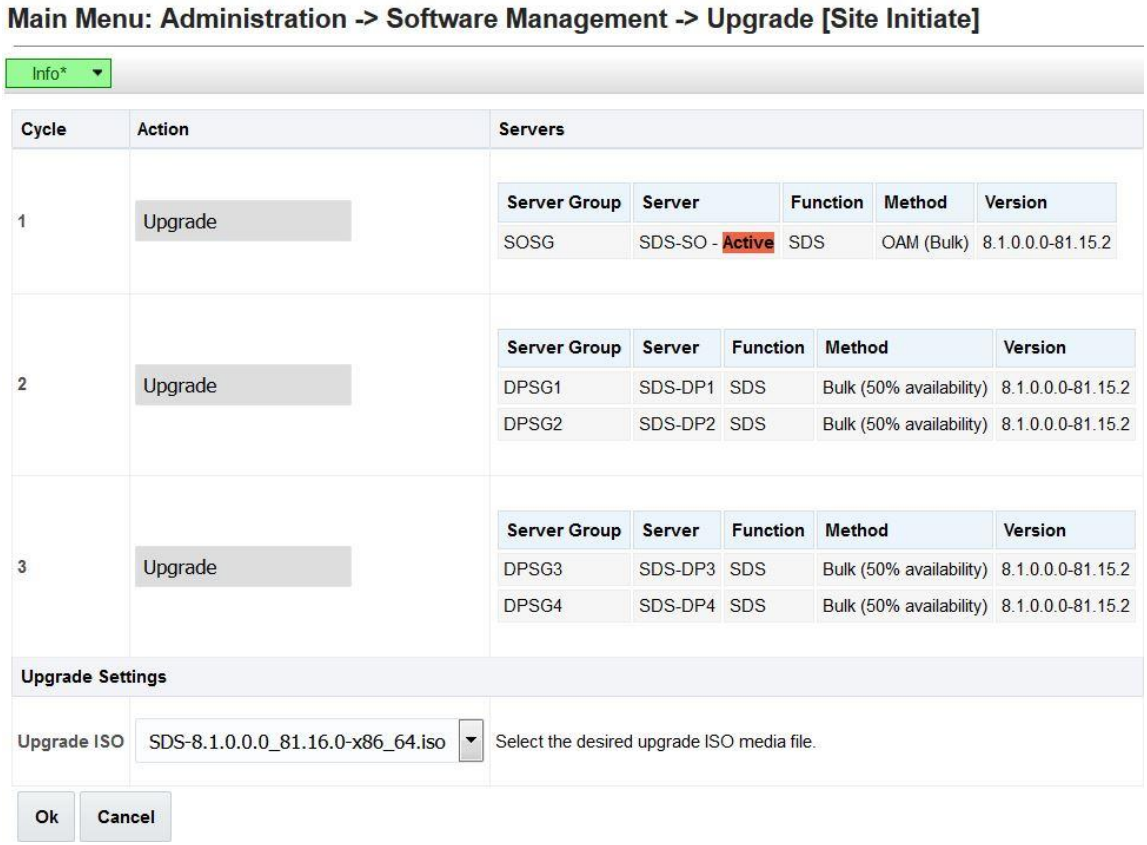


Figure 14. Restarting Site Upgrade.

7. Automated Server Group Upgrade

The Automated Server Group (ASG) upgrade feature allows the user to upgrade all of the servers automatically in a server group simply by specifying a set of controlling parameters.

The purpose of ASG is to simplify and automate segments of the SDS upgrade. The SDS has long supported the ability to select multiple servers for upgrade. In doing so however, it was incumbent on the user to determine ahead of time which servers could be upgraded in parallel, considering traffic impact. If the servers were not carefully chosen, the upgrade could adversely impact system operations.

When a server group is selected for upgrade, ASG upgrades each of the servers serially, or in parallel, or a combination of both, while enforcing minimum service availability. The number of servers in the server group that are upgraded in parallel is user selectable. The procedures in this document provide the detailed steps specifying when to use ASG and the appropriate parameters that should be selected for each server group type.

ASG is the default upgrade method for NOAM and SOAM server group types associated with the SDS. DP's use Auto Site Upgrade feature. However, there may be some instances in which the manual upgrade method is preferred. In all cases where ASG is used, procedures for a manual upgrade are also provided.

Note: To use ASG on a server group, no servers in that server group can be already upgraded – either by ASG or manually.

SDS continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

For SDS Automated Server Group (ASG) upgrade refer the steps as specified in Appendix D.

7.1 Cancel and Restart Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be manually cancelled from the **Status & Manage > Active Tasks** screen (Figure 15) if necessary. Once the task is cancelled, it cannot be restarted. However, a new ASG task can be started using the Upgrade Administration screen.

For example, in Figure 15, task ID #1 (SO_SG Server Group Upgrade) is an ASG task, while task ID #2 is the corresponding individual server upgrade task. When the ASG task is selected (highlighted in green), the **Cancel** button is enabled. Cancelling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tasks that were started by the ASG task (that is, task ID #2 in Figure 15). Because the ASG task is cancelled, no new server upgrade is initiated by the task.

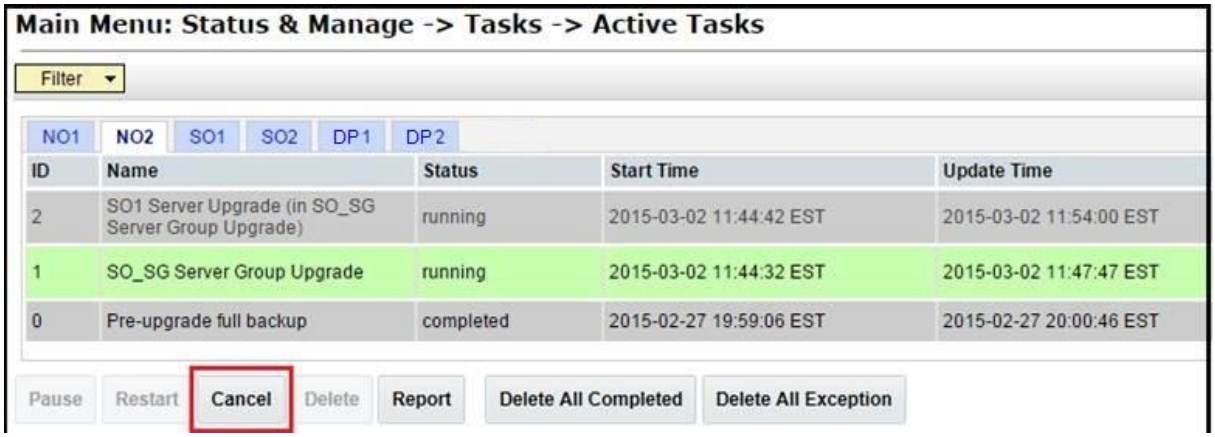


Figure 15. Server Group Upgrade Active Tasks

If a server fails upgrade, the server automatically rolls back to the previous release in preparation for backout_restore and fault isolation. Any other servers in that server group, which are in the process of upgrading, continue to upgrade to completion; however, the ASG task itself is automatically cancelled and no other servers in that server group are upgraded. Cancelling the ASG task provides an opportunity for troubleshooting to correct the problem. Once the problem is corrected, the server group upgrade can be restarted by initiating a new server group upgrade on the upgrade screen.

7.2 Site Accept

Before SDS 8.0, the customer was required to “Accept” the upgrade of individual servers in each server group of a site. While the Accept is a relatively quick operation, it could nonetheless be a tedious task for larger sites with numerous servers. In DSR 8.0, a new feature has been added to make the upgrade Accept much easier for all customers, large and small.

The **Site Accept** button on the upgrade screen provides the capability to nearly simultaneously accept the upgrade of some or all servers for a given site. When the button is selected, a subsequent screen displays the servers that are ready for the Accept action.

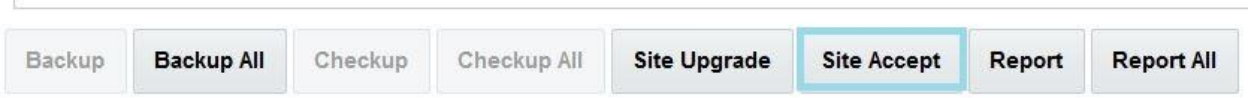


Figure 16. Site Accept Button

A checkbox on the Upgrade Site Accept screen allows for the selective application of the Accept action. However, normal procedure calls for the Accept to be applied to all of the servers at a site only after the upgrade to the new release is stable and the back out option is no longer needed. After verifying the information presented is accurate, clicking the **OK** button results in a confirmation screen that requires action. Confirming the action causes the server upgrade to be accepted.

The Accept command is issued to the site servers at a rate of approximately one server every second. The command takes approximately 10 seconds per server to complete. As the commands are completed, the server status on the Upgrade Administration screen transitions to **Backup Needed**.

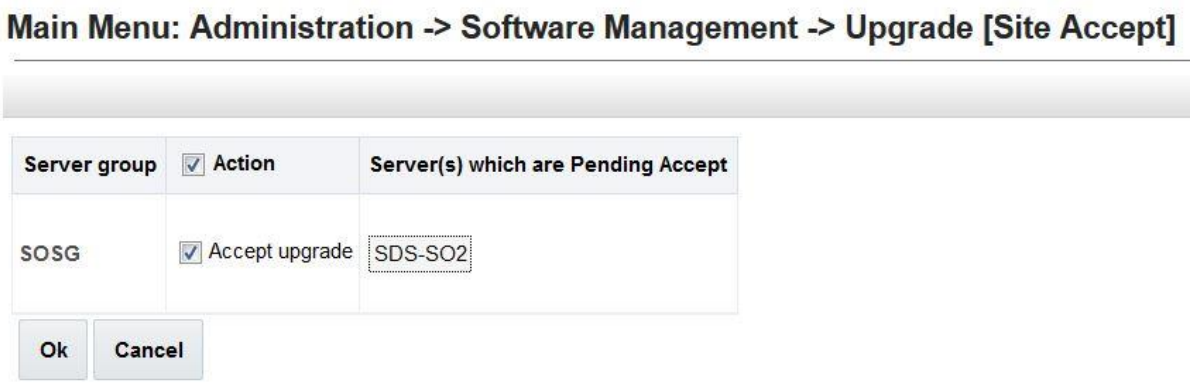


Figure 17. Site Accept Screen

8. Primary/DR SDS NOAM Upgrade Execution

Call My Oracle Support (MOS) and inform them of your plans to upgrade this system before executing this upgrade.

Refer to Appendix T for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix A. This check ensures the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if the upgrade can proceed with alarms.

WARNING!

If there are servers in the system, which are not in a Normal state, these servers should be brought to the **Normal** or **Application Disabled** state before the upgrade process starts. The sequence of upgrade is such that servers providing support services to other servers are upgraded first.

WARNING!

If a procedural step fails to execute successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact **MOS** for assistance before attempting to continue.

Procedure completion times shown are estimates. Times may vary due to differences in database size, user experience, and user preparation.

Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:

- Session banner information such as time and date.
- System-specific configuration information such as hardware locations, IP addresses, and hostnames.
- ANY information marked with **XXXX** or **YYYY**. Where appropriate, instructions are provided to determine what output should be expected in place of **XXXX** or **YYYY**.
- Aesthetic differences unrelated to functionality such as browser attributes: window size, colors, toolbars, and button layouts.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade marks the provided checkbox. For procedures, which are executed multiple times, a mark can be made below the checkbox (in the same column) for each additional iteration that the step is executed.

Retention of captured data is required as a future support reference if this procedure is executed by someone other than Oracle's Customer Care Center.

Note: To minimize possible impacts due to database schema changes, primary and DR SDS network elements must be upgraded within the same maintenance window.

8.1 Perform Health Check (Primary/DR NOAM Pre-Upgrade)

This procedure is part of software upgrade preparation and is used to determine the health and status of the entire SDS network and servers. This may be executed multiple times, but must also be executed at least once within the period of 24-36 hours before starting a maintenance window.

☐ Execute SDS Health Check procedures as specified in Appendix A.

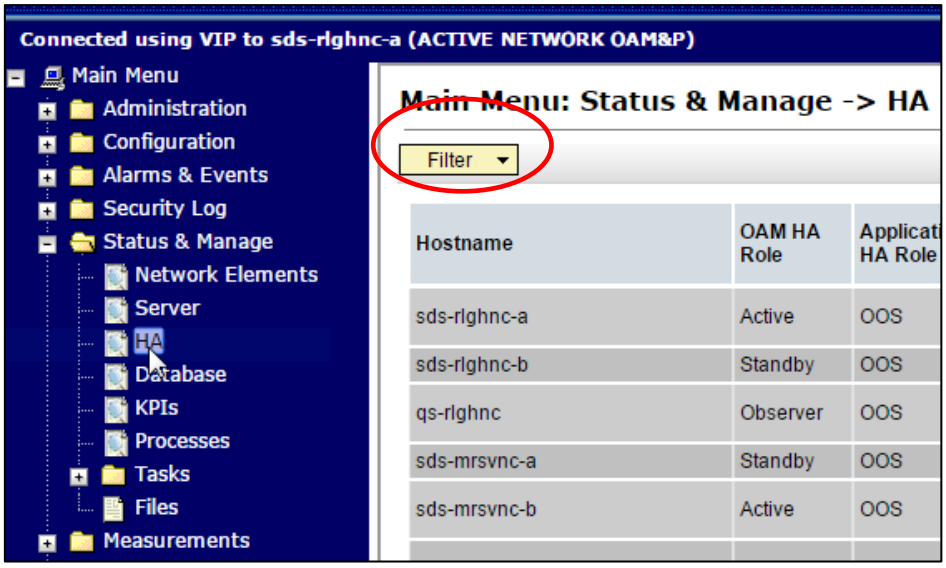
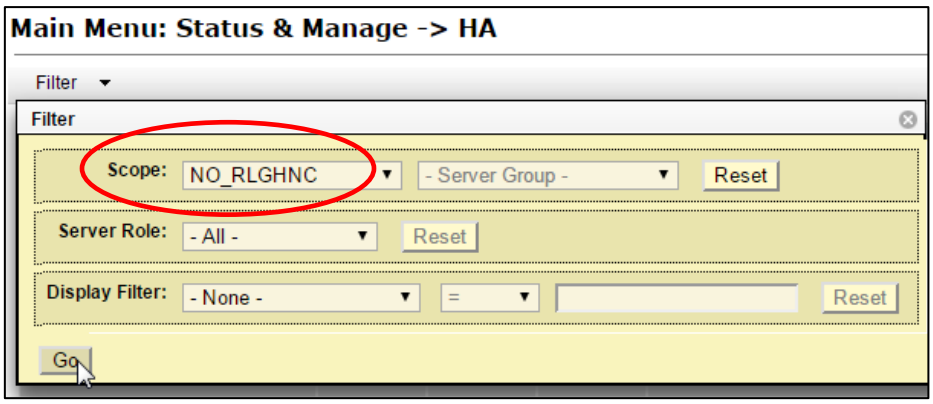
☐ Execute Appendix M Increase Maximum Number of Open Files.

8.2 Upgrade the Primary SDS NOAM

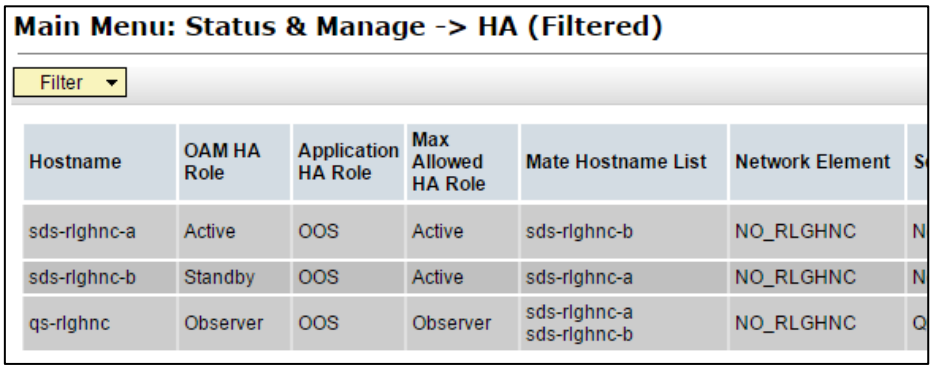
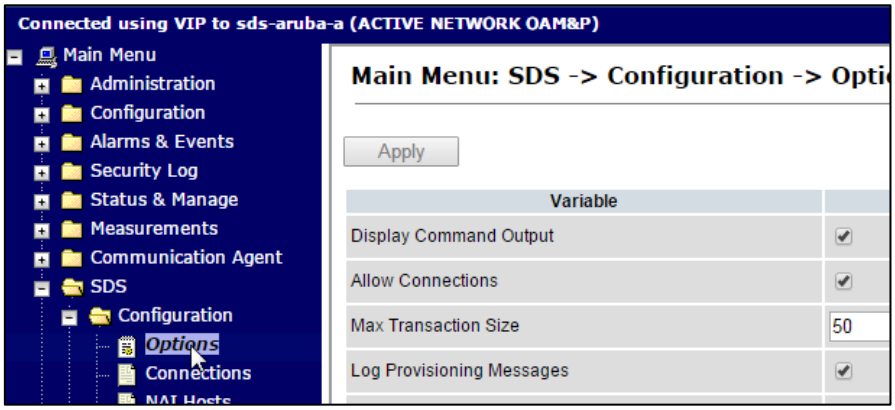
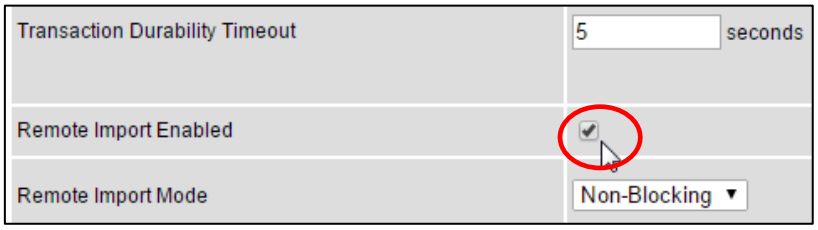
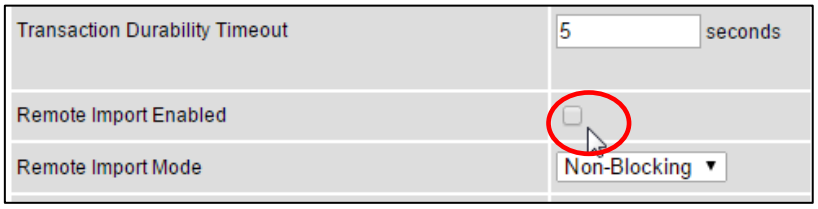
This procedure is used to upgrade the SDS NOAM servers.

WARNING The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 6. See section 3.4 for more details before proceeding.

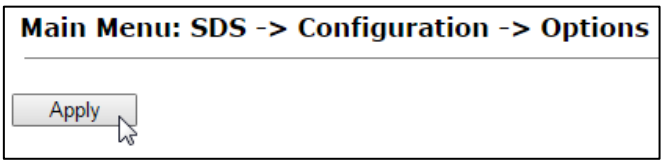
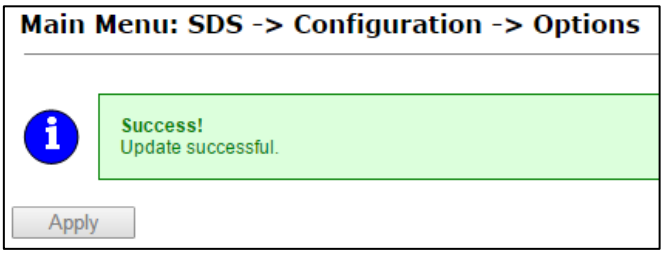
Procedure 5. Upgrade the Primary SDS NOAM

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP GUI**	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**. 
3. ☐	**Primary SDS NOAM VIP GUI**: Locate the primary SDS NOAM NE	1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the primary SDS NOAM Network Element from the **Scope** field. 2. Click **Go**. 

Procedure 5. Upgrade the Primary SDS NOAM

4. ☐	**Primary SDS NOAM VIP GUI**: Identify servers and record server names	Identify each server by **Hostname**, **Server Role**, and **OAM HA Role** and record the name of each server.  Main Menu: Status & Manage -> HA (Filtered) Filter Hostname | OAM HA Role | Application HA Role | Max Allowed HA Role | Mate Hostname List | Network Element sds-rlghnc-a | Active | OOS | Active | sds-rlghnc-b | NO_RLGHNC sds-rlghnc-b | Standby | OOS | Active | sds-rlghnc-a | NO_RLGHNC qs-rlghnc | Observer | OOS | Observer | sds-rlghnc-a sds-rlghnc-b | NO_RLGHNC Active Primary SDS NOAM: _____ Standby Primary SDS NOAM: _____ Primary Query Server (if equipped): _____
5. ☐	**Primary SDS NOAM VIP GUI**: Remote Import Enable state	1. Navigate to **SDS > Configuration > Options**.  Connected using VIP to sds-aruba-a (ACTIVE NETWORK OAM&P) Main Menu Administration Configuration Alarms & Events Security Log Status & Manage Measurements Communication Agent SDS Configuration Options Connections Main Menu: SDS -> Configuration -> Opti Apply Variable Display Command Output Allow Connections Max Transaction Size 50 Log Provisioning Messages 2. Locate the **Remote Import Enabled** checkbox and record the pre-upgrade state.  Transaction Durability Timeout 5 seconds Remote Import Enabled Remote Import Mode Non-Blocking ☐ Checked ☐ Not Checked 3. Unmark the **Remote Import Enabled** checkbox if it was checked.  Transaction Durability Timeout 5 seconds Remote Import Enabled Remote Import Mode Non-Blocking

Procedure 5. Upgrade the Primary SDS NOAM

6. ☐	**Primary SDS NOAM VIP**: Apply change and verify	1. Click **Apply**.  2. Verify a successful response in the banner. 
Note: The next two steps can be executed in parallel.		
7. ☐	**Primary SDS NOAM VIP**: Upgrade the **Standby Primary SDS NOAM** server	Upgrade the **Standby Primary SDS NOAM** server (as identified and recorded in step 4 of this procedure) using Appendix C Upgrade Server Administration on SDS 7.x if source release is SDS 7.x, or Appendix D Upgrade Server Administration on SDS 8.x if source release is SDS 8.x.

8. ☐	**Primary SDS NOAM VIP (CLI)**: Access the active primary SDS NOAM	Use the VIP address to log into the active primary SDS NOAM with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`

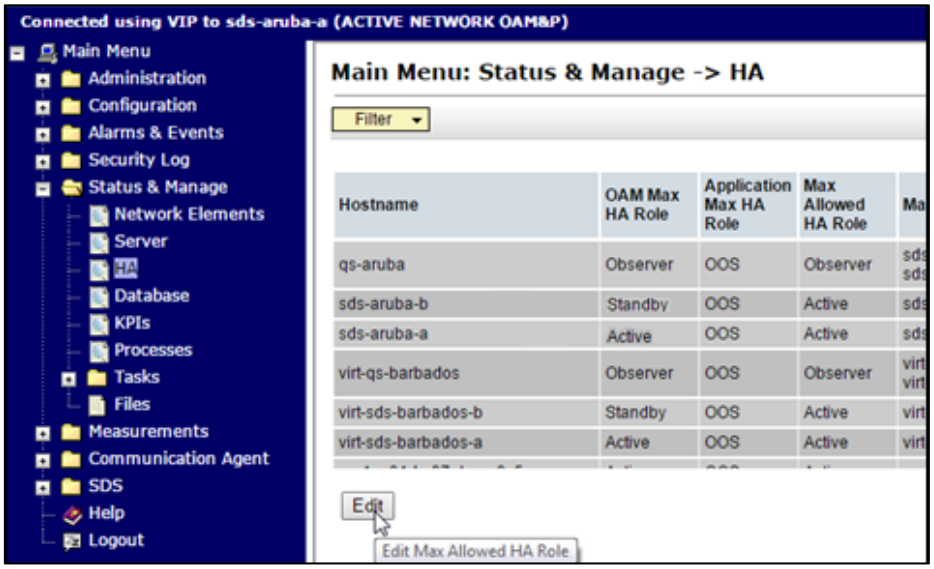
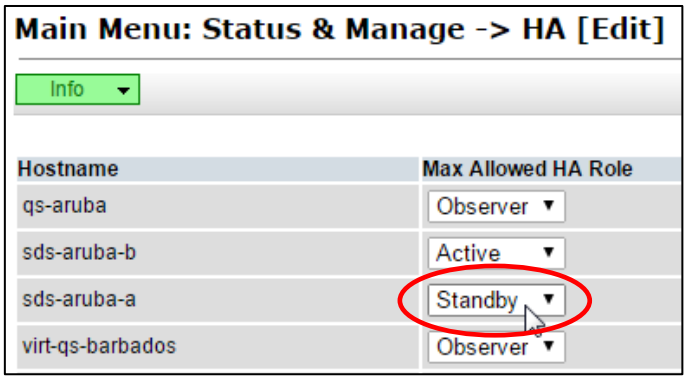
Procedure 5. Upgrade the Primary SDS NOAM

9. ☐	**Primary SDS NOAM VIP**: Verify status	1. Verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM** and **Query Server**, if equipped.
		`[admusr@sds-rlghnc-a ~]$ sudo irepstat -w`
		`-- Policy 0 ActStb [DbReplication]`
		`AA To sds-rlghnc-b Active 0 0.25 1%R 0.05%cpu 47B/s`
		`AA To qs-rlghnc Active 0 0.25 1%R 0.05%cpu 56B/s`
		`AA To sds-mrsvnc-a Active 0 0.50 1%R 0.04%cpu 47B/s`
		`AB To kauai-sds-SO-b Active 0 0.50 1%R 0.04%cpu 63B/s`
		`AB To florence-sds-SO-a Active 0 0.51 1%R 0.03%cpu 65B/s`
		`AB To turks-sds-SO-b Active 0 0.50 1%R 0.04%cpu 65B/s`
		`irepstat ( 8 lines) (h)elp`
		2. If a **DbReplication** status is received as **Audit,** then repeat the command until **Active** is returned.
		Important: Do **not** proceed until the status is **Active**.
		Check Replication is showing as **Active** for the standby primary SDS NOAM, Query server, active DR SDS NOAM, and standby DR SDS NOAM (if equipped).
		3. Repeat the step until the status is **Active** for all the mentioned servers.
		Important: If a DbReplication status is received as **Audit** or some other value for these servers, repeat this step until a status of **Active** is returned. Servers are:
		• Standby Primary SDS NOAM
		• Query Server
		• Active DR SDS NOAM
		• Standby DR SDS NOAM
		4. If required, contact My Oracle Support (MOS) for any assistance.

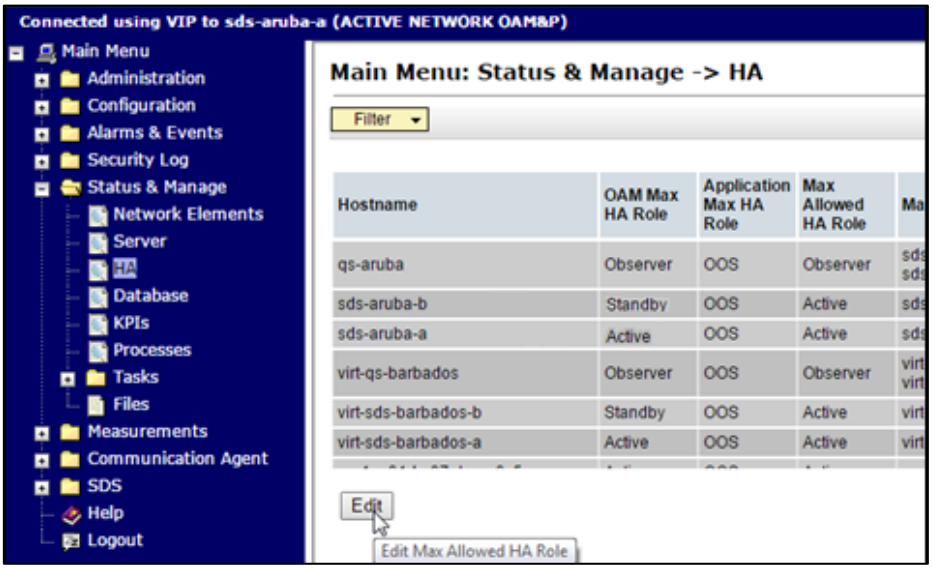
10. ☐	**Primary SDS NOAM VIP**: Exit CLI	Exit the CLI for the **Active Primary SDS NOAM**.
		`[admusr@sds-rlghnc-a filemgmt]$ exit`
		`logout`

11. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

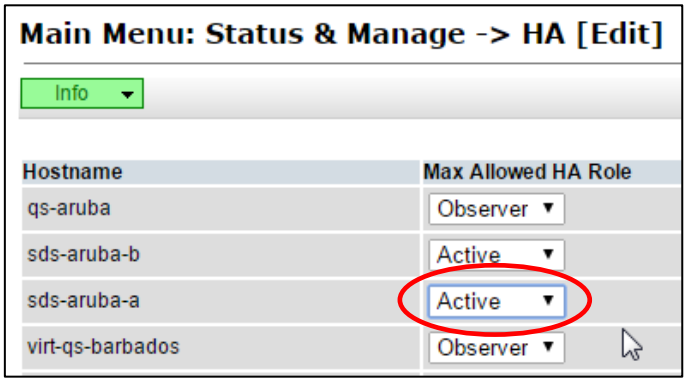
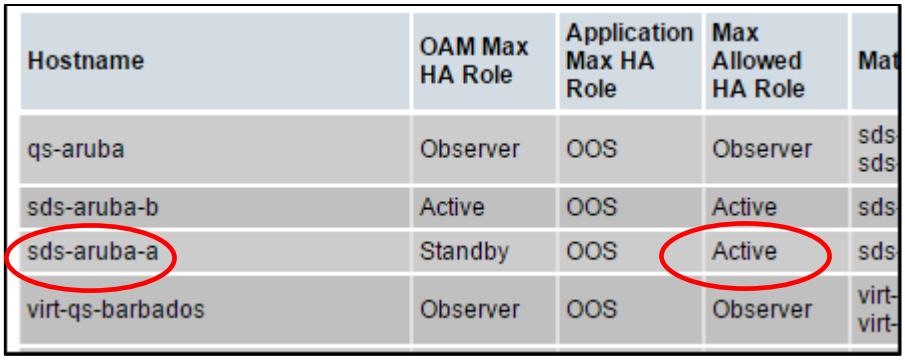
Procedure 5. Upgrade the Primary SDS NOAM

12. ☐	**Primary SDS NOAM VIP**: Edit server	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 
13. ☐	**Primary SDS NOAM VIP**: Change Max Allowed HA Role status	1. Select the **Active Primary SDS NOAM** server and change a **Max Allowed HA Role** value from **Active** to **Standby**.  2. Click **OK**. The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the standby server. 3. If not automatically logged out of the GUI, click **Logout** to log out of the SDS NOAM GUI.

Procedure 5. Upgrade the Primary SDS NOAM

14. ☐	**Primary SDS NOAM VIP (GUI)**: Clear cached data	JavaScript libraries, images, and other objects are often modified in the upgrade. Browsers can sometimes cause GUI problems by holding on to the old objects in the built-in cache. To prevent these problems, always clear the browser cache before logging into an OAM GUI that has just been upgraded: 1. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers). 2. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, etc.). Other browsers may label these objects differently. 3. Clear the cached data. ***Note***: Do NOT proceed until the browser cache has been cleared.
15. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
16. ☐	**Primary SDS NOAM VIP**: Edit server	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 

Procedure 5. Upgrade the Primary SDS NOAM

17. ☐	**Primary SDS NOAM VIP**: Change **Max Allowed HA Role** status	1. Select the **Standby Primary SDS NOAM** server and change a **Max Allowed HA Role** value from **Standby** to **Active**.  2. Click **OK**.
18. ☐	**Primary SDS NOAM VIP**: Verify change to **Active** state	Verify the **Max Allowed HA Role** value has been updated to **Active** for the **Standby Primary SDS NOAM** server. 
19. ☐	**Primary SDS VIP**: CmHA restart	If the server in topology shows as an **Out of Service** state, perform a **CmHA** restart; otherwise, proceed to the next step. Refer to Appendix O for more details. ***Note***: You will see Out of Service state on the server on which CmHA restart is performed. Ignore this state and continue with the upgrade.
Note: The next two steps of this procedure can be executed in paraellel.		
20. ☐	**Primary SDS VIP**: Upgrade the current **Standby Primary SDS NOAM** server	Upgrade the current **Standby Primary SDS NOAM** server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.
21. ☐	**Primary SDS NOAM VIP**: Upgrade the **Primary SDS Query** server	Upgrade the **Primary Query** server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x. ***Note***: If the Query server status is not reported on the **Status and Manage** server screen, refer to Appendix S for more details.

Procedure 5. Upgrade the Primary SDS NOAM

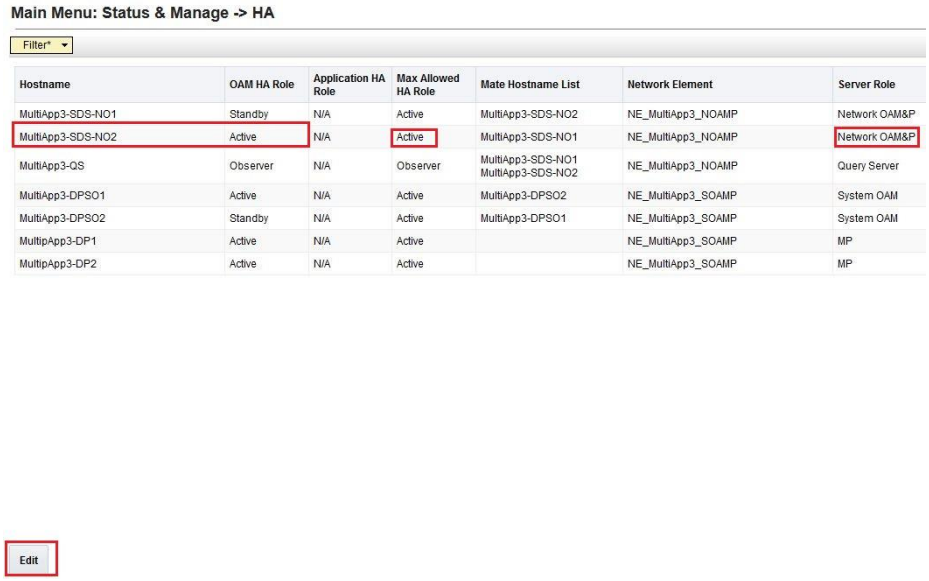
22. ☐	**Primary SDS NOAM VIP**: Verify status	1. Perform a replication check as explained in step 9. ***Note***: The replication link between the primary and secondary (DR-NO site) server is broken at this point until the DR-NO servers are upgraded completely. 2. Proceed to step 37 for remote import.

23. ☐	**Primary SDS NOAM VIP (CLI)**: Login	Using the VIP address, log into the **Active Primary SDS NOAM** with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		*** TRUNCATED OUTPUT ***
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`

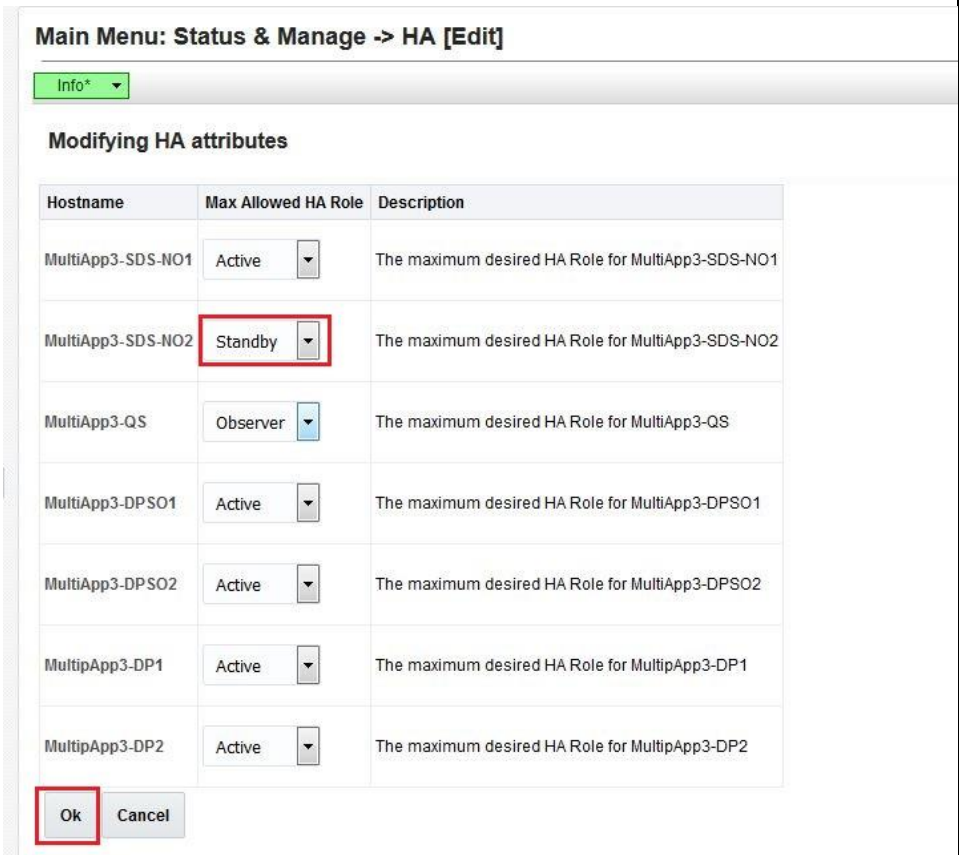
24. ☐	**Primary SDS NOAM VIP (CLI)**: Verify status	1. Verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM**, **Query Server**, **Active DR SDS NOAM**, and **Standby NOAM** servers (if equipped).
		`[admusr@sds-rlghnc-a ~]$ sudo irepstat -w`
		`-- Policy 0 ActStb [DbReplication]`
		`AA To sds-rlghnc-b Active 0 0.25 1%R 0.05%cpu 47B/s`
		`AA To qs-rlghnc Active 0 0.25 1%R 0.05%cpu 56B/s`
		`AA To sds-mrsvnc-a Active 0 0.50 1%R 0.04%cpu 47B/s`
		`AB To kauai-sds-SO-b Active 0 0.50 1%R 0.04%cpu 63B/s`
		`AB To florence-sds-SO-a Active 0 0.51 1%R 0.03%cpu 65B/s`
		`AB To turks-sds-SO-b Active 0 0.50 1%R 0.04%cpu 65B/s`
		`irepstat ( 8 lines) (h)elp`
		2. Repeat the step until the status is **Active** for all mentioned servers.
		IMPORTANT
		If a DbReplication status is received as **Audit** or some other value for these servers, repeat this step until a status of **Active** is returned. Servers are:
		• Standby Primary SDS NOAM
		• Query Server
		• Active DR SDS NOAM
		• Standby DR SDS NOAM
		3. If required, contact My Oracle Support (MOS) for any assistance.

Procedure 5. Upgrade the Primary SDS NOAM

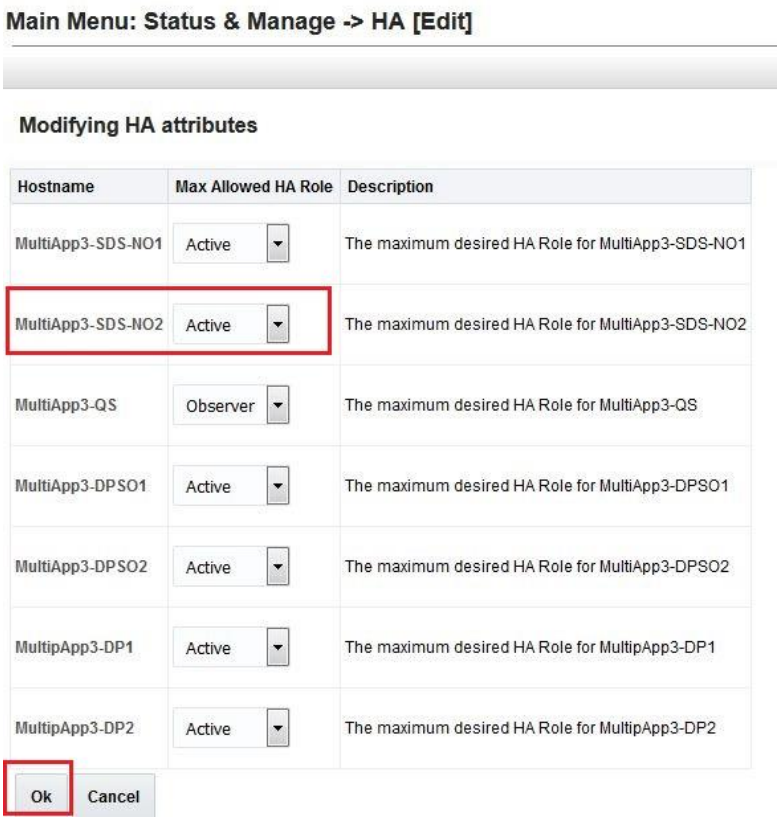
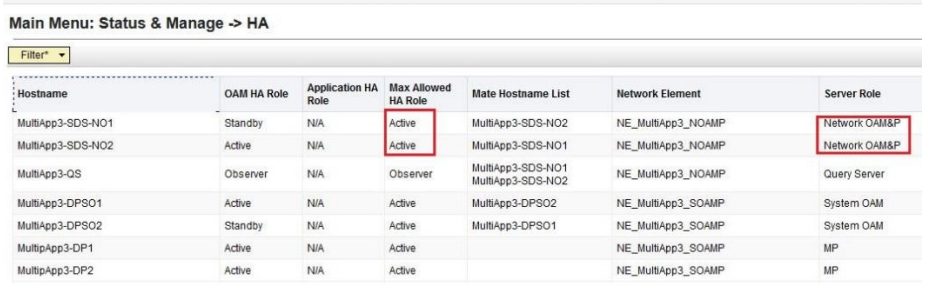
25. ☐	**Primary SDS NOAM VIP**: Exit CLI	Exit the CLI for the **Active Primary SDS NOAM**.
		`[admusr@sds-rlghnc-a filemgmt]$ exit`
		`logout`

26. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
27. ☐	**Primary SDS NOAM VIP (GUI)**: Manual switchover of NOAM server	1. Navigate to **Status & Manage > HA**. 2. Select the **Active NOAM server**. 3. Click **Edit**. 

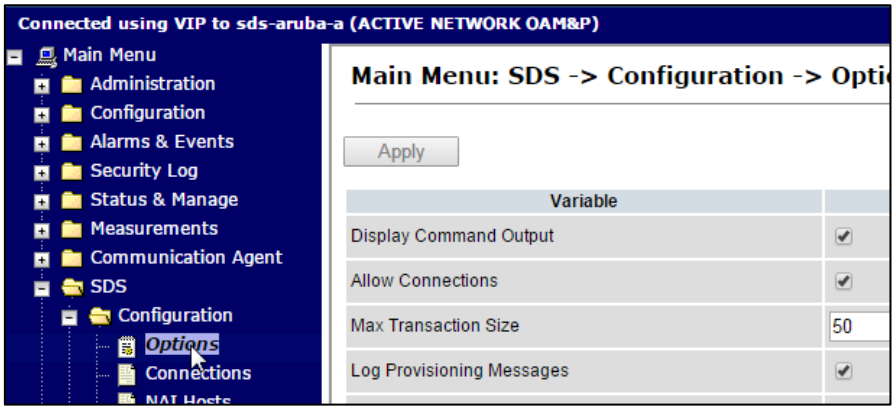
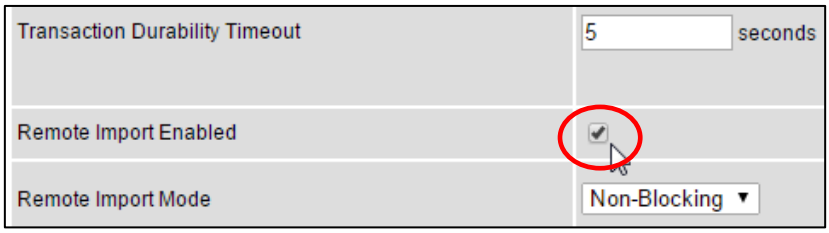
Procedure 5. Upgrade the Primary SDS NOAM

28. ☐	**Primary SDS NOAM VIP (GUI)**: Manual switchover of NOAM server	1. Change **Max Allowed HA Role** for the Active SDS NOAM Server to **Standby**.  2. Click **OK**. **IMPORTANT**: This causes HA activity switchover to the mate primary SDS NOAM server. ***Note***: The GUI logs out automatically.
29. ☐	Access the primary SDS NOAM GUI	1. Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A **again**. 2. Make sure NOAM logged in is the second SDS NOAM and is primary by checking the bottom of the screen on the GUI.

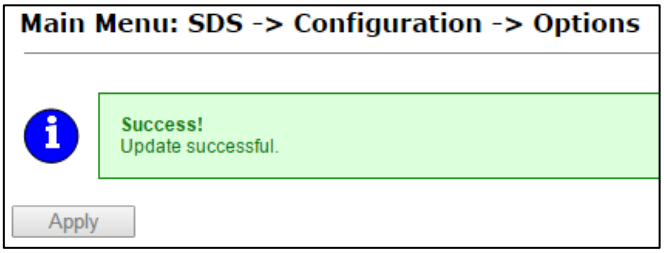
Procedure 5. Upgrade the Primary SDS NOAM

30. ☐	**Primary SDS NOAM VIP (GUI)**: Change Max Allowed HA Role for new standby NOAM server back to active	1. Change **Max Allowed HA Role** for the SDS NOAM server to **Active**.  2. Click **OK**.
31. ☐	**Primary SDS NOAM VIP GUI**: Verify the role has changed	Verify the **Max Allowed HA Role** for the NOAM server is **Active**. 
32. ☐	**Primary SDS NOAM VIP (CLI)**: Verify status 	1. Verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM**, **Query Server**, **DR Site Active**, and **Standby NOAM** servers (if equipped). 2. Repeat steps 9 to 12 to verify **irepstat** is showing **Active**. 3. Make sure Replication is **Active** for the **Standby Primary SDS NOAM**, **Query Server**, **Active DR SDS NOAM**, and **Standby DR SDS NOAM** servers (if equipped).

Procedure 5. Upgrade the Primary SDS NOAM

33. ☐	**Primary SDS VIP**: CmHA restart	If the server in topology shows as an **Out of Service** state, perform a **CmHA** restart; otherwise, proceed to the next step. Refer to Appendix O for more details. ***Note***: You will see Out of Service state on the server on which CmHA restart is performed. Ignore this state and continue with the upgrade.
Note: The next two steps of this procedure can be executed in parallel.		
34. ☐	**Primary SDS VIP**: Upgrade the current **Standby Primary SDS NOAM** server	Upgrade the current **Standby Primary SDS NOAM** server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x. In step 5 of this procedure, mark the associated checkbox as the upgrade is completed for the upgraded **Active Primary SDS NOAM** server.
35. ☐	**Primary SDS NOAM VIP**: Upgrade the **Primary SDS Query** server	Upgrade the **Primary Query** server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x. In step 5 of this procedure, mark the associated checkbox as the upgrade is completed for the upgraded **Primary Query** server.
36. ☐	**Primary SDS NOAM VIP**: Verify status	Perform a replication check as explained in step 24. ***Note***: The replication link between the primary and secondary (DR-NO site) server is broken at this point until the DR-NO servers are upgraded completely.
37. ☐	**Primary SDS NOAM VIP**: Re-enable provisioning Remote Import (if applicable)	Re-enable the **Remote Import Enabled** checkbox if the checkbox recorded in step 5 of this procedure was **Checked**. If the **Remote Import Enabled** checkbox recorded in step 5 of this procedure was **NOT CHECKED**, then **this procedure is complete**. 1. Navigate **to SDS > Configuration > Options**.  2. Locate the **Remote Import Enabled** checkbox and mark it. 

Procedure 5. Upgrade the Primary SDS NOAM

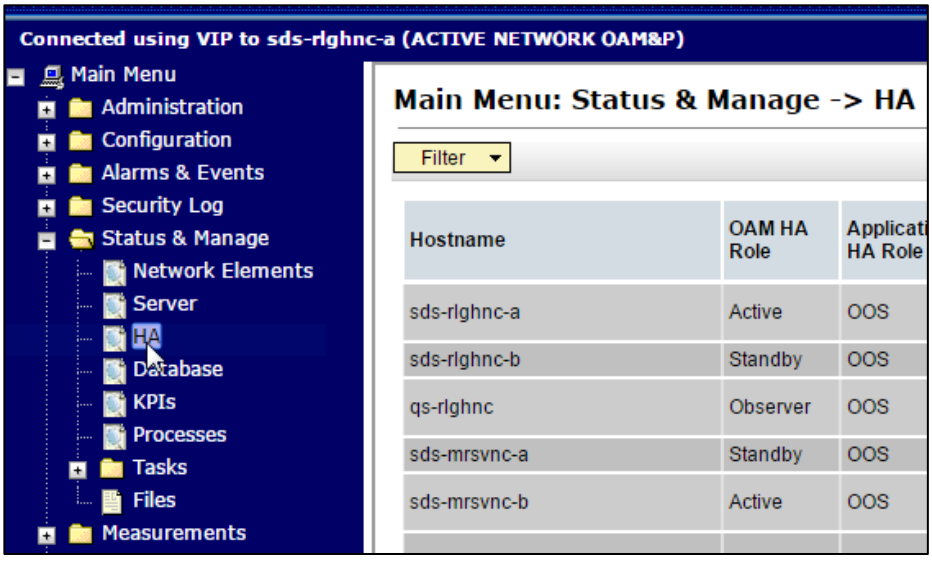
38. ☐	**Primary SDS NOAM VIP**: Apply change and verify	1. Click **Apply**. 2. Verify a successful response in the banner. 

8.3 Upgrade DR SDS NOAM

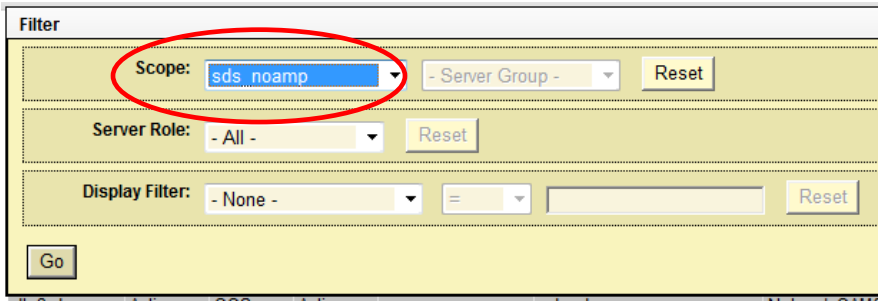
This procedure upgrades the DR SDS NOAM servers.

WARNING The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 6. See section 3.4 for more details before proceeding.

Procedure 6. Upgrade DR SDS NOAM

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP**: Record name of **DR SDS NE** site	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**. 

Procedure 6. Upgrade DR SDS NOAM

<table>
<tr><td>3. ☐</td><td>Primary SDS NOAM VIP: List servers</td><td>1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the DR SDS Network Element from the Scope field.
2. Click Go.
 
</td></tr>
<tr><td>4. ☐</td><td>Primary SDS NOAM VIP: Identify servers and record server names</td><td>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th></tr>
<tr><td>dts3-sds-a</td><td>Active</td><td>OOS</td><td>Active</td><td>dts3-sds-b</td><td>sds_noamp</td><td>Network OAM&P</td></tr>
<tr><td>dts3-sds-b</td><td>Standby</td><td>OOS</td><td>Active</td><td>dts3-sds-a</td><td>sds_noamp</td><td>Network OAM&P</td></tr>
<tr><td>dts3-qs-1</td><td>Observer</td><td>OOS</td><td>Observer</td><td>dts3-sds-a
dts3-sds-b</td><td>sds_noamp</td><td>Query Server</td></tr>
</table>
Active DR SDS NOAM: _____
Standby DR SDS NOAM: _____
DR SDS Query Server (if equipped): _____</td></tr>
<tr><td>5. ☐</td><td>Primary SDS NOAM VIP: Upgrade the standby DR SDS server</td><td>Upgrade the Standby DR SDS NOAM server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.</td></tr>
<tr><td colspan="3">Note: The next two steps of this procedure can be executed in parallel using the Upgrade Server option.</td></tr>
<tr><td>6. ☐</td><td>Primary SDS NOAM VIP: Upgrade the active DR SDS server</td><td>Upgrade the Active DR SDS NOAM server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.
Important: This causes an HA activity failover to the mate primary SDS NOAM server. This happens a couple minutes after initiating the upgrade.</td></tr>
<tr><td>7. ☐</td><td>Primary SDS NOAM VIP: Upgrade the DR Query server</td><td>Upgrade the DR SDS Query server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.</td></tr>
</table>

8.4 Perform Health Check (Primary/DR NOAM Post Upgrade)

This procedure is used to determine the health and status of the entire SDS network and servers after Primary and DR NOAM upgrade has been completed.

☐ Execute SDS Health Check procedures as specified in Appendix A.

8.5 SNMP Configuration Update (Post Primary/DR NOAM Upgrade)

Refer Workaround for SNMP Configuration to apply SNMP workaround in following cases:

- If SNMP is not configured in SDS.
- If SNMP is already configured and **SNMPv3** is selected as enabled version.

This can be checked by navigating to **Administration > Remote Servers >SNMP Trapping** screen using GUI session of NOAM server VIP IP address.

9. Site Upgrade Execution

This section contains the procedures for upgrading an entire site — starting with the pre-upgrade activities, upgrading the SOAMs and DP servers, and finishing with verifying the upgrade.

Table 12. Site Upgrade Planning — Automed vs. Manual Upgrade

Atomated	Manual
There are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature upgrades an entire site (SOAMs and DP servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade automatically prepares the server(s), performs the upgrade, and sequences to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity. Automated Site Upgrade can be used to upgrade the SOAM and DP servers.	A manual upgrade affords the maximum level of control over upgrade sequencing and intermediate observations. With this method, the upgrade of each server is individually initiated, allowing the user to control the level of parallelism and speed of the upgrade.
Note: A site upgrade can include a combination of Automated Server Group upgrade and manual upgrades to improve efficiency. For example, SOAMs can be upgraded with Automated Server Group or Manual upgrade, while the DPs may be upgraded manually to control the order of upgrade for traffic continuity.	
The Automated Site Upgrade procedures are in section 9.1.	The manual site upgrade procedures are in section 9.2.

9.1 Automated Site Upgrade

Call My Oracle Support (MOS) and inform them of your plans to upgrade this system before executing this upgrade.

Refer to Appendix T for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix A. This check ensures the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if the upgrade can proceed with alarms.

WARNING!

If there are servers in the system, which are not in a Normal state, these servers should be brought to the **Normal** or **Application Disabled** state before the upgrade process starts. The sequence of upgrade is such that servers providing support services to other servers are upgraded first.

WARNING!

If a procedural step fails to execute successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact **MOS** for assistance before attempting to continue.

Procedure completion times shown are estimates. Times may vary due to differences in database size, user experience, and user preparation.

Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:

- Session banner information such as time and date.
- System-specific configuration information such as hardware locations, IP addresses, and hostnames.
- ANY information marked with **XXXX** or **YYYY**. Where appropriate, instructions are provided to determine what output should be expected in place of **XXXX** or **YYYY**.
- Aesthetic differences unrelated to functionality such as browser attributes: window size, colors, toolbars, and button layouts.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade marks the provided checkbox. For procedures, which are executed multiple times, a mark can be made below the checkbox (in the same column) for each additional iteration that the step is executed.

Retention of captured data is required as a future support reference if this procedure is executed by someone other than Oracle's Customer Care Center.

Note: For large systems containing multiple signaling network elements, it may not be feasible to apply the software upgrade to every network element within a single maintenance window.

9.1.1 Perform Health Check (Pre-Upgrade)

This procedure is part of software upgrade preparation and is used to determine the health and status of the entire SDS network and servers. This may be executed multiple times, but must also be executed at least once within the period of 24-36 hours before starting a maintenance window.

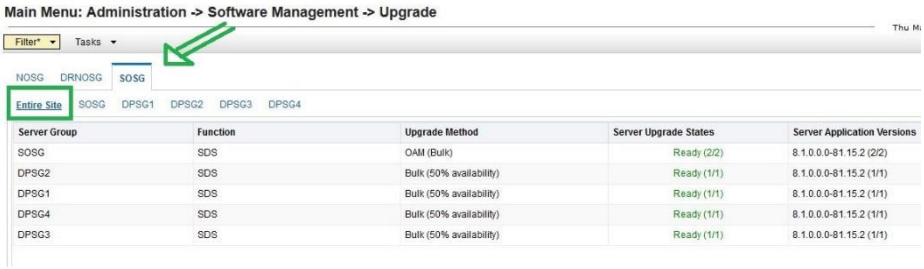
☐ Execute SDS Health Check procedures as specified in Appendix A.

9.1.2 Upgrade SOAM

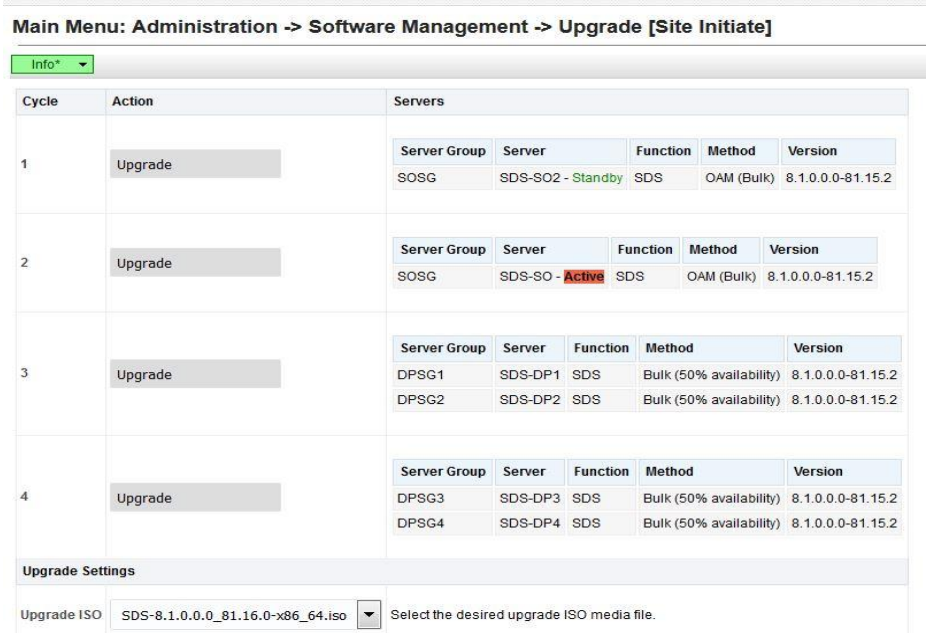
The following procedure details how to upgrade SDS SOAM sites.

Caution When upgrading an SDS topology, it is permissible to upgrade multiple SOAM sites in parallel. However, every attempt should be made to avoid upgrading mated SOAM sites in the same maintenace window.

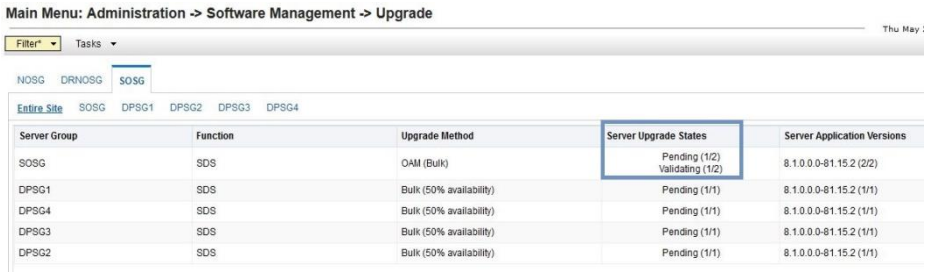
Procedure 7. Upgrade SOAM

1. ☐	Review site upgrade plan and site readiness	This step verifies the servers and server groups to be upgraded are in the proper state. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Select the SOAM tab of the site to be upgraded. 4. Verify the **Entire Site** link is selected. The Entire Site screen provides a summary of the server states and upgrade readiness. More detailed server status is available by selecting a specific server group link.  ***Note***: The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including **Accept or Reject**, **Ready**, **Backup Needed**, **Failed**, or **Not Ready**. Only the servers in the **Ready** state or **Failed** state are upgrade eligible.

Procedure 7. Upgrade SOAM

2. ☐	**Active NOAM VIP**: Initiate the site upgrade	1. Verify no Server Groups are selected on the upgrade administration screen. The **Site Upgrade** button is not available if a Server Group is selected. 2. Click **Site Upgrade**. 3. Review the upgrade plan as presented on the Site Initiate screen. This plan represents an approximation of how the servers will be upgraded. Due to the dynamic nature of upgrade, some servers (typically only C-level) may be upgraded in a different cycle than displayed here.  ***Note***: If you need to rearrange the upgrade cycle, see section 9.1.3. 4. In the Upgrade Settings section of the form, use the **Upgrade ISO** option to select the target ISO. 5. Click **OK** to start the upgrade sequence. Control returns to the Upgrade Administration screen.

Procedure 7. Upgrade SOAM

3. ☐	**Active NOAM VIP**: View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 4 of this procedure for instructions if the upgrade fails or if execution time exceeds 60 minutes. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the upgrade shows as **Failed**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. With the **Entire Site** link selected, a summary of the upgrade status for the selected site displays. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. This view can be used to monitor the upgrade status of the overall site.  Main Menu: Administration -> Software Management -> Upgrade Filter Tasks NOSG DRNOSG SOSG Entire Site SOSG DPSG1 DPSG2 DPSG3 DPSG4 Server Group / Function / Upgrade Method / Server Upgrade States / Server Application Versions SOSG / SDS / OAM (Bulk) / Pending (1/2) Validating (1/2) / 8.1.0.0.0-81.15.2 (2/2) DPSG1 / SDS / Bulk (50% availability) / Pending (1/1) / 8.1.0.0.0-81.15.2 (1/1) DPSG4 / SDS / Bulk (50% availability) / Pending (1/1) / 8.1.0.0.0-81.15.2 (1/1) DPSG3 / SDS / Bulk (50% availability) / Pending (1/1) / 8.1.0.0.0-81.15.2 (1/1) DPSG2 / SDS / Bulk (50% availability) / Pending (1/1) / 8.1.0.0.0-81.15.2 (1/1) More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group. During the upgrade, the servers may have some or all of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)** ***Note***: Do not accept any upgrades at this time. It is recommended to contact My Oracle Support (MOS) by referring to Appendix T of this document and provide these files. Refer to Appendix I for failed server recovery procedures.

Procedure 7. Upgrade SOAM

4. ☐	**Active NOAM VIP**: View In-Progress Status (monitor)	Upon completion of a successful upgrade, every server in the site is in the **Accept or Reject** state.
5. ☐	**Server CLI**: If the upgrade of a server fails	If the upgrade of a server fails, access the server command line (using SSH or a console), and collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/platcfg.log It is recommended to contact My Oracle Support (MOS) by referring to Appendix T of this document and provide these files. Refer to Appendix C Upgrade Server Administration on SDS 7.x for failed server recovery procedures.

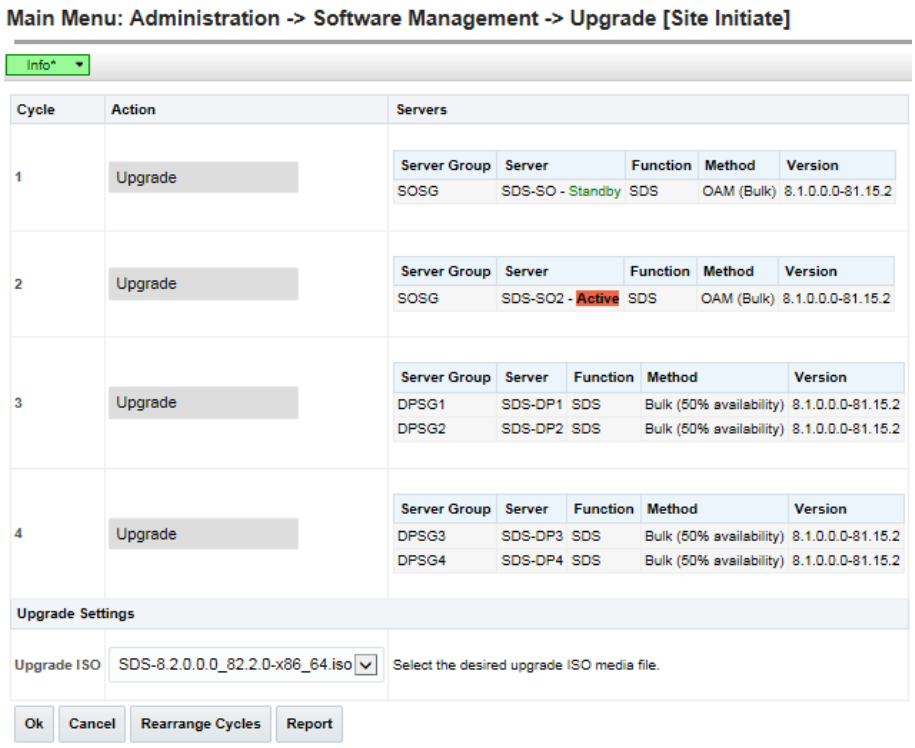
6. ☐	**Server CLI**: Update the tuned profile	After successful upgrade has been verified above, access each of the servers on command line (using SSH or console), and update the tuned profile:
		`$ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh`
		Verify whether tuned profile has been successfully set to **comcol_app**:
		`$ sudo tuned-adm active`
		Sample Output:
		`[admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`
		`[admusr@SOAM1 ~]$`

9.1.3 Rearrange Automate Site Upgrade Cycles

This procedure provides the details to rearrange the Automated Site Upgrade cycles if required.

Automated Site Upgrade provides an option to rearrange servers in the cycles thus eliminating the risks of a potential network outage. ASU provides the flexibility to user to order the servers within the cycles without breaking the Minimum Availability and DA-MP Leader criteria.

Procedure 8. Rearrange Automated Site Upgrade Cycles

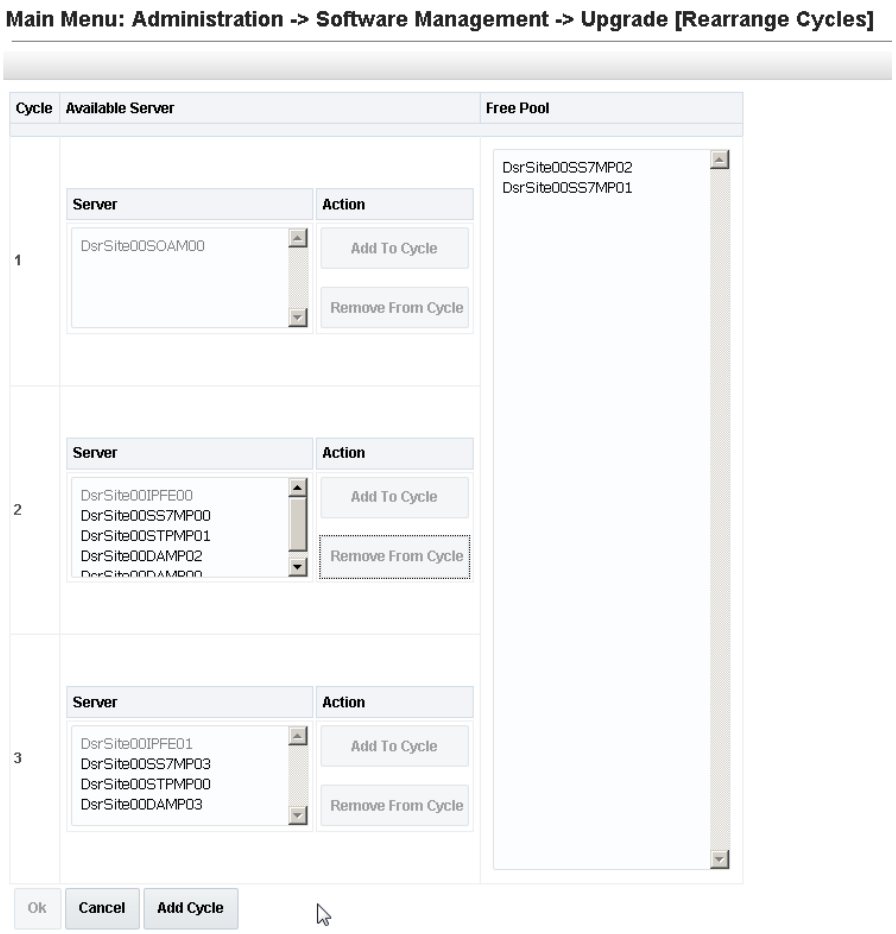
<table>
<tr>
<td>1. ☐</td>
<td>Active NOAM VIP: Rearrange the upgrade cycle as needed</td>
<td>Click Rearrange Cycles.
 
</td>
</tr>
<tr>
<td>2. ☐</td>
<td>Active NOAM VIP: Rearrange servers in cycles</td>
<td>1. Click Rearrange Cycles on the Upgrade screen to rearrange servers.</td>
</tr>
</table>

Procedure 8. Rearrange Automated Site Upgrade Cycles

2. When a server needs to be removed from cycle and needs to be added in an existing cycle or a new cycle, do this:
   1. Select the desired server in the list and click **Remove from Cycle**.

      The server moves to the Free Pool on the right side.

Procedure 8. Rearrange Automated Site Upgrade Cycles

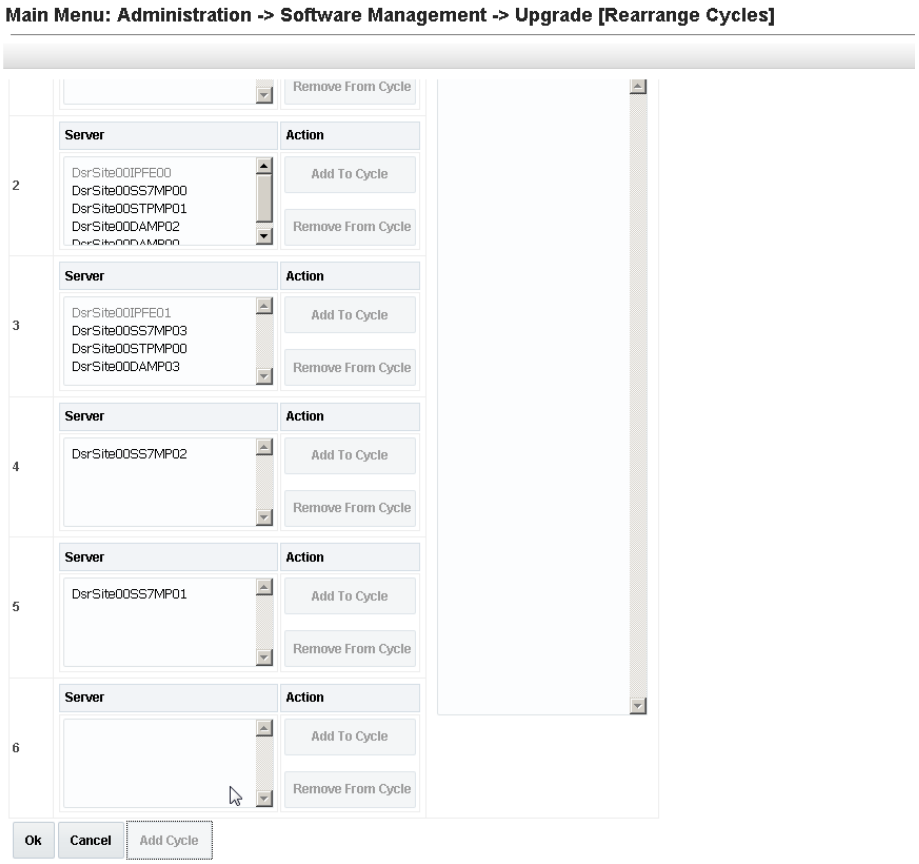


2. Add the servers in Free Pool to another existing cycle or new cycle.

   The next step describes how to add a new cycle, if required.

If there is no need to add a new cycle, then steps to rearrange the cycle are complete.

Procedure 8. Rearrange Automated Site Upgrade Cycles

3. ☐	**Active NOAM VIP**: Add new cycle (If required)	1. Click **Add Cycle**.  After adding new cycle, servers available in free pool can be added in new cycle. 2. Click **OK**.

9.1.4 Perform Health Check (Post Upgrade)

This procedure is part of software upgrade preparation and is used to determine the health and status of the SDS network and servers.

☐ Execute SDS Health Check procedures as specified in Appendix A.

9.2 SOAM Upgrade Execution (Manual and Automated Server Group)

Call My Oracle Support (MOS) and inform them of your plans to upgrade this system before executing this upgrade.

Refer to Appendix T for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix A. This check ensures the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if the upgrade can proceed with alarms.

WARNING!

If there are servers in the system, which are not in a Normal state, these servers should be brought to the **Normal** or **Application Disabled** state before the upgrade process starts. The sequence of upgrade is such that servers providing support services to other servers are upgraded first.

WARNING!

If a procedural step fails to execute successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact **MOS** for assistance before attempting to continue.

Procedure completion times shown are estimates. Times may vary due to differences in database size, user experience, and user preparation.

Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:

- Session banner information such as time and date.
- System-specific configuration information such as hardware locations, IP addresses, and hostnames.
- ANY information marked with **XXXX** or **YYYY**. Where appropriate, instructions are provided to determine what output should be expected in place of **XXXX** or **YYYY**.
- Aesthetic differences unrelated to functionality such as browser attributes: window size, colors, toolbars, and button layouts.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade marks the provided checkbox. For procedures, which are executed multiple times, a mark can be made below the checkbox (in the same column) for each additional iteration that the step is executed.

Retention of captured data is required as a future support reference if this procedure is executed by someone other than Oracle's Customer Care Center.

Note: For large systems containing multiple signaling network elements, it may not be feasible to apply the software upgrade to every network element within a single maintenance window.

9.2.1 Perform Health Check (SOAM Pre-Upgrade)

This procedure is part of software upgrade preparation and is used to determine the health and status of the entire SDS network and servers. This may be executed multiple times, but must also be executed at least once within the period of 24-36 hours before starting a maintenance window.

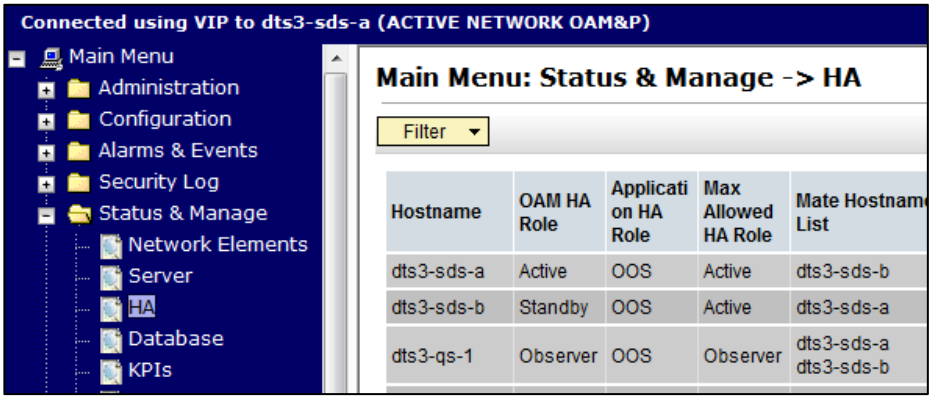
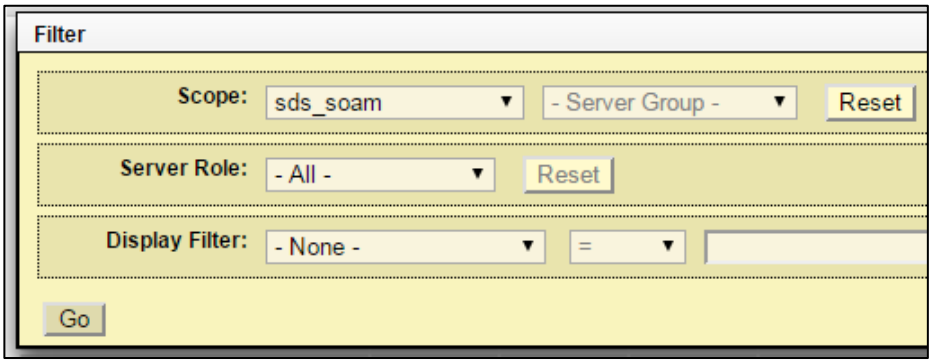
☐ Execute SDS Health Check procedures as specified in Appendix A.

9.2.2 Upgrade SOAM

The following procedure details how to upgrade SDS SOAM sites.

Caution When upgrading an SDS topology, it is permissible to upgrade multiple SOAM sites in parallel. However, every attempt should be made to avoid upgrading mated SOAM sites in the same maintenace window.

Procedure 9. Upgrade SOAM

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP (GUI)**: Record name of the **SOAM NE** site	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**.  3. Using the information provided in section 3.1.2 Logins, Passwords, and Site Information, record the name of the SOAM NE site. SOAM NE: _____
3. ☐	**Primary SDS NOAM VIP**: List servers	1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the primary SDS SOAM Network Element from the **Scope** field. 2. Click **Go**. 

Procedure 9. Upgrade SOAM

<table>
<tr><td>4. ☐</td><td>Primary SDS NOAM VIP: Identify servers and record server names</td><td>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.
<table><tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th></tr><tr><td>dts3-so-a</td><td>Active</td><td>OOS</td><td>Active</td><td>dts3-so-b</td><td>sds_soam</td><td>System OAM</td></tr><tr><td>dts3-so-b</td><td>Standby</td><td>OOS</td><td>Active</td><td>dts3-so-a</td><td>sds_soam</td><td>System OAM</td></tr><tr><td>dts3-dp-1</td><td>Active</td><td>OOS</td><td>Active</td><td></td><td>sds_soam</td><td>MP</td></tr></table>Record the names of SOAM NE site servers:
Active SOAM Server: _____
Standby SOAM Server: _____
DP 1 Server: _____ DP 6 Server: _____
DP 2 Server: _____ DP 7 Server: _____
DP 3 Server: _____ DP 8 Server: _____
DP 4 Server: _____ DP 9 Server: _____
DP 5 Server: _____ DP 10 Server: _____</td></tr>
<tr><td>5. ☐</td><td>Primary SDS NOAM VIP: Upgrade the Standby SOAM server</td><td>Upgrade the Standby SOAM server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.
Note: If using the Auto Upgrade option, SOAM servers are upgraded serially (standby then active).</td></tr>
<tr><td>6. ☐</td><td>Primary SDS NOAM VIP: Upgrade the Active SOAM server</td><td>Upgrade the Active SOAM server (as identified and recorded in step 4 of this procedure) using Appendix D Upgrade Server Administration on SDS 8.x.</td></tr>
<tr><td colspan="3">Note: Up to ½ of the installed DP servers at a SOAM site may be upgraded in parallel using the Upgrade Server option for each individual DP server as described in Appendix D Upgrade Server Administration on SDS 8.x.</td></tr>
<tr><td>7. ☐</td><td>Primary SDS NOAM VIP: Upgrade up to ½ of the installed DP servers in parallel</td><td>Upgrade up to ½ (for example, 1 of 2, 2 of 4, etc.) of the DP server(s) (as identified and recorded in step 4 of this procedure) in parallel usng the Upgrade Server option for each DP server as described in Appendix D Upgrade Server Administration on SDS 8.x.</td></tr>
<tr><td>8. ☐</td><td>Primary SDS NOAM VIP: Upgrade all remaining DP servers</td><td>Upgrade all remaining DP Servers in this SOAM NE site (as identified and recorded in step 4 of this procedure) in parallel usng the Upgrade Server option for each DP server as described in Appendix D Upgrade Server Administration on SDS 8.x..</td></tr>
</table>

9.2.3 Perform Health Check (SOAM Post Upgrade)

This procedure is part of software upgrade preparation and is used to determine the health and status of the SDS network and servers.

☐ Execute SDS Health Check procedures as specified in Appendix A.

9.3 Post Upgrade Procedures

This section contains procedures that are executed after all servers have been upgraded.

To update the SOAM VM profile to support 1 billion subscribers, follow the procedures in Appendix J Add New SOAM Profile on Existing VM.

9.3.1 Accept the Upgrade

The upgrade needs either to be accepted or rejected before any subsequent upgrades may be performed in the future.

Event ID: 32532 Server Upgrade Pending Accept/Reject displays for each server until **Accept** or **Reject** is performed.

STOP

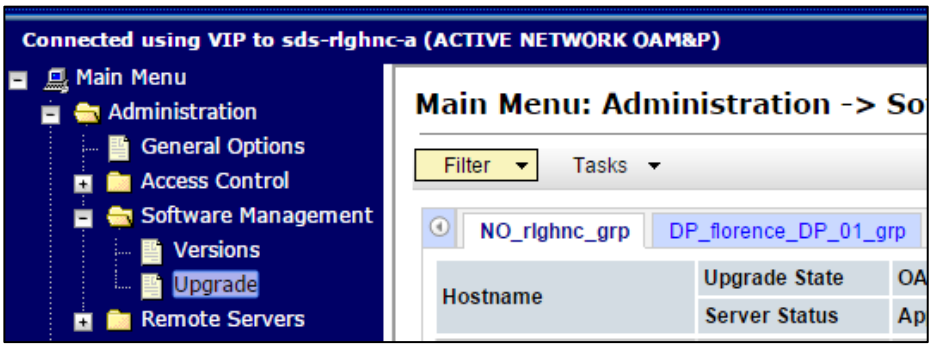
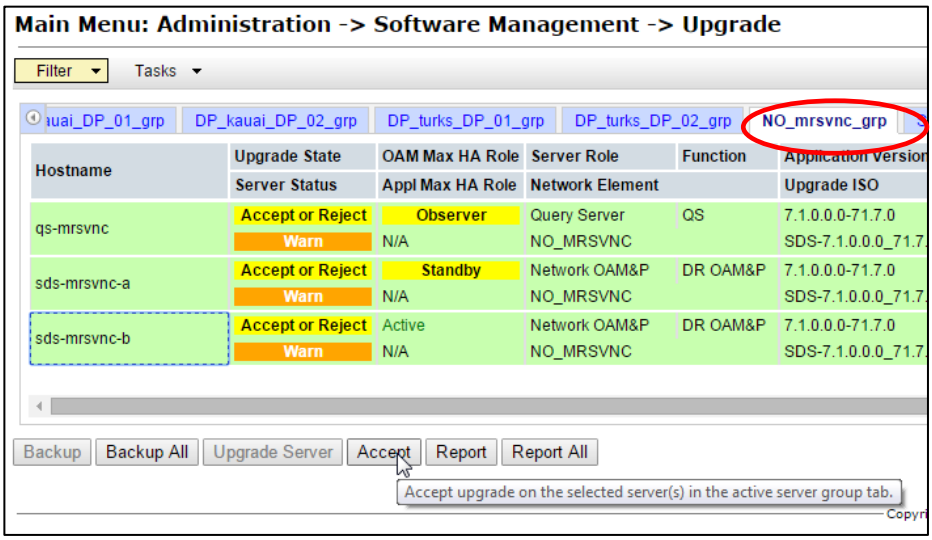
An upgrade should be **Accepted** only after all servers in the **SDS** topology have successfully completed upgrade to the target release.

The user should also be aware that **Upgrade Acceptance prevents any possibility of backout to the previous release!!!**

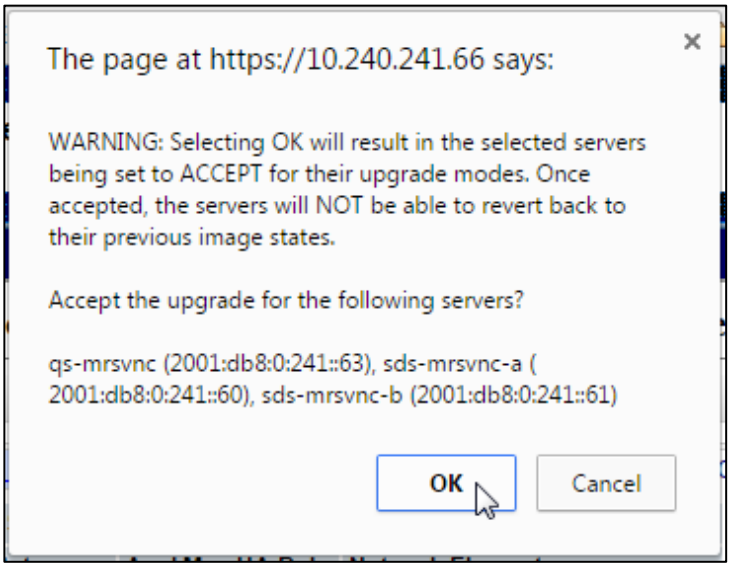
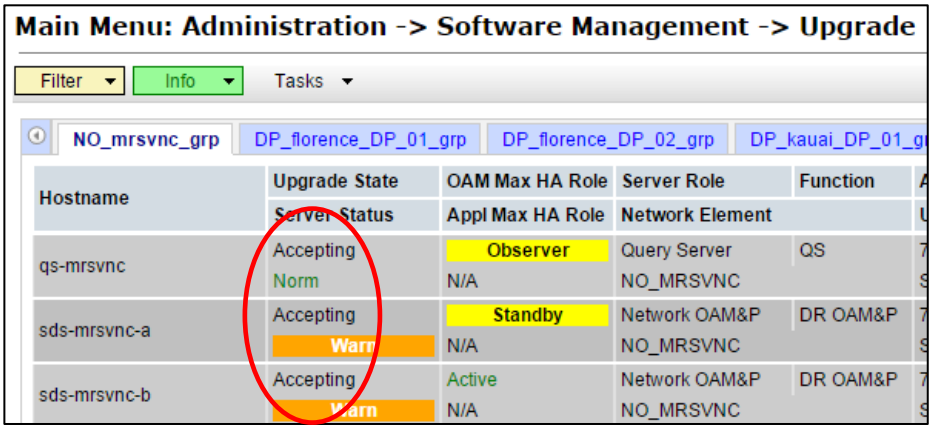
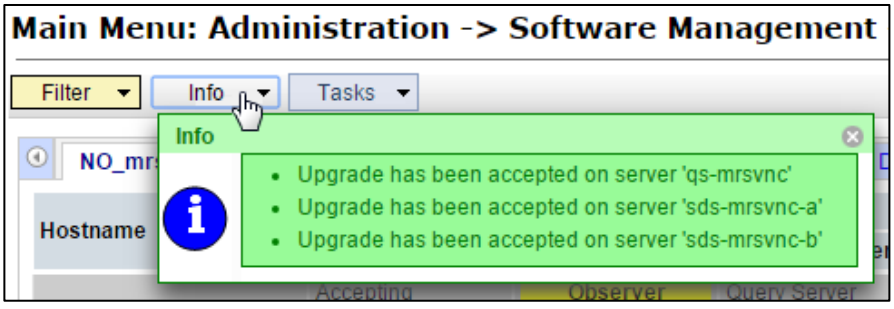
Procedure 10. Accept the Upgrade

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

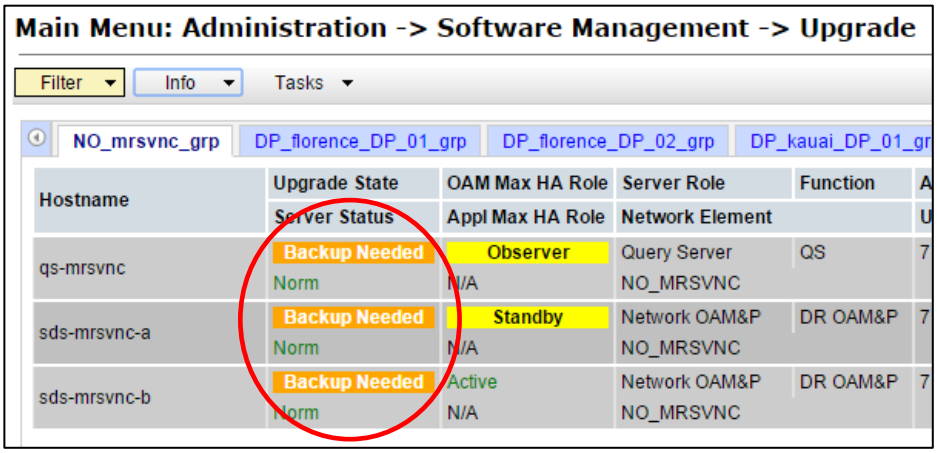
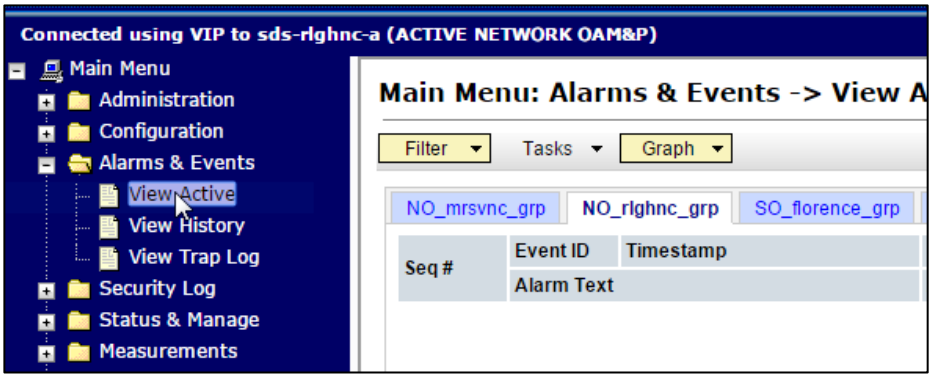
Procedure 10. Accept the Upgrade

2. ☐	**Primary SDS NOAM VIP**: Accept the upgrade	1. Navigate to **Administration > Software Management > Upgrade**.  2. Select the Server Group tab containing the server(s) to **Accept** the upgrade. 3. Press and hold the **Ctrl** key to select multiple server(s) in the server group. 4. Click **Accept**. ***Note***: If you are upgrading from a release prior to SDS 7.1 and upgrade to release 7.1 or later, DNS port needs to be enabled. Refer to Appendix N for more information. 

Procedure 10. Accept the Upgrade

3. ☐	**Primary SDS NOAM VIP**: Monitor status	Click **OK** to confim.  The **Upgrade State** changes to **Accepting**.  The banner displays an **Upgrade has been accepted on . . .** each server. 

Procedure 10. Accept the Upgrade

4. ☐	**Primary SDS NOAM VIP**: Monitor status	The **Upgrade State** changes to **Backup Needed**.  ***Important***: The **Backup Needed Upgrade State** is expected to remain until the next software upgrade is performed. **DO NOT** re-run COMCOL backups except when directed to do so during the upgrade process.
	WARNING	Accepting of upgrade may take several minutes. Do not try to accept again or an improper upgrade accepting states in the "Server Upgrade States" column on the Upgrade Administration screen.
5. ☐	**Primary SDS NOAM VIP**: Repeat for each remaining server group	Repeat steps 2 — 4 of this procedure for each additional Server Group tab until the upgrade has been accepted on all servers in the SDS topology.
6. ☐	**Primary SDS NOAM VIP**: Verify upgrade acceptance	1. Navigate to **Alarms & Events > View Active**.  2. Verify the **Event ID: 32532 Server Upgrade Pending Accept/Reject** alarm no longer displays for any server in the SDS topology.

9.3.2 SOAM VM Profile Update

C-class deployments are required to update the SOAM VM profile after upgrading to SDS release 7.2 and later. The updated profile allocates additional resources required to support expanded subscriber capacity. The profile update is to be applied only after the upgrade has been accepted (Procedure 10).

- The SOAM VM profile update applies only to SDS 7.2 and later.
- The SOAM VM profile update can be applied only after the upgrade to SDS 7.2/7.3/8.0/8.1 has been accepted.
- The SOAM VM profile update does not apply to VE-DSR and cloud deployments.

Appendix J is an independent procedure and may be executed at any time after the upgrade has been accepted. It is recommended that the customer schedule a separate maintenance window for implementation of the new SOAM VM profile.

☐ To update the SOAM VM profile to support 1 billion subscribers, execute Appendix J; otherwise, skip this step.

10. Recovery Procedures

Upgrade procedure recovery issues should be directed to the Oracle's Tekelec Customer Care. Before executing any of these procedures, refer to Appendix T for information on contacting My Oracle Support (MOS). Persons performing the upgrade should be familiar with these documents.

Recovery procedures are covered under the Disaster Recovery Guide. Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.

WARNING

It is recommended to contact My Oracle Support (MOS) before performing these backout procedures.

Note: Refer to Appendix T for information on contacting My Oracle Support (MOS).

Backout procedures cause traffic loss!

Note: These recovery procedures are provided for the backout of an upgrade only (for examplle, for the backout from a failed target release to the previously installed release).

Backout of an initial installation is not supported!

Caution

SDS Upgrade

If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes.

10.1 Backout Setup

Identify IP addresses of all servers that need to be backed out.

1. Navigate to **Administration > Software Management > Upgrade**.
2. Based on the **Application Version** column, identify all the hostnames that need to be backed out.
3. Navigate to **Configuration > Servers**.
4. Identify the IMI IP addresses of all the hostnames identified in step 2. These are required to access the server when performing the backout.

The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedure causes traffic loss. Since all possible reasons cannot be predicted ahead of time, contact My Oracle Support (MOS) as stated in the Warning box above.

Note: Verify the two backup archive files created in using Procedure 4 Full Database Backup (PROV and COMCOL Env for All Servers are present on every server that is to be backed-out.

These archive files are located in the **/var/TKLC/db/filemgmt** directory and have different filenames from other database backup files.

The filenames have the following format:

- Backup.<application>.<server>.FullDBParts.<role>.<date_time>.UPG.tar.bz2
- Backup. <application>.<server>.FullRunEnv.<role>.<date_time>.UPG.tar.bz2

10.2 Perform Backout

The following procedures to perform a backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. Contact the Oracle Customer Care Center as stated in the **Warning** box above to identify if all corrective setup steps have been taken.

During the backout, the servers may have some or all of the following expected alarms until the server is completely backed out, but are not limited to Event IDs:

- Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
- Alarm ID = 31109 (Topology config error)
- Alarm ID = 31114 (DB Replication over SOAP has failed)
- Alarm ID = 31106 (DB Merge To Parent Failure)
- Alarm ID = 31134 (DB replication to slave failure)
- Alarm ID = 31102 (DB replication from master failure)
- Alarm ID = 31282 (HA management fault)

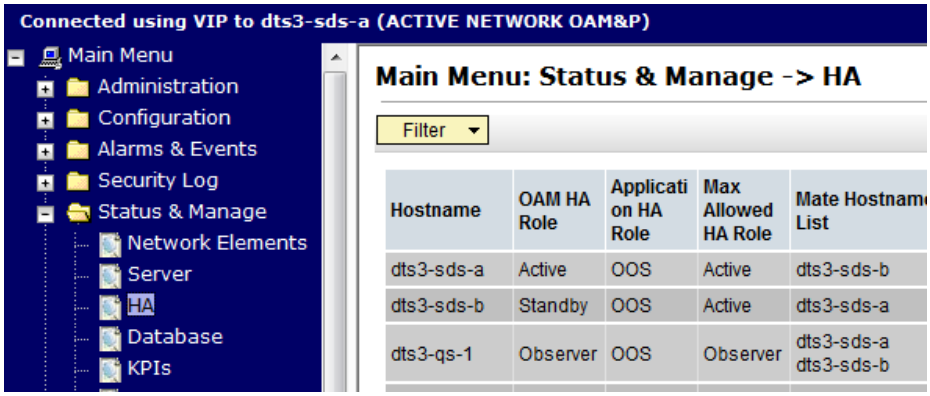
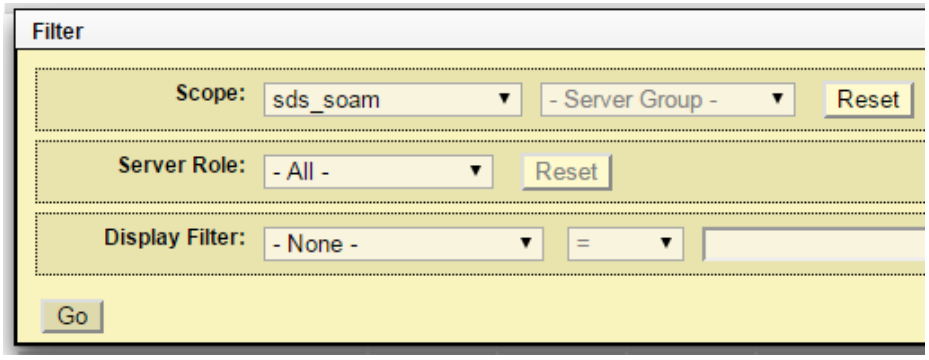
10.2.1 Back Out the SOAM

The following procedure details how to perform software backout for servers in the SOAM NE.

Procedure 11. Back Out the SOAM

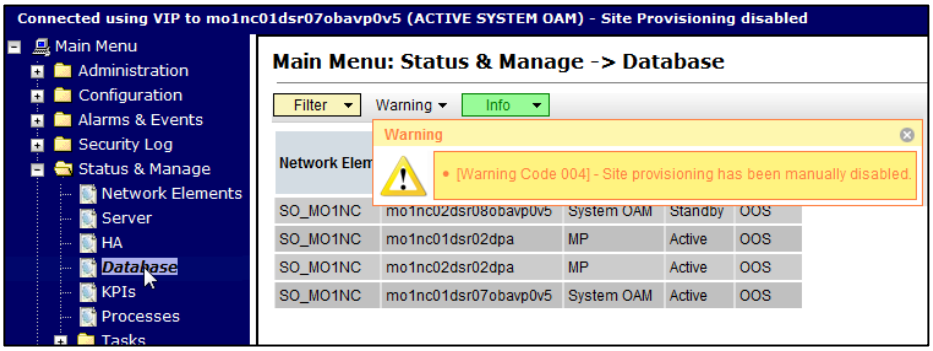
1. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 11. Back Out the SOAM

2. ☐	**Primary SDS NOAM VIP (GUI)**: Record name of the **SOAM NE** site	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**. 
3. ☐	**Primary SDS NOAM VIP**: List servers	1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the primary SDS SOAM Network Element from the **Scope** field. 2. Click **Go**. 
4. ☐	**Primary SDS NOAM VIP**: Identify servers and record server names	Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server. Record the names of SOAM NE site servers: Active SOAM Server: _____ Standby SOAM Server: _____ DP 1 Server: _____ DP 6 Server: _____ DP 2 Server: _____ DP 7 Server: _____ DP 3 Server: _____ DP 8 Server: _____ DP 4 Server: _____ DP 9 Server: _____ DP 5 Server: _____ DP 10 Server: _____

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role
dts3-so-a	Active	OOS	Active	dts3-so-b	sds_soam	System OAM
dts3-so-b	Standby	OOS	Active	dts3-so-a	sds_soam	System OAM
dts3-dp-1	Active	OOS	Active		sds_soam	MP

Procedure 11. Back Out the SOAM

5. ☐	**Primary SDS NOAM VIP**: Downgrade DP 1 Server	Downgrade DP 1 server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server.
6. ☐	**Primary SDS NOAM VIP**: Downgrade all remaining DP servers in this SOAM NE site	Downgrade all remaining DP servers in serial or parallel (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server. Repeat this step until all DP servers requiring the downgrade within this SOAM NE site have been backed out.
7. ☐	**Primary SDS NOAM VIP**: Downgrade the Standby SOAM server	Downgrade the **Standby SOAM** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**. During the backout, the servers may have the following expected alarms: • Alarm ID = 31114 (DB replication over SOAP has failed) • Alarm ID = 31282 (HA management fault)
WARNING		Do not proceed with the next step until steps 5 through 7 of this procedure have been successfully completed.
8. ☐	**Primary SDS NOAM VIP**: Downgrade the Active SOAM Server	Downgrade the **Active SOAM** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**.
9. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
10. ☐	**SOAM VIP (GUI)**: Enable site provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Site Provisioning**. 3. Click **OK** to confirm.

Procedure 11. Back Out the SOAM

11. ☐	**SOAM VIP**: Log out	Click **Logout** to log out of the SOAM GUI.
12. ☐	**Primary SDS NOAM VIP**: Execute downgrade for the remaining SOAM NE site(s)	Repeat all above steps of this procedure for the remaining SOAM NE site(s) (as identified and recorded in section 3.1.2) until all SOAM NE site(s) requiring the downgrade have been backed out.
13. ☐	**Primary SDS NOAM VIP**: Execute health check at this time only if no other servers require the downgrade; otherwise, proceed with the next backout procedure	Execute Health Check procedures (Post Backout) as specified in Appendix A, if backout procedures have been completed for all required servers.

10.2.2 Back Out the DR SDS NOAM

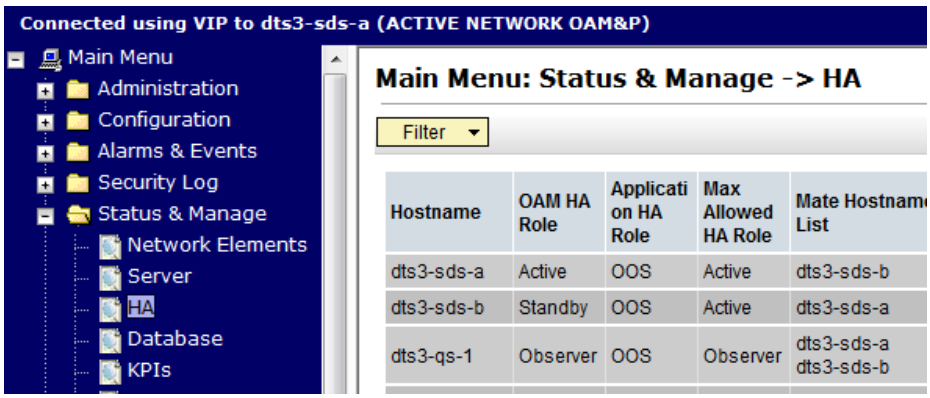
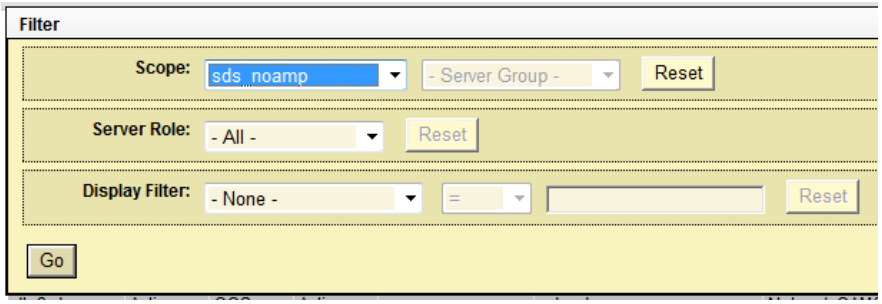
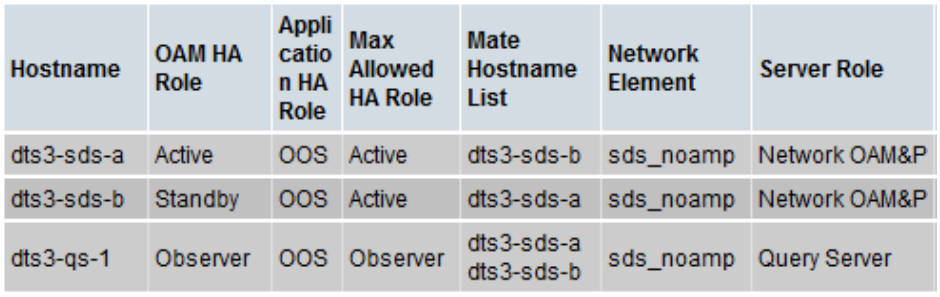
The following procedure details how to perform software backout for servers in the DR SDS NOAM NE.

WARNING The order of the backout for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 9. See section 3.7 for more details before proceeding.

Procedure 12. Back Out the DR SDS NOAM

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 12. Back Out the DR SDS NOAM

2. ☐	**Primary SDS NOAM VIP**: Record name of **DR SDS NE** site	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**. 
3. ☐	**Primary SDS NOAM VIP**: List servers	1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the DR SDS Network Element from the **Scope** field. 2. Click **Go**. 
4. ☐	**Primary SDS NOAM VIP**: Identify servers and record server names	Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.  Record the names of primary DR SDS NE site servers: Active DR SDS NOAM: _____ Standby DR SDS NOAM: _____ DR SDS Query Server (if equipped): _____
5. ☐	**Primary SDS NOAM VIP**: Downgrade DR SDS Standby server	Downgrade the **Standby DR SDS NOAM** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**.

Procedure 12. Back Out the DR SDS NOAM

WARNING		Do not proceed with the next step until step 5 of this procedure has been successfully completed.
Note: The next 2 steps of this procedure may be executed in parallel using the **Upgrade Server** option.		
6. ☐	**Primary SDS NOAM VIP**: Downgrade DR SDS Query server	Downgrade the **DR SDS Query** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**.
7. ☐	**Primary SDS NOAM VIP**: Downgrade Active DR SDS server	Downgrade the **Active DR SDS** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**. ***Important***: This causes an HA activity failover to the mate DR SDS server. This happens a couple minutes after initiating the upgrade.
8. ☐	**Primary SDS NOAM VIP**: Execute health check at this time only if no other servers require the downgrade; otherwise, proceed with the next backout procedure	Execute Health Check procedures (Post Backout) as specified in Appendix A, if backout procedures have been completed for all required servers.

10.2.3 Back Out the Primary SDS NOAM

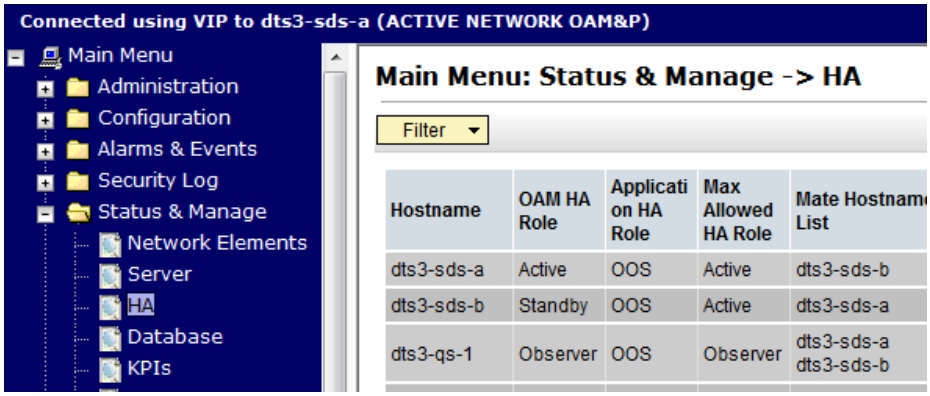
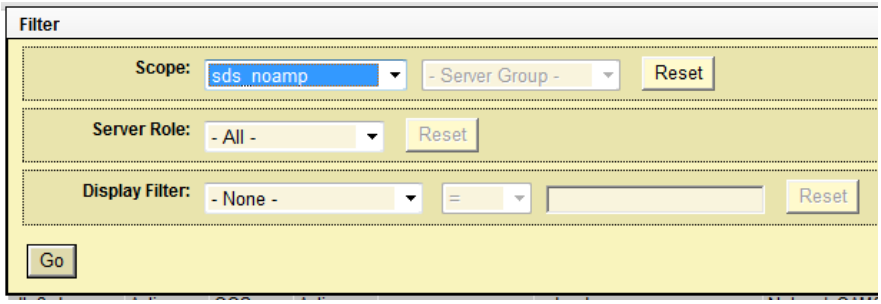
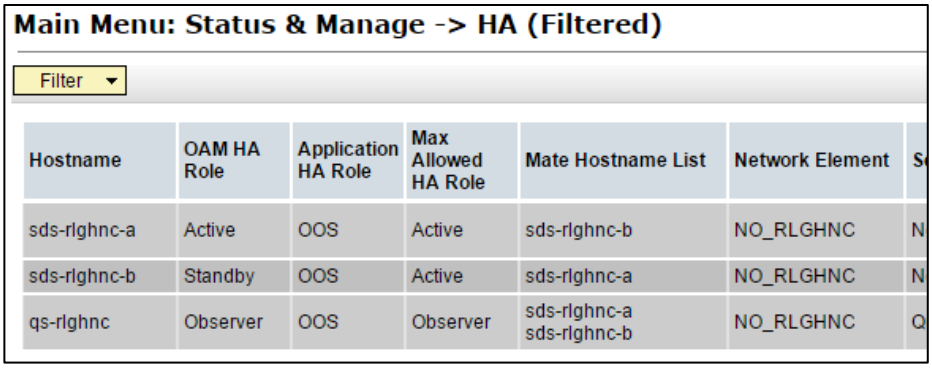
The following procedure details how to perform software backout for servers in the primary SDS NOAM NE.

WARNING	The order of the backout for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 9. See section 3.7 for more details before proceeding.

Procedure 13. Back Out Primary SDS NOAM

1. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in **Appendix A**.

Procedure 13. Back Out Primary SDS NOAM

2. ☐	**Primary SDS NOAM VIP**	1. Navigate to **Status & Manage > HA**. 2. Click **Filter**. 
3. ☐	**Primary SDS NOAM VIP**: Locate the primary SDS NOAM NE	1. Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the primary SDS Network Element from the **Scope** field. 2. Click **Go**. 
4. ☐	**Primary SDS NOAM VIP**: Identify servers and record server names	Identify each server by **Hostname**, **Server Role**, and **OAM HA Role** and record the name of each server.  Active Primary SDS NOAM: _____ Standby Primary SDS NOAM: _____ Primary SDS Query Server (if equipped): _____

Procedure 13. Back Out Primary SDS NOAM

5. ☐	**Primary SDS NOAM VIP**: Downgrade the **Standby Primary SDS NOAM** server	Downgrade **Standby Primary SDS NOAM** server (as identified and recorded in step 4 of this procedure) using **Appendix E Back Out a Single Server**.

6. ☐	**Primary SDS NOAM VIP (CLI)**: Access the active primary SDS NOAM	Use the VIP address to log into the active primary SDS NOAM with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`
		`[admusr@sds-rlghnc-a ~]$`

Procedure 13. Back Out Primary SDS NOAM

<table>
<tr><td>7. ☐</td><td>Primary SDS NOAM VIP: Verify status</td><td>1. Verify the DbReplication status is Active for the Standby Primary SDS NOAM and Query Server, if equipped.
<pre>[admusr@sds-rlghnc-a ~]$ sudo irepstat -w
-- Policy 0 ActStb [DbReplication]
AA To sds-rlghnc-b   Active 0 0.25 1%R 0.05%cpu 47B/s
AA To qs-rlghnc   Active 0 0.25 1%R 0.05%cpu 56B/s
AA To sds-mrsvnc-a   Active 0 0.50 1%R 0.04%cpu 47B/s
AB To kauai-sds-SO-b   Active 0 0.50 1%R 0.04%cpu 63B/s
AB To florence-sds-SO-a Active 0 0.51 1%R 0.03%cpu 65B/s
AB To turks-sds-SO-b   Active 0 0.50 1%R 0.04%cpu 65B/s
irepstat (8 lines) (h)elp</pre>
2. If a DbReplication status is Audit is received, then repeat the command until Active is returned.

Important: Do not proceed until the status is Active.
Check Replication is showing Active for Standby Primary SDS NOAM, Query Server, Active DR SDS NOAM and Standby DR SDS NOAM (if equipped).
3. Repeat the step until the status is Active for all the mentioned servers.

Important: If a DbReplication status is received as Audit or some other value for these servers, repeat this step until a status of Active is returned. Servers are:
• Standby Primary SDS NOAM
• Query Server
• Active DR SDS NOAM
• Standby DR SDS NOAM
4. If required, contact My Oracle Support (MOS) for any assistance.</td></tr>
<tr><td>8. ☐</td><td>Primary SDS NOAM VIP: Exit CLI</td><td>Exit the CLI for the Active Primary SDS NOAM.
<pre>[admusr@sds-rlghnc-a filemgmt]$ exit
logout</pre></td></tr>
<tr><td colspan="3">Note: The next 2 steps of this procedure may be executed in parallel.</td></tr>
<tr><td>9. ☐</td><td>Primary SDS NOAM VIP: Downgrade Primary SDS Query server</td><td>Downgrade Primary Query server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server.</td></tr>
<tr><td>10. ☐</td><td>Primary SDS NOAM VIP: Downgrade Primary SDS Active server.</td><td>Downgrade Active Primary SDS NOAM server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server.
Important: This causes an HA activity failover to the mate primary SDS NOAM server. This occurs within a few minutes of initiating the upgrade.</td></tr>
</table>

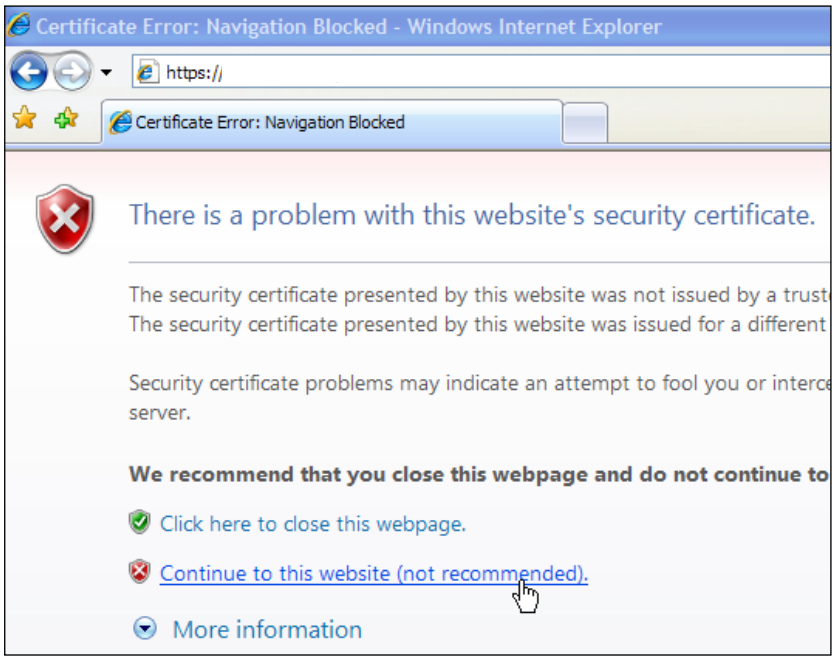
Procedure 13. Back Out Primary SDS NOAM

11. ☐	Allow system to auto-clear temporary alarm states	Wait up to 10 minutes for Alarms associated with server backout to auto-clear. ***Important***: If PDB Relay was recorded as **Enabled** in **Appendix E**, step 7 then Event 14189 (pdbRelay Time Lag) may persist for several hours post upgrade. This alarm can safely be ignored and automatically clears when the PDBI (HLRR) queue catches up with real-time replication.
12. ☐	Execute Health Check	Execute Health Check procedures (Post Backout) as specified in Appendix A, if downgrade procedures have been completed for all required servers.

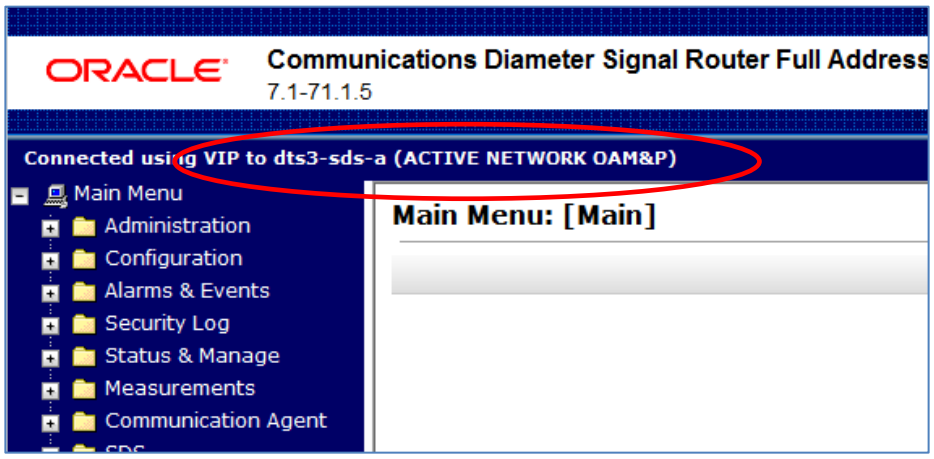
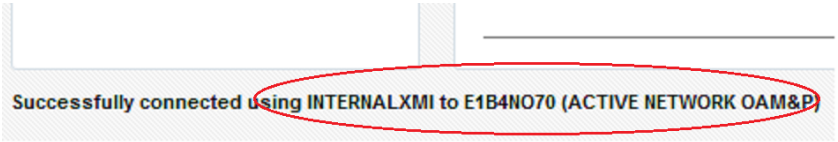
Appendix A Access the OAM GUI Using the VIP (NOAM/SOAM)

This procedure describes how to access and log into the NOAM GUI.

Procedure 14. Access the OAM GUI Using the VIP (NOAM/SOAM)

1. ☐	**OAM VIP (GUI)**: Log into the OAM site	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the XMI virtual IP address (VIP) assigned to the OAM site (primary SDS site or SOAM site). If a certificate error is received, click on the **Continue to this website (not recommended)** link.  ***Note***: Not applicable for cloud deployments

Procedure 14. Access the OAM GUI Using the VIP (NOAM/SOAM)

2. ☐	**OAM VIP (GUI)**: Login	Login using the default user and password.
3. ☐	**OAM VIP**: Verify connection to the active OAM server.	Verify the browser is using the **VIP** connected to the active OAM server.  If source release is 8.x, the banner is at the bottom of the screen.  ***Note***: The message may show the connection to either a **NETWORK OAM&P** or a **SYSTEM OAM** depending on the selected NE.

Appendix B Health Check Procedures

This procedure is part of software upgrade preparation and is used to determine the health and status of the SDS network and servers.

Note: If syscheck fails on any server during Pre-Upgrade Checks or in early checks stating that "cpu: FAILURE:: No record in alarm table for FAILURE!", please see Appendix Q Workaround to Resolve Syscheck Error for CPU Failure.

If the **31201 - Process Not Running** alarm displays, for instance, as cmsoapa, then execute Appendix R Workaround to Fix cmsoapa Restart to solve this issue.

WARNING

For release 7.2 only: if the **restoretemp** directory is not created in the **/var/TKLC/db/filemgmt** path on each server, then create it using this command:

```
$ sudo mkdir -p /var/TKLC/db/filemgmt/restoretemp
```

```
$ sudo chown awadmin:awadm
/var/TKLC/db/filemgmt/restoretemp
```

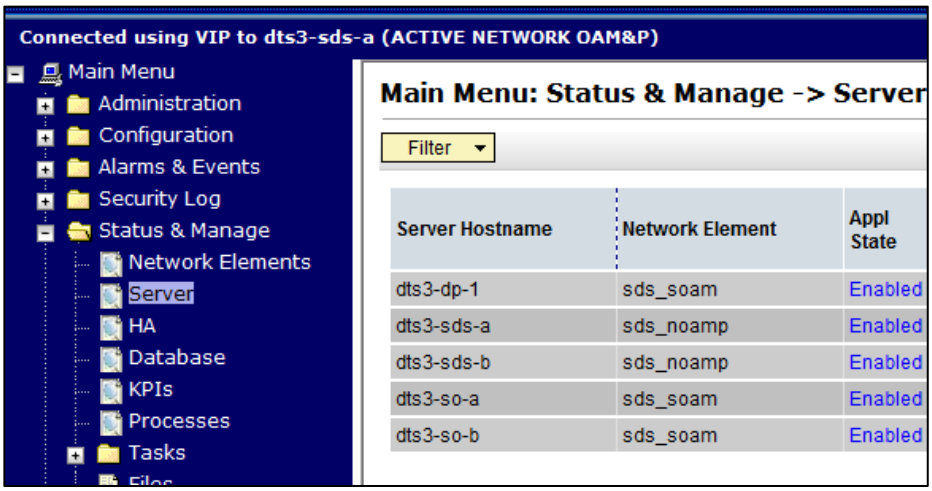
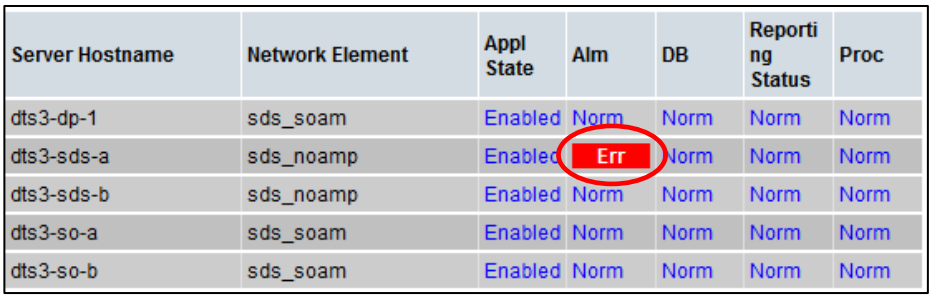
```
$ sudo chmod 775
/var/TKLC/db/filemgmt/restoretemp
```

Skipping this step leads to an upgrade failure.

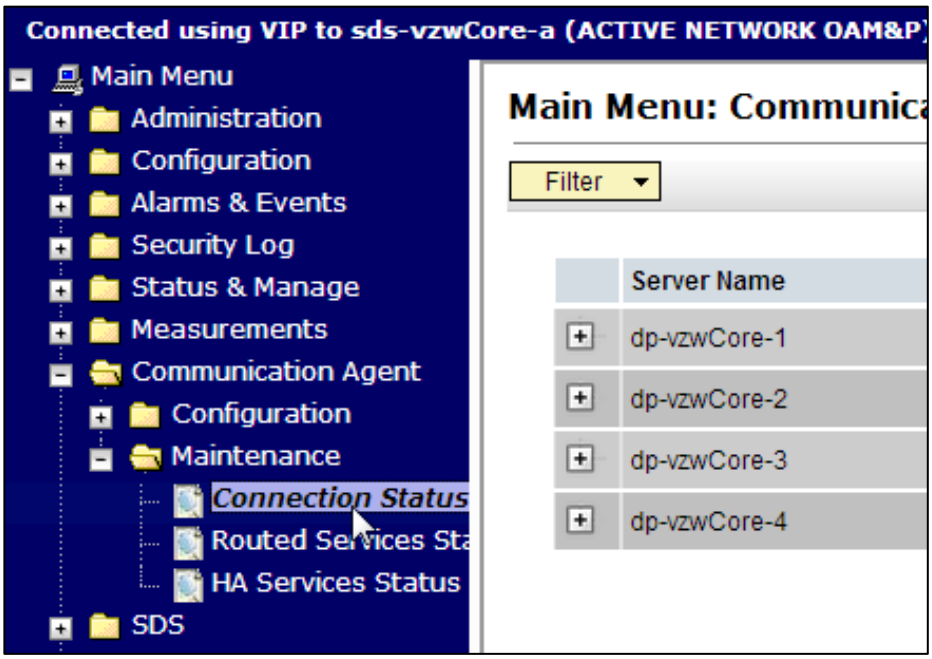
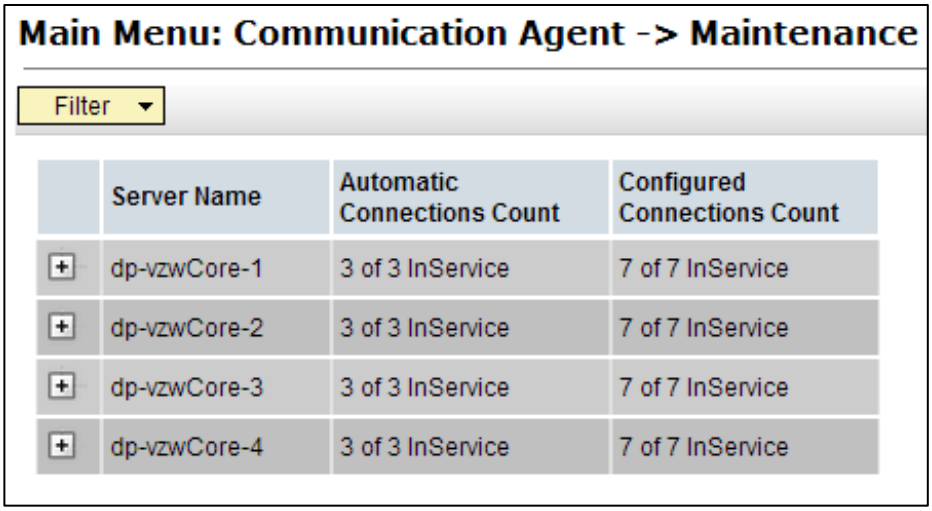
Procedure 15. Health Check Procedure

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

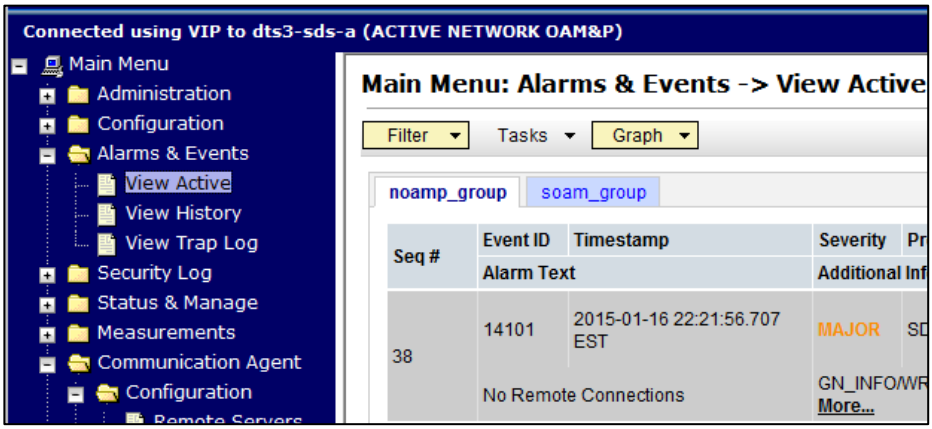
Procedure 15. Health Check Procedure

2. ☐	**Primary SDS NOAM VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify Server Status is Normal (**Norm**) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).  If any other server status displays, it appears in a colored box. ***Note***: Other server states include Err, Warn, Man, and Unk. ***Note***: Post-Upgrade, upgraded servers have an **Alm** status of **Err** due to the **Event ID (s): 32532 Server Upgrade Pending Accept/Reject** expected alarm. This alarm displays until the upgrade is accepted and may be ignored at this time. ***Note***: During any time of upgrade in case 31149- DB Late Write Nonactive alarm is seen, please ignore it. This alarm does not have any effect on any functionality. If 31201 - Process Not Running alarm is getting raised for Instance as cmsoapa then execute Appendix R Workaround to Fix cmsoapa Restart to solve this issue.

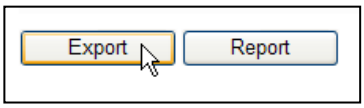
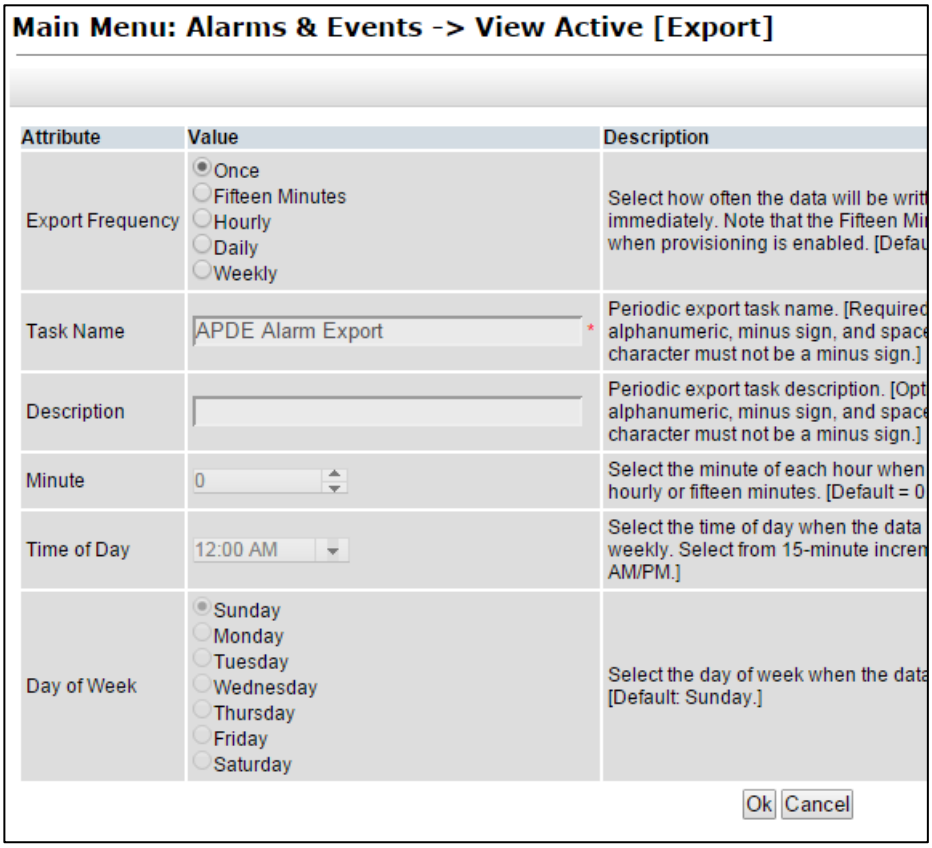
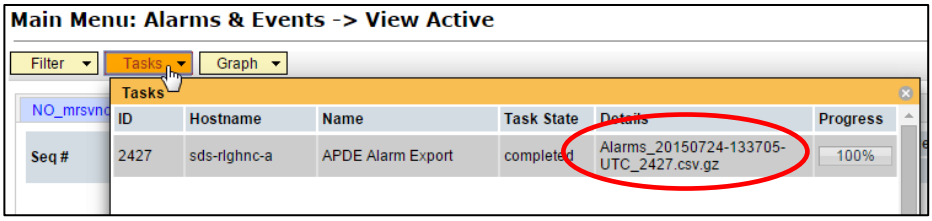
Procedure 15. Health Check Procedure

3. ☐	**Primary SDS NOAM VIP**: Verify connection counts	1. Navigate to **Communication Agent > Maintenance > Connection Status**.  2. Verify all **Connection Counts** show equivalent counts (that is, n of n InService for Automatic or y of y InService for Configured)  ***Note***: **DPs** show a **Configured Connections Count** of **1 of 2 InService** for Active/Standby configurations. This is normal and can be ignored.

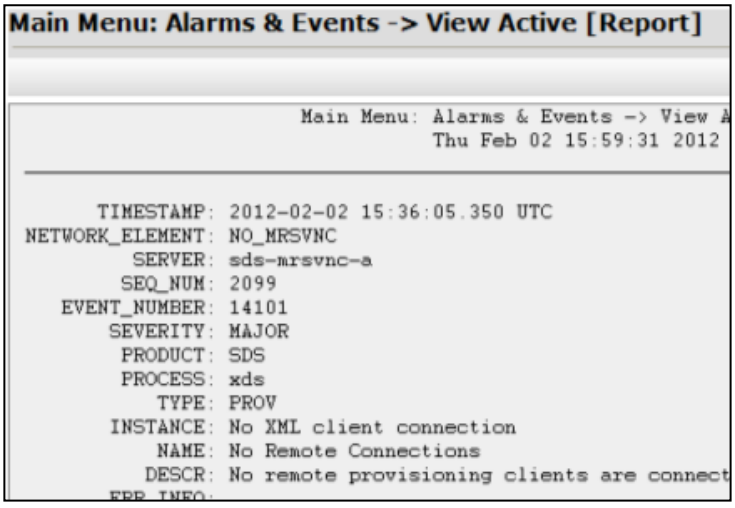
Procedure 15. Health Check Procedure

4. ☐	**Primary SDS NOAM VIP**: View alarm status	Navigate to **Alarms & Events > View Active**.  **When viewing pre-upgrade status**, if any alarms are present, STOP and contact My Oracle Support (MOS) for assistance before attempting to continue. **When viewing post-upgrade status**: Active NO server may have the following expected alarms: **Alarm ID = 10075 (Application processes have been manually stopped)** Servers that still have replication disabled have the following expected alarm: **Alarm ID = 31113 (Replication Manually Disabled)** The following alarms may also be seen: **Alarm ID = 10010 (Stateful database not yet synchronized with mate database)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)** Following alarms can be ignored during the upgrade: **Alarm ID = 31109 (Topology Config Error)** **Alarm ID = 31282 (HA Management Fault)** **Alarm ID = 31283 (Lost Communication with server)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 10009 (Config and Prov DB not yet synchronized)** ***Note***: If Alarm 10009 persists after the upgrade, reboot the server once using the `sudo init 6` command on the effected server. These alarms may display until all the NOAM and DR-NOAM servers upgrade has been completed.

Procedure 15. Health Check Procedure

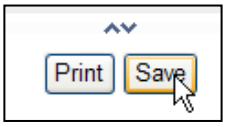
5. ☐	**Primary SDS NOAM VIP**: Create **Alarms and Events** report	1. Click **Export**.  2. Click **OK**.  The name of the exported alarms CSV file displays in the Tasks tab. 

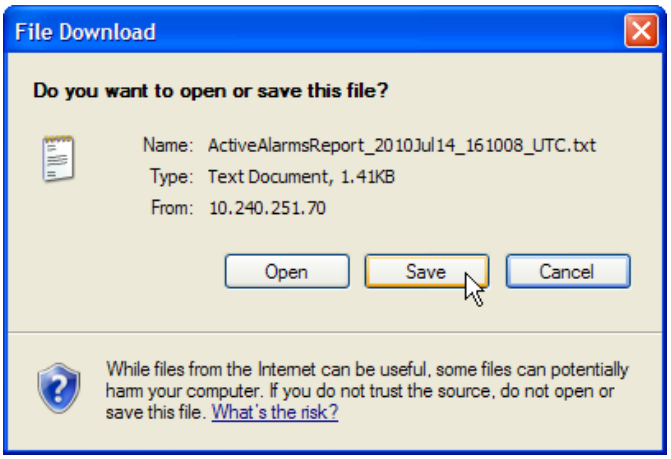
Procedure 15. Health Check Procedure

6. ☐	**Primary SDS NOAM VIP**: Record the filenames	Record the filenames of alarm CSV files. Example: Alarms<yyyymmdd>_<hhmmss>.csv Pre ISO Administration: Alarms _____ - _____ .csv.gz Post ISO Administration: Alarms _____ - _____ .csv.gz Pre Primary NOAM Upgrade (MW1): Alarms _____ - _____ .csv.gz Post DR NOAM Upgrade (MW1): Alarms _____ - _____ .csv.gz Pre SOAM Upgrade (MW2): Alarms _____ - _____ .csv.gz Post SOAM Upgrade (MW2): Alarms _____ - _____ .csv.gz Pre SOAM Upgrade (MW3): Alarms _____ - _____ .csv.gz Post SOAM Upgrade (MW3): Alarms _____ - _____ .csv.gz Pre SOAM Upgrade (MW4): Alarms _____ - _____ .csv.gz Post SOAM Upgrade (MW4): Alarms _____ - _____ .csv.gz Pre SOAM Upgrade (MW5): Alarms _____ - _____ .csv.gz Post SOAM Upgrade (MW5): Alarms _____ - _____ .csv.gz
7. ☐	**Primary SDS NOAM VIP**: Save the **Alarms and Events** report	1. Click **Report**. 

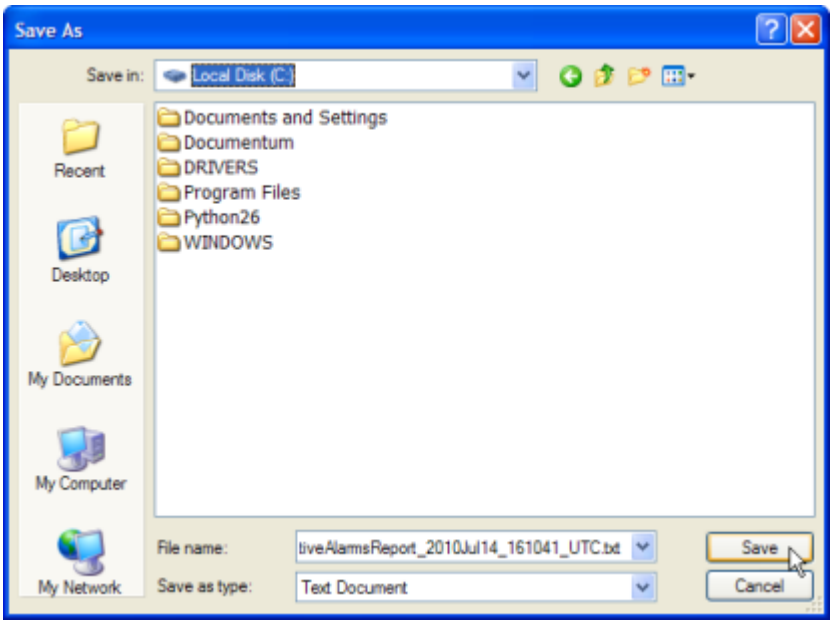
Procedure 15. Health Check Procedure

2. Click **Save** on the **Alarms and Events** report and click **Save** on the File Download screen.

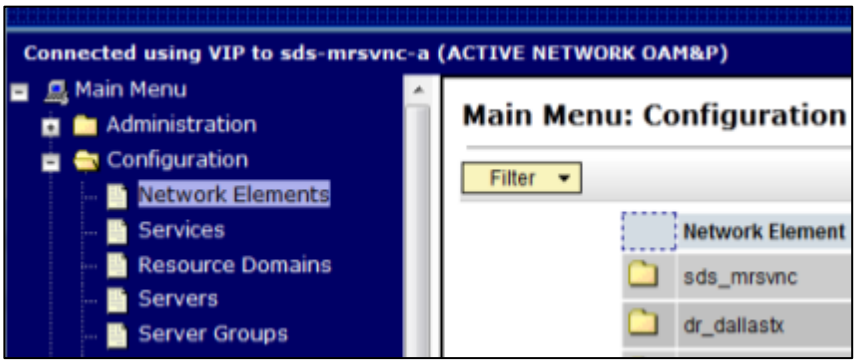
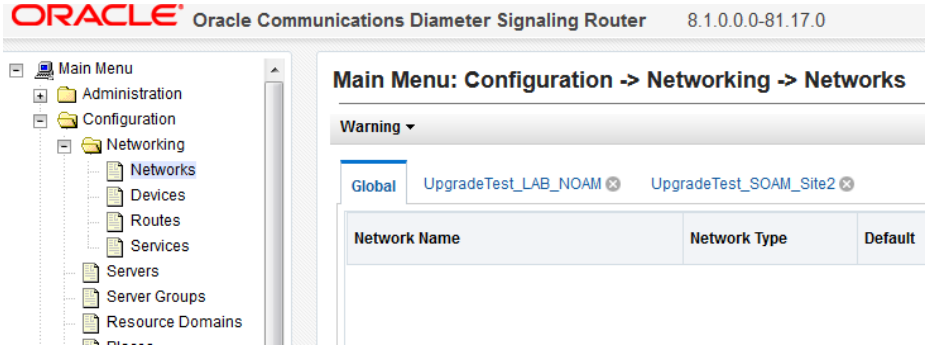
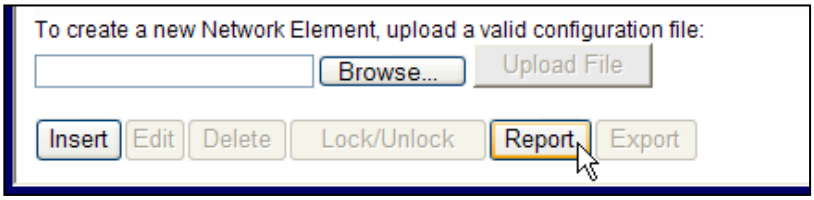
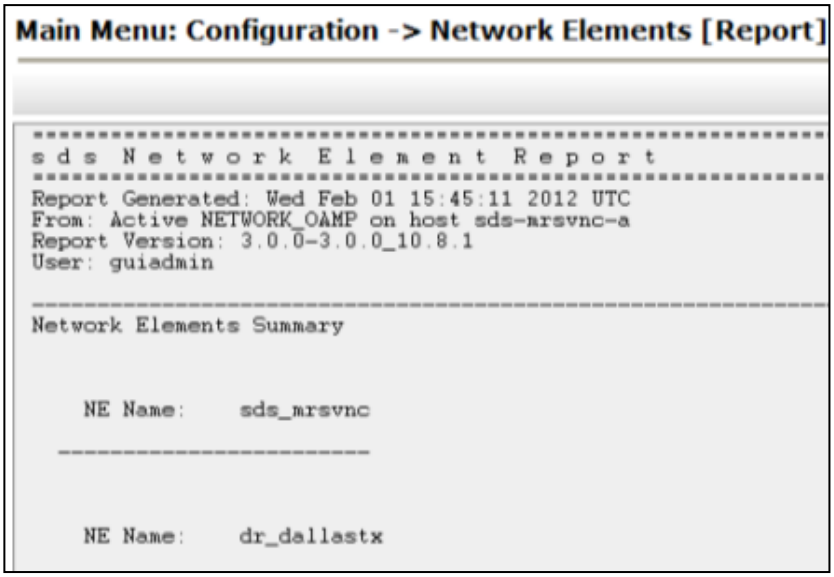




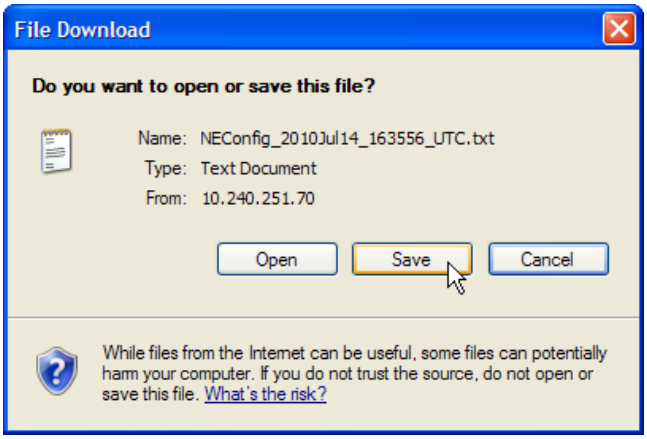
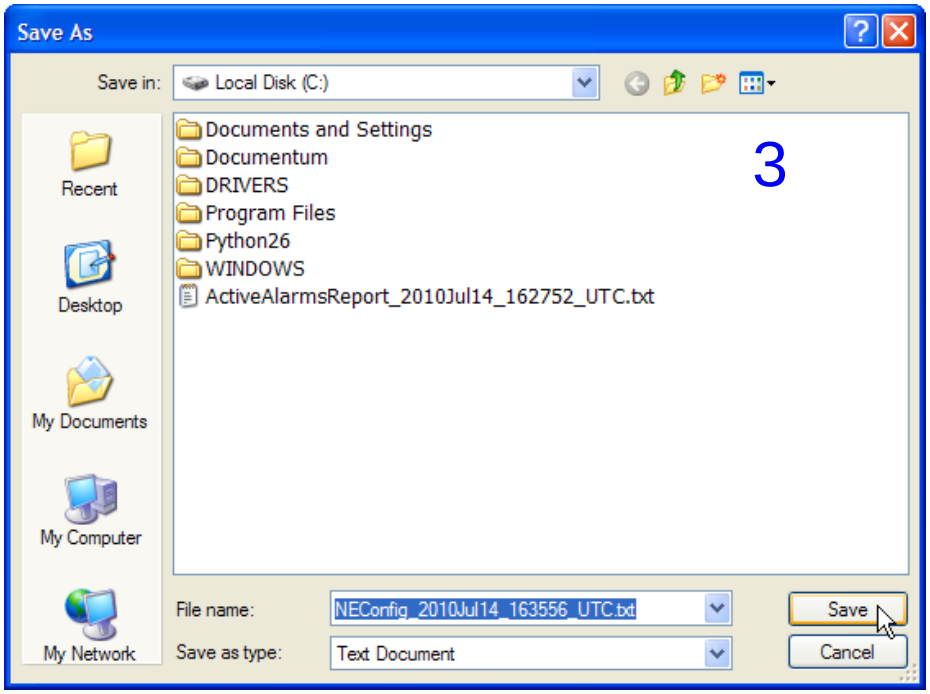
3. Select a directory on a local disk drive to store the active **Alarms and Events** report and click **Save**.



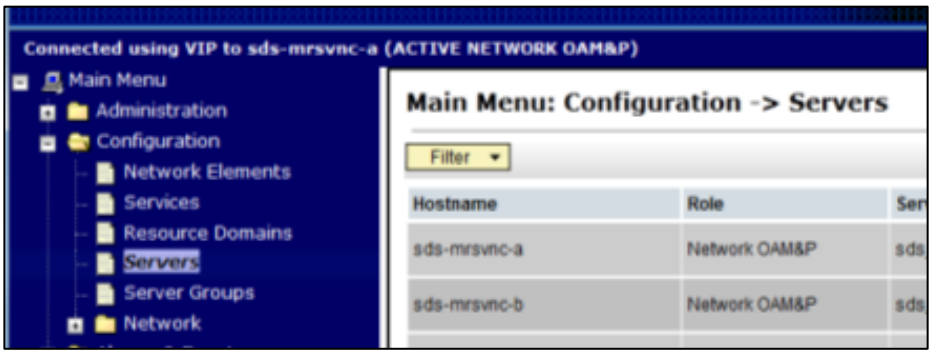
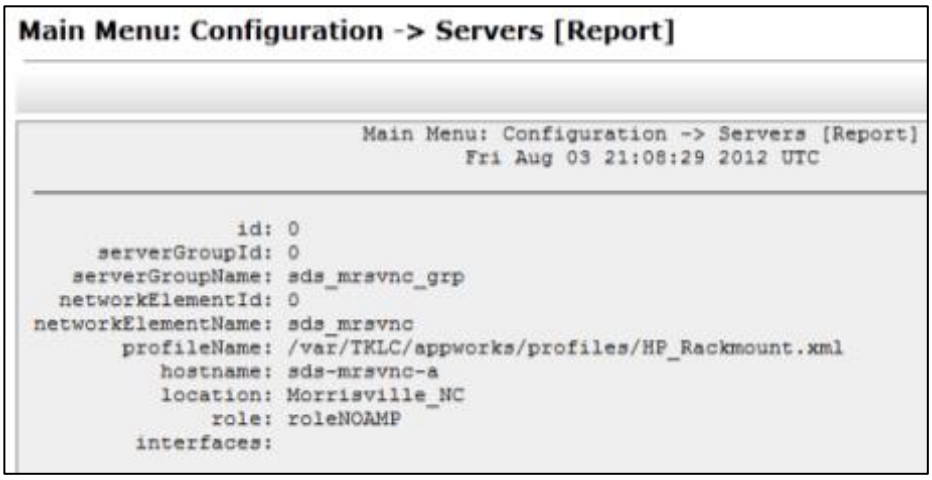
Procedure 15. Health Check Procedure

8. ☐	**Primary SDS NOAM VIP**: Create **Network Element** report	1. Before 8.x, navigate to **Configuration > Network Elements**.  If the release is 8.x, navigate to **Configuration > Networking > Networks**.  2. Click **Report**.  The **Network Element Report** is generated. 

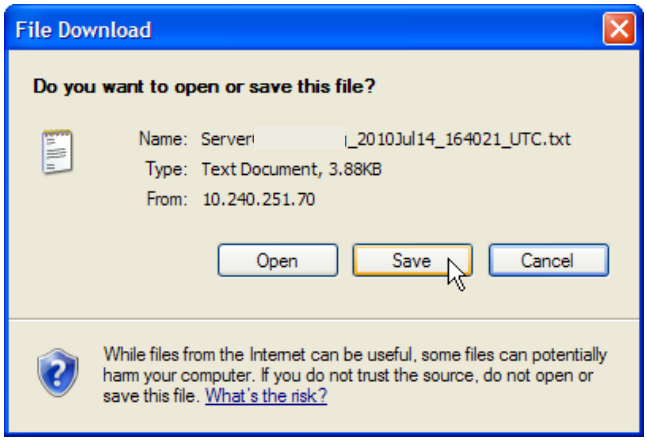
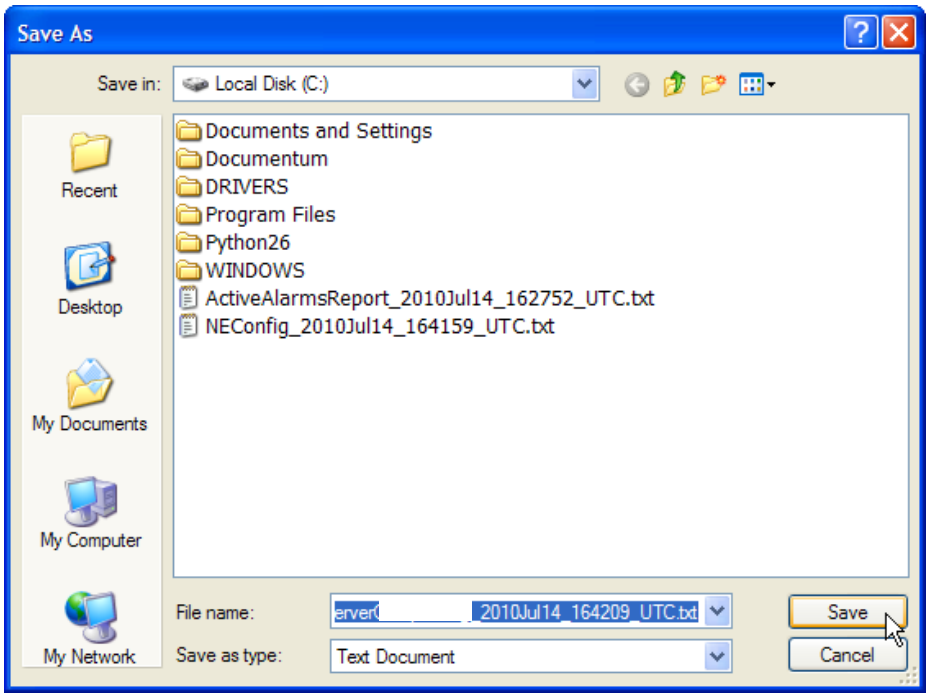
Procedure 15. Health Check Procedure

9. ☐	**Primary SDS NOAM VIP**: Save the **Network Element** report	1. Click **Save** on the **Network Element** report and click **Save** on the File Download screen.  2. Select a directory on a local disk drive to store the **Network Element** report and click **Save**. 

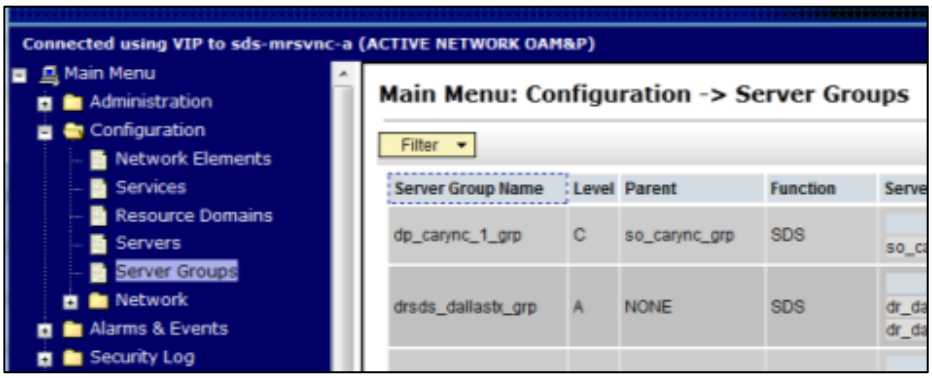
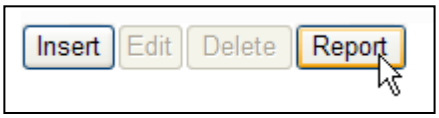
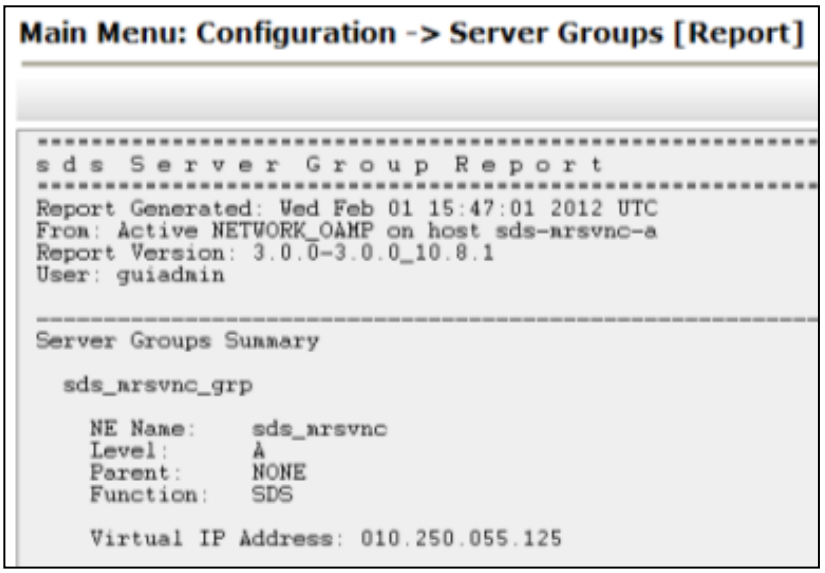
Procedure 15. Health Check Procedure

10. ☐	**Primary SDS NOAM VIP**: Create **Servers** the report	1. Navigate to **Configuration > Servers**.  2. Click **Report**. 

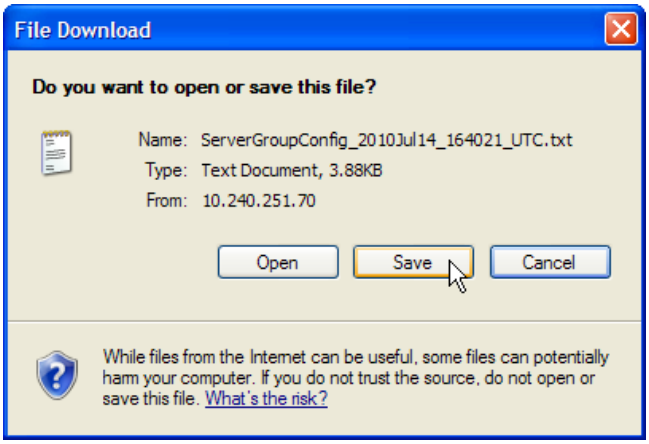
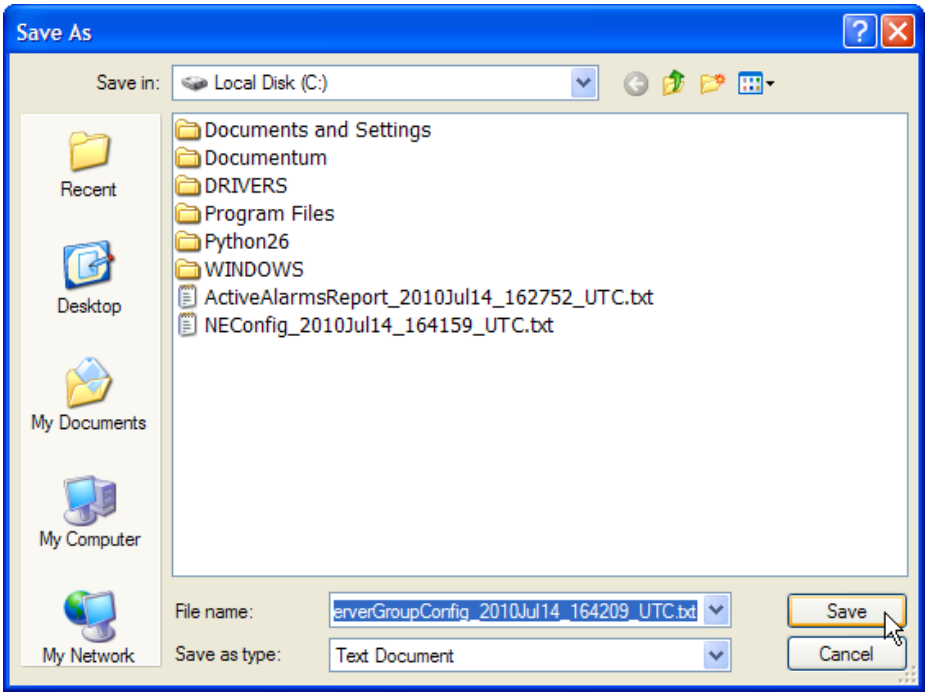
Procedure 15. Health Check Procedure

11. ☐	**Primary SDS NOAM VIP**: Save the **Servers** report	1. Click **Save** on the **Servers** report and click **Save** on the File Download screen.  2. Select a directory on a local disk drive to store the **Servers** report and click **Save**. 

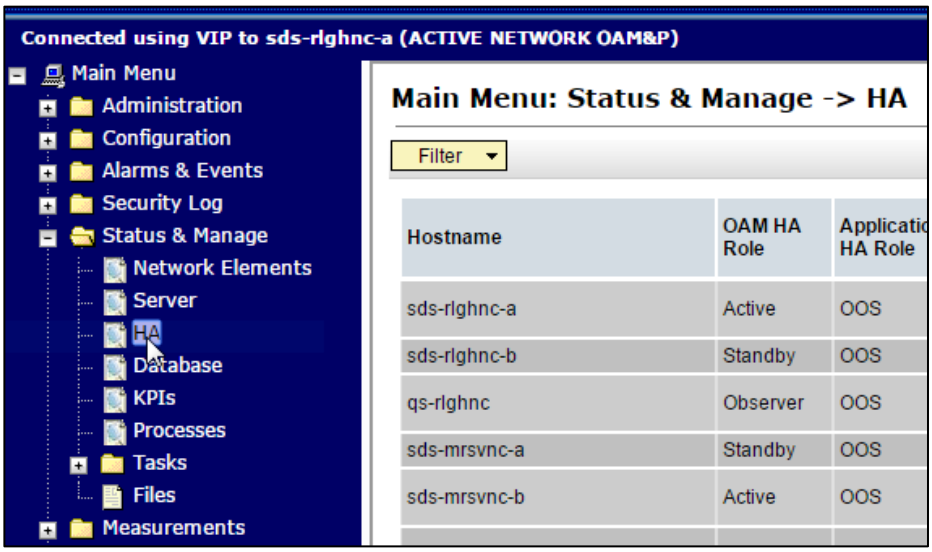
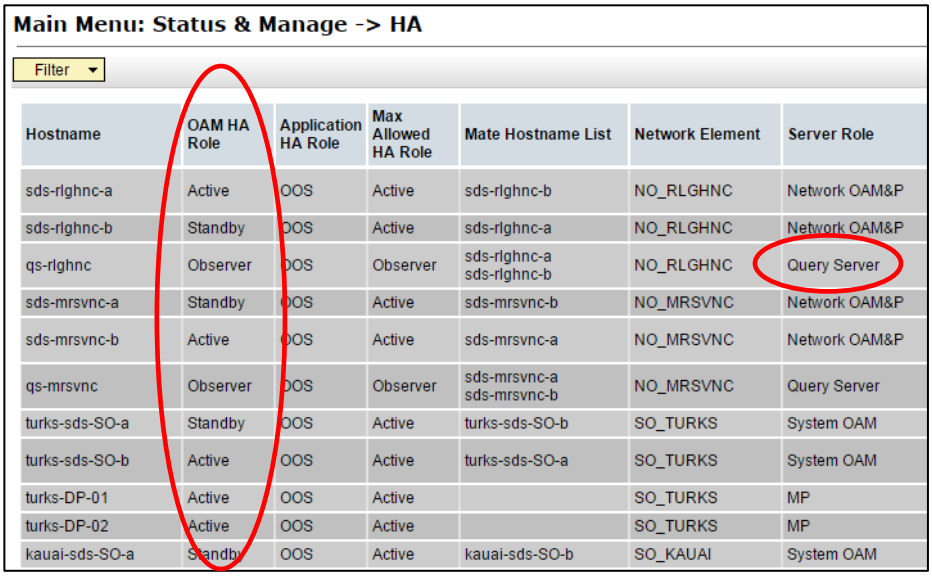
Procedure 15. Health Check Procedure

12. ☐	**Primary SDS NOAM VIP**: Create **Server Goups** the report	1. Navigate to **Configuration > Server Groups**.  2. Click **Report**.  

Procedure 15. Health Check Procedure

13. ☐	**Primary SDS NOAM VIP**: Save the **Server Groups** report	1. Click **Save** on the **Server Groups** report and click **Save** on the File Download screen.  2. Select a directory on a local disk drive to store the active **Server Groups** report and click **Save**. 
14. ☐	Provide saved report files to My Oracle Support (MOS)	If executing this procedure as a pre- or post-upgrade health check (HC1/HC2/HC3), provide the saved report files to Oracle's Customer Care Center for proper health check analysis: • Active **Alarms and Events** report (Appendix A, step 7) • **Network Elements** report (Appendix A, step 9) • **Server** report (Appendix A, step 11) • **Server Group** report (Appendix A, step 13)

Procedure 15. Health Check Procedure

15. ☐	**Primary SDS NOAM VIP**: Verify OAM HA Role status	1. Navigate to **Status & Manage > HA**.  2. Verify the **OAM HA Role** for all servers shows either **Active** or **Standby**.  ***Note***: An **OAM HA Role** shown as **Observer** is allowed when the server role is **Query Server**. 3. Verify the **OAM HA Role** for all remaining servers.
16. ☐	**Primary SDS NOAM VIP:**	Verify the **"OAM HA Role"** for all remaining servers on the **[Main Menu: Status & Manage → HA]** screen. • Scroll thru each page of the **[Main Menu: Status & Manage → HA]** screen until the **"OAM HA Role"** for has been verified for all servers in the topology.

Procedure 15. Health Check Procedure

17. ☐	Firewall configuration for source release 7.1.x	**Firewall configuration for source release 7.1.x** Validate the DNS server before upgrading when the source release for upgrade is 7.1.x. Refer to Appendix S to enable the DNS port. **Firewall configuration for source release 7.2.x** From DSR release 7.2, the DNS feature replaces the **/etc/hosts** mechanism. If your firewall prohibits the DNS rndc dumpdb traffic from passing between the geo-redundant sites, the DSR software will not work well after upgrading from 7.1.x to 8.1. To fix this, change the network firewall settings to allow the **rndc dumpdb** traffic to pass between the geo-redundant sites.

Appendix C Upgrade Server Administration on SDS 7.x

STOP

Unless executing parallel upgrades, DO NOT PROCEED until the **Upgrade State** is **Accept or Reject**.

For release 7.2only: if the **restoretemp** directory is not created in the **/var/TKLC/db/filemgmt** path on each server, then create it using this command:

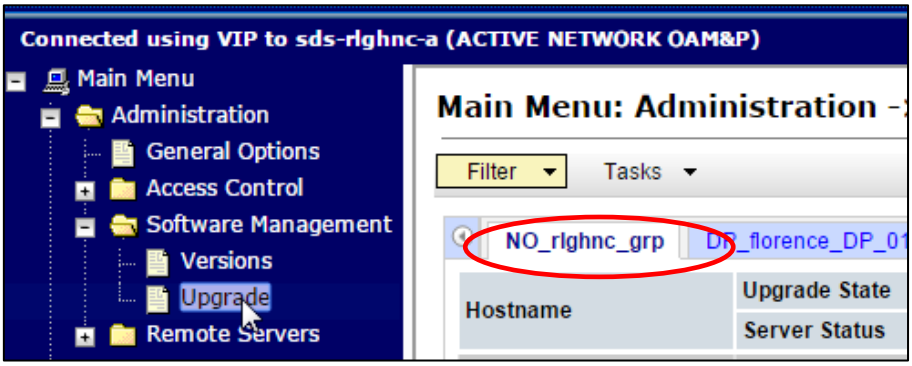
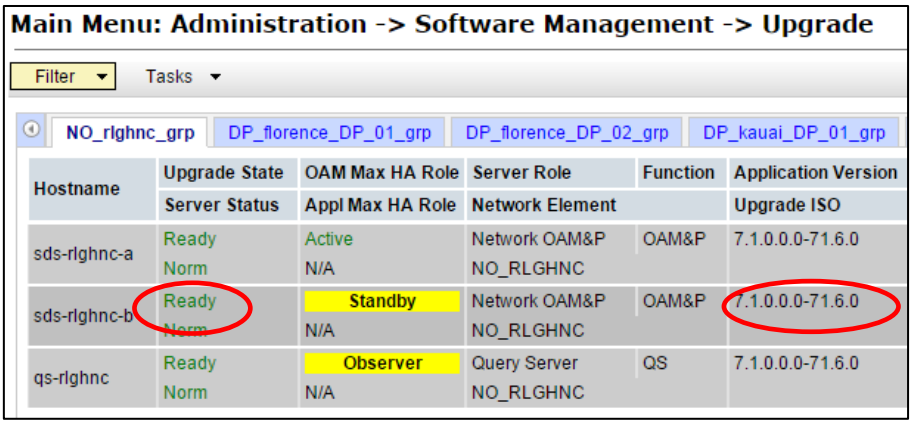
```
$ sudo mkdir -p /var/TKLC/db/filemgmt/restoretemp
$ sudo chown awadmin:awadm
/var/TKLC/db/filemgmt/restoretemp
$ sudo chmod 775 /var/TKLC/db/filemgmt/restoretemp
```

If an upgrade failure is experienced (that is, Upgrade State = Failed), refer to Appendix I Recover from a Failed Upgrade.

Procedure 16. Upgrade Server Administration on SDS 7.x

1. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 16. Upgrade Server Administration on SDS 7.x

2. ☐	**Primary SDS NOAM VIP**: Verify status and application version	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the Server Group tab for the server(s) to be upgraded.  3. Verify the **Upgrade Status** displays as **Ready** for the server(s) to be upgraded. 4. Verify the **Application Version** for the server(s) is the source software release version. 

CAUTION

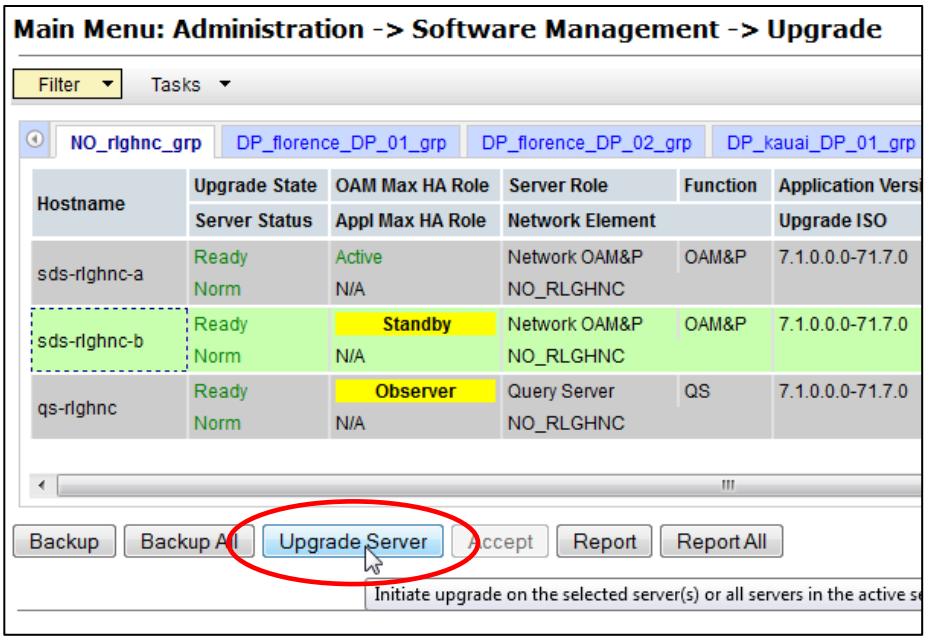
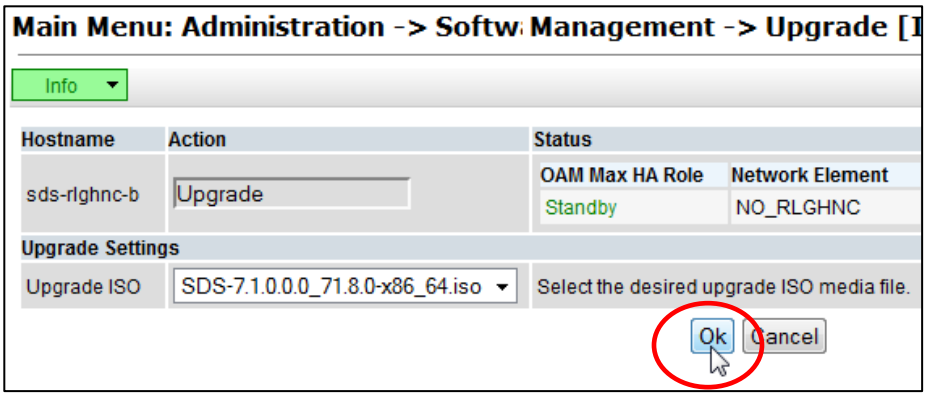
If executing Server Group **Auto Upgrade**, then SKIP to step 4 of this procedure.

- Allowed for DR NOAM, SOAM, and DP server groups only!

If executing Single Server (or multi-selected) upgrade, then continue with the next step of this procedure.

- Required for primary NOAM and DP server groups.

Procedure 16. Upgrade Server Administration on SDS 7.x

3. ☐	This step is for single server (or multi-selected) upgrade only! **Primary SDS NOAM VIP**: Upgrade server(s)	1. Press and hold the **Ctrl** key to select multiple servers that need to be upgraded. 2. Click **Upgrade Server**.  3. Select the Upgrade ISO file to use for the upgrade. 4. Click **OK**.  5. Go to step 5 of this procedure. ***Note***: During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all NOAM and DR-NOAM server upgrades have been completed. ***Note***: If Alarm 10009 persists after the upgrade, reboot the server once using the `sudo init 6` command on the effected server.
4. ☐	This step is for Server Group **Auto Upgrade**	1. Click **Auto Upgrade**. ***Note***: Do NOT select any servers with this option.

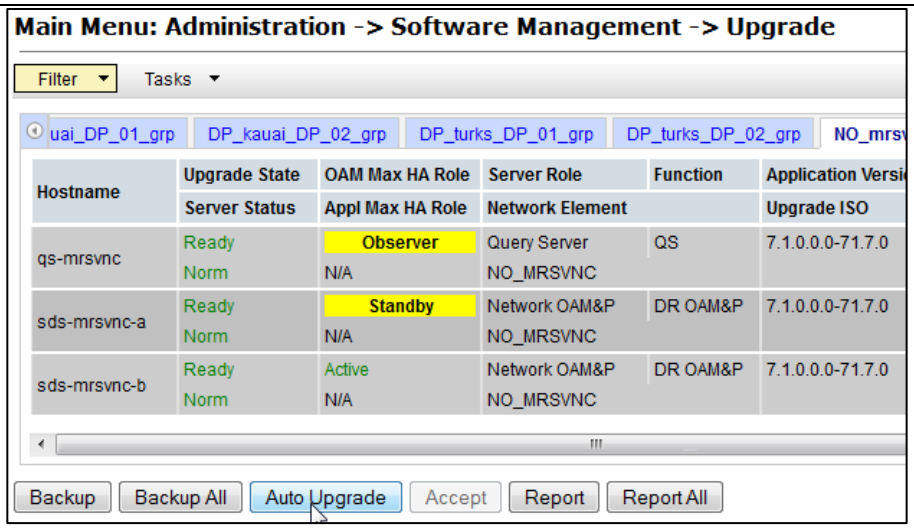
Procedure 16. Upgrade Server Administration on SDS 7.x

only!

WARNING!

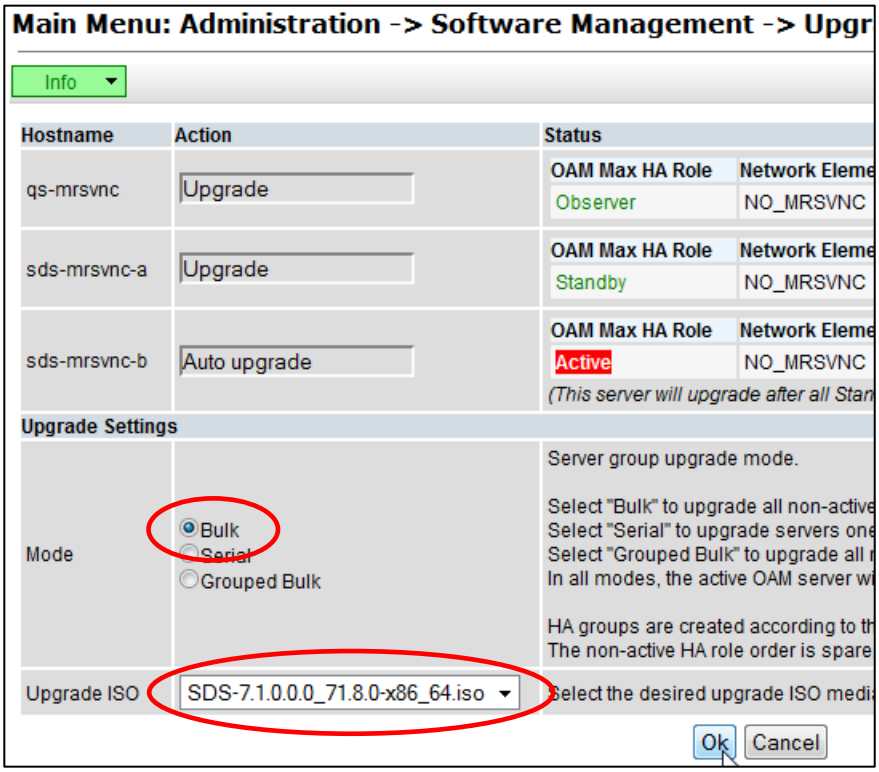
DO NOT use the **Auto Upgrade** option when upgrading the primary SDS NOAM server group.

Primary SDS NOAM VIP: Upgrade servers



2. Select the **Bulk** option.
3. Select the Upgrade ISO file to use for the upgrade.
4. Click **OK**.

   All non-active servers are upgraded first (for example, standby, query, etc.).

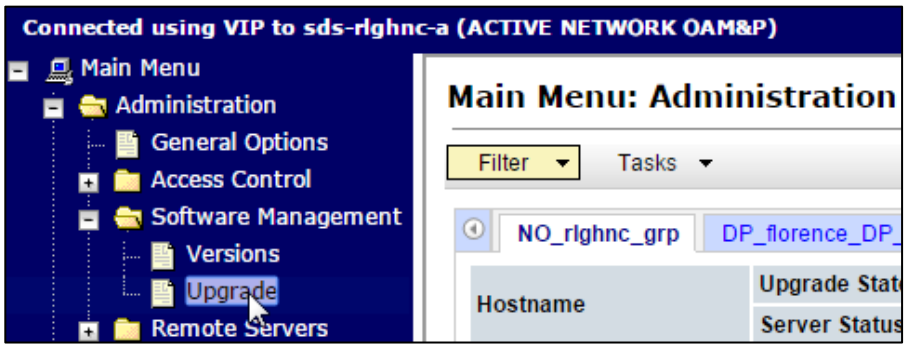
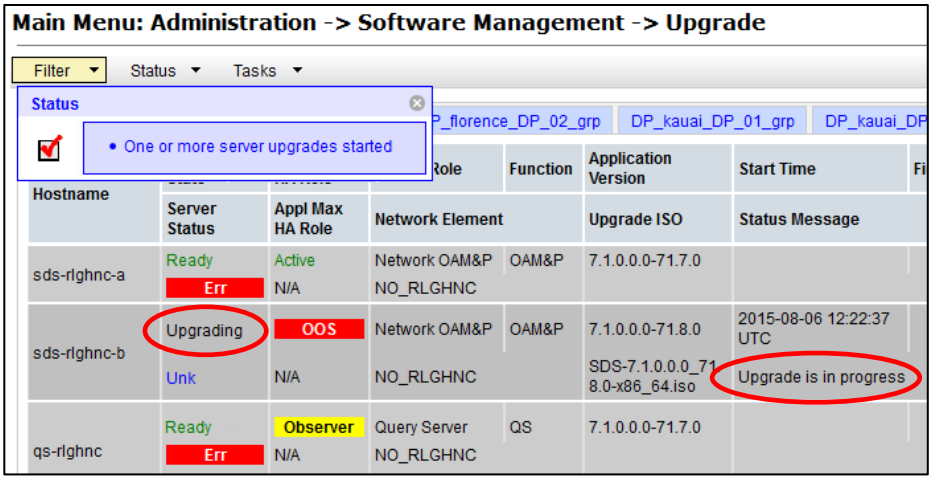


Note: During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all the NOAM and DR-NOAM servers have been upgraded.

Procedure 16. Upgrade Server Administration on SDS 7.x

	CAUTION	If upgrading the formerly active primary SDS NOAM server (that is, 2nd NOAM to be upgraded), then continue with the next step of this procedure; otherwise, skip to 9 of this procedure.
5. ☐	**Primary SDS NOAM VIP**: If upgrading the active primary SDS NOAM server, an HA failover occurs	The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the **Standby** server.
6. ☐	**Primary SDS NOAM VIP**: Log out	Click **Logout** to log out of the SDS NOAM GUI.
7. ☐	**Primary SDS NOAM VIP (GUI)**: Clear cached data	JavaScript libraries, images, and other objects are often modified in the upgrade. Browsers can sometimes cause GUI problems by holding on to the old objects in the built-in cache. To prevent these problems, always clear the browser cache before logging into an OAM GUI that has just been upgraded: 1. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers). 2. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, etc.). Other browsers may label these objects differently. 3. Clear the cached data. ***Note***: Do NOT proceed until the browser cache has been cleared.
8. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 16. Upgrade Server Administration on SDS 7.x

9. ☐	**Primary SDS NOAM VIP**: Monitor status	1. Navigate to **Administration > Software Management > Upgrade**.  2. Monitor the **Upgrade State** and the **Status Message** for the servers being upgraded.  As the upgrade executes, the following states can be observed: **Sequence** / **Upgrade State** / **Status Message** 1 / Pending / Pending upgrade 2 / Preparing / Upgrade task started 3 / Validating / Validating upgrade ISO image 4 / Upgrading / Upgrade is in progress 5 / Rebooting / Warn: failed to get TPD task state, server could be rebooting 6 / Not Ready / Success: Upgraded server to new ISO 7 / Accept of Reject / Success: Server upgrade is complete ***Note***: Some states may transition faster than the screen refresh rate and appear to skip. ***Note***: In the unlikely event SDS fails to restart after the upgrade, the **Upgrade State** will be **Backout Ready** and the Status Message displays **Server could not restart the application to complete the upgrade**. Perform Appendix K to restore the server to full operational status and return to this procedure to continue the upgrade.

Procedure 16. Upgrade Server Administration on SDS 7.x

10. ☐	**Primary SDS NOAM VIP**: View post-upgrade status	View post-upgrade status of the server(s). Post-upgrade, upgraded servers have the **Event ID (s): 32532 (Server Upgrade Pending Accept/Reject)** expected alarm.

11. ☐	**Server CLI**: Update the tuned profile	After a successful upgrade has been verified, access the server on command line (using SSH or console) and update the tuned profile:
		`$ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh`
		Verify whether the tuned profile has been successfully set to **comcol_app**:
		`$ sudo tuned-adm active`
		Sample Output:
		`[admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`

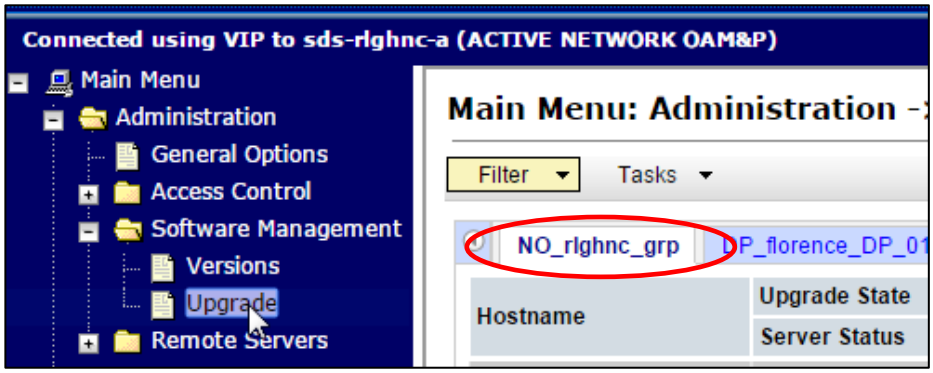
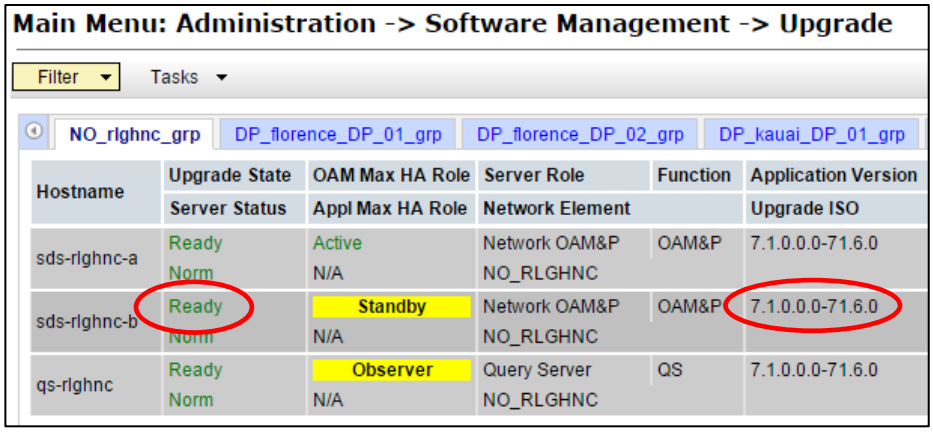
Appendix D Upgrade Server Administration on SDS 8.x

CAUTION	Unless executing parallel upgrades, DO NOT PROCEED until the **Upgrade State** is **Accept or Reject**.
	For release 7.2only: if the **restoretemp** directory is not created in the **/var/TKLC/db/filemgmt** path on each server, then create it using this command:
	`$ sudo mkdir -p /var/TKLC/db/filemgmt/restoretemp`
	`$ sudo chown awadmin:awadm /var/TKLC/db/filemgmt/restoretemp`
	`$ sudo chmod 775 /var/TKLC/db/filemgmt/restoretemp`
	If an upgrade failure is experienced (that is, Upgrade State = Failed), refer to Appendix I Recover from a Failed Upgrade

Procedure 17. Upgrade Server Administration on SDS 8.x

1. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 17. Upgrade Server Administration on SDS 8.x

2. ☐	**Primary SDS NOAM VIP**: Verify status and application version	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the Server Group tab for the server(s) to be upgraded.  3. Verify the **Upgrade Status** displays as **Ready** for the server(s) to be upgraded. 4. Verify the **Application Version** for the server(s) is the source software release version. 

CAUTION

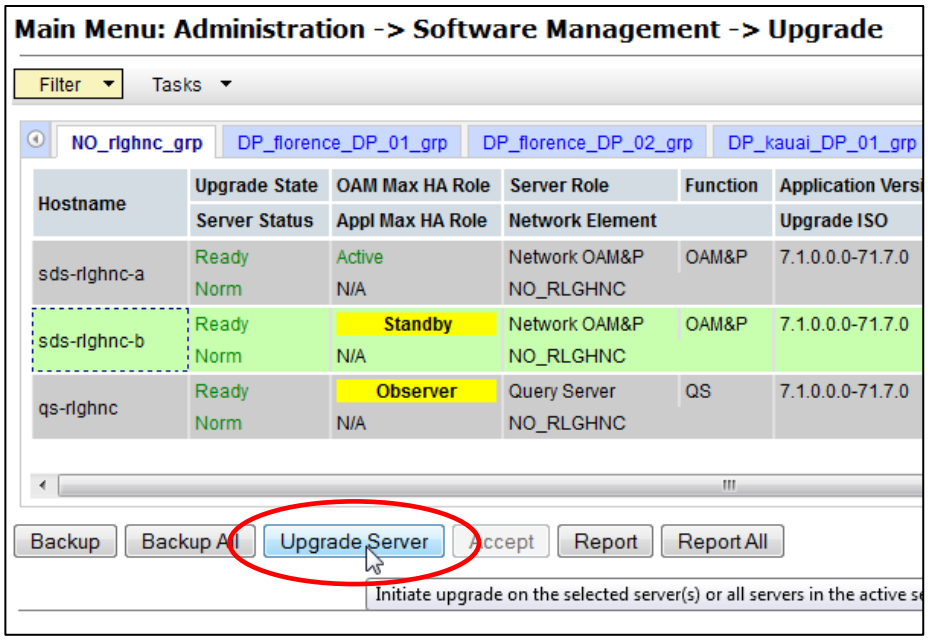
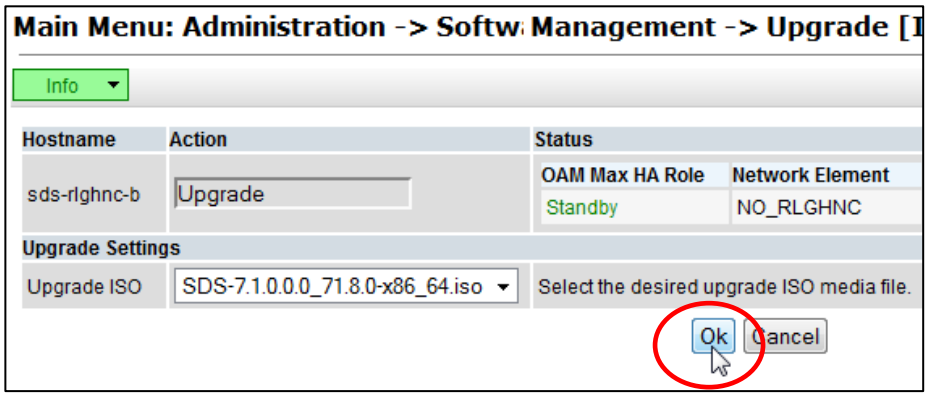
If executing Server Group **Auto Upgrade**, then SKIP to step 4 of this procedure.

- Allowed for DR NOAM, SOAM, and DP server groups only!

If executing Single Server (or multi-selected) upgrade, then continue with the next step of this procedure.

- Required for primary NOAM and DP server groups.

Procedure 17. Upgrade Server Administration on SDS 8.x

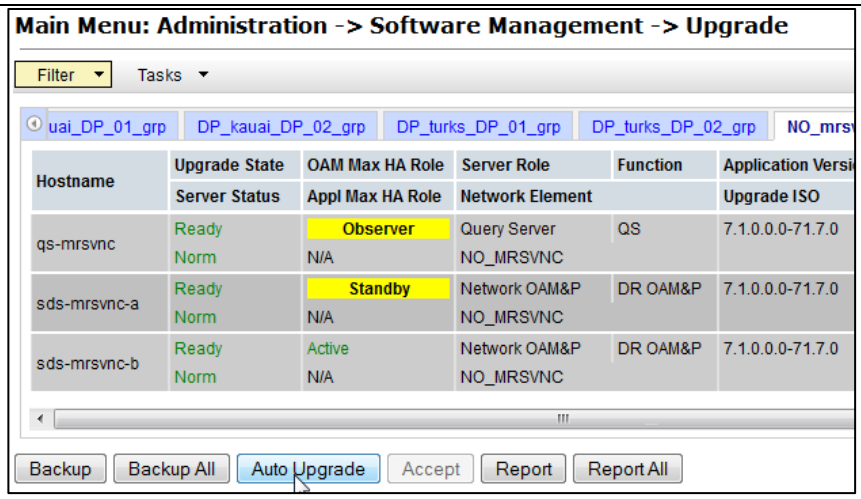
3. ☐	This step is for single server (or multi-selected) upgrade only! **Primary SDS NOAM VIP**: Upgrade server(s)	1. Press and hold the **Ctrl** key to select multiple servers that need to be upgraded. 2. Click **Upgrade Server**.  3. Select the Upgrade ISO file to use for the upgrade. 4. Click **OK**.  5. Go to step 4 of this procedure. ***Note***: During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all the NOAM and DR-NOAM servers upgrade has been completed. ***Note***: If Alarm 10009 persists after the upgrade, reboot the server once using the `sudo init 6` command on the effected server.
4. ☐	This step is for Server Group **Auto Upgrade** only!	1. Click **Auto Upgrade**. ***Note***: Do NOT select any servers with this option.

Procedure 17. Upgrade Server Administration on SDS 8.x

WARNING!

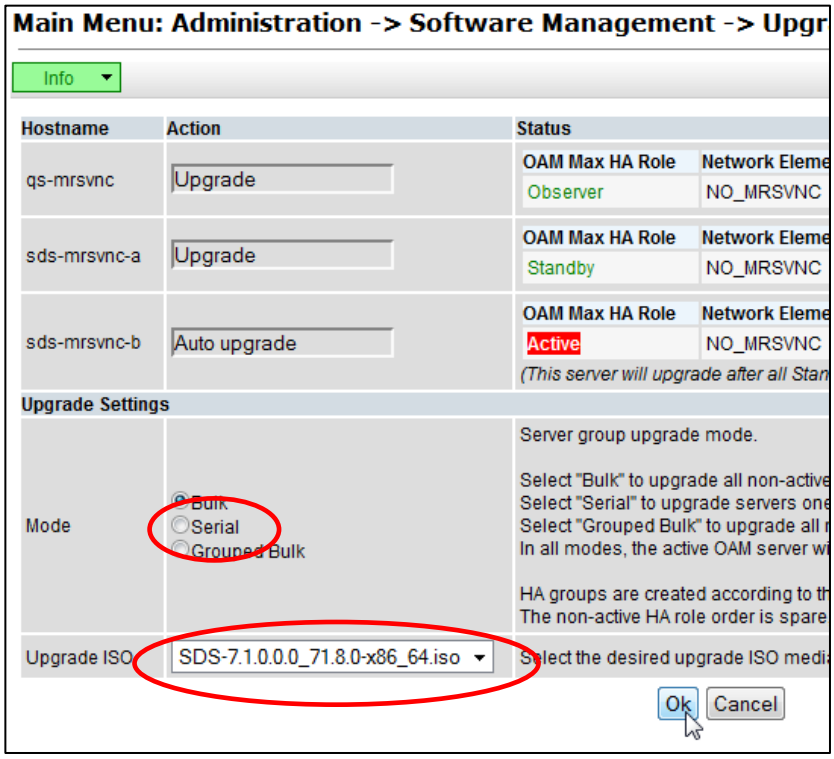
DO **NOT** use the **Auto Upgrade** option when upgrading the primary SDS NOAM server group.

Primary SDS NOAM VIP: Upgrade servers



2. Select the **Bulk** option.
3. Select the **Upgrade ISO** file to use for the upgrade.
4. Click **OK**.

   All non-active servers are upgraded first (for example, standby, query, etc.).



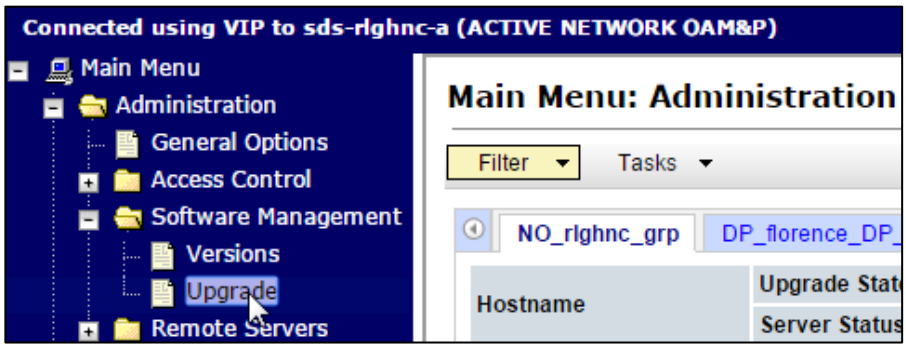
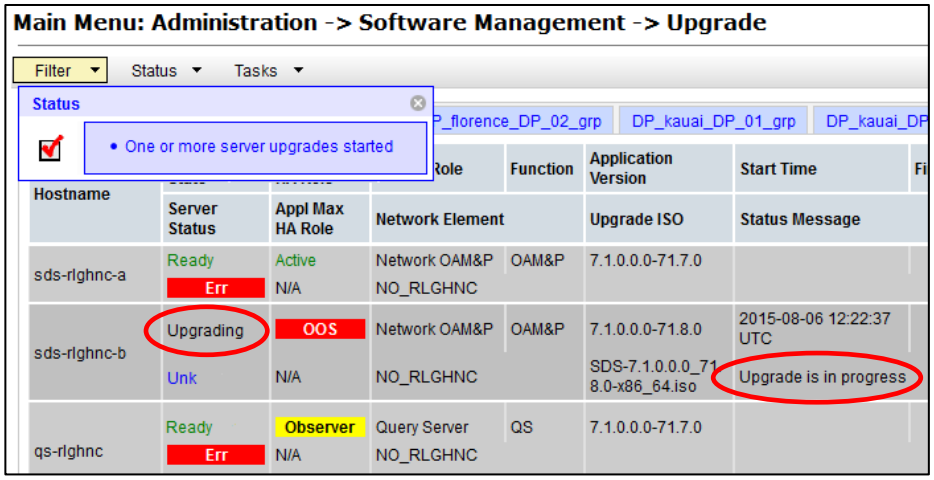
Note: During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all the NOAM and DR-NOAM servers upgrade has been completed.

Note: If Alarm 10009 persists after the upgrade, reboot the server once using the `sudo init 6` command on the effected server.

Procedure 17. Upgrade Server Administration on SDS 8.x

	CAUTION	If upgrading the formerly active primary SDS NOAM server (ithat is 2nd NOAM to be upgraded), then continue with the next step of this procedure; otherwise, SKIP to step 9 of this procedure.
5. ☐	**Primary SDS NOAM VIP**: If upgrading the active primary SDS NOAM server, an HA failover occurs	The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the **Standby** server.
6. ☐	**Primary SDS NOAM VIP**: Log out	Click **Logout** to log out of the SDS NOAM GUI.
7. ☐	**Primary SDS NOAM VIP (GUI)**: Clear cached data	JavaScript libraries, images, and other objects are often modified in the upgrade. Browsers can sometimes cause GUI problems by holding on to the old objects in the built-in cache. To prevent these problems, always clear the browser cache before logging into an OAM GUI that has just been upgraded: 1. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers). 2. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, etc.). Other browsers may label these objects differently. 3. Clear the cached data. ***Note***: Do NOT proceed until the browser cache has been cleared.
8. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 17. Upgrade Server Administration on SDS 8.x

9. ☐	**Primary SDS NOAM VIP**: Monitor status	1. Navigate to **Administration > Software Management > Upgrade**.  2. Monitor the **Upgrade State** and the **Status Message** for the servers being upgraded.  As the upgrade executes, the following states can be observed:

Sequence	Upgrade State	Status Message
1	Pending	Pending upgrade
2	Preparing	Upgrade task started
3	Validating	Validating upgrade ISO image
4	Upgrading	Upgrade is in progress
5	Rebooting	Warn: failed to get TPD task state, server could be rebooting
6	Not Ready	Success: Upgraded server to new ISO
7	Accept of Reject	Success: Server upgrade is complete

Note: Some states may transition faster than the screen refresh rate and appear to skip.

Note: In the unlikely event SDS fails to restart after the upgrade, the **Upgrade State** will be **Backout Ready** and the Status Message displays **Server could not restart the application to complete the upgrade**. Perform Appendix K to restore the server to full operational status and return to this procedure to continue the upgrade.

Procedure 17. Upgrade Server Administration on SDS 8.x

	CAUTION	Unless executing parallel upgrades, DO NOT PROCEED until the **Upgrade State** is **Accept or Reject**. If an upgrade failure is experienced (for example, Upgrade State = Failed), refer to Appendix I Recover from a Failed Upgrade.
10. ☐	**Primary SDS NOAM VIP**: View post-upgrade status	View post-upgrade status of the server(s). Post-upgrade, upgraded servers have the **Event ID (s): 32532 (Server Upgrade Pending Accept/Reject)** expected alarm.

11. ☐	**Server CLI**: Update the tuned profile	After a successful upgrade has been verified, access the server on command line (using SSH or console) and update the tuned profile:
		`$ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh`
		Verify whether the tuned profile has been successfully set to **comcol_app**:
		`$ sudo tuned-adm active`
		Sample Output:
		`[admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`

Appendix E Back Out a Single Server

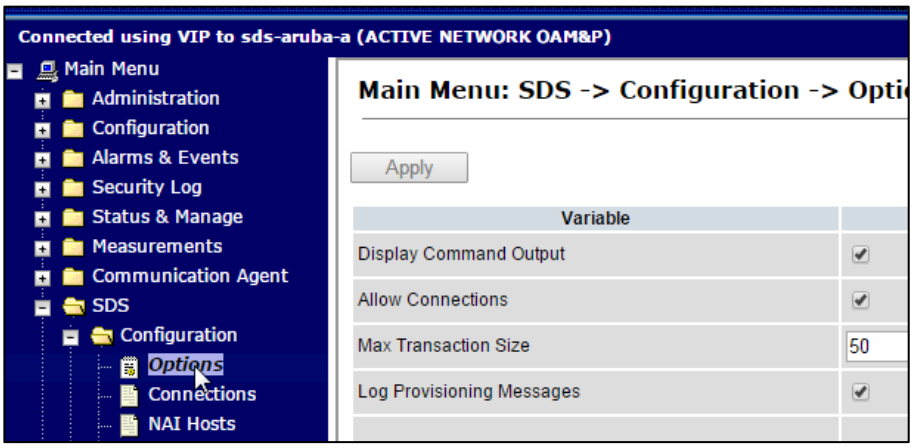
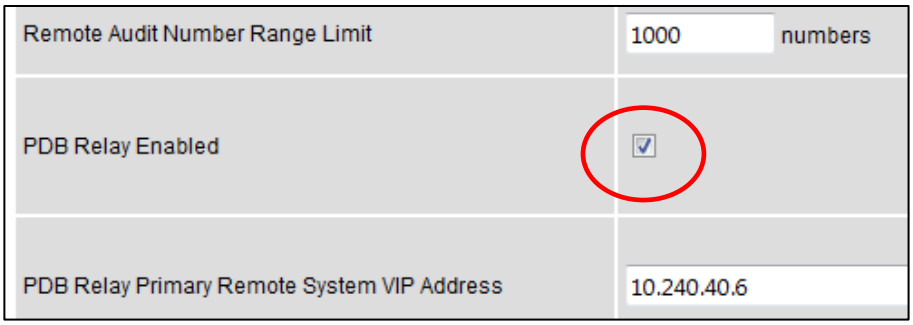
Procedure 18. Back Out a Single Server

1. ☐	**Primary SDS NOAM VIP**: Ensure the server to be downgraded is in the **Accept or Reject** state	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the tab containing the server(s) to be backed out. 3. Verify the Upgrade State is **Accept or Reject**.
2. ☐	**Primary SDS NOAM VIP**: Set the Max Allowed HA Role to **Standby**	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 3. Select the server(s) to be backed out and select a Max Allowed HA Role value of **Standby** (unless it is a **Query server**, in which case the value should remain set to **Observer**). 4. Click **OK**.
	CAUTION	If downgrading the active primary SDS NOAM server, then continue with the next step of this procedure; otherwise, skip to step 4 of this procedure.
3. ☐	**Primary SDS NOAM VIP**: If downgrading the active primary SDS NOAM server, an HA failover occurs	The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the **Standby** server. ***Note***: If the server being backed out is the active NOAM and an HA failover does not happen after step 2, and the OAM HA Role of the NOAMP server to be backed out on the HA status screen is still **Active**, then you have encountered a known issue. Apply the workaround using Appendix O to have the NOAMP HA fail over.

Procedure 18. Back Out a Single Server

4. ☐	**Primary SDS NOAM VIP**: Log out	Click **Logout** to log out of the SDS NOAM GUI.
5. ☐	**Primary SDS NOAM VIP**: Clear cached data	JavaScript libraries, images, and other objects are often modified in the upgrade. Browsers can sometimes cause GUI problems by holding on to the old objects in the built-in cache. To prevent these problems, always clear the browser cache before logging into an OAM GUI that has just been upgraded: 1. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers). 2. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, etc.). Other browsers may label these objects differently. 3. Clear the cached data. ***Note***: Do NOT proceed until the browser cache has been cleared.
6. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.

Procedure 18. Back Out a Single Server

7. ☐	**Primary SDS NOAM VIP**: Record PDB Relay Enabled state	1. Navigate to **SDS > Configuration > Options**.  2. Locate the **PDB Relay Enable** checkbox and record if it is checked or not checked.  **CHECKED** (Yes/No) **PDB Relay Enabled** _____

CAUTION

If the PDB Relay Enabled checkbox is CHECKED, then continue with the next step of this procedure.

If the PDB Relay Enabled checkbox is NOT CHECKED, then skip to step 18 of this procedure.

Procedure 18. Back Out a Single Server

8. ☐	**Primary SDS NOAM VIP (CLI)**: Access the active primary SDS NOAM	Use the VIP address to log into the active primary SDS NOAM with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`
		`[admusr@sds-rlghnc-a ~]$`

9. ☐	**Primary SDS NOAM VIP**: Set the pdbRelay TimeStamp to 0	`[admusr@sds-rlghnc-b ~]$ sudo iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"`

10. ☐	**Primary SDS NOAM VIP**: Exit CLI	Exit the **CLI** for the active primary SDS NOAM.
		`[admusr@sds-rlghnc-b ~]$ exit`
		`logout`

11. ☐	**Primary SDS NOAM VIP**: Stop the software	1. Navigate to **Status & Manage > Server**. 2. Select the serve(s)r to be backed out and click **Stop**. 3. Click **OK** to confirm. 4. Verify the Appl State updates to **Disabled**.
12. ☐	**Primary SDS NOAM VIP**: Verify the server(s) are backout ready	1. Navigate to **Administration > Software Management** > **Upgrade**. 2. Select the tab for the server group containing the server(s) to be backed out. ***Note***: It may take a couple minutes for the grid to update. 3. Verify the Upgrade State displays as **Backout Ready**. ***Note***: If this is the active server in an Active-Standby pair, these steps cause an HA failover. The HA failover is an expected outcome. Continue with the steps on the new active NOAMP.

13. ☐	**Server CLI**: SSH to the server(s) to be backed out	Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: If direct access to the XMI is not available, then access the target server using a connection through the active NO. SSH to the active NO XMI first. Once logged into the NO, SSH to the target server's XMI address.

Procedure 18. Back Out a Single Server

14. ☐	**Server CLI**: Execute the backout	Execute the backout using the reject script:
		`$ sudo /var/TKLC/backout/reject`
		***** TRUNCATED OUTPUT *****
		`Executing.. /var/TKLC/backout/backout_server --check`
		`Verifying that backout is possible.`
		`Checking for stale RPM DB locks...`
		`Current platform version:  7.0.2.0.0-86.30.0`
		`Continue backout?  [y/N]: y`
		Answer **y** to continue the backout.
		The server reboots and the user is automatically logged out.

15. ☐	**Server CLI**: SSH to the server(s) to be backed out	Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as:  admusr`
		`password:  <enter password>`

16. ☐	Server CLI: Verify the Backout	Examine the upgrade logs in the **/var/TKLC/log/upgrade** directory and verify no errors are reported. `$ grep ERROR /var/TKLC/log/upgrade/upgrade.log` ***Note***: The following errors can be ignored: • DEBUG: 'iqt' command failed (is IDB running?) • 1477080063::ERROR: TKLCsds-7.0.0-7.0.1_70.12.0: Failure running command '/usr/TKLC/appworks/bin/eclipseHelp reconfig' • 1477080521::ERROR: prod.dbdown: unknown option (-i) • 1517455316::ERROR: Cannot execute command! • 1517455316::ERROR: CMD: /usr/sbin/hpacucli controller all show config detail • 1517455316::ERROR: ERROR: No such file or directory • 1517455316::ERROR: Unable to get the HP disk configuration! • 1517455316::ERROR: Command Failed! • 1517455316::ERROR: Child process has exited with: • 1517455316::SYSERROR: No such file or directory If the backout was not successful, because other errors were recorded in the logs, then contact My Oracle Support (MOS) for further instructions. If the backout was successful (no errors or failures), then continue with the remaining steps.

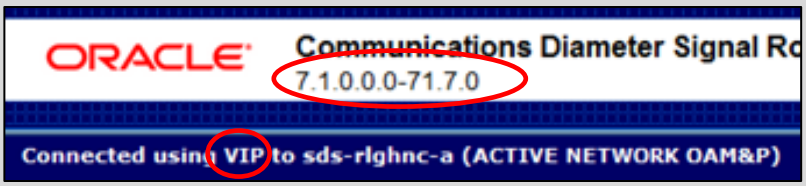
Procedure 18. Back Out a Single Server

17. ☐	**Server CLI**: Restore the COMCOL Full DB/Run environment	Execute the backout_restore utility to restore the full database run environment.
		`$ sudo /var/tmp/backout_restore`
		***** TRUNCATED OUTPUT *****
		`This process will totally destroy the existing DB on this server. This should only be done to recover a server when an upgrade has been backed-out/rolled-back.`
		`Are you sure you want to proceed? (y|n): y`
		Answer **y** to continue the restore.
		Note: The COMCOL restore process may take several minutes to complete.
		If the restore was successful, the following displays:
		`Success: Full restore of COMCOL run env has completed.`
		If an error is encountered and reported by the utility, then work with My Oracle Support (MOS) for further instructions.
		Note: In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory, resulting in the **/var/tmp/backout_restore: No such file or directory** error message. If this message occurs, copy the file using sudo from **/usr/TKLC/appworks/sbin** to **/var/tmp** and repeat the command.

18. ☐	**Server CLI**: Reboot the server	`$ sudo init 6` This step can take several minutes and terminates the SSH session.

19. ☐	**Server CLI**: SSH to the server(s) that was backed out	Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`

Procedure 18. Back Out a Single Server

<table>
<tr>
<td>20. ☐</td>
<td>Server CLI: Verify the httpd service has restarted</td>
<td>
1. If this is an NO or SO, verify httpd service is running.
<code>$ sudo service httpd status</code>
<code>httpd (pid xxxx) is running...</code>
Note: The process IDs are variable so the actual number value can be ignored.
2. If httpd is not running, wait for a few minutes and retry the command. If httpd is still not running after 3 minutes, then services have failed to restart. Contact My Oracle Support (MOS) for further instructions.
3. Verify if the file id_dsa has required ownership:
3. Check the ownership of the file:
<code>ls -ltr /home/awadmin/.ssh/</code>
The file permission should be defined as shown:
<pre>[admusr@HPC-NO1 ~]$ sudo ls -lrt /home/awadmin/.ssh/
total 20
-rw------- 1 awadmin awadm 1281 Sep 27 16:19 config
-rw-r----- 1 awadmin awadm 605 Nov 18 13:20 id_dsa.pub
-rw------- 1 awadmin awadm 668 Nov 18 13:20 id_dsa
-rw------- 1 awadmin awadm 7275 Nov 18 18:09 authorized_keys</pre>
4. If the file ownership is not set for awadmin, then change the permission:
<code>sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa</code>
5. Verfiy file ownership is changed to awadmin awadm.
</td>
</tr>
<tr>
<td>21. ☐</td>
<td>Primary SDS NOAM VIP: Verify the server(s) application version and upgrade state</td>
<td>
1. Navigate to Administration > Software Management > Upgrade.
2. Select the tab containing the server(s) that were backed out.
3. Verify the Application Version value for this server has been backed out to the source release version.
4. Verify the Upgrade State.
Note: Full audit between active NO and backed out server is conducted and it may take up to 10 minutes before the Upgrade State is changed to Ready.
</td>
</tr>
<tr>
<td colspan="3">
CAUTION
For primary active SDS at release 7.1 or later:
• If the Upgrade State is Not Ready, then continue with the next step of this procedure.
• If the Upgrade State is Ready, then skip to step 27 of this procedure.
Note: The primary active SDS release displays on the NOAM GUI banner (using the VIP).


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

Procedure 18. Back Out a Single Server

22. ☐	**Primary SDS NOAM VIP**: Set the Max Allowed HA Role to Active	Due to back out being initiated from the command line instead of through the GUI, modify the backed out server so its Upgrade State changes to **Ready**. 1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 3. Select the backed out server(s) and choose a Max Allowed HA Role value of **Active** (unless it is a **Query server**, in which case the value should remain set to **Observer**). 4. Click **OK**. 5. Verify the Max Allowed HA Role is set.
23. ☐	**Primary SDS NOAM VIP**: Restart the software	1. Navigate to **Status & Manage > Server**. 2. If the server(s) that was backed out displays an Appl State state of **Enabled**, skip to the next step. 3. If the server(s) that was backed out displays an Appl State state of **Disabled**, select the server(s) and click **Restart**. 4. Click **OK** to confirm. 5. Verify the Appl State changes to **Enabled**.
24. ☐	**Primary SDS NOAM VIP**: Verify the Upgrade State	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the tab of the server group containing the server(s) that was backed out. 3. Verify the Upgrade State is now **Ready** (it may take several seconds for the grid to update).
25. ☐	**Primary SDS NOAM VIP**: Stop the software (if necessary)	Due to backout being initiated from the command line instead of through the GUI, modify the Upgrade State of the backed out server(s) to achieve a state of **Not Ready**. 1. Navigate to **Status & Manage > Server**. 2. If the server(s) that was backed out displays an Appl State state of **Enabled**, then select the server(s) and click **Stop**.
26. ☐	**Primary SDS NOAM VIP**: Verify the server(s) Upgrade State	1. Navigate to **Administration > Software Management > Upgrade**. 2. If the server(s) that was backed out displays an Upgrade State of **Not Ready**, then go back to step 22 of this procedure.

Procedure 18. Back Out a Single Server

27. ☐	**Primary SDS NOAM VIP**: Complete the backout action (if necessary)	If the server(s) that was backed out displays an Upgrade State of **Ready** or **Success**, then 1. Select the server(s) that was backed out and click **Complete**. Leave the Action set to its default value of **Complete**. 2. Click **OK** to confirm the action. This changes the **Max Allowed HA Role** of the backed out server(s) to **Active**, which causes the server **Upgrade State** to change to **Not Ready**. The user may see the following SOAP error display on the GUI banner. **SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]** It is safe to ignore this error message.

Appendix F Manually Perform ISO Validation

Note: This a procedure assumes that the **ISO** file to be validated has already been uploaded to the server in question and is present in the **/var/TKLC/db/filemgmt/**, **/var/TKLC/db/filemgmt/isos/** or **/var/TKLC/upgrade/** directory.

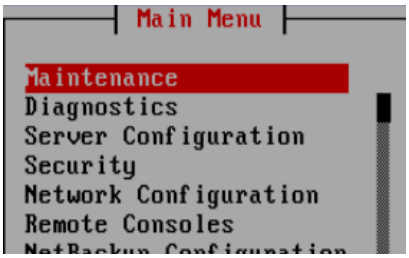
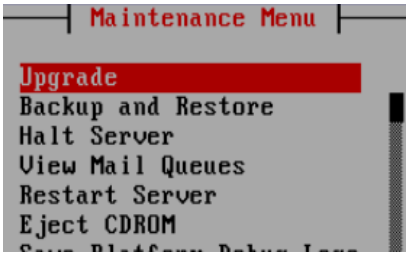
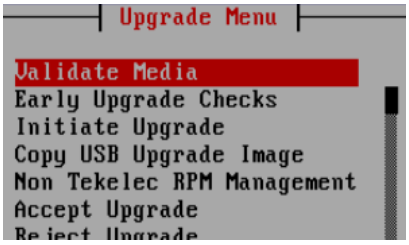
Procedure 19. Manually Perform ISO Validation

1. ☐	**Primary SDS NOAM VIP**: Access the active primary SDS NOAM	Use the VIP address to log into the active primary SDS NOAM with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`

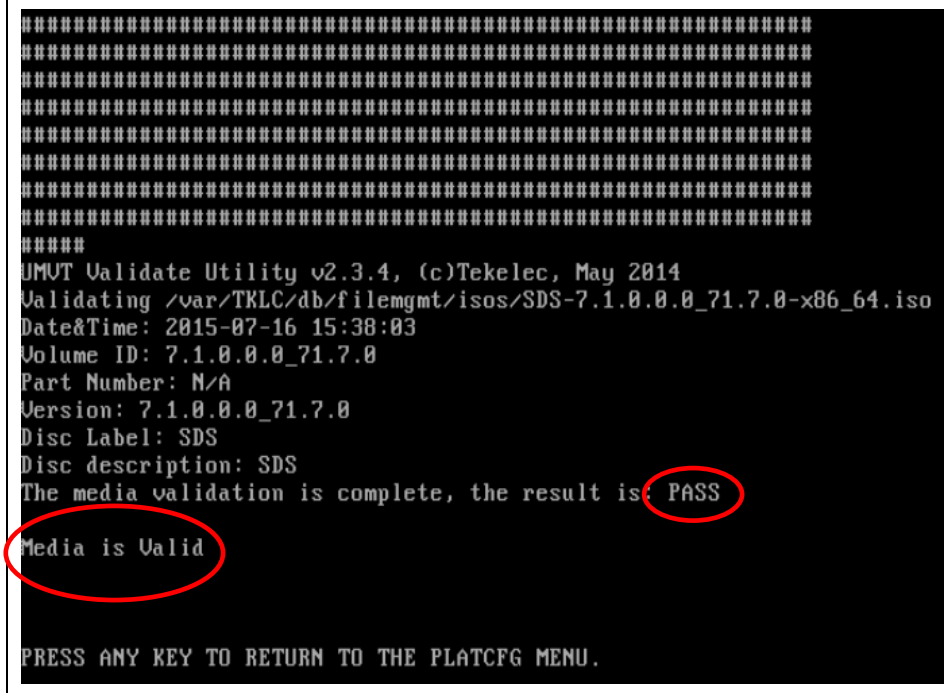
2. ☐	**Primary SDS NOAM VIP**: Verify ISO file is in the /var/TKLC/upgrade/ directory.	1. Verify the ISO file is located in the **/var/TKLC/upgrade/** directory.
		`[admusr@sds-rlghnc-a ~]$ ls /var/TKLC/upgrade/`
		`SDS-8.0.0.0.0_80.22.0-x86_64.iso`
		2. If the ISO file is **not** present, copy the ISO file to the **var/TKLC/upgrade/** directory.
		`[admusr@sds-rlghnc-a ~]$ cp –p /var/TKLC/db/filemgmt/SDS-8.0.0.0.0_80.22.0-x86_64.iso /var/TKLC/upgrade/`

3. ☐	**Primary SDS NOAM VIP**: Become the **platcfg** user	Become the **platcfg** user by using the **su** command.
		For password information, refer to Table 3. Logins, Passwords, and Site Information, if necessary.
		`[admusr@sds-rlghnc-a ~]$ su – platcfg`
		`Password: <platcfg_password>`

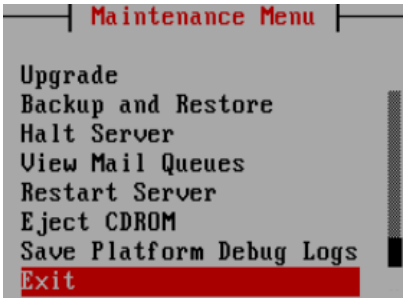
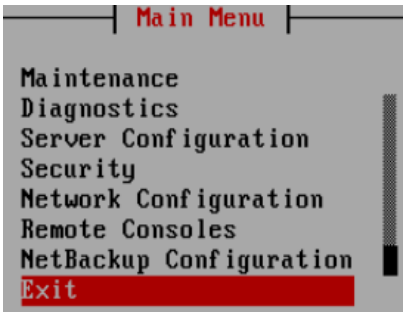
Procedure 19. Manually Perform ISO Validation

4. ☐	**Primary SDS NOAM VIP**: Select the ISO file	1. From the platcfg menu, select **Maintenance** and press **Enter**.  2. Select **Upgrade** and press **Enter**.  3. Select **Validate Media** and press **Enter**.  Select **Choose Upgrade Media Menu**, select the target ISO file, and press **Enter**.

Procedure 19. Manually Perform ISO Validation

5. ☐	**Primary SDS NOAM VIP**: Verfiy ISO media	1. Verify ISO media is **Valid**.  2. Press **Enter** to return to the platcfg menu.

Procedure 19. Manually Perform ISO Validation

6. ☐	**Primary SDS NOAM VIP**: Exit from menus	1. Select **Exit** and press **Enter**. 2. Select **Exit** and press **Enter**. 3. Select **Exit** and press **Enter**.  4. Select **Exit** and press **Enter**. 

7. ☐	**Primary SDS NOAM VIP**: Exit CLI	Exit the **CLI** for the **Active Primary SDS NOAM**.
		`[admusr@sds-rlghnc-a ~]$ exit`
		`logout`

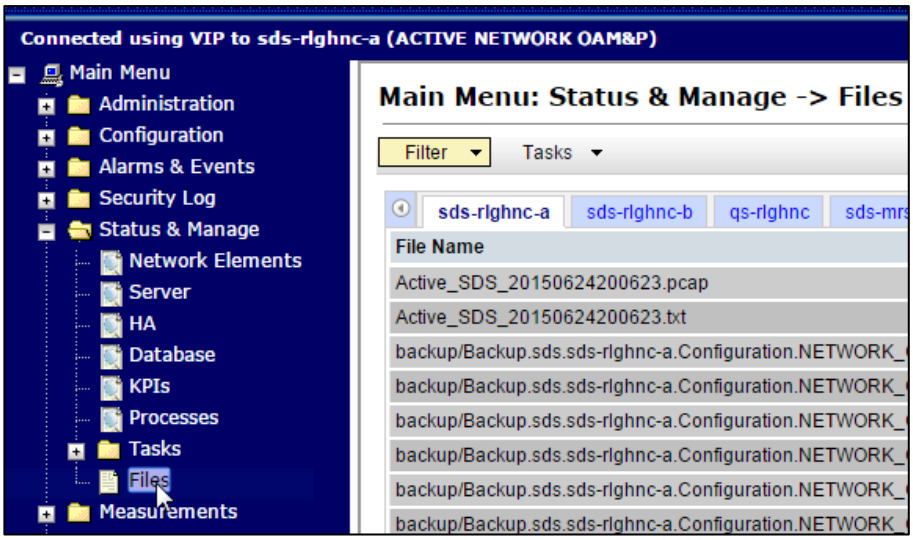
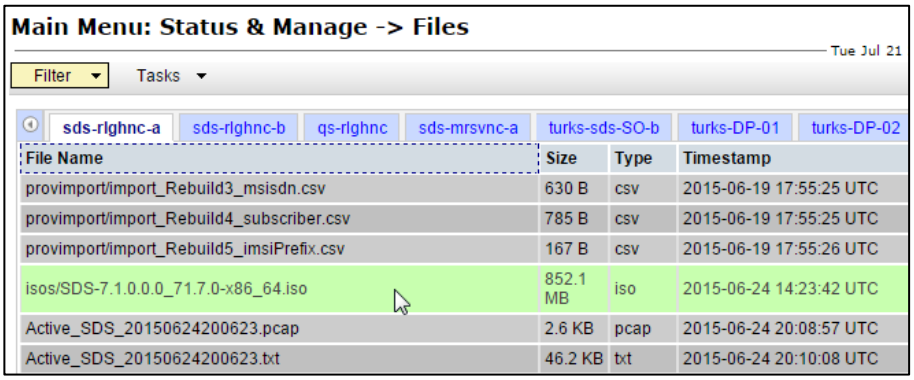
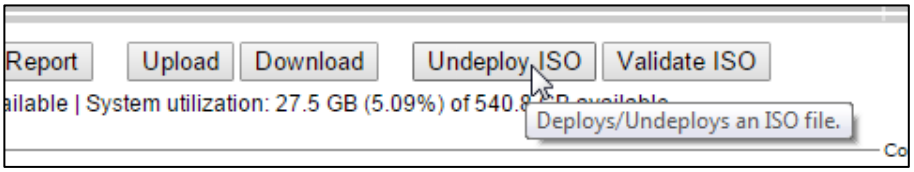
8. ☐	Return to the referring procedure	Return to the procedure step that directed the execution of this procedure.

Appendix G Undeploy an ISO File (Post Upgrade Acceptance)

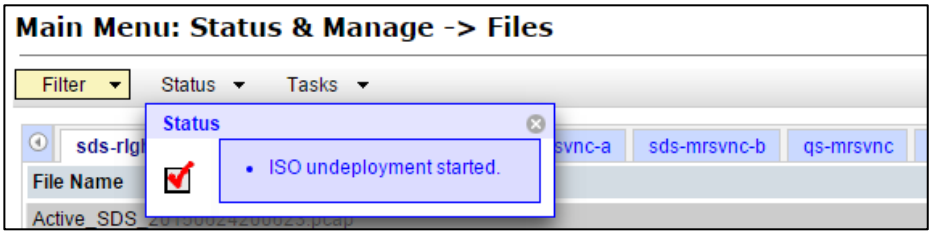
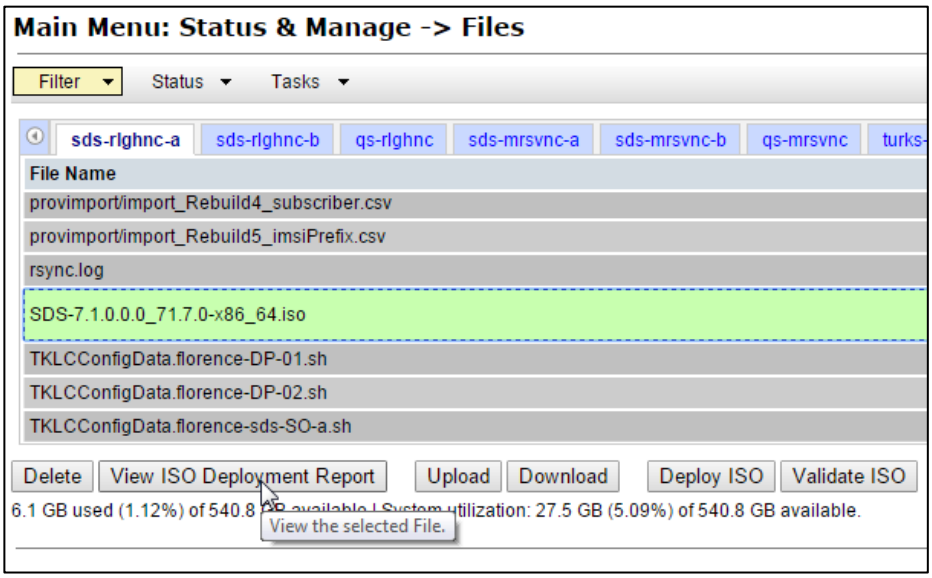
This procedure should only be executed post Upgrade Acceptance and removes a deployed **ISO** file from all servers in the SDS topology except the **active primary NOAM** server. At the end of the procedure, the ISO is still present in the **/var/TKLC/db/filemgmt/isos/** directory on the **active primary NOAM** server.

Once this procedure is complete, the file may then be manually deleted (if desired) from the SDS NOAM GUI (VIP) under the **Status & Manage > Files**.

Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance

1. ☐	**SDS NOAM GUI**: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP**: Undeploy the ISO	1. Navigate to **Status & Manage > Files**.  2. Select the ISO file for the target release.  3. Click **Undeploy ISO**.  4. Click **OK**.

Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance

3. ☐	**Primary SDS VIP**: Monitor the ISO undeployment status	1. The Status tab in the banner displays the **ISO undeployment started** confirmation message.  2. Reselect the ISO file for the target release and click **View ISO Deployment Report**.  3. The Deployment report indicates the current status of undeployment to all servers in the topology. Click **Back** and then click **View ISO Deployment Report** again to refresh the report.

Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance

		Main Menu: Status & Manage -> Files [View] Main Menu: Status & Manage -> Files [View] Tue Jul 21 20:08:34 2015 UTC Deployment report for SDS-7.1.0.0.0_71.7.0-x86_64.iso: Deployed on 0/18 servers. sds-rlghnc-a: Not Deployed sds-rlghnc-b: Not Deployed qs-rlghnc: Not Deployed sds-mrsvnc-a: Not Deployed sds-mrsvnc-b: Not Deployed qs-mrsvnc: Not Deployed turks-sds-SO-a: Not Deployed turks-sds-SO-b: Not Deployed turks-DP-01: Not Deployed turks-DP-02: Not Deployed kauai-sds-SO-a: Not Deployed kauai-sds-SO-b: Not Deployed kauai-DP-01: Not Deployed kauai-DP-02: Not Deployed florence-sds-SO-a: Not Deployed florence-sds-SO-b: Not Deployed florence-DP-01: Not Deployed florence-DP-02: Not Deployed 4. Repeat until the ISO displays **Not Deployed** on all servers in the topology.

Appendix H Add the SDS ISO to the PMAC Software Repository

STOP This procedure is not applicable if SDS is deployed in a cloud environment.

This procedure must be done once for each PMAC at each DSR signaling site that contains SDS SOAM/DP servers.

Procedure 21. Add the SDS ISO to the PMAC Software Repository

1. ☐	**Primary SDS NOAM VIP**: Access the active primary SDS NOAM	Use the VIP address to log into the active primary SDS NOAM with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-rlghnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`

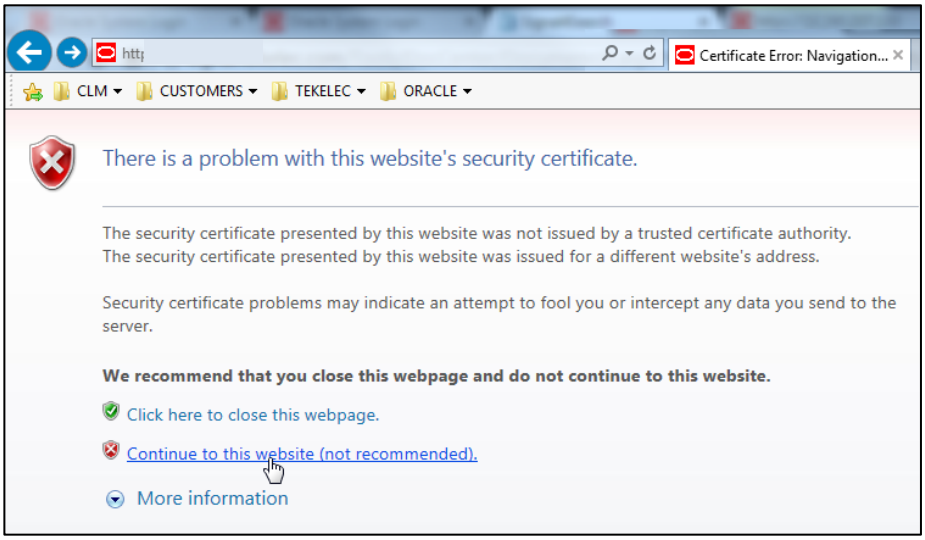
Procedure 21. Add the SDS ISO to the PMAC Software Repository

2. ☐	**Primary SDS NOAM VIP**: Acess filemgmt directory	Access the **filemgmt** directory where the target ISO file was uploaded.
		`[admusr@sds-rlghnc-a ~]$ cd /var/TKLC/db/filemgmt/`
		`[admusr@sds-rlghnc-a filemgmt]$`

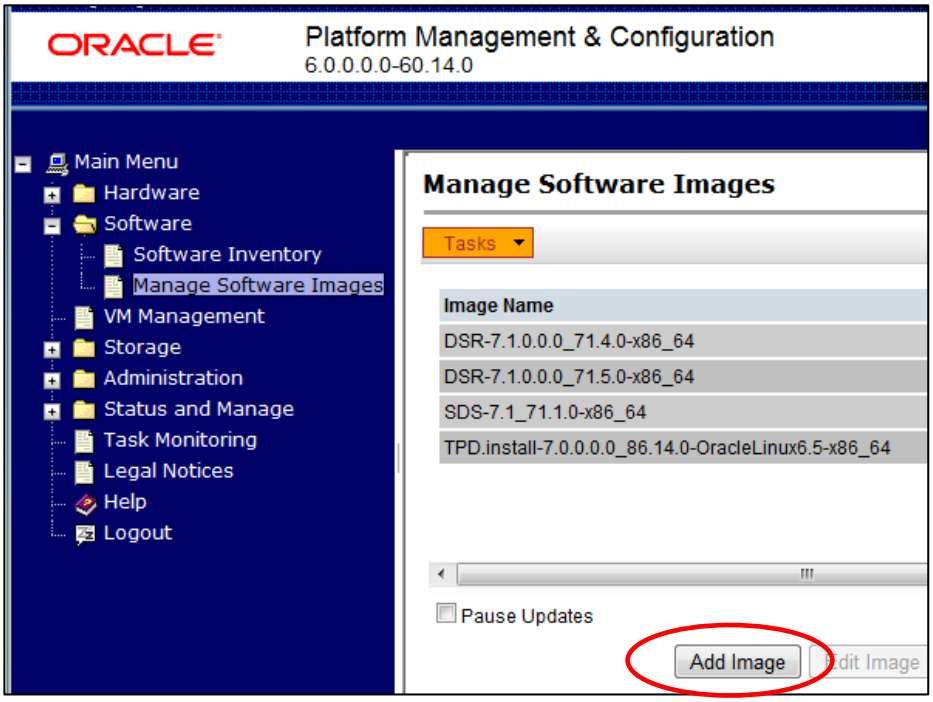
3. ☐	**Primary SDS NOAM VIP**: Identify ISO file and copy it	1. Identify the exact name of the target ISO file.
		`[admusr@sds-rlghnc-a filemgmt]$ ls -l *.iso`
		`-rw-rw-r-- 1 awadmin awadm 893536256 Jun 24 14:23 SDS-8.0.0.0.0_80.22.0-x86_64.iso`
		2. Use Secure Copy (scp) to copy the target ISO file to the **/var/TKLC/upgrade/** directory of the remote PMAC server as the **admusr** user.
		`$ scp -p SDS-8.0.0.0.0_80.22.0-x86_64.iso admusr@10.240.246.7:/var/TKLC/upgrade/`
		`FIPS integrity verification test failed.`
		`The authenticity of host '10.240.246.7 (10.240.246.7)' can't be established. RSA key fingerprint is 23:aa:7e:12:40:d6:20:d6:19:62:c0:07:9d:20:30:35.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added '10.240.246.7' (RSA) to the list of known hosts.`
		`Password: <admusr_password>`
		`SDS-8.0.0.0.0_80.22.0-x86_64.iso 100% 852MB 11.2MB/s 01:16`

4. ☐	**Primary SDS NOAM VIP**: Exit CLI	Exit the **CLI** for the **Active Primary SDS NOAM**.
		`[admusr@sds-rlghnc-a filemgmt]$ exit`
		`logout`

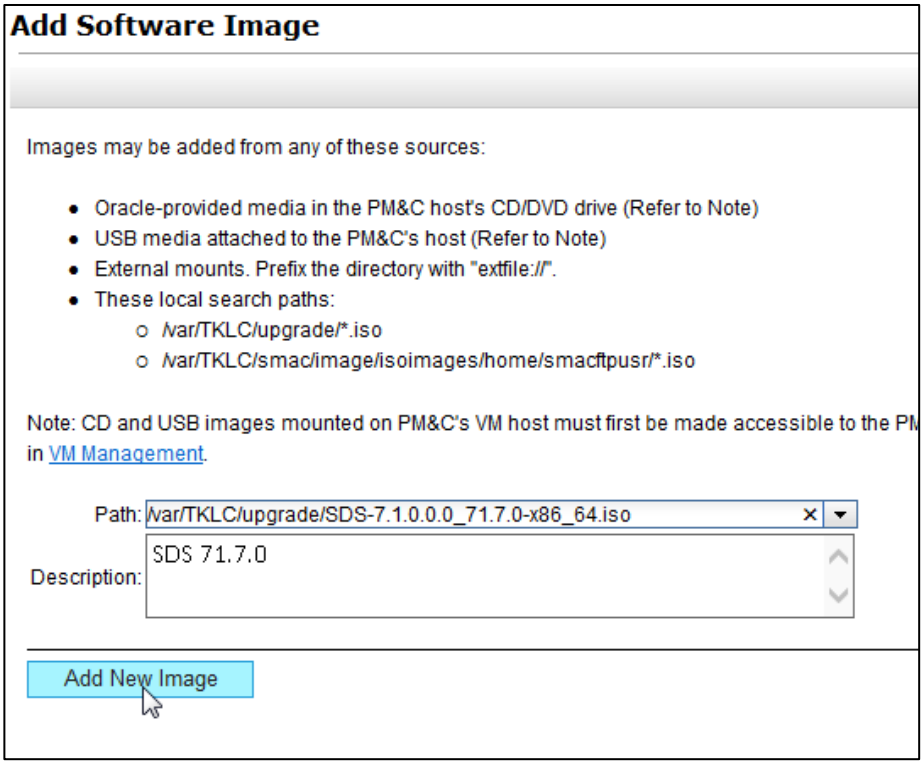
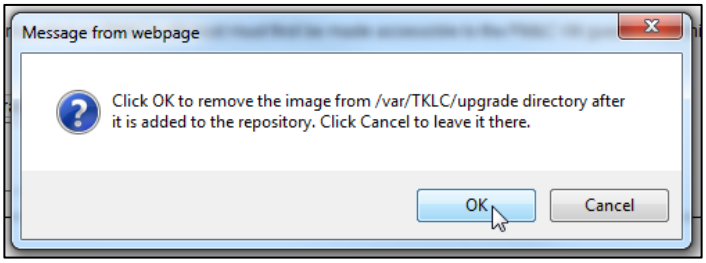
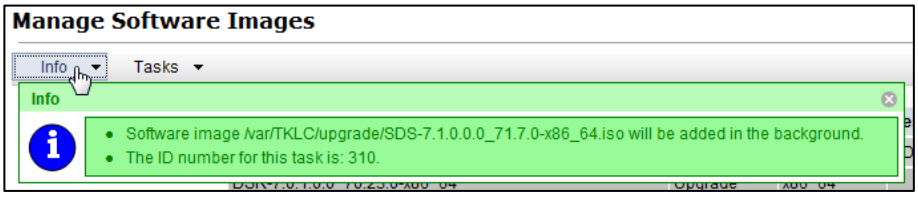
Procedure 21. Add the SDS ISO to the PMAC Software Repository

5. ☐	**PMAC Server (GUI)**: Log into the Platform Management and Configuration application	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the management IP address assigned to the PMAC server associated with the SDS SOAM NE. If a certificate error is received, click on the **Continue to this website (not recommended)** link. 
6. ☐	**PMAC Server**: Login	Login using the default user and password.

Procedure 21. Add the SDS ISO to the PMAC Software Repository

7. ☐	**PMAC Server**: Add an image	1. Navigate to **Software > Manage Software Images**. 2. Click **Add Image**. 

Procedure 21. Add the SDS ISO to the PMAC Software Repository

8. ☐	**PMAC Server**: Add an image	1. Select a **Path** from the list. 2. Add a **Description**. 3. Click **Add New Image**.  4. Click **OK** when asked to confirm.  An **Info** message displays to show the task. 

Procedure 21. Add the SDS ISO to the PMAC Software Repository

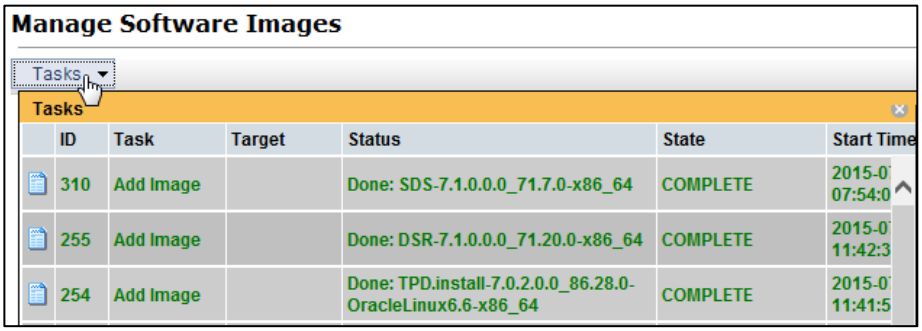
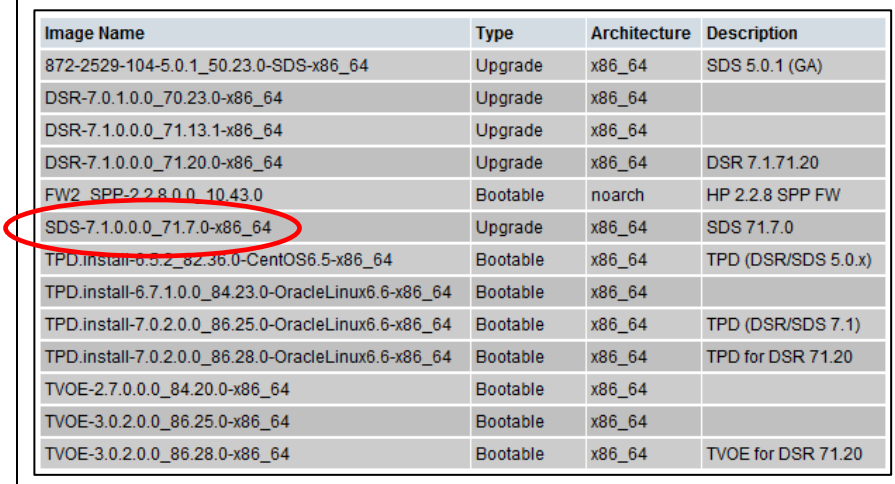
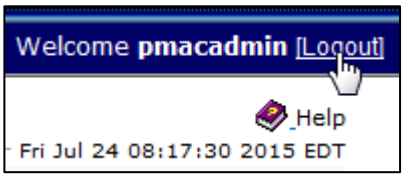
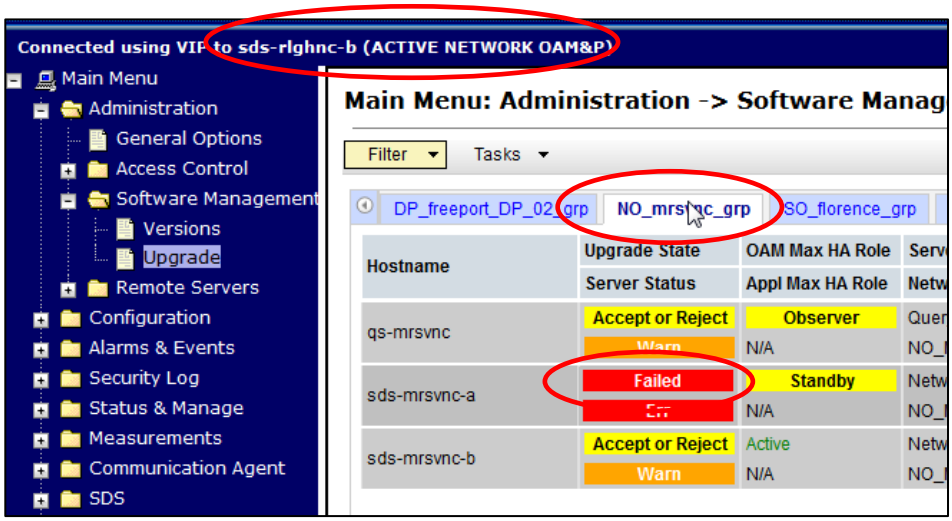
9. ☐	**PMAC Server**: Monitor progress	Monitor the progress using Tasks tab in the banner.  **Manage Software Images** Tasks Tasks ID | Task | Target | Status | State | Start Time 310 | Add Image | Done: SDS-7.1.0.0.0_71.7.0-x86_64 | COMPLETE | 2015-0 07:54:0 255 | Add Image | Done: DSR-7.1.0.0.0_71.20.0-x86_64 | COMPLETE | 2015-0 11:42:3 254 | Add Image | Done: TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64 | COMPLETE | 2015-0 11:41:5 The new software displays in the list when complete. 
10. ☐	**PMAC Server**: Log out	Click **Logout**.  Welcome **pmacadmin** [Logout] Help Fri Jul 24 08:17:30 2015 EDT

Image Name	Type	Architecture	Description
872-2529-104-5.0.1_50.23.0-SDS-x86_64	Upgrade	x86_64	SDS 5.0.1 (GA)
DSR-7.0.1.0.0_70.23.0-x86_64	Upgrade	x86_64	
DSR-7.1.0.0.0_71.13.1-x86_64	Upgrade	x86_64	
DSR-7.1.0.0.0_71.20.0-x86_64	Upgrade	x86_64	DSR 7.1.71.20
FW2_SPP-2.2.8.0.0_10.43.0	Bootable	noarch	HP 2.2.8 SPP FW
SDS-7.1.0.0.0_71.7.0-x86_64	Upgrade	x86_64	SDS 71.7.0
TPD.install-6.5.2_82.36.0-CentOS6.5-x86_64	Bootable	x86_64	TPD (DSR/SDS 5.0.x)
TPD.install-6.7.1.0.0_84.23.0-OracleLinux6.6-x86_64	Bootable	x86_64	
TPD.install-7.0.2.0.0_86.25.0-OracleLinux6.6-x86_64	Bootable	x86_64	TPD (DSR/SDS 7.1)
TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64	Bootable	x86_64	TPD for DSR 71.20
TVOE-2.7.0.0.0_84.20.0-x86_64	Bootable	x86_64	
TVOE-3.0.2.0.0_86.25.0-x86_64	Bootable	x86_64	
TVOE-3.0.2.0.0_86.28.0-x86_64	Bootable	x86_64	TVOE for DSR 71.20

Appendix I Recover from a Failed Upgrade

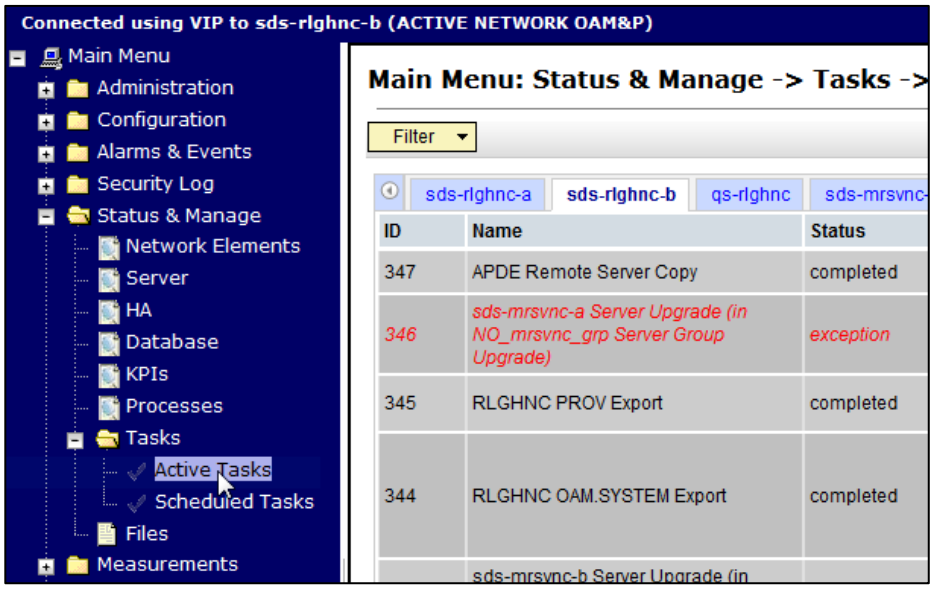
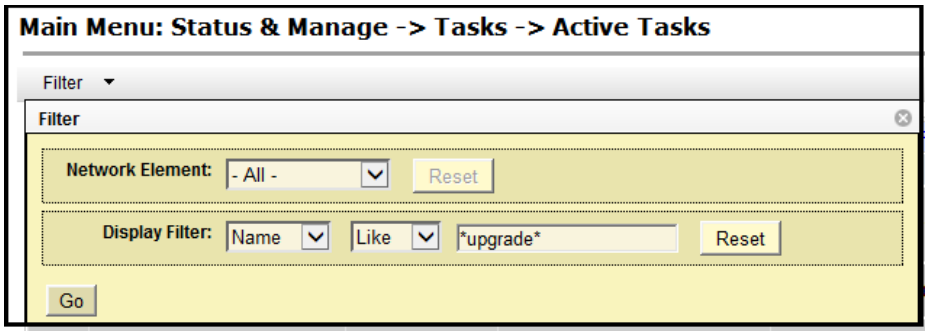
Procedure 22. Recover from a Failed Upgrade

1. ☐	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. ☐	**Primary SDS NOAM VIP**: Verify upgrade state	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the hostname of the primary active SDS NOAM server from the GUI banner. 3. Select the Server Group tab for the server(s) being upgraded. 4. Verify the **Upgrade State** for each server undergoing the software upgrade and identify any servers with a **Failed** state. 

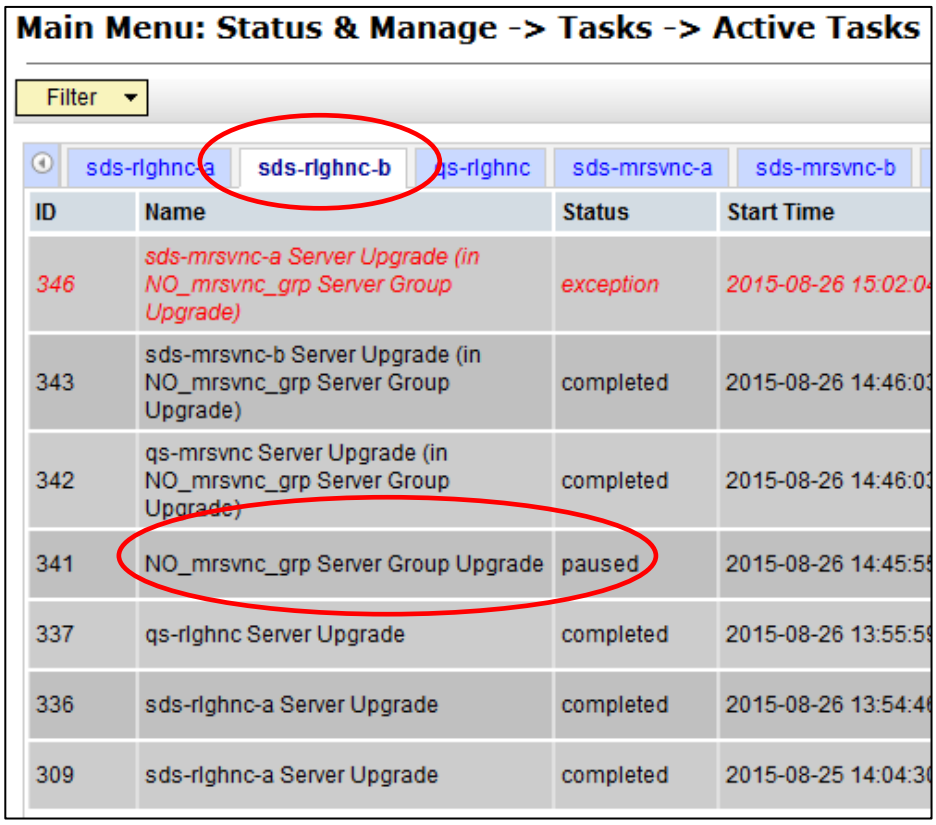
CAUTION

- If the **Failed Server** was upgraded using the **Auto Upgrade** option, that is, Auto Server Group Upgrade**,** then continue to the next step of this procedure.
- If the **Failed Server** was upgraded using the **Upgrade Server** option**,** then skip to step 7 of this procedure.

Procedure 22. Recover from a Failed Upgrade

3. ☐	**Primary SDS NOAM VIP**: Filter the servers that need upgrading	1. Navigate to **Status & Manage > Tasks > Active Tasks**.  2. From the **Filter** option, enter the following filter values: Network Element: **All** Display Filter: **Name Like *upgrade*** 3. Click **Go**. 

Procedure 22. Recover from a Failed Upgrade

4. ☐	**Primary SDS NOAM VIP**: Locate the Server Group Upgrade task	1. If not already selected, select the tab displaying the hostname of the active SDS NOAM server. 2. Locate the task for the **Server Group Upgrade**. It shows a status of **paused**. 

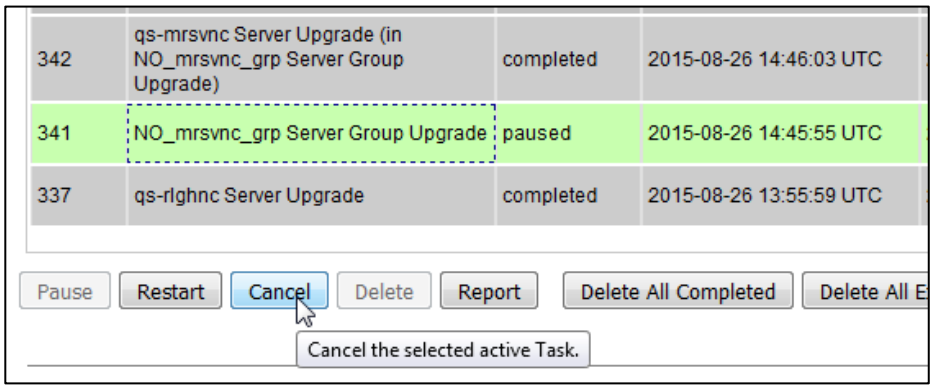
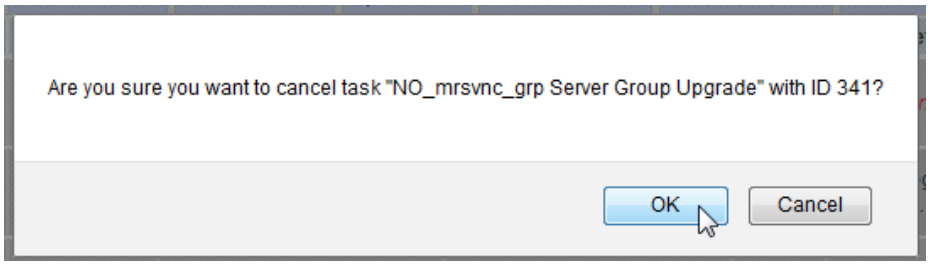
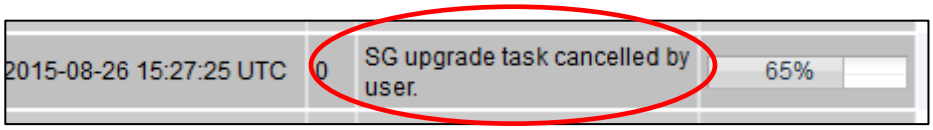
Note: Consider the case of an upgrade cycle where it is seen that the upgrade of one or more servers in the server group has the status as exception (that is, failed), while the other servers in that server group have upgraded successfully. However, the server group upgrade task still shows as running. In this case, cancel the running (upgrade) task for that server group before reattempting ASU for the same.

CAUTION

Before clicking **Cancel** for the server group uprade task, ensure the upgrade status of the individual servers in that particular server group should have status as completed or exception (that is, failed for some reason).

Make sure you are not cancelling a task with some servers still in running state.

Procedure 22. Recover from a Failed Upgrade

5. ☐	**Primary SDS NOAM VIP**: Cancel the Server group Upgrade task	1. Click the Server Group Upgrade task to select it. 2. Click **Cancel** to cancel the task.  3. Click **OK** on the confirmation screen to confirm the cancellation. 
6. ☐	**Primary SDS NOAM VIP**: Verify the Server Group Upgrade task is cancelled	1. On the Active Tasks screen, verify the Status changed from **paused** to **completed**. 2. Verify the Result Details column now states “SG upgrade task cancelled by user. 

Procedure 22. Recover from a Failed Upgrade

7. ☐	**Failed Server (CLI)**: Access the failed server	Use the XMI address to log into the failed server with the **admusr** account.
		`CentOS release 5.7 (Final)`
		`Kernel 2.6.18-274.7.1.e15prerel5.0.0_72.32.0 on an x86_64`
		`sds-mrsvnc-a login: admusr`
		`Password: <admusr_password>`
		***** TRUNCATED OUTPUT *****
		`RELEASE=6.4`
		`RUNID=00`
		`VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds`
		`PRODPATH=/opt/comcol/prod`
		`RUNID=00`

8. ☐	**Failed Server (CLI)**: Inspect the upgrade.log file	Identify the reason for the failure in the **upgrade.log** file.
		`[admusr@sds-mrsvnc-a ~]$ tail /var/TKLC/log/upgrade/upgrade.log`
		`1439256874:: INFO: Removing '/etc/my.cnf' from RCS repository`
		`1439256874:: INFO: Removing '/etc/pam.d/password-auth' from RCS repository`
		`1439256874:: INFO: Removing '/etc/pam.d/system-auth' from RCS repository`
		`1439256874:: INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0' from RCS repository`
		`1439256874:: INFO: Removing '/var/lib/prelink/force' from RCS repository`
		`1439256874::Marking task 1439256861.0 as finished.`
		`1439256874::`
		`1440613685::Early Checks failed for the next upgrade`
		`1440613691::Look at earlyChecks.log for more info`
		`1440613691::`

Procedure 22. Recover from a Failed Upgrade

9. ☐	**Failed Server (CLI)**: Inspect the earlyChecks.log file	Identify the reason for the failure in the **earlyChecks.log** file.
		`[admusr@sds-mrsvnc-a upgrade]$ grep ERROR /var/TKLC/log/upgrade/earlyChecks.log`
		`ERROR: There are alarms on the system!`
		`ERROR: <<< OUTPUT >>>`
		`ERROR: SEQ: 15 UPTIME: 2070747 BIRTH: 1438969736 TYPE: SET ALARM: TKSPLATMI10|tpdNTPDaemonNotSynchronizedWarning|1.3.6.1.4.1.323.5.3.18.3.1.3.10|32509|Communications|Communications Subsystem Failure`
		`ERROR: <<< END OUTPUT >>>`
		`ERROR: earlyUpgradeChecks() code failed for Upgrade::EarlyPolicy::TPDEarlyChecks`
		`ERROR: Failed running earlyUpgradeChecks() code`
		`ERROR: Early Upgrade Checks Failed!`

	CAUTION	• Although outside of the scope of this document, the user is expected to use standard troubleshooting techniques to clear the alarm condition from the failed server. • If troubleshooting assistance is needed, it is recommended to contact My Oracle Support (MOS) as described in Appendix T. • DO NOT PROCEED THE NEXT STEP UNTIL THE ALARM CONDITION HAS BEEN CLEARED!
10. ☐	**Failed Server (CLI)**: Verify platform alarms are cleared from the failed server	Use the alarmMgr utility to verify all platform alarms have been cleared from the system. `[admusr@sds-mrsvnc-b ~]$ alarmMgr –alarmStatus`

11. ☐	**Failed Server (CLI)**: Exit CLI	Exit the CLI for the failed server.
		`[admusr@sds-mrsvnc-a ~]$ exit`
		`logout`

12. ☐	Primary SDS NOAM VIP (GUI): Execute the server upgrade again.	Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option. ***Note***: Once a server has failed while using the Automated Server Group Upgrade option, the Auto Upgrade option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the Upgrade Server option.

Appendix J Add New SOAM Profile on Existing VM

CAUTION

The procedures in this appendix can be run ONLY AFTER the SDS has been upgraded to release 8.0/8.1 and the upgrade has been accepted.

Updating the SOAM VM profile is an independent procedure from the SDS upgrade and should be scheduled in a separate maintenance window.

This appendix updates the SOAM VM profile to support 1 billion subscribers. **This appendix applies only to systems that have been upgraded to release 8.0/8.1. The upgrade must be accepted before initiating these procedures.**

The SOAM VMs are updated with the new profile using the following sequence:

1. Add the SDS 8.0 ISO to the PMAC repository
2. Remove the SOAM from the SOAM server group
3. Delete the existing SOAM VM and recreate the SOAM VM with the new profile
4. Add the new SOAM VM to the SOAM server group

To access the 1 billion subscriber VM profile, the SDS 8.0 ISO must be available in the PMAC software repository. Following procedure copies the SDS 8.0 ISO from the SDS to the PMAC and adds the image to the repository.

Procedure 23. Add SDS Software Images to PMAC Server

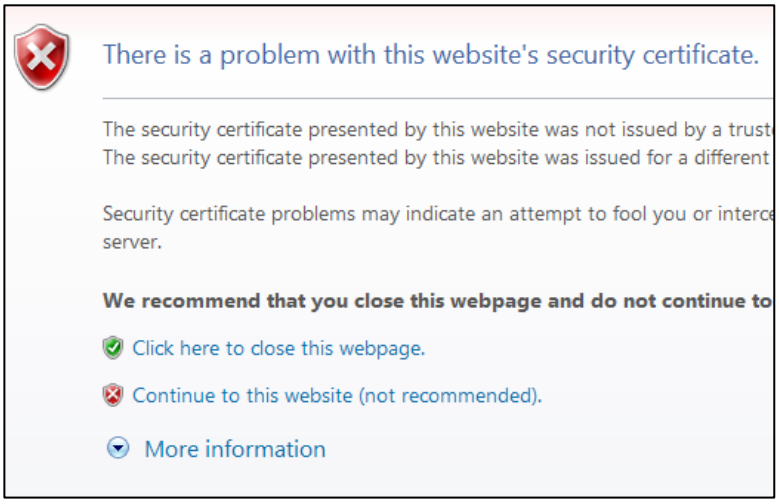
1. ☐	**Active SDS VIP (CLI)**: Login	From the command prompt, log into the server as the **admusr**.
		`login: admusr`
		`Using keyboard-interactive authentication.`
		`Password: <admusr_password>`

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

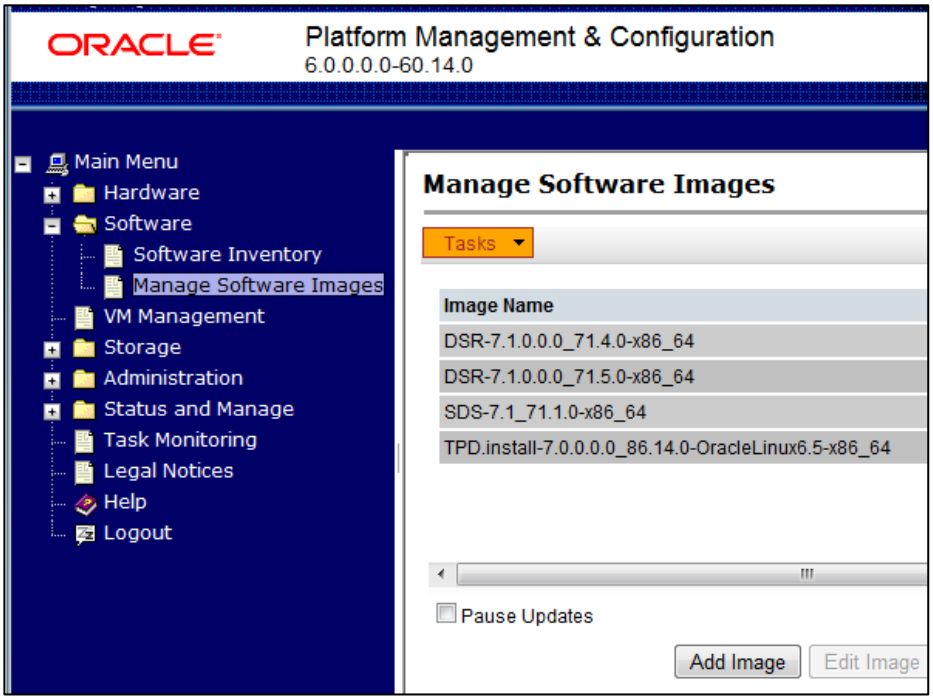
3. ☐	**Active SDS VIP (CLI)**: Verify the ISO file	Verify the SDS ISO file is present.
		`$ ls`
		`SDS-8.0.0.0.0_80.22.0-x86_64.iso`

4. ☐	**Active SDS VIP (CLI)**: Copy the file	**scp** to the SDS ISO file to the PMAC server.
		`$ scp -p SDS-8.0.0.0.0_80.22.0-x86_64.iso admusr@<PMAC_Mgmt_IP_address>:/var/TKLC/upgrade/`
		`Password: <admusr_password>`
		`SDS-8.0.0.0.0_80.22.0-x86_64.iso 100% 853MB 53.3MB/s 00:16`

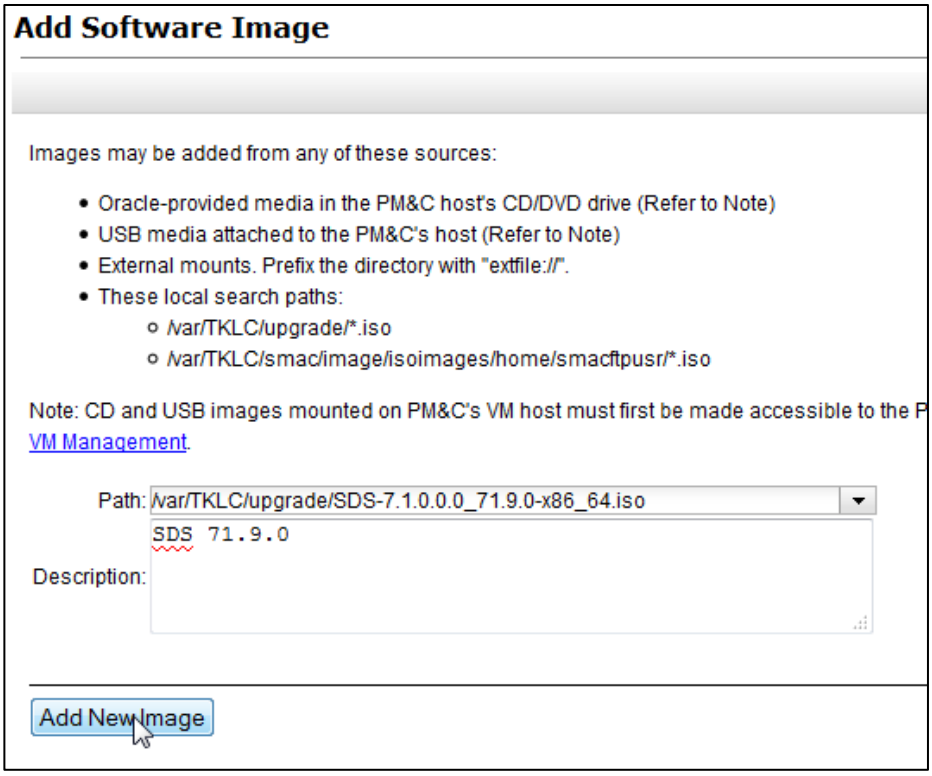
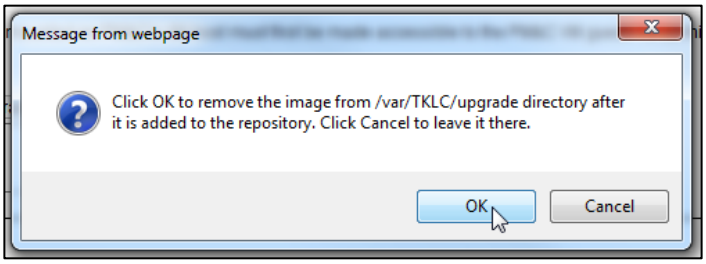
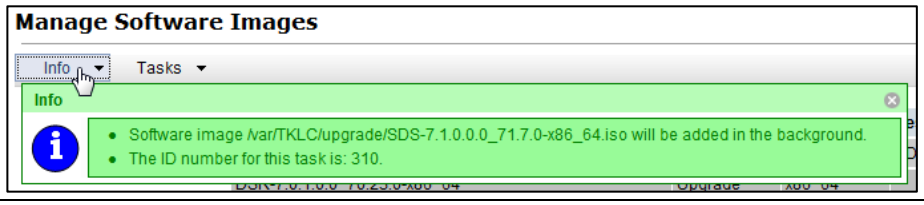
Procedure 23. Add SDS Software Images to PMAC Server

5. ☐	**PMAC Server (GUI)**: Log into the Platform Management and Configuration application	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the management IP address assigned to the PMAC server associated with the SDS SOAM NE. If a certificate error is received, click on the **Continue to this website (not recommended)** link. 
6. ☐	**PMAC Server**: Login	Login using the default user and password.

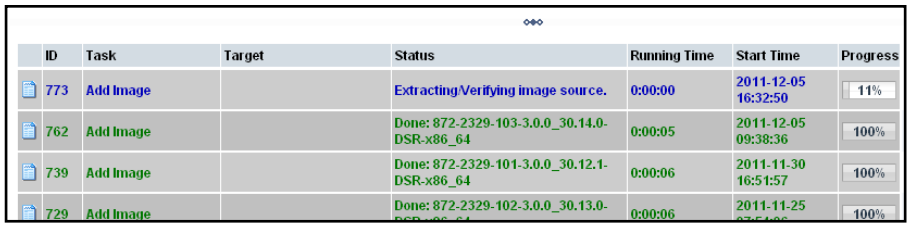
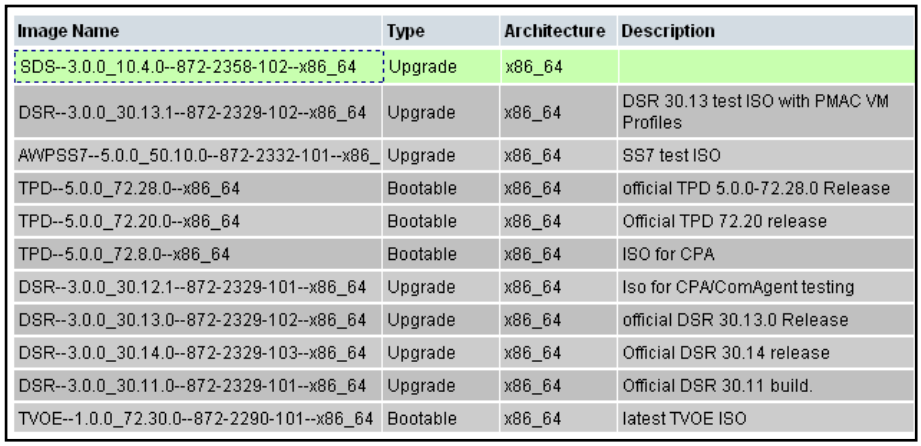
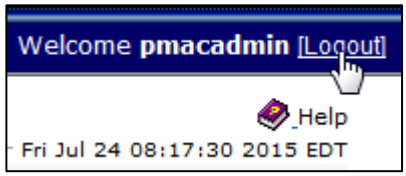
Procedure 23. Add SDS Software Images to PMAC Server

7. ☐	**PMAC Server**: Add an image	1. Navigate to **Software > Manage Software Images**. 2. Click **Add Image**. 

Procedure 23. Add SDS Software Images to PMAC Server

8. ☐	**PMAC Server**: Add an image	1. Select a **Path** from the list. 2. Add a **Description**. 3. Click **Add New Image**.  4. Click **OK** when asked to confirm.  An **Info** message displays to show the task. 

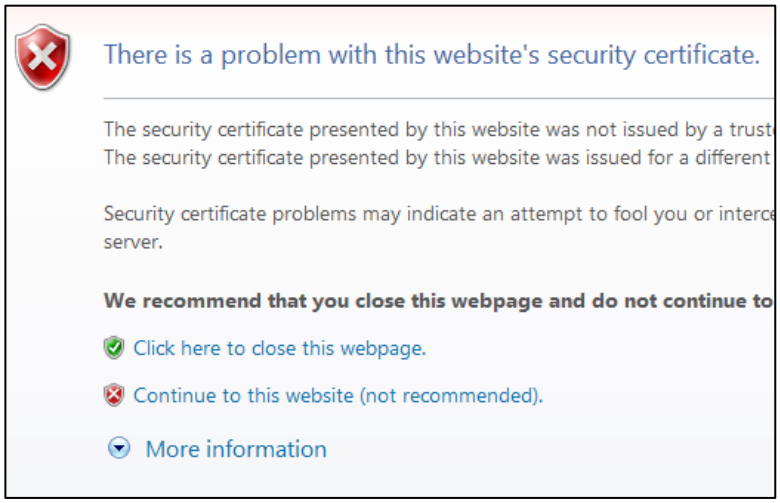
Procedure 23. Add SDS Software Images to PMAC Server

9. ☐	**PMAC Server**: Monitor progress	Monitor the progress using Tasks tab in the banner.  The new software image displays in the list when complete. 
10. ☐	**PMAC Server**: Log out	Click **Logout**. 
11. ☐	SDS Health Check	Execute SDS Health Check procedures as specified in Appendix A.

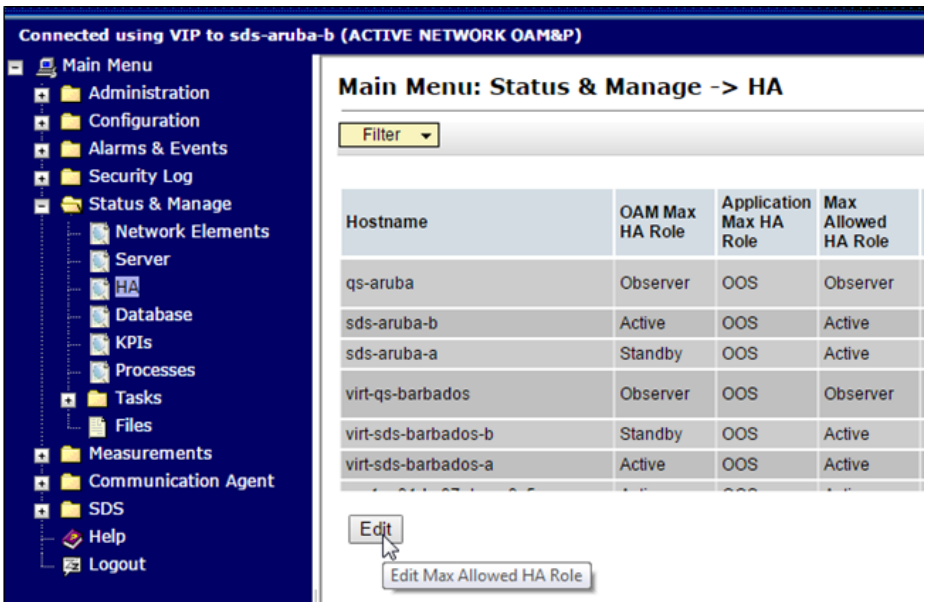
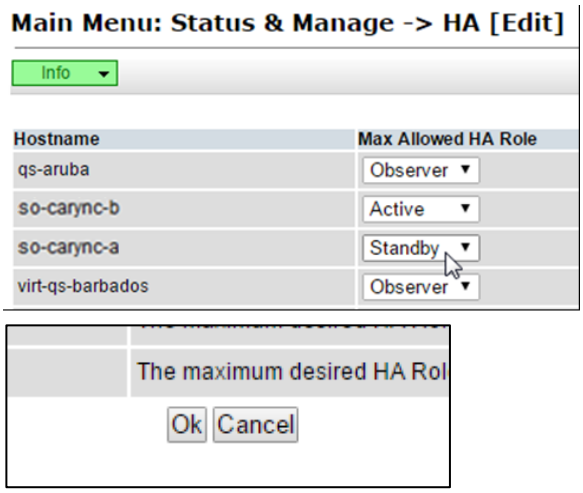
ID	Task	Target	Status	Running Time	Start Time	Progress
773	Add Image		Extracting/Verifying image source.	0:00:00	2011-12-05 16:32:50	11%
762	Add Image		Done: 872-2329-103-3.0.0_30.14.0-DSR-x86_64	0:00:05	2011-12-05 09:38:36	100%
739	Add Image		Done: 872-2329-101-3.0.0_30.12.1-DSR-x86_64	0:00:06	2011-11-30 16:51:57	100%
729	Add Image		Done: 872-2329-102-3.0.0_30.13.0-	0:00:06	2011-11-25	100%

Image Name	Type	Architecture	Description
SDS--3.0.0_10.4.0--872-2358-102--x86_64	Upgrade	x86_64	
DSR--3.0.0_30.13.1--872-2329-102--x86_64	Upgrade	x86_64	DSR 30.13 test ISO with PMAC VM Profiles
AWPSS7--5.0.0_50.10.0--872-2332-101--x86_	Upgrade	x86_64	SS7 test ISO
TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	official TPD 5.0.0-72.28.0 Release
TPD--5.0.0_72.20.0--x86_64	Bootable	x86_64	Official TPD 72.20 release
TPD--5.0.0_72.8.0--x86_64	Bootable	x86_64	ISO for CPA
DSR--3.0.0_30.12.1--872-2329-101--x86_64	Upgrade	x86_64	Iso for CPA/ComAgent testing
DSR--3.0.0_30.13.0--872-2329-102--x86_64	Upgrade	x86_64	official DSR 30.13.0 Release
DSR--3.0.0_30.14.0--872-2329-103--x86_64	Upgrade	x86_64	Official DSR 30.14 release
DSR--3.0.0_30.11.0--872-2329-101--x86_64	Upgrade	x86_64	Official DSR 30.11 build.
TVOE--1.0.0_72.30.0--872-2290-101--x86_64	Bootable	x86_64	latest TVOE ISO

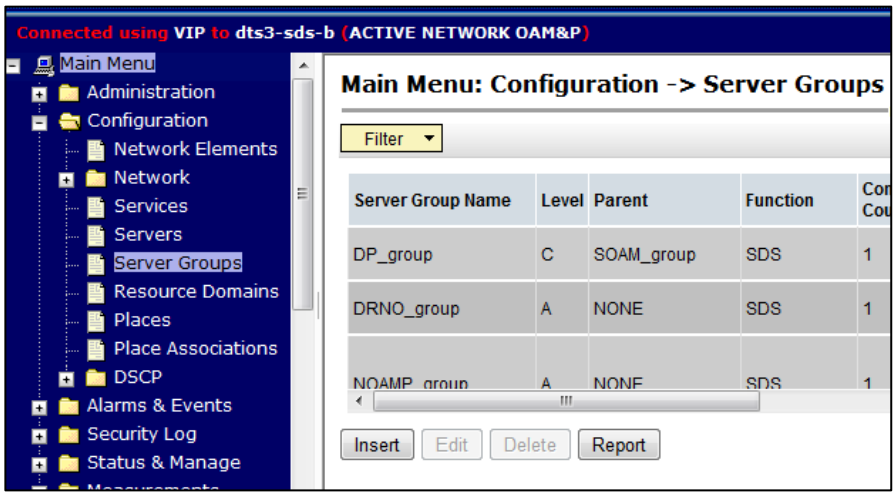
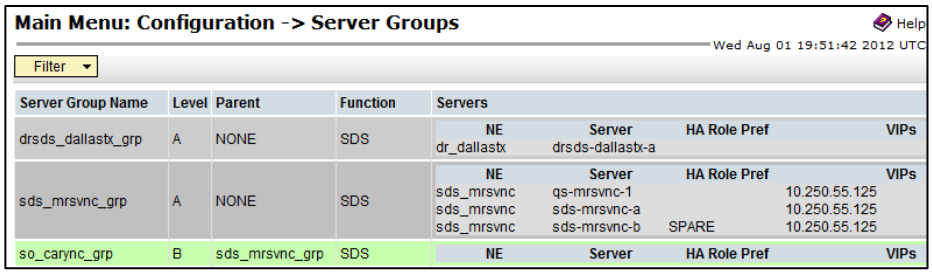
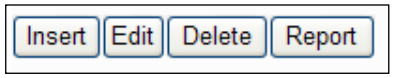
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group

1. ☐	**Primary NOAM VIP**: Log into the NOAM VIP address	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the NOAM VIP address. If a certificate error is received, click on the **Continue to this website (not recommended)** link. 
2. ☐	**Primary NOAM VIP**: Login	Login using the default user and password.

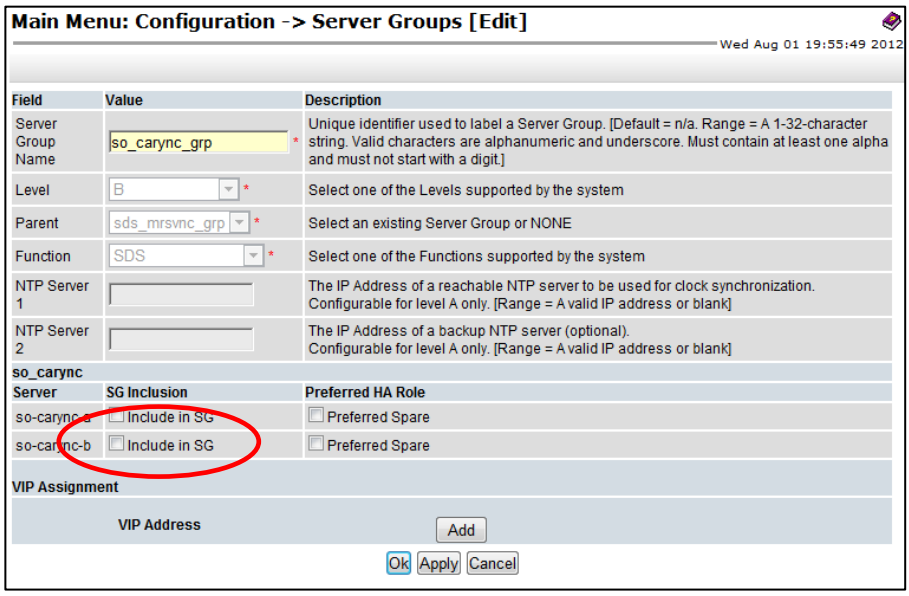
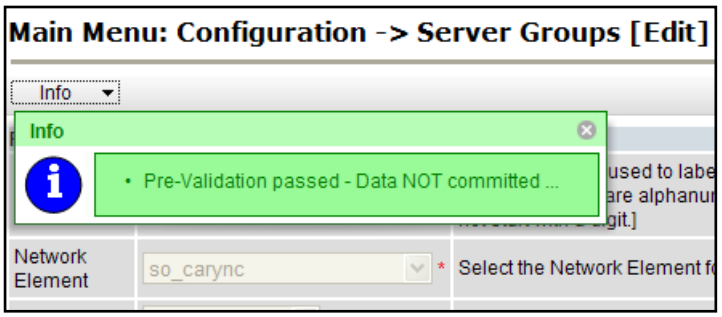
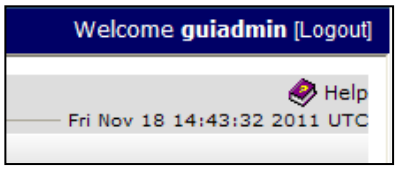
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group

3. ☐	**Primary SDS NOAM VIP**: Edit an HA role	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 
4. ☐	**Primary SDS NOAM VIP**: Change the SOAM server HA role to Standby	1. Select the active primary SDS SOAM server and change the **Max Allowed HA Role** to **Standby**. 2. Click **OK**. 

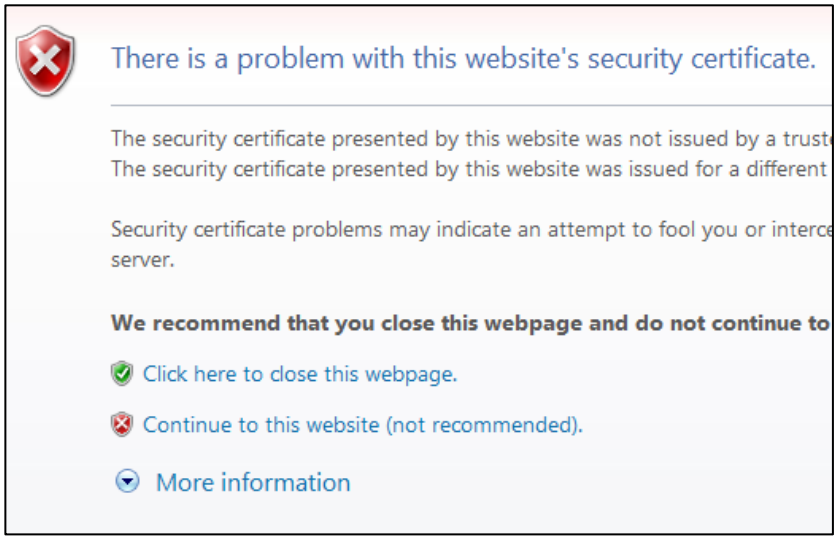
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group

5. ☐	**Primary NOAM VIP**: Edit the SOAM server	1. Navigate to **Configuration > Server Groups**.  2. Select the server group with the SOAM server to be converted to the aB subscriber.  3. Click **Edit**.  ***Note***: You may need to scroll to see the **Edit** button.

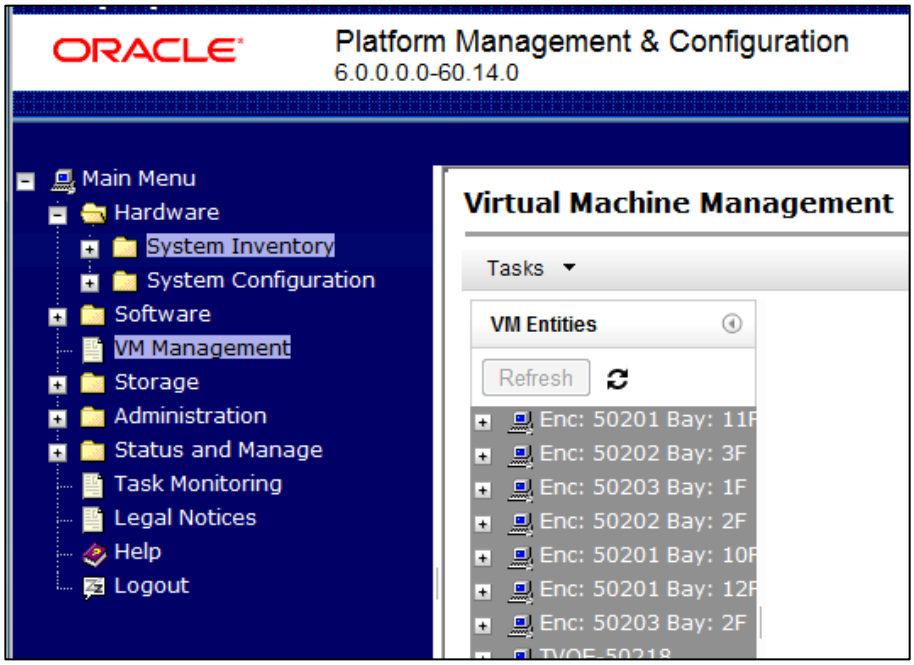
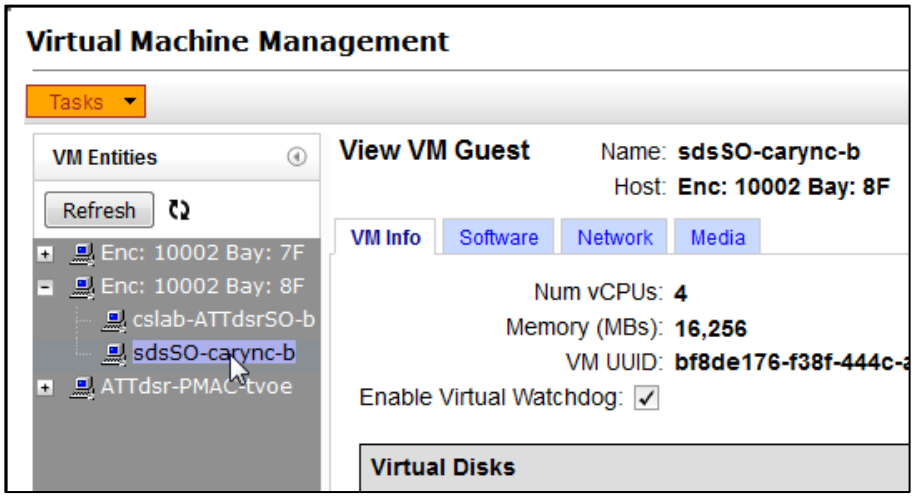
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group

6. ☐	**Primary NOAM VIP**: Ready server for pre-validation	1. Remove the **SG Inclusion** checkmark from the server group.  2. When the **Pre-Validation passed** message displays, click **Apply**. 
7. ☐	**Primary NOAM VIP**: Log out	Click **Logout** to log out of the SDS GUI. 

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

1. ☐	**PMAC Server (GUI)**: Log into the Platform Management and Configuration application	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the management IP address assigned to the PMAC server associated with the SDS SOAM NE. If a certificate error is received, click on the **Continue to this website (not recommended)** link. 
2. ☐	**PMAC Server**: Login	Login using the default user and password.

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

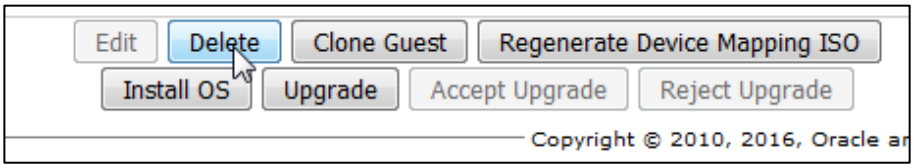
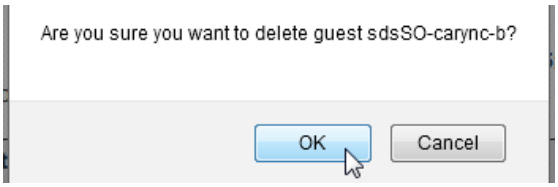
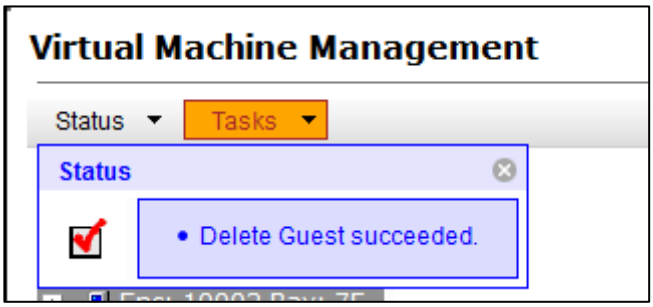
3. ☐	**PMAC Server GUI**: Access VM Management screen	Navigate to **VM Management**. 
4. ☐	**PMAC Server GUI**: Select the 1B subscriber profile	1. In the VM Entities box, click the plus sign (+) to expand the folder for the OAM blade containing the SOAM VM to be converted to the 1B Subscriber profile. 2. Click on the SOAM VM to be converted to the 1B Subscriber profile. 

CAUTION

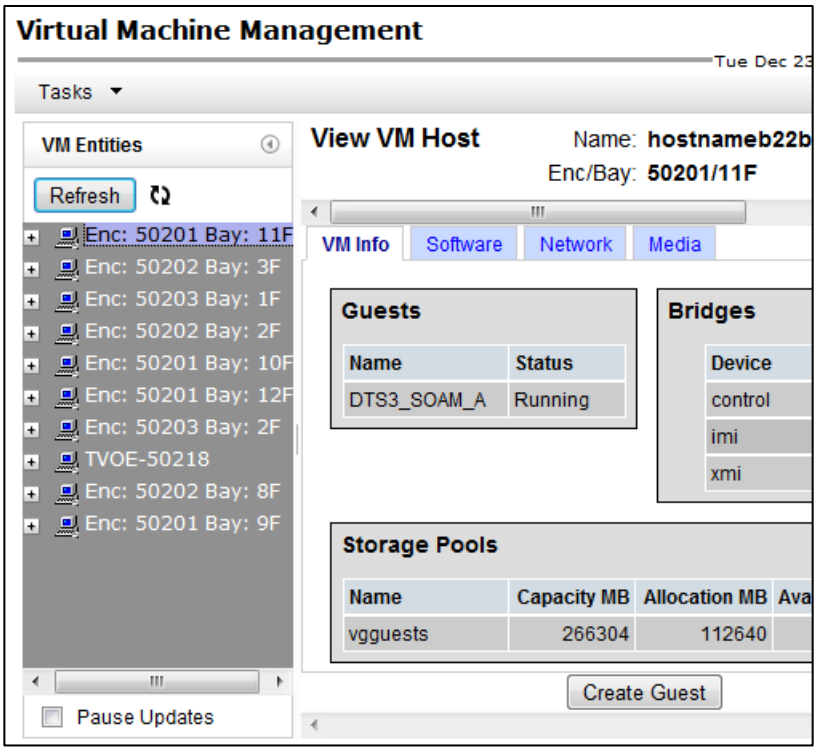
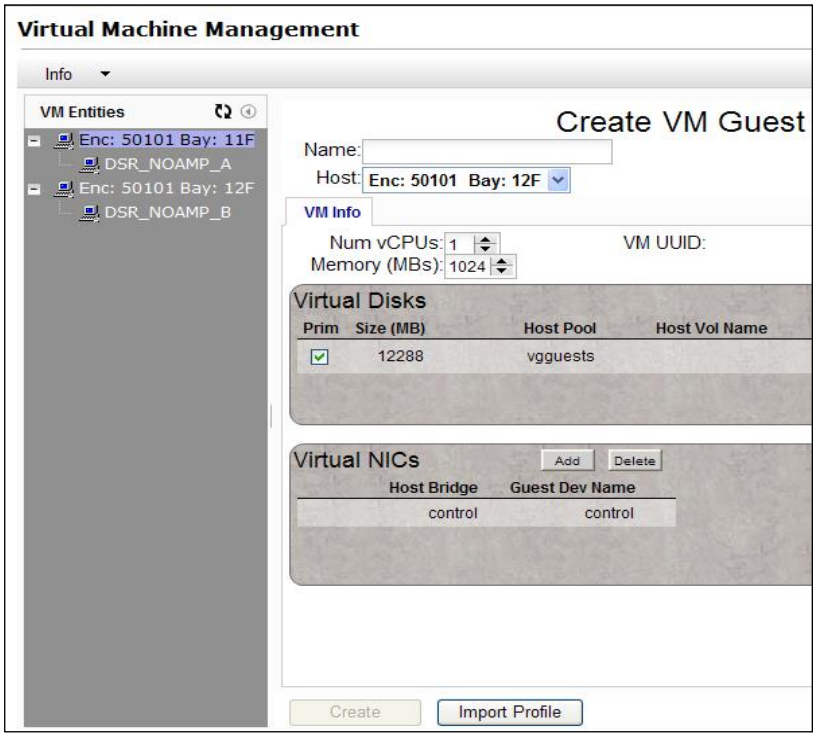
Verify the correct SDS SOAM VM is selected since the next step deletes the VM from the OAM blade.

It is imperative that only the SDS SOAM VM removed from the server group (Procedure 24) is selected for deletion.

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

5. ☐	**PMAC Server GUI**: Delete the VM	1. Click **Delete**.  2. Click **OK** to confirm.  Wait for the **Delete Guest succeeded** confirmation banner (up to a minute). 

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

6. ☐	**PMAC Server GUI**: Create the profile on the server	1. Select the OAM blade containing the SOAM VM to be converted to the 1B Subscriber profile. 2. Click **Create Guest**.  3. Click **Import Profile**. 

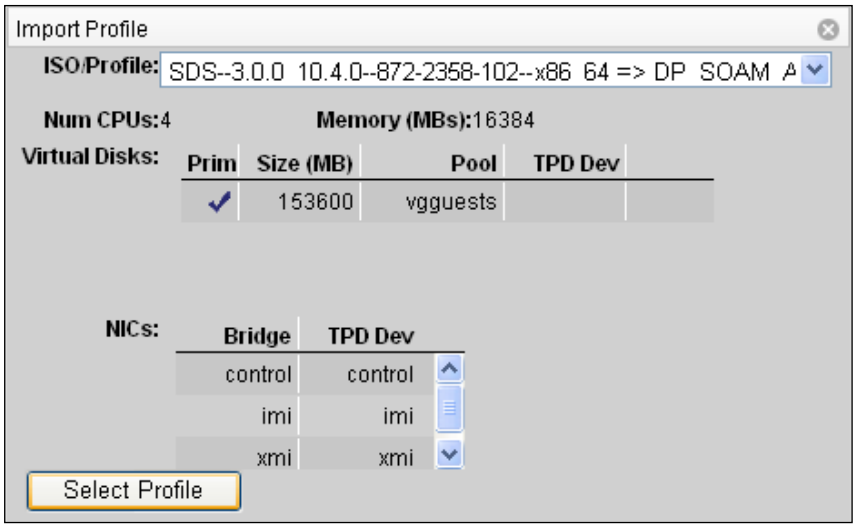
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

7. ☐ **PMAC Server GUI**: Select the ISO/Profile value

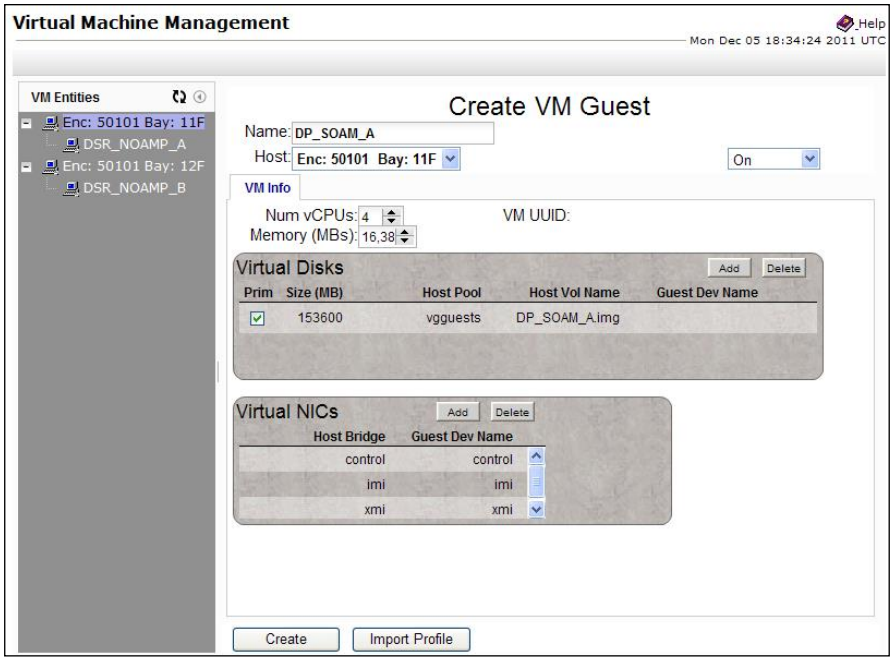
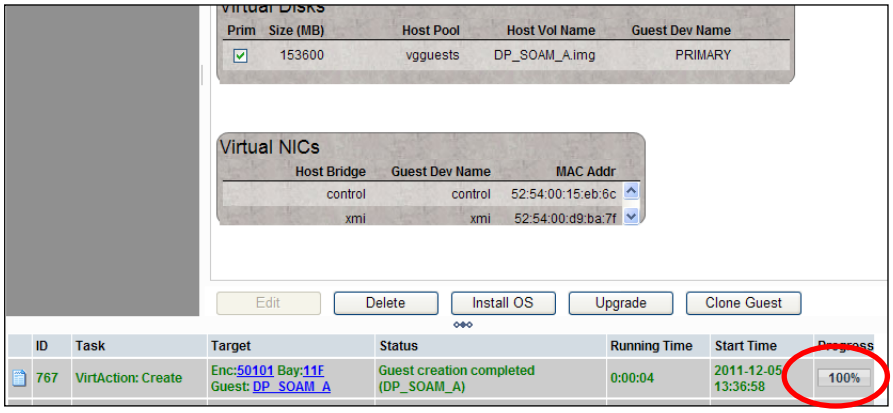
1. Select the **ISO/Profile** option that matches the hardware your SOAM VM TVOE server is running.

Release	OAM Blade HW Type	ISO File	Profile
SDS 7.1	HP BL460 G6	7.1.1.0.0_xx.xx.xx-x86_64	DP_SOAM_A DP_SOAM_B
SDS 7.1	HP BL460 Gen8/Gen9	7.1.1.0.0_xx.xx.xx-x86_64	DP_SOAM_A DP_SOAM_B
SDS 7.2	HP BL460 G6	7.2.0.0.0_xx.xx.xx-x86_64	Not Supported
SDS 7.2	7	7.2.0.0.0_xx.xx.xx-x86_64	DP_SOAM_1B_RE
SDS 7.3	HP BL460 G6	7.3.0.0.0_xx.xx.xx-x86_64	Not Supported
SDS 7.3	HP BL460 Gen8/Gen9	7.3.0.0.0_xx.xx.xx-x86_64	DP_SOAM_1B_RE
SDS 8.0	HP BL460 Gen8/Gen9	8.0.0.0.0_xx.xx.xx-x86_64	DP_SOAM_1B_RE

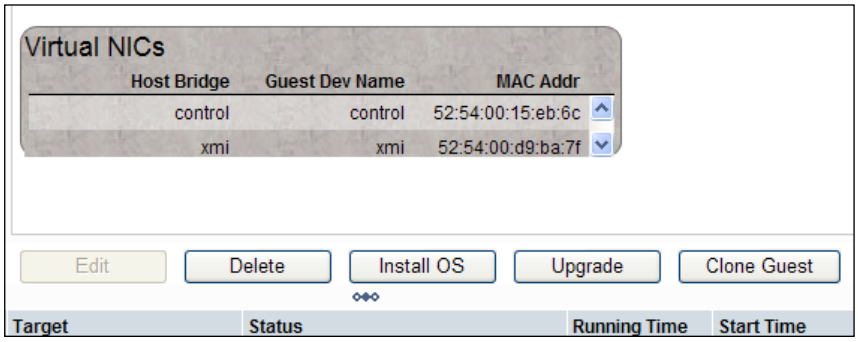
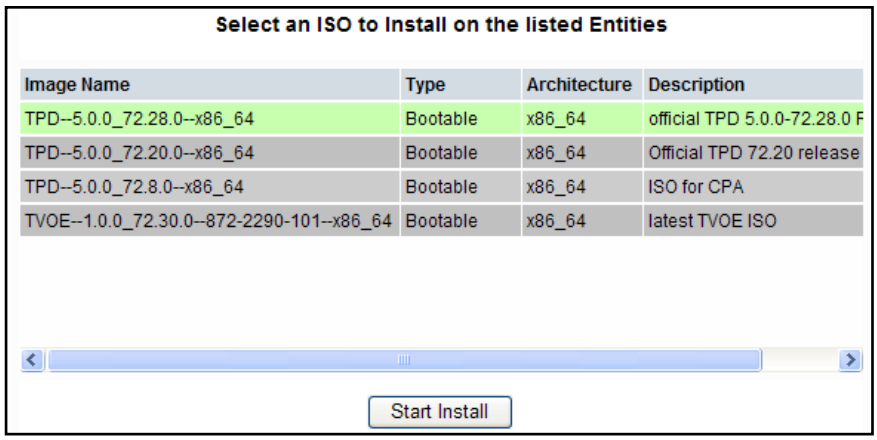
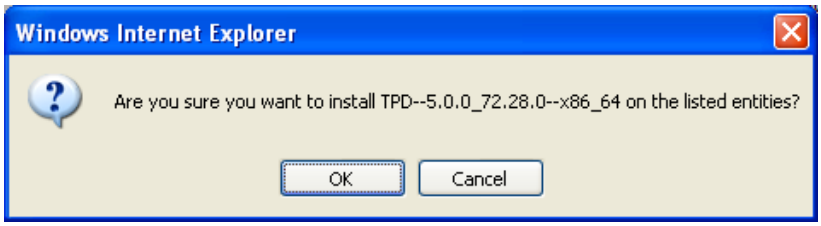
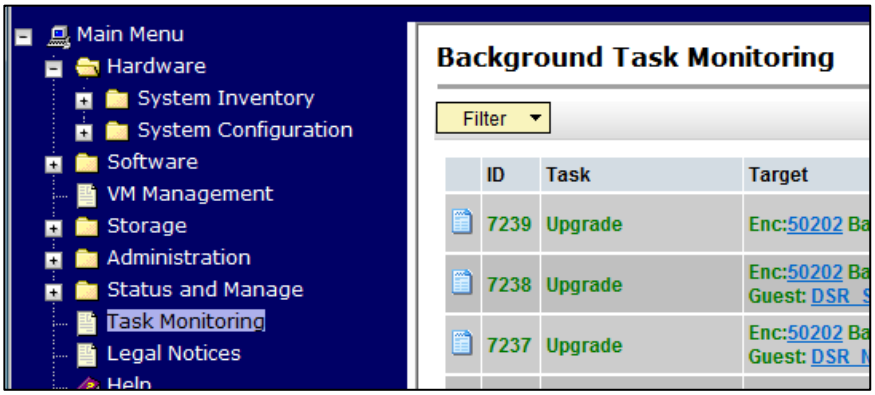
2. Click **Select Profile**.



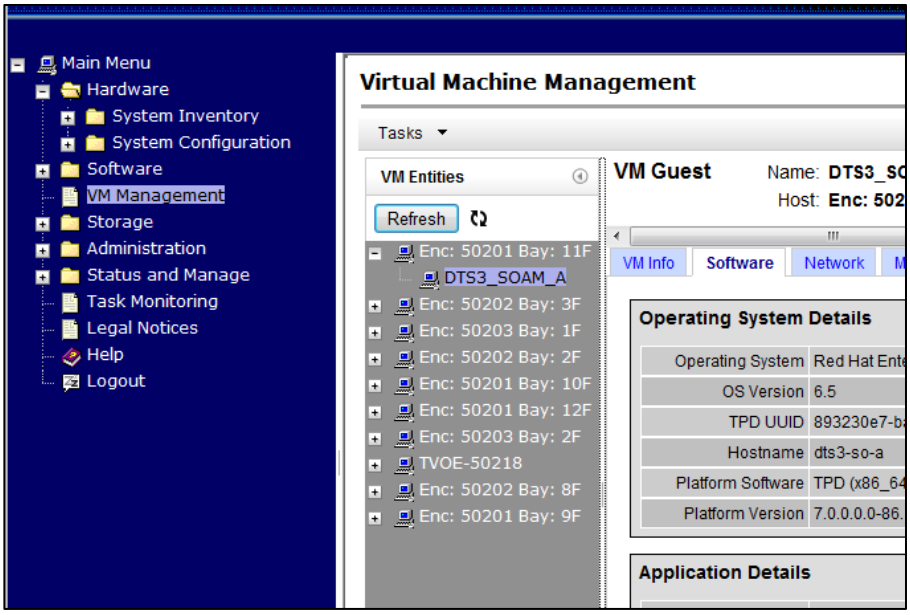
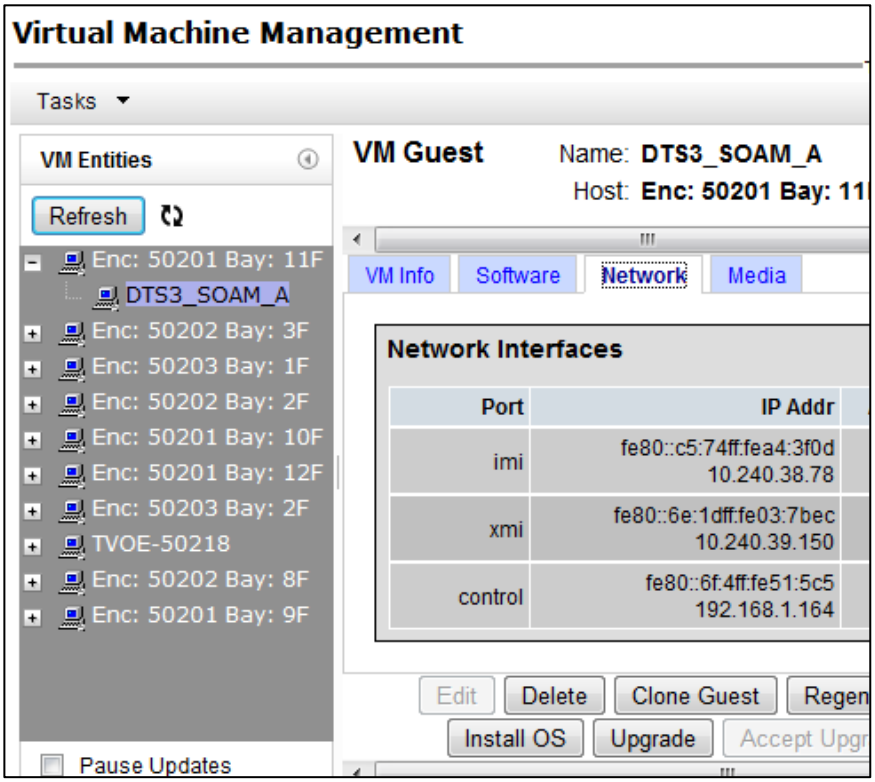
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

8. ☐	**PMAC Server GUI**: Create VM host	1. Type the server host **Name** (for example, so-mrsvnc-a). 2. Click **Create**.  ***Note***: If the VM guest creation fails due to a **Host resources are oversubscribed** error, contact My Oracle Support (MOS) as described in Appendix T. 3. Verify the task successfully completes by watching the **Progress** value change to 100%. 

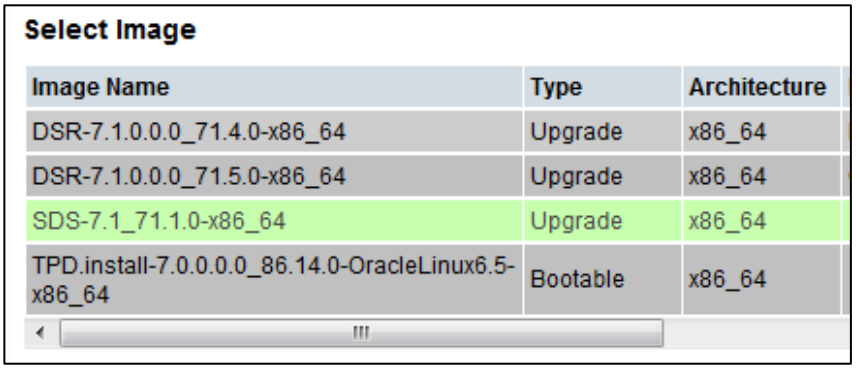
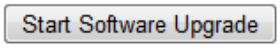
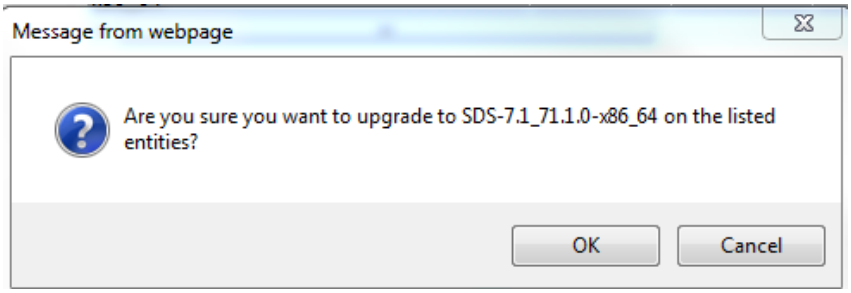
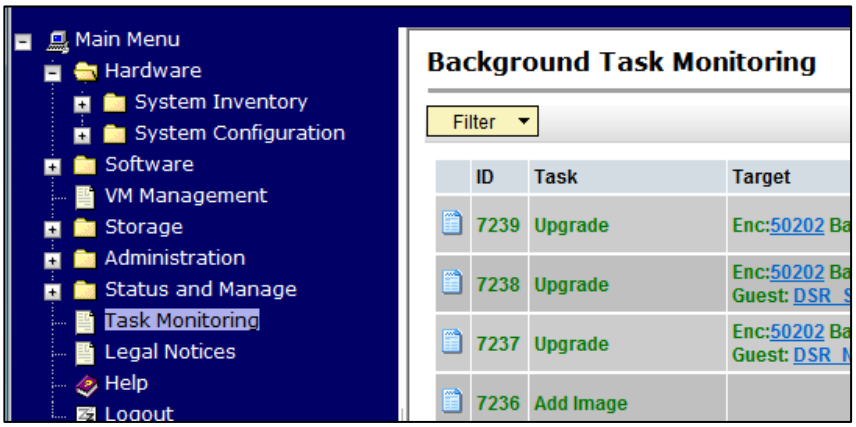
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

9. ☐	**PMAC Server GUI**: Install the operating system	Click **Install OS**. 
10. ☐	**PMAC Server GUI**: Start the installation of the TPD image	1. Select the TPD image and click **Start Install**.  2. Click **OK** to confirm.  3. Monitor the installation task by navigating to **Task Monitoring**. It should take about 11 minutes until you see the **Progress** value change to 100%. 

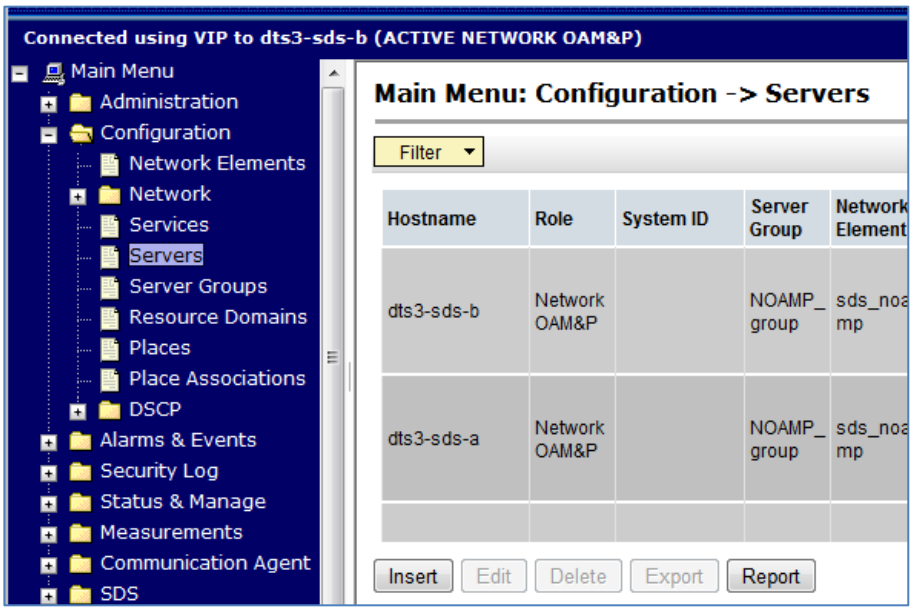
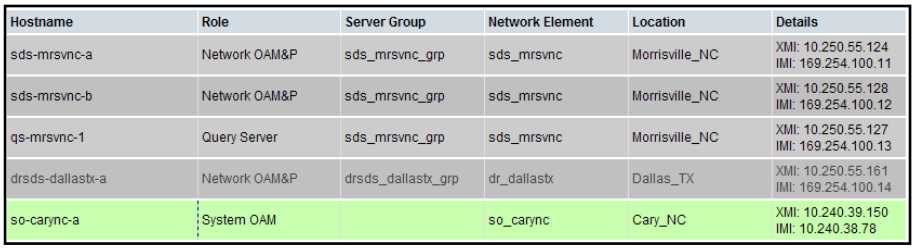
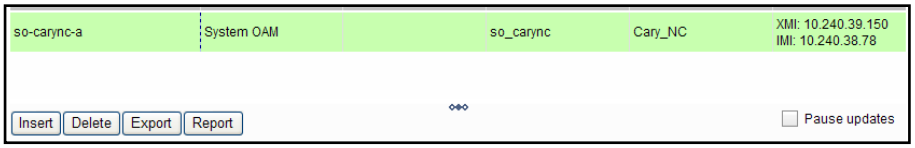
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

11. ☐	**PMAC Server GUI**: Verify installation	1. Navigate to **VM Management**. 2. From the Tasks tab, verify the operating system has been installed. The **Application Details** section is blank. 
12. ☐	**PMAC Server GUI**: Upgrade the network.	1. From the Network tab, record the control IP address for this SOAM VM (to be used later). 2. Click **Upgrade**. 

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

13. ☐	**PMAC Server GUI**: Start the software upgrade	1. Selet the SDS version from the **Image Name** column and click **Start Software Upgrade**.   2. Click **OK** to confirm.  3. Navigate to **Task Monitoring** to monitor the upgrade. 

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

14. ☐	**Primary SDS VIP**: Export the recreated SOAM server	1. Navigate to **Configuration > Servers**.  2. Select the recreated SOAM server from the list.  3. Click **Export**. 
15. ☐	**SDS VIP CLI**: Access the active NOAM server CLI	Connect to the active SDS NOAM CLI using SSH terminal session to the NOAM VIP address.

16. ☐	**SDS VIP CLI**: Login	Log into the server as the **admusr** user.
		`login: admusr`
		`Password: <admusr_password>`

17. ☐	**SDS VIP CLI**: Change directory	Change directory into the file management location. `$ cd /var/TKLC/db/filemgmt`

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

18. ☐	**SDS VIP CLI**: Directoy list	Get a directory listing and find the configuration file containing the SOAM server name
		`$ ls –ltr TKLCConfigData*.sh`
		***** TRUNCATED OUTPUT *****
		`-rw-rw-rw- 1 root root 2208 Dec 19 16:50 TKLCConfigData.so-carync-b.sh`

19. ☐	**SDS VIP CLI**: Copy configuration file	Copy the configuration files found in the previous step to the PMAC.
		`$ scp -p <configuration_file> admusr@<PMAC_Mgmt_IP>:/tmp/`
		`admusr@xxx.xxx.xxx.xxx's password: <admusr_password>`
		`TKLCConfigData.so-carync-b.sh 100% 1741 1.7KB/s 00:00`

20. ☐	**SDS VIP CLI**: Log out of the active NOAM CLI	`$ exit`

21. ☐	**PMAC Server CLI**: Login	Use SSH to log into the PMAC guest VM server as the **admusr** user.
		`login: admusr`
		`Password: <admusr_password>`

22. ☐	**PMAC Guest VM**: Copy configuration file	Copy the server configuration file to the control IP for the SDS SOAM VM.
		`$ scp -p /tmp/<configuration_file> admusr@<SDS_SOAM_VM_Control_IP>:/tmp/`
		`admusr@xxx.xxx.xxx.xxx's password:`
		`TKLCConfigData.so-carync-a.sh 100% 1741 1.7KB/s 00:00`
		Note: The control IP for each the SOAM VM was recorded in step 12 of this procedure.

23. ☐	**PMAC Guest VM**: Connect to the SOAM server CLI	Connect to the SOAM server CLI from the PMAC server console.
		`$ ssh <SDS_SOAM_VM_Control_IP>`
		`admusr@xxx.xxx.xxx.xxx's password: <admusr_password>`

24. ☐	**SOAM Guest VM**: Copy configuration file	Copy the server configuration file to the **/var/tmp** directory on the server, making sure to rename the file by omitting the server hostname from the file name. **Example**: **TKLCConfigData.<server_hostname>.sh** translates to **TKLCConfigData.sh** `$ cp –p /tmp/TKLCConfigData.so-carync-b.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.

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

25. ☐	**SOAM Guest VM**: Monitor for broadcast message sent to the terminal	***Note***: The time to complete this step varies by server and may take from 3-5 minutes to complete.
		*** NO OUTPUT FOR ≈ 3-5 MINUTES ***
		`Broadcast message from root (Mon Dec 14 15:47:33 2009):`
		`Server configuration completed successfully!`
		`See /var/TKLC/appw/logs/Process/install.log for details.`
		`Remove the USB flash drive if connected and reboot the server.`
		`<ENTER>`

26. ☐	**SOAM Guest VM**: 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`
		`Checking /tmp/appworks_temp`
		`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 '/var/lib/prelink/force' from RCS repository`
		`INFO: Removing '/etc/my.cnf' from RCS repository`

27. ☐	**SOAM Guest VM**: Verify the desired time zone is currently in use	`$ date`
		`Mon Aug 10 19:34:51 UTC 2015`
		Configure the time zone (optional)
		`$ sudo set_ini_tz.pl <time_zone>`
		Note: The following command example sets the time to the **UTC** (aka GMT) time zone, which is recommneded for all sites.
		Replace, as appropriate, with the customer requested time zone for this site installation. See Appendix H from reference [1] for a list of valid time zones.
		`$ sudo set_ini_tz.pl "Etc/UTC"`

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

28. ☐	**SOAM Guest VM**: Reboot the SOAM server	Reboot the SOAM server.
		`$ sudo init 6`
		Sample output:
		`Connection to xxx.xxx.xxx.xxx closed by remote host.`
		`Connection to xxx.xxx.xxx.xxx closed.`

29. ☐	**PMAC Guest VM**: Reboot the SOAM server console	Reboot and reconnect to the SOAM server console from the PMAC server console.
		`$ ssh <SDS_SOAM_VM_Control_IP>`
		`admusr@xxx.xxx.xxx.xxx's password: <admusr_password>`

30. ☐	**SOAM Guest VM**: Verify address	Verify IMI and XMI addresses have been applied.
		`$ 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`

31. ☐	**SOAM Guest VM**: Check health of server	**Syscheck** the current health of the server.
		`$ sudo syscheck`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class disk...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

32. ☐	**SOAM Guest VM**: PING the XMI IP address	From the SOAM Guest, **ping** the IMI IP address of the mate SOAM VM 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`

33. ☐	**SOAM Guest VM**: PING the XMI IP address	From the SOAM Guest, **ping** the XMI IP address of the mate SOAM VM 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`

34. ☐	**SOAM Guest VM**: PING the gateway	From the SOAM 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`

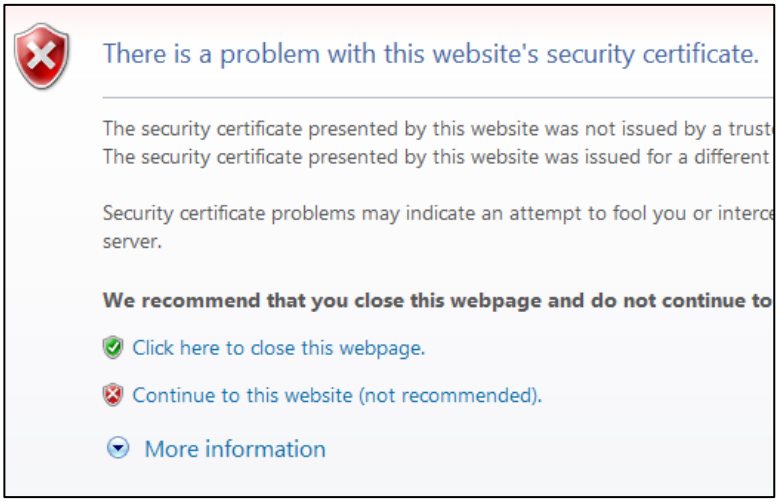
35. ☐	**SOAM Guest VM**: Verify server connectivity	Use the **ntpq** command to verify the server has connectivity to at least one of the assigned NTP server(s).
		Note: NTP connectivity is denoted by the presence of an asterisk (*) to the left of one of the **remote** IP addresses.
		`$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================`
		`+10.250.32.10 192.5.41.209 2 u 139 1024 377 2.008 1.006 1.049`
		`*10.250.32.51 192.5.41.209 2 u 979 1024 377 0.507 1.664 0.702`

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

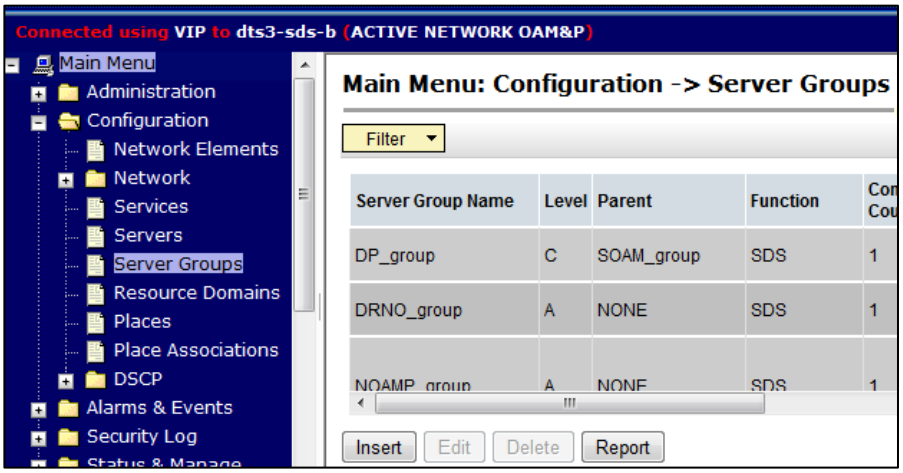
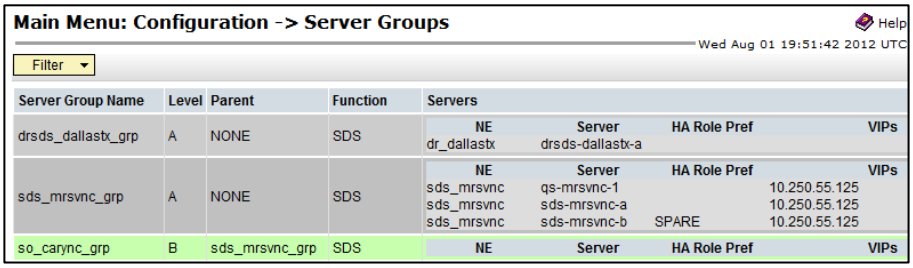
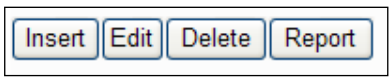
	CAUTION	If connectivity to the NTP server(s) cannot be established, stop and repeat the previous step until NTP connectivity is established before continuing to the next step.
36. ☐	**SOAM Guest VM**: Exit from the SOAM	Exit from the SOAM command line to return the PMAC server console prompt. `$ exit`
37. ☐	**PMAC Guest VM**: Exit from the PMAC server	`$ exit`

Procedure 26 adds the newly created SOAM VM to the SOAM server group.

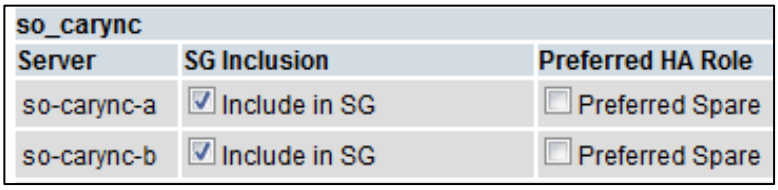
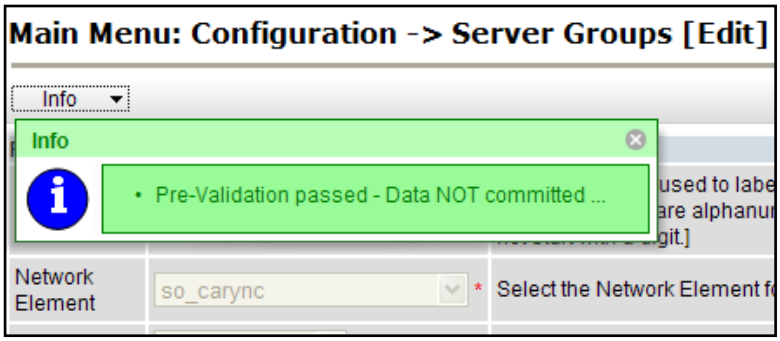
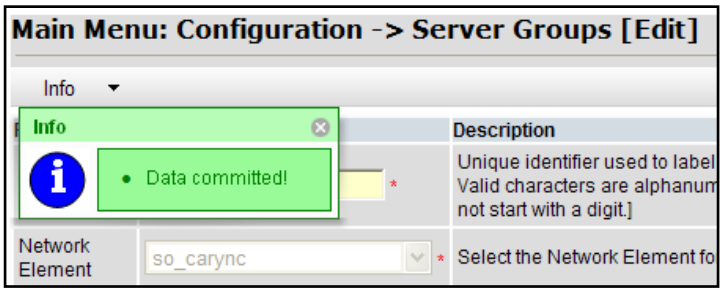
Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

1. ☐	**SDS NOAM VIP**: Log into the NOAM VIP address	Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the SDS NOAM VIP address. If a certificate error is received, click on the **Continue to this website (not recommended)** link. 

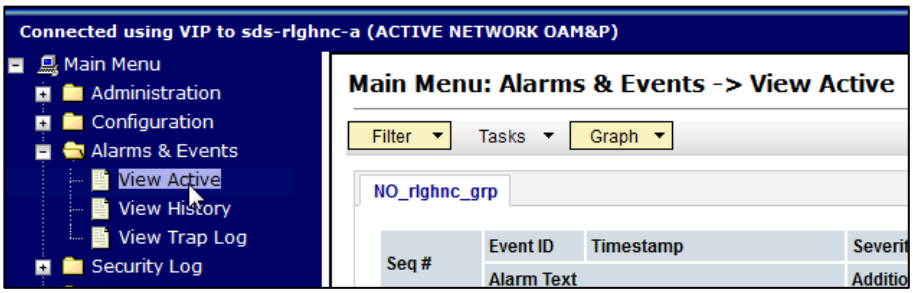
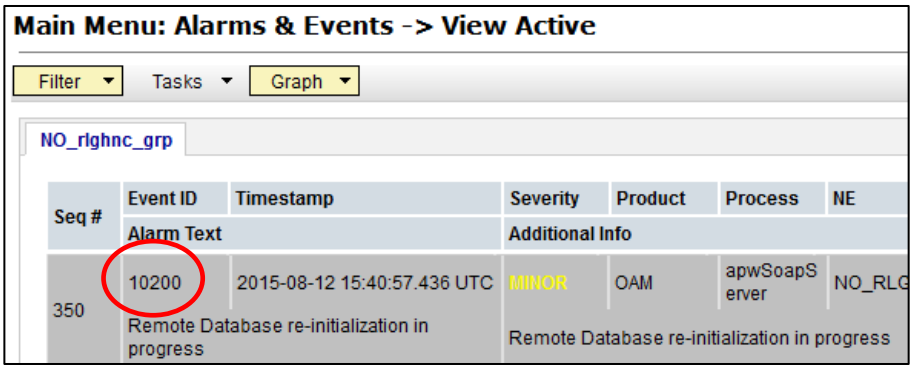
Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

2. ☐	**SDS NOAM VIP**: Login	Login using the default user and password.
3. ☐	**SDS NOAM VIP**: Edit the SOAM server	1. Navigate to **Configuration > Server Groups**.  2. Select the SOAM server that was converted to the 1B Subscriber profile.  3. Click **Edit**.  ***Note***: You may need to scroll to see the **Edit** button.

Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

4. ☐	**SDS NOAM VIP**: Ready server for pre-validation	1. Mark the **SG Inclusion** checkbox for the server.  2. When the **Pre-Validation passed** message displays, click **Apply**.  The Info banner changes to **Data committed**. 

Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

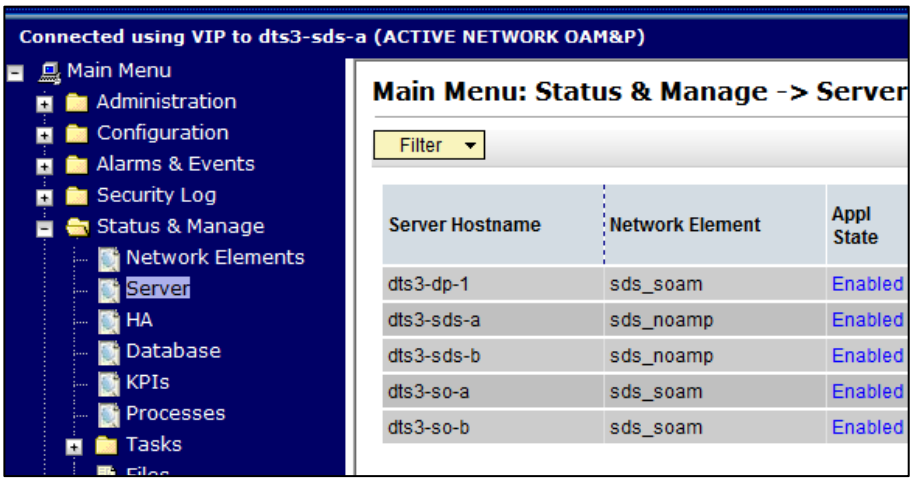
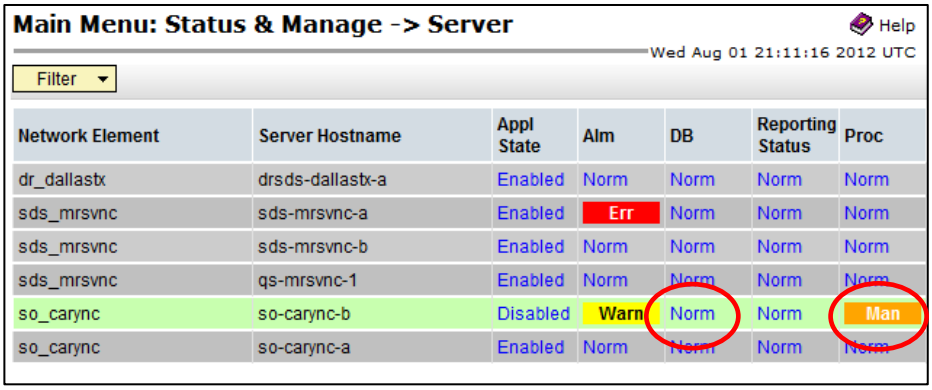
5. ☐	**SDS NOAM VIP**: View alarm status	1. Navigate to **Alarms & Events > View Active**.  2. Verify **Event ID 10200 Remote Database re-initialization in progress** is present with the SDS SOAM server hostname. 

CAUTION

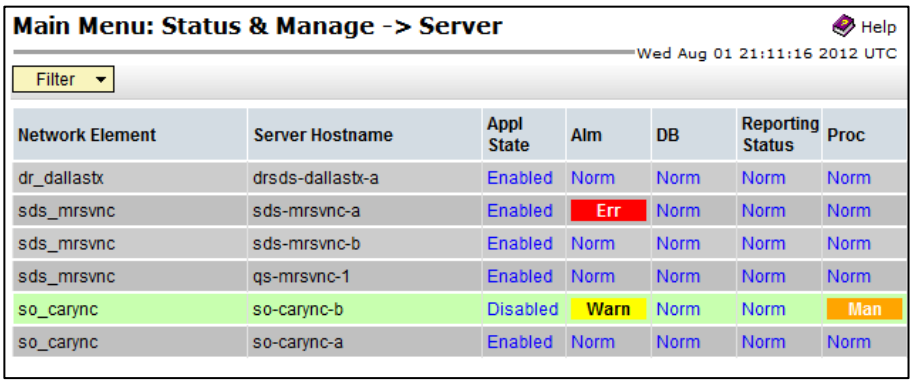
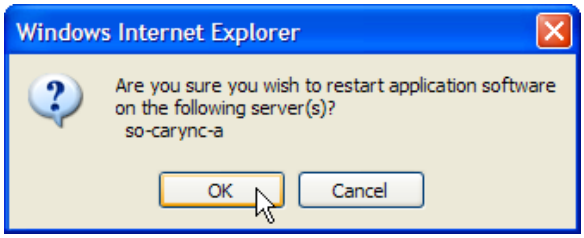
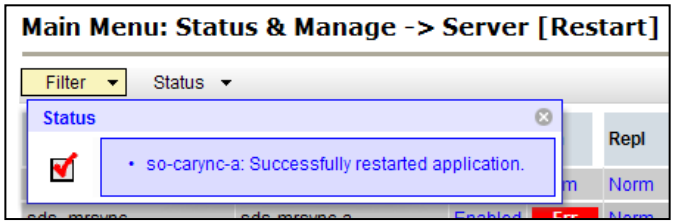
Monitor the Event ID **10200 Remote Database re-initialization in progress** alarm.

Do not proceed to the next step until the alarm clears for the SDS SOAM server.

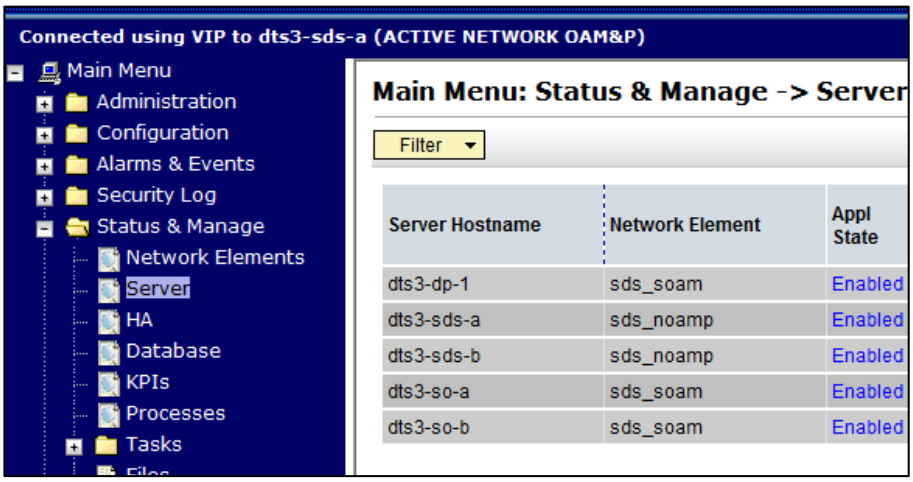
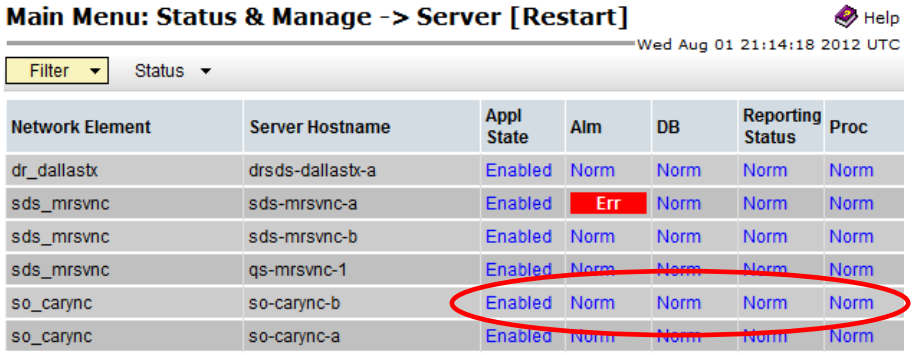
Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

6. ☐	**SDS NOAM VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify Server Status is Normal (**Norm**) for Database (DB) and **Man** for Processes (Proc). 

Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

7. ☐	**SDS NOAM VIP**: Restart the SOAM server	1. Select the SOAM server.  2. Click **Restart**. 3. Click **OK** to confirm.  A **Successfully restarted application** message displays in the banner. 

Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

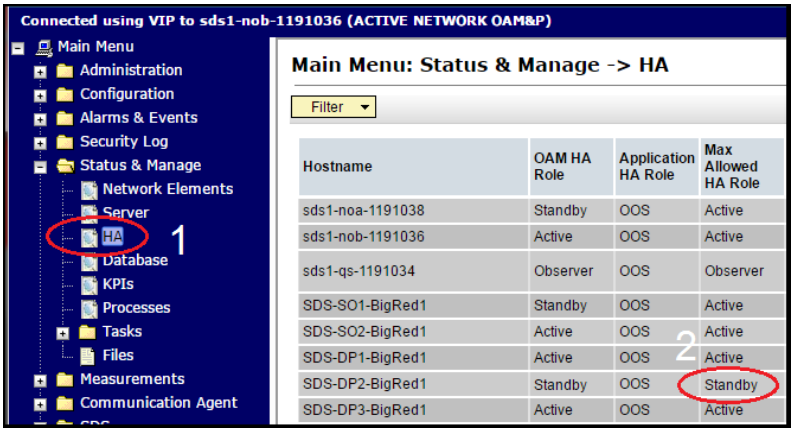
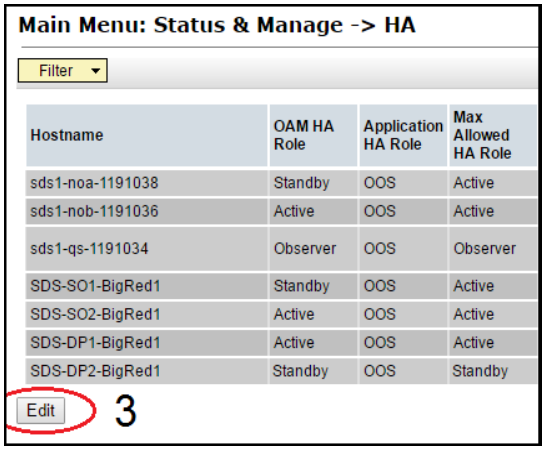
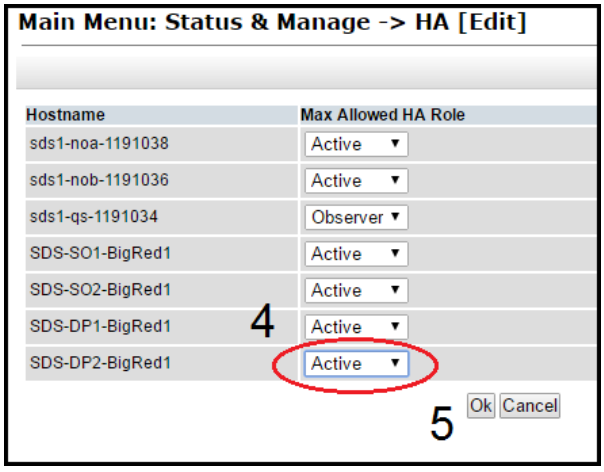
8. ☐	**SDS NOAM VIP**: Verify status	1. Navigate to **Status & Manage > Server**.  2. Verify Appl State is **Enabled** and Server Status is Normal (**Norm**) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).  ***Note**:* To refresh the Server Status screen in advance of the default setting (15-30 sec.), navigate to **Status & Manage > Server** again.
9. ☐	**SDS NOAM VIP**: Log out	Click **Logout** to log out of the SDS GUI.
10. ☐	SDS Health Check	Execute SDS Health Check procedures as specified in Appendix A.

Appendix K Manual Completion of Server Upgrade

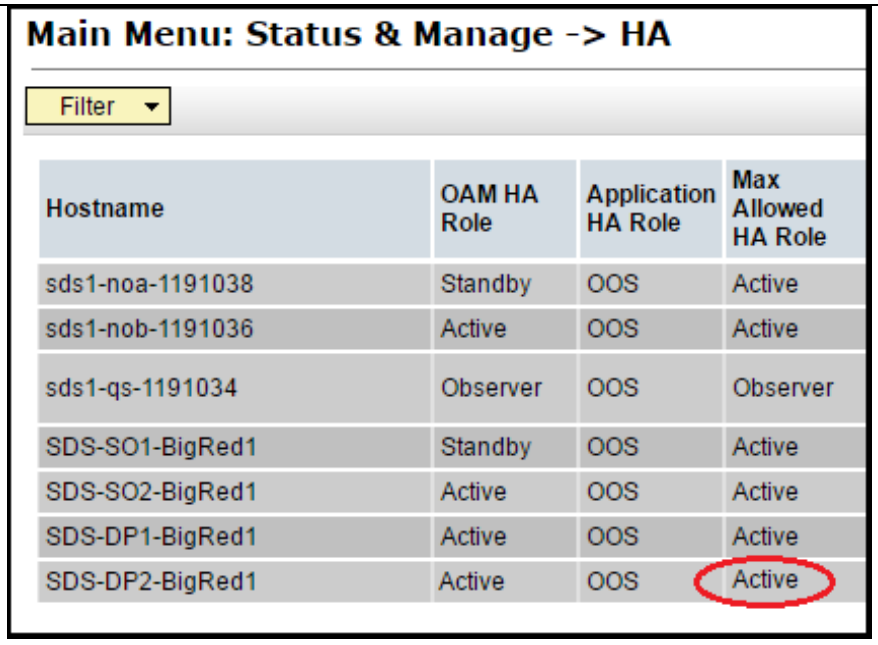
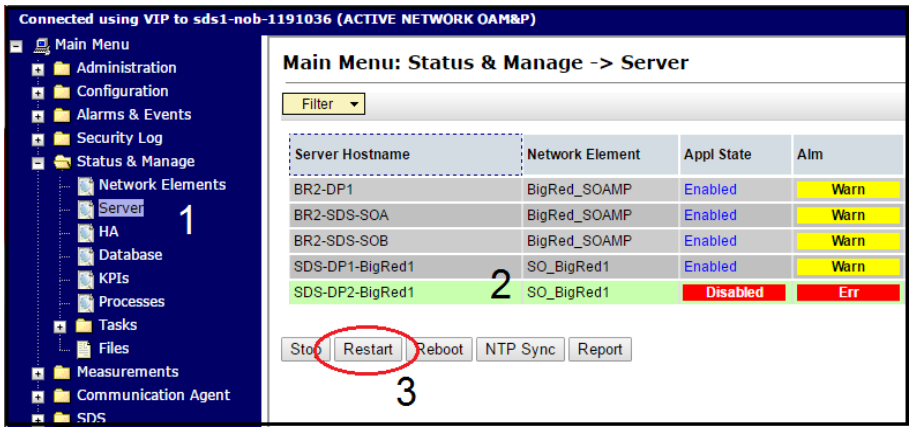
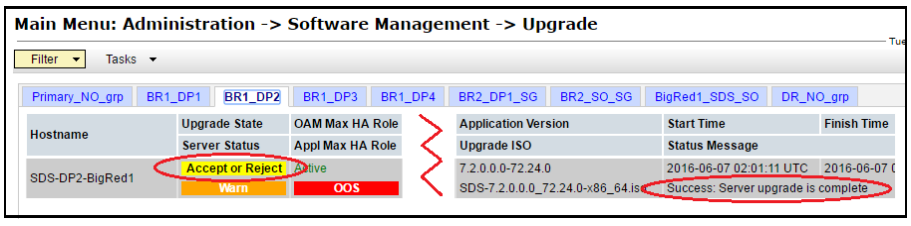
This procedure is performed to recover a server that did not properly complete an upgrade. This procedure should be performed only when directed by MOS or by another procedure within this document.

In the normal upgrade scenario, the steps in this procedure are automatically performed by the upgrade process.

Procedure 27. Manual Completion of Server Upgrade

1. ☐	**Primary SDS NOAM VIP**: Edit the Max Allowed HA Role	1. Navigate to **Status & Manage > HA**. 2. Locate the server to be completed and verify the Max Allowed HA Role is **Standby**.  3. Click **Edit**.  4. Change the Max Allowed HA Role to **Active**. 5. Click **OK**. 

Procedure 27. Manual Completion of Server Upgrade

2. ☐	**Primary SDS NOAM VIP**: Verify the Max Allowed HA Role changes to **Active**	
3. ☐	**Primary SDS NOAM VIP**: Restart the server	1. Navigate to **Status & Manage > Server**. 2. Select the server to be completed and click **Restart**.  After a few minutes, the Appl State changes to **Enabled**.
4. ☐	**Primary SDS NOAM VIP**: Verify server completion	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the Upgrade State changes to **Accept or Reject** and the status message changes to **Success: Server manually completed**. 

Appendix L ISO Link Correction

This procedure performs the ISO symlink correction and is required when upgrading from Release 7.1, 7.2, 7.3, or 7.4 to SDS 8.0 and later. In SDS 7.x, the ISO image management was changed to put a symlink in the **/var/TKLC/upgrade** directory to the actual file in the **/var/TKLC/db/filemgmt** directory. However, to support the storage reclamation feature used in SDS 8.0, in preparation for future dual image upgrade, the symlinks to the ISO image in the **/var/TKLC/db/filemgmt/isos** directory must be removed and replaced with direct copies of the ISO image in the **/var/TKLC/upgrade** directory. This must be executed after the application ISO has been deployed, but before the software upgrade in section 7. This may be done in a maintenance window before the actual upgrade maintenance window.

This procedure is not required if the source release is 8.x.

WARNING Failure to perform this procedure may cause the upgrade to fail.

Procedure 28. ISO Link Correction

1. ☐	Verify this procedure should be run	• Is the topology of servers to be upgraded currently running SDS release 7.1, 7.2, 7.3, or 7.4? • Has the SDS 8.x ISO been deployed? If **Yes** to the above questions, then proceed to the next step. If **No**, this procedure is complete.
2. ☐	**Active NOAM GUI**: Undeploy all unneeded ISO images	1. Navigate to **Status & Manage > Files**. 2. Select to remove all unneeded old ISO images from the /var/TKLC/upgrade directory. Keep the ISO image file being used for this upgrade. 3. Click **Undeploy ISO**. This saves space in the **/var/TKLC/upgrade** directory. 4. Click **OK** to confirm the ISO undeployment. This launches the ISO un-deployment to the entire topology. This function removes the symlink in **/var/TKLC/upgrade** to the ISO in the isos directory. The Tasks menu displays the status of the undeployment for each server. 5. Click **View ISO Deployment Report**.

3. ☐	**Active NOAM CLI**: Log into the active NOAM	Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the active NOAM.
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`

4. ☐	**Active NOAM CLI**: Mount the ISO image	Mount the SDS 8.0 ISO image. The following example uses a SDS ISO image name as an example. Use the appropriate application ISO image name. `$ sudo mount -o loop /var/TKLC/db/filemgmt/isos/SDS-8.0.0.0.0_80.x.y-x86_64.iso /mnt/upgrade`
5. ☐	**Active NOAM CLI**: Copy the script	Copy the script from the mounted ISO to **/var/tmp** to use it. `$ cp /mnt/upgrade/upgrade/bin/changeLinksToFiles.php /var/tmp`

Procedure 28. ISO Link Correction

6. ☐	**Active NOAM CLI**: Unmount the ISO image	Unmount the SDS 8.0 ISO image. `$ sudo umount /mnt/upgrade`

7. ☐	**Active NOAM CLI**: Verify the script is executable	Make the script executable.
		`$ chmod +x /var/tmp/changeLinksToFiles.php`
		`$ ls -l /var/tmp/changeLinksToFiles.php`
		`-r-x------ 1 admusr admgrp 2652 Dec 2 14:07 /var/tmp/changeLinksToFiles.php`
		In the above example, the **x** is present for admusr, indicating the script is indeed executable for the user.

8. ☐	**Active NOAM CLI**: Execute the script	Execute the script to change the symlink into a copy of the ISO image file.
		`$ /var/tmp/changeLinksToFiles.php`
		The script uses SSH to contact all servers in the topology and convert any link to an ISO images in **/var/TKLC/upgrade** into a copy of the ISO image file.
		Example output for each server in the entire topology.
		`$ /var/tmp/changeLinksToFiles.php`
		`server: NO1`
		`hostname alias based on service: no1-internalimi`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`found link /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`Remove command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`Copy command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso`
		The following expected messages can be ignored:
		`FIPS integrity verification test failed.`
		`Warning: Permanently added '<host>-internalimi,<ip address>' (RSA) to the list of known hosts.`
		If any unexpected failure messages occur, it is recommended to contact My Oracle Support (MOS) for guidance.

Appendix M Increase Maximum Number of Open Files

This procedure finds the maximum files open in the SDS system, and whether a workaround is required or not.

This procedure is required when upgrading from release 5.x or 7.x to SDS 8.x and later.

This pertains to any SDS site that has more than 1024 open files on the system.

The way to find out if the system needs these workaround steps is to find out how many open files are currently being read or written to. The idbsvc process handles all the files being merged to the NOAM, so this process determines and increases, if necessary, the maximum number of current open files.

Procedure 29. Increase Maximum Number of Open Files

1. ☐	**Active NOAM**: Log into the active NOAM and find the process ID of idbsvc	Determine the number of files currently open.
		1. Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in section 3.1.2.
		2. Retrieve the pid of idbsvc. The pid is highlighted in blue in the sample output shown:
		`$ ps -ef | grep -i idbsvc`
		`root 4369 idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2`
		3. The number of open files displays with the **lsof** command. Use the highlighted value in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1278`
		4. Record the number of files currently open: _____
		5. Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below:
		`$ ps -ef | grep -i tpdProvd`
		`tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd`
		6. The number of open files displays with the **lsof** command. Use the highlighted value in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1280`
		7. Record the number of files currently open: _____

Procedure 29. Increase Maximum Number of Open Files

2. ☐	**Active NOAM**: Find out the maximum number of open files permitted in system	Display the maximum number of open files for idbsvc.
		1. Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  32768  32768  files`
		2. The output of the cat command displays the maximum number of files that can be open by the idbsvc process.
		3. Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____
		Display the maximum number of open files for tpdProvd.
		4. Use the highlighted value from step 1, sub-step 4 for tpdProvd in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  1024  4096  files`
		5. The output of the cat command displays the maximum number of files that can be open by the tpdProvd process.
		6. Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____

3. ☐	**Active NOAM**: Check if current number of open files (used by idbsvc) is in safe limit	• If the number of currently open files (step 1, sub-step 3) of idbsvc is less than the maximum allowed (step 2, sub-step 2 Soft Limit for tpdProvd), for example, number of currently open files (used by idbsvc) is less than 1024, then this procedure is complete. • If the number of currently open files are more than the maximum allowed (step 2, sub-step 2 Soft Limit for tpdProvd), that is, 1024, go to the next step. Repeat this procedure (if required) for other NOAM servers.
4. ☐	**Active NOAM**: Check if maximum number of open files for tpdProvd is already set	• If the maximum number of open files value (step 2, sub-step 2 - Soft Limit) for tpdProvd is already set to 32768, this procedure is complete. • If maximum value is not already set, then go to the next step. Repeat this procedure (if required) for other NOAM servers.

Procedure 29. Increase Maximum Number of Open Files

5. ☐	**Active NOAM**: Increase maximum number of open files	1. Use a text editor with sudo, edit the **/etc/init/tpdProvd.conf** file to add the following two lines just before the **Start the daemon** comment line:
		`# increase open file limit`
		`limit nofile 32768 32768`
		Example:
		`#`
		`# restart tpdProvd up to 10 times within a 100 second period.`
		`# If tpdProvd fails to start 10 times within a 100 second period then`
		`# it most likely has a deeper problem that restarting will not overcome.`
		`respawn limit 10 100`
		`# increase open file limit`
		`limit nofile 32768 32768`
		`#`
		`# Start the daemon`
		`script`
		2. Save the file and close the editor.
		Caution: Do not edit any other line in this file. You can back up the file, if required.

6. ☐	**Active NOAM**: Restart the tpdProvd process	1. Type the following command to stop tpdProvd:
		`$ sudo initctl stop tpdProvd`
		2. Type the following command to restart tpdProvd
		`$ sudo initctl start tpdProvd`
		Sample output:
		`tpdProvd start/running, process 186743`

7. ☐	**Active NOAM CLI**: Recheck the open file maximum limit is set for tpdProvd	1. Retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below:
		`$ ps -ef | grep -i tpdProvd`
		`tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd`
		2. Use the highlighted value in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files 32768 32768 files`
		3. Verify the output displays the maximum number of open files is 32768. If the value is NOT 32768, it is recommended to contact My Oracle Support (MOS) per Appendix T.

Appendix N Advanced Health Check

This procedure verifies if UDP/TCP port 53 is open between NOAM and each DR NOAM site, NOAM site, and each SOAM site; and between MPs and each name server of the /etc/resolv.conf file.

Procedure 30. Advanced Health Check

1. ☐	Verify if UDP/TCP port 53 is open between NOAM and each DR-NOAM site	1. From the command prompt of the server with the alarm, execute:
		`sudo nmap -sTU -p 53 <DR-NOAM hostname>`
		2. Verify that the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
		Example:
		`[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-DRNOAM-A`
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:57 EST`
		`Nmap scan report for Icepick-DRNOAM-A (10.75.202.173)`
		`Host is up (0.00025s latency).`
		`rDNS record for 10.75.202.173: Icepick-DRNOAM-A.platform.cgbu.us.oracle.com`
		`PORT STATE SERVICE`
		`53/tcp open domain`
		`53/udp open domain`
		`MAC Address: 02:05:39:E0:60:8A (Unknown)`
		`Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds`
		If the port is in any state other than **Open**, then inform the customer before accepting the upgrade.
		Note: If the ports are **Closed**, it may be because no services are running on the far end. Check with the customer to make sure the firewall has been configured to allow DNS traffic on port 53.
		If the port is **Filtered,** then the port is likely blocked by a firewall and the upgrade MUST not be accepted until the customer confirms their network allows DNS traffic on port 53.

Procedure 30. Advanced Health Check

2. ☐	Verify if UDP/TCP port 53 is open between NOAM and each SOAM site	1. From the command prompt of the server with the alarm, execute:
		`sudo nmap -sTU -p 53 <SOAM hostname>`
		2. Verify the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
		Example:
		`[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-SO-A`
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:57 EST`
		`Nmap scan report for Icepick-SO-A (10.75.202.173)`
		`Host is up (0.00025s latency).`
		`rDNS record for 10.75.202.173: Icepick-SO-A.platform.cgbu.us.oracle.com`
		`PORT STATE SERVICE`
		`53/tcp open domain`
		`53/udp open domain`
		`MAC Address: 02:05:39:E0:60:8A (Unknown)`
		`Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds`
		If the port is in any state other than **Open**, then inform the customer before accepting the upgrade.
		Note: If the ports are **Closed**, it may be because no services are running on the far end. Check with the customer to make sure the firewall has been configured to allow DNS traffic on port 53.
		If the port is **Filtered,** then the port is likely blocked by a firewall and the upgrade MUST not be accepted until the customer confirms their network allows DNS traffic on port 53.

Procedure 30. Advanced Health Check

3. ☐	Verify if UDP/TCP port 53 is open between MP and each name server of the file /etc/resolv.conf	1. List the contents of the /etc/resolv.conf file.
		`sudo cat etc/resolv.conf`
		2. Verify the customer firewall is configured to allow DNS traffic on UDP/TCP port 53 to the addressed from the file /etc/resolv.conf:
		`[admusr@Icepick-DAMP-1 ~]$ sudo cat /etc/resolv.conf (lookups)`
		`domain platform.cgbu.us.oracle.com`
		`nameserver 10.240.50.134`
		`nameserver 10.240.50.133`
		`search platform.cgbu.us.oracle.com 500lab.com labs.tekelec.com labs.nc.tekelec.com`
		`[admusr@Icepick-DAMP-1 ~]$`
		`[admusr@Icepick-DAMP-1 ~]$ sudo nmap -sTU -p 53 10.240.50.134 10.240.50.133`
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:46 EST`
		`Nmap scan report for Icepick-SO-B-imi.platform.cgbu.us.oracle.com (10.240.50.134)`
		`Host is up (0.00022s latency).`
		`PORT STATE SERVICE`
		`53/tcp open domain`
		`53/udp open domain`
		`MAC Address: 02:17:B4:4F:DA:B6 (Unknown)`
		`Nmap scan report for Icepick-SO-A-imi.platform.cgbu.us.oracle.com (10.240.50.133)`
		`Host is up (0.00025s latency).`
		`PORT STATE SERVICE`
		`53/tcp open domain`
		`53/udp open domain`
		`MAC Address: 02:EE:13:E2:2C:EF (Unknown)`
		`Nmap done: 2 IP addresses (2 hosts up) scanned in 5.66 seconds`
		If the port is in any state other than **Open**, then inform the customer before accepting the upgrade.
		Note: If the ports are **Closed**, it may be because no services are running on the far end. Check with the customer to make sure the firewall has been configured to allow DNS traffic on port 53.
		If the port is **Filtered,** then the port is likely blocked by a firewall and the upgrade MUST not be accepted until the customer confirms their network allows DNS traffic on port 53.

Appendix O Workaround to Resolve Server HA Failover Issue

Procedure 31 resolves the HA failover issue by restarting the cmha process on the server.

Note: All UI displays are sample representations of upgrade screens. The actual display may vary slightly.

Procedure 31. Workaround to Resolve Server HA Failover Issue

1. ☐	**Server CLI**: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the NOAM server which is experiencing the HA failover issue :
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Server CLI**: Resolve HA failover issue(s)	Execute this command: `sudo pm.kill cmha`
3. ☐	Repeat, if needed	Repeat procedure on each affected server, if required. Return to procedure/step in upgrade process which pointed to refer this procedure.

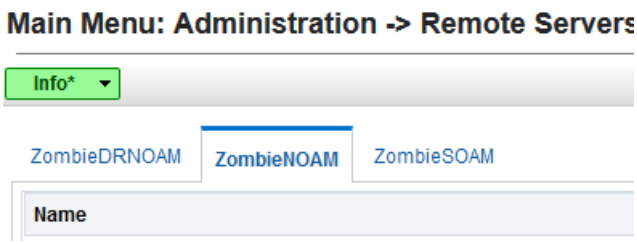
Appendix P Workaround for SNMP Configuration

Procedure 32 configures or updates the SNMP with **SNMPv2c and SNMPv3** as the enabled versions for SNMP traps configuration, as PMAC does not support SNMPv3.

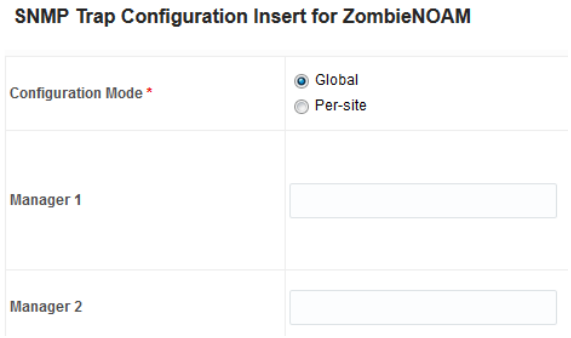
Perform this workaround step in the following cases:

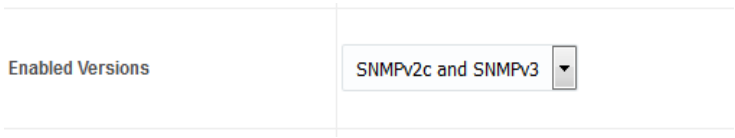
- If SNMP is not configured.
- If SNMP is already configured and SNMPv3 (V3Only) is selected as enabled version.

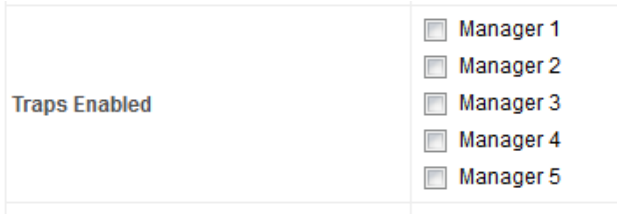
Procedure 32. Workaround for SNMP Configuration

1. ☐	**NOAMP VIP GUI**: Login	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Remote Servers > SNMP Trapping**. 3. Select the Server Group tab for SNMP trap configuration: 

Procedure 32. Workaround for SNMP Configuration

<table>
<tr>
<td>2. ☐</td>
<td>NOAM VIP GUI:
Configure/Update system-wide SNMP trap receiver(s)</td>
<td>
1. Type the IP address or hostname of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP's XMI network. If already configured SNMP with SNMPv3 as enabled version, another server needs to be configured here.
2. Continue to fill in additional secondary, tertiary, etc., Manager IPs in the corresponding slots if desired.


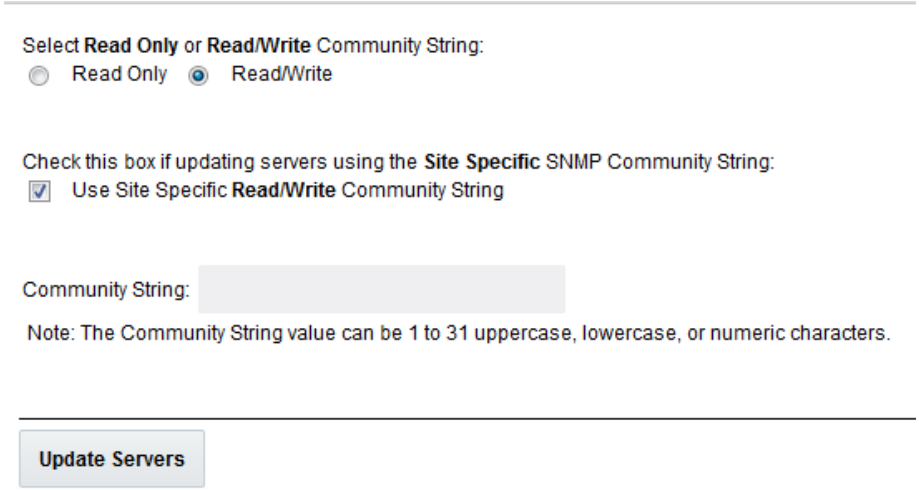
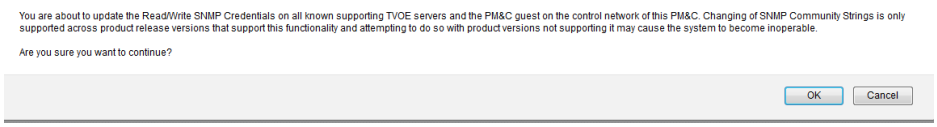
3. Set the Enabled Versions as SNMPv2c and SNMPv3.


Note: In case, enabled versions of already configured SNMP is V3Only, then update the enabled versions as above.
4. Mark the Traps Enabled checkboxes for the Manager servers being configured.


5. Type the SNMP Community Name.

6. Leave all other fields at their default values.
7. Click OK.
</td>
</tr>
<tr>
<td>3. ☐</td>
<td>PMAC GUI:
Login</td>
<td>
1. If needed, open a web browser and enter:
<code>http://<pmac_management_ip></code>
2. Login as the pmacadmin user.
</td>
</tr>
</table>

Procedure 32. Workaround for SNMP Configuration

4. ☐	**PMAC GUI**: Update the TVOE host SNMP community string	1. Navigate to **Administration > Credentials > SNMP Community String Update**. 2. Mark the **Use Site Specific Read/Write Community String** checkbox.  3. Click **Update Servers**.  4. Click **OK**. 5. Return to the procedure step that directed the execution of this procedure.

Appendix Q Workaround to Resolve Syscheck Error for CPU Failure

This procedure resolves the syscheck errors for CPU failure.

Procedure 33. Workaround to Resolve Syscheck Error for CPU Failure

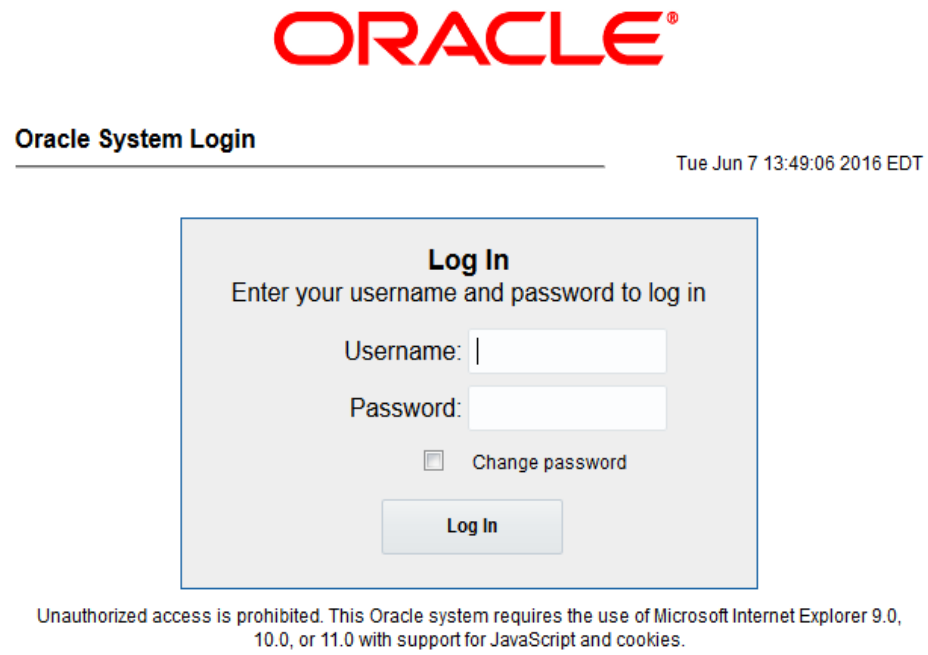
1. ☐	Log into server using CLI on which syscheck is failing	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.
		`ssh admusr@<SERVER_XMI>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Server CLI**: Execute workaround	1. Edit the cpu config file.
		`$ sudo vim /usr/TKLC/plat/lib/Syscheck/modules/system/cpu/config`
		2. Comment out the text that reads: "EXPECTED_CPUS=" by putting # in the beginning of the line. For example:
		`# EXPECTED_CPUS=2`
		3. Save the cpu config file.
		4. Reconfig the syscheck.
		Run the below commands:
		`sudo syscheck --unconfig`
		`sudo syscheck --reconfig`
		`sudo syscheck`
		CPU related errors do not display.

Appendix R Workaround to Fix cmsoapa Restart

When the upgrade path is from 7.x, 8.0 to 8.1, the cmsoapa process continuously restarts on the lower-level node after the higher-level node has been upgraded, that is, on SOAM after NOAM was upgraded and on DP server after SOAM has been upgraded.

Procedure 34. Workaround to Fix the cmsoapa Restart

1. ☐	**NOAMP VIP GUI**: Login	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Log into the NOAM GUI as the **guiadmin** user: 
2. ☐	**NOAM VIP GUI**: Identify the servers with the 31201 alarm for the cmsoapa process not running	1. Navigate to current alarm details and identify the server on which 31201 - Process Not Running alarm is getting raised for Instance as cmsoapa. 2. Navigate to **Alarms & Events > View Active**. 3. Look for **31201** alarm instances and make a list of servers with the cmsoapa alarm instance.

3. ☐	Login into Server using CLI on which cmsoapa is restarting	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.
		`ssh admusr@<SERVER_XMI>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server

Procedure 34. Workaround to Fix the cmsoapa Restart

4. ☐	**Server CLI**: Execute workaround	1. Execute workaround:
		`$ sudo prod.dbdown`
		2. After few minutes, when processes are down. Execute prod.start.
		`$ sudo prod.start`
		3. Repeat the steps on all server(s) where the alarm is, that is, where the cmsoapa process is restarting.

Appendix S Workaround to Fix DNS Issue

After completing upgrade of SDS primary query server, if DNS resolution fails, perform the following steps:

Procedure 35. Workaround to Fix DNS Issue

1. ☐	Verify the QS server transitions to a “A” State	1. Login to QS Server with the **admusr** account.
		2. Execute the command:
		`[admusr@SG2-SDS-QS ~]$ sudo prod.state`
		`...prod.state (RUNID=00)...`
		`...getting current state...`
		`Current state: A (product under procmgr)`
		1. If current state is **A**, stop and continue completing the upgrade.
		2. If not, then continue to the next step.

2. ☐	Verify the permissions of the /etc/resolv.conf file is 644	Execute:
		`[admusr@SG2-SDS-QS ~]$ ll /etc/resolv.conf`
		`-rw-r--r-- 1 root root 73 Feb 21 19:47 /etc/resolv.conf`

3. ☐	Verify the /etc/resolv.conf file contains the upgraded standby server	Check the file content:
		`[admusr@SG2-SDS-QS ~]$ sudo cat /etc/resolv.conf`
		`<Primary Server A>`
		`<Primary Server B>`
		`<Secondary Server B>`
		If not, checkout and edit the file as shown using the steps below

4. ☐	Using the rcstool checkout the /etc/resolv.conf file	Checkout the conf file:
		`[admusr@SG2-SDS-QS ~]$ sudo rcstool co /etc/resolv.conf`
		`RCS_VERSION=x.x`

5. ☐	Edit the /etc/resolv.conf file	Edit the conf file: `[admusr@SG2-SDS-QS ~]$ sudo vi /etc/resolv.conf`

6. ☐	Double Check that the /etc/resolv.conf file updates are as desired from edit above	Recheck the conf file:
		`[admusr@SG2-SDS-QS ~]$ sudo cat /etc/resolv.conf`
		`<Primary Server A>`
		`<Primary Server B>`
		`<Secondary Server B>`

Procedure 35. Workaround to Fix DNS Issue

7. ☐	Using the rcstool check in the /etc/resolv.conf file	Checkin the conf file: `[admusr@SG2-SDS-QS ~]$ sudo rcstool ci /etc/resolv.conf`
8. ☐	Clear DNS cache using the nscd command	Clear DNS cache: `[admusr@SG2-SDS-QS ~]$ sudo nscd -i hosts`

9. ☐	Verify the QS server transitions to a "A" State	Check the QS server state:
		`[admusr@SG2-SDS-QS ~]$ sudo prod.state`
		`...prod.state (RUNID=00)...`
		`...getting current state...`
		`Current state: A (product under procmgr)`

Appendix T My Oracle Support (MOS)

My Oracle Support

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

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

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:

   For technical issues such as creating a new Service Request (SR), select **1**.

   For non-technical issues such as registration or assistance with MOS, select **2**.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the 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 the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

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 appears. Most products covered by these documentation sets display under the headings N**etwork 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. 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.