

Oracle® Communications

Diameter Signaling Router

SDS Software Upgrade Guide

Release 8.3

E93225-01

September 2018

Oracle® Communications DSR, SDS Software Upgrade Guide, Release 8.3

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 Check	11
2. General Description	12
2.1 SDS 8.3 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	17
3.5 SOAM Upgrade Execution Overview	18
3.6 Post Upgrade Execution Overview	18
3.7 Recovery Procedures Overview	18
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)	20
5.4 Perform Health Check (Upgrade Preparation)	21
5.5 ISO Administration	21
5.6 Back Up TKLCCConfigData File	25
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	31
6.1 Site Upgrade Execution	31
6.2 Minimum Server Availability	35

6.3 Site Upgrade Options	35
6.4 Cancel and Restart Auto Site Upgrade	36
7. Automated Server Group Upgrade.....	38
7.1 Cancel and Restart Automated Server Group Upgrade.....	38
7.2 Site Accept.....	39
8. Primary/DR SDS NOAM Upgrade Execution	40
8.1 Perform Health Check (Primary/DR NOAM Pre-Upgrade)	40
8.2 Upgrade the Primary SDS NOAM	41
8.3 Upgrade DR SDS NOAM	50
8.4 Perform Health Check (Primary/DR NOAM Post Upgrade)	52
8.5 SNMP Configuration Update (Post Primary/DR NOAM Upgrade)	52
9. Site Upgrade Execution.....	52
9.1 Automated Site Upgrade	53
9.1.1 Perform Health Check (Pre-Upgrade).....	53
9.1.2 Upgrade SOAM	54
9.1.3 Rearrange Automate Site Upgrade Cycles	58
9.1.4 Perform Health Check (Post Upgrade)	61
9.2 SOAM Upgrade Execution (Manual and Automated Server Group).....	62
9.2.1 Perform Health Check (SOAM Pre-Upgrade)	62
9.2.2 Upgrade SOAM	63
9.2.3 Perform Health Check (SOAM Post Upgrade).....	65
9.3 Post Upgrade Procedures	65
9.3.1 Accept the Upgrade.....	65
9.3.2 SOAM VM Profile Update.....	69
10. Recovery Procedures	69
10.1 Backout Setup	69
10.2 Perform Backout.....	70
10.2.1 Back Out the SOAM	70
10.2.2 Back Out the DR SDS NOAM	73
10.2.3 Back Out the Primary SDS NOAM	75
Appendix A. Access the OAM GUI Using the VIP (NOAM/SOAM).....	79
Appendix B. Health Check Procedures	81
Appendix C. Upgrade Server Administration on SDS 7.x	94
Appendix D. Upgrade Server Administration on SDS 8.x	100
Appendix E. Back Out a Single Server	106
Appendix F. Manually Perform ISO Validation	116
Appendix G. Undeploy an ISO File (Post Upgrade Acceptance).....	120

Appendix H.	Add the SDS ISO to the PMAC Software Repository	122
Appendix I.	Recover from a Failed Upgrade.....	127
Appendix J.	Add New SOAM Profile on Existing VM.....	134
J.1	Add SDS Software Images to PMAC Server	134
J.2	Remove the SDS SOAM VM from the SOAM Server Group	139
J.3	Delete Existing SOAM VM and Recreate SDS SOAM VM with New Profile	143
J.4	Add the New SOAM VM to the SOAM Server Group	157
Appendix K.	Manual Completion of Server Upgrade.....	164
Appendix L.	ISO Link Correction	167
Appendix M.	Increase Maximum Number of Open Files	169
Appendix N.	Workarounds	172
N.1	Resolve Server HA Failover Issue	172
N.2	SNMP Configuration.....	172
N.3	Resolve Syscheck Error for CPU Failure	174
N.4	Fix cmsoapa Restart.....	175
N.5	Fix DNS Issue.....	176
Appendix O.	My Oracle Support (MOS)	177

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	17
Table 7.	SOAM Upgrade Procedures	18
Table 8.	Post Upgrade Procedures.....	18
Table 9.	Backout Procedures.....	18
Table 10.	SDS Upgrade Matrix	19
Table 11.	SDS Upgrade – List of Procedures.....	19
Table 12.	Site Upgrade Planning — Automated vs. Manual Upgrade	52

List of Figures

Figure 1.	Example Procedure Steps Used in This Document	10
Figure 2.	SDS 8.3 Supported Upgrade Paths.....	13
Figure 3.	Upgrade Perspective of SDS Site Topology.....	31

Figure 4. Site Upgrade — NOAM View.....	32
Figure 5. Site Upgrade — Entire Site View.....	32
Figure 6. Site Upgrade — Site Initiate Screen	33
Figure 7. Site Upgrade Monitoring.....	34
Figure 8. Server Group Upgrade Monitoring.....	34
Figure 9. Server Group Upgrade Monitoring.....	34
Figure 10. Auto Site Upgrade General Options	35
Figure 11. Site Upgrade Active Tasks	36
Figure 12. User Cancelled the Site Upgrade Tasks	36
Figure 13. Partially Upgraded Site	37
Figure 14. Restarting Site Upgrade.	37
Figure 15. Server Group Upgrade Active Tasks	38
Figure 16. Site Accept Button	39
Figure 17. Site Accept Screen	39

List of Procedures

Procedure 1. Required Materials Check.....	20
Procedure 2. ISO Administration	21
Procedure 3. TKLCCConfigData Backup.....	25
Procedure 4. Full Database Backup (PROV and COMCOL Env for All Servers	26
Procedure 5. Upgrade the Primary SDS NOAM.....	41
Procedure 6. Upgrade DR SDS NOAM.....	50
Procedure 7. Upgrade SOAM.....	54
Procedure 8. Rearrange Automated Site Upgrade Cycles.....	58
Procedure 9. Upgrade SOAM.....	63
Procedure 10. Accept the Upgrade	65
Procedure 11. Back Out the SOAM.....	70
Procedure 12. Back Out the DR SDS NOAM.....	73
Procedure 13. Back Out Primary SDS NOAM.....	75
Procedure 14. Access the OAM GUI Using the VIP (NOAM/SOAM).....	79
Procedure 15. Health Check Procedure	81
Procedure 16. Upgrade Server Administration on SDS 7.x	94
Procedure 17. Upgrade Server Administration on SDS 8.x	100
Procedure 18. Back Out a Single Server.....	106
Procedure 19. Manually Perform ISO Validation.....	116
Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance.....	120
Procedure 21. Add the SDS ISO to the PMAC Software Repository	122

Procedure 22.	Recover from a Failed Upgrade	127
Procedure 23.	Add SDS Software Images to PMAC Server	134
Procedure 24.	Remove the SDS SOAM VM from the SOAM Server Group.....	139
Procedure 25.	Recreate the SDS SOAM VM with the 1B Subscriber Profile	143
Procedure 26.	Place the SDS SOAM VM into the SOAM Server Group	157
Procedure 27.	Manual Completion of Server Upgrade.....	165
Procedure 28.	ISO Link Correction.....	167
Procedure 29.	Increase Maximum Number of Open Files	169
Procedure 30.	Workaround to Resolve Server HA Failover Issue	172
Procedure 31.	Workaround for SNMP Configuration	172
Procedure 32.	Workaround to Resolve Syscheck Error for CPU Failure	174
Procedure 33.	Workaround to Fix the cmsopa Restart	175
Procedure 34.	Workaround to Fix DNS Issue	176

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 8.3
- Minor upgrade from SDS release 8.3.x to a later 8.3.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 8.3 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 8.3 Initial Installation and Configuration Guide
- [2] Database Management: Backup and System Restoration
- [3] SDS 8.3 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
MP	Message Processing or Message Processor

Acronym	Meaning
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
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management 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 7.3 to SDS 8.3.
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 8.3.0.0.0_83.3.0 to 8.3.0.0.0_83.4.0.
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.
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: <ul style="list-style-type: none"> • 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 O 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.

<p>Each step has a checkbox the user should check to keep track of the progress of the procedure.</p> <p>The Title column describes the operations to perform during that step.</p> <p>Each command the user enters, and any response output, is formatted in 10-point Courier font.</p>		
SL.	Title/Instructions	Directive/Result Steps
1. <input type="checkbox"/>	Change directory	Change to the backout directory. <code>\$ cd /var/TKLC/backout</code>
2. <input type="checkbox"/>	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 O 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 8.3 before upgrading to NetBackup 7.7.


1.8.2 Upgrade Check



In case of the following error comes up, contact My Oracle Support (MOS).

"Post Upgrade validation failed for <server_name>. Please check server status. Cancelling the upgrade."

ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress
25	Camaro-SO-B Server Upgrade (in Camaro_SO_SG Server Group Upgrade)	completed	2018-06-22 07:07:28 EDT	2018-06-22 07:28:09 EDT	0	Server upgrade execution complete.	100%
24	Nova-SO-Sp Server Upgrade (in Camaro_SO_SG Server Group Upgrade)	exception	2018-06-22 07:07:12 EDT	2018-06-22 07:42:08 EDT	-1	Post Upgrade validation failed for Nova-SO-Sp. Please check server status. Cancelling the upgrade.	90%



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.

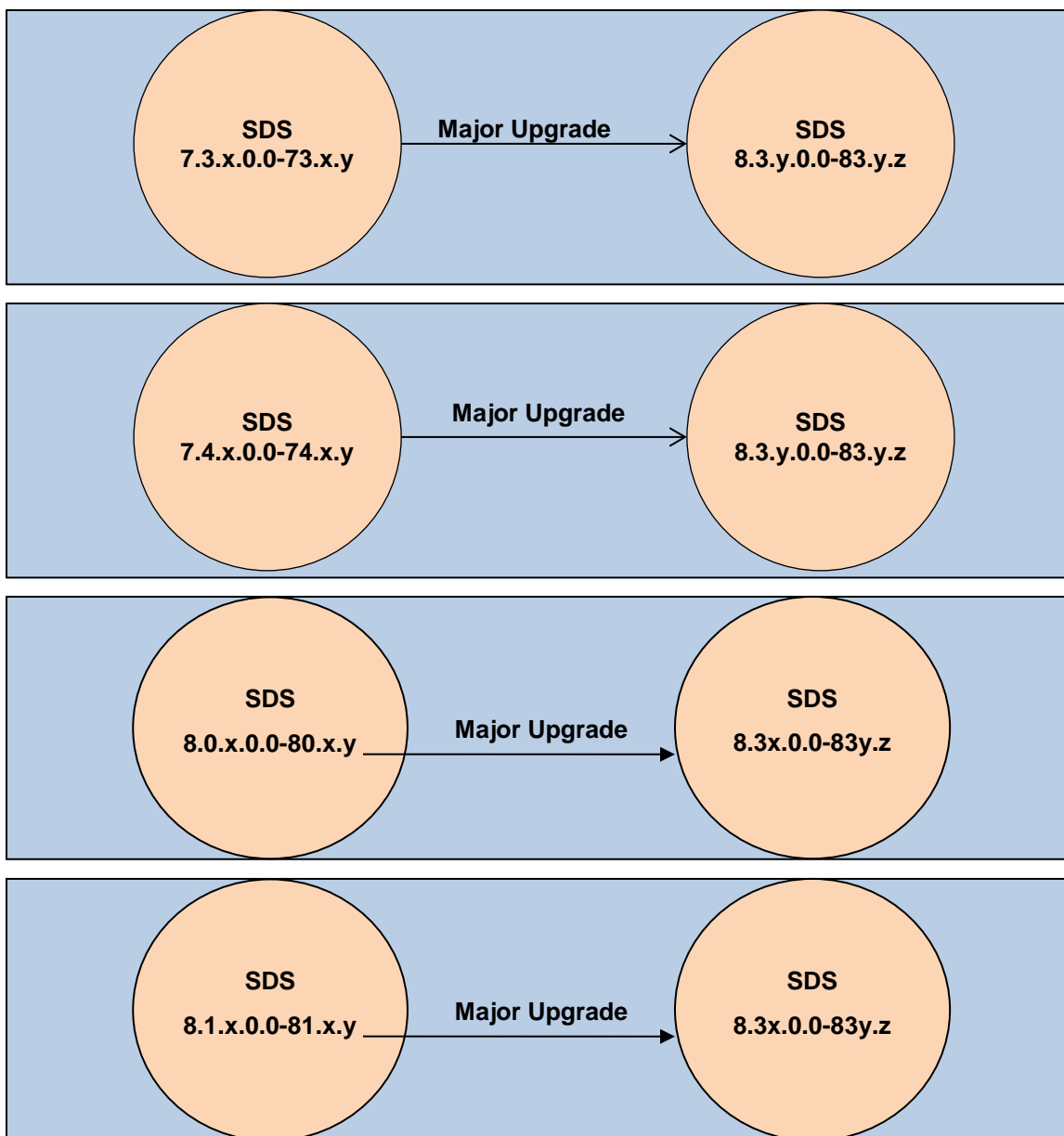
2. General Description

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 8.3 Initial Installation and Configuration Guide for more information.

2.1 SDS 8.3 Supported Upgrade Paths

The supported SDS 8.3 upgrade paths are shown in the Figure 2.



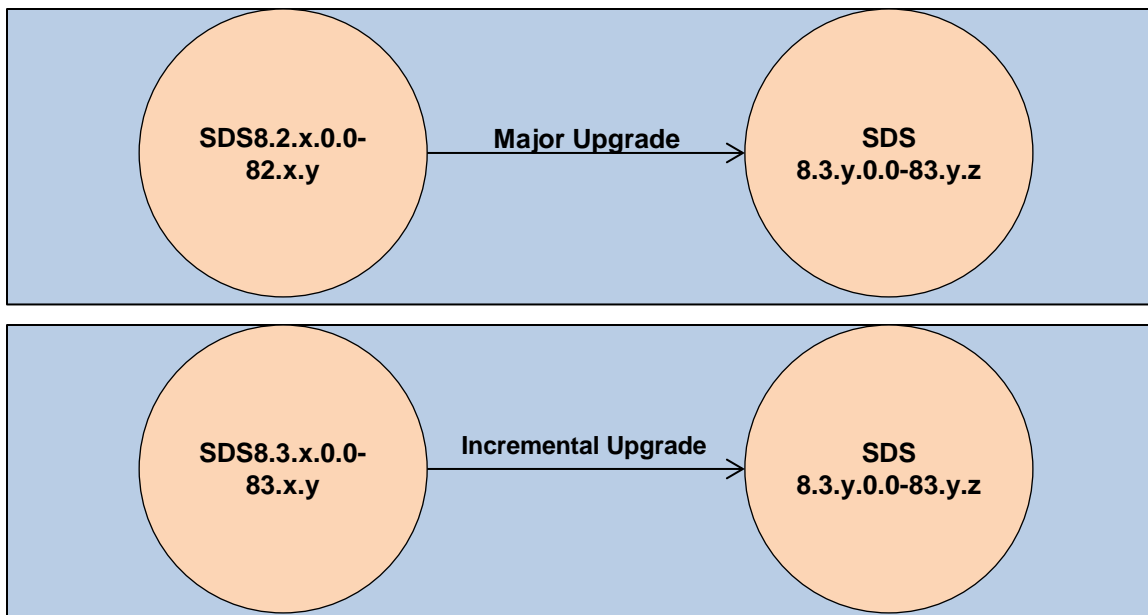


Figure 2. SDS 8.3 Supported Upgrade Paths

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-8.3.0.0.0_83.4.0-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-8.3.0.0.0_83.4.0-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

<p>Maintenance Window 1</p> <p>Date: _____</p>	<ol style="list-style-type: none"> 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. Mark the associated checkbox as each server upgrade is completed. <p>Primary SDS NE site name: _____</p> <p><input type="checkbox"/> Primary SDS active server: _____</p> <p><input type="checkbox"/> Primary SDS standby server: _____</p> <p><input type="checkbox"/> Primary SDS query server: _____</p> <p>DR SDS NE site name: _____</p> <p><input type="checkbox"/> DR SDS active server: _____</p> <p><input type="checkbox"/> DR SDS standby server: _____</p> <p><input type="checkbox"/> DR SDS query server: _____</p>
<p>Maintenance Window 2</p> <p>Date: _____</p>	<ol style="list-style-type: none"> Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. Mark the associated checkbox as each server upgrade is completed. <p>SOAM NE site name: _____</p> <p><input type="checkbox"/> Active SOAM Server: _____</p> <p><input type="checkbox"/> Standby SOAM Server: _____</p> <p><input type="checkbox"/> DP 1 Server: _____ <input type="checkbox"/> DP 6 Server: _____</p> <p><input type="checkbox"/> DP 2 Server: _____ <input type="checkbox"/> DP 7 Server: _____</p> <p><input type="checkbox"/> DP 3 Server: _____ <input type="checkbox"/> DP 8 Server: _____</p> <p><input type="checkbox"/> DP 4 Server: _____ <input type="checkbox"/> DP 9 Server: _____</p> <p><input type="checkbox"/> DP 5 Server: _____ <input type="checkbox"/> DP 10 Server: _____</p>

<p>Maintenance Window 2</p> <p>Date: _____</p>	<ol style="list-style-type: none"> Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. Mark the associated checkbox as each server upgrade is completed. <p>SOAM NE site name: _____</p> <p><input type="checkbox"/> Active SOAM Server: _____</p> <p><input type="checkbox"/> Standby SOAM Server: _____</p> <p><input type="checkbox"/> DP 1 Server: _____ <input type="checkbox"/> DP 6 Server: _____</p> <p><input type="checkbox"/> DP 2 Server: _____ <input type="checkbox"/> DP 7 Server: _____</p> <p><input type="checkbox"/> DP 3 Server: _____ <input type="checkbox"/> DP 8 Server: _____</p> <p><input type="checkbox"/> DP 4 Server: _____ <input type="checkbox"/> DP 9 Server: _____</p> <p><input type="checkbox"/> DP 5 Server: _____ <input type="checkbox"/> DP 10 Server: _____</p>
<p>Maintenance Window 2</p> <p>Date: _____</p>	<ol style="list-style-type: none"> Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. Mark the associated checkbox as each server upgrade is completed. <p>SOAM NE site name: _____</p> <p><input type="checkbox"/> Active SOAM Server: _____</p> <p><input type="checkbox"/> Standby SOAM Server: _____</p> <p><input type="checkbox"/> DP 1 Server: _____ <input type="checkbox"/> DP 6 Server: _____</p> <p><input type="checkbox"/> DP 2 Server: _____ <input type="checkbox"/> DP 7 Server: _____</p> <p><input type="checkbox"/> DP 3 Server: _____ <input type="checkbox"/> DP 8 Server: _____</p> <p><input type="checkbox"/> DP 4 Server: _____ <input type="checkbox"/> DP 9 Server: _____</p> <p><input type="checkbox"/> DP 5 Server: _____ <input type="checkbox"/> DP 10 Server: _____</p>
<p>Maintenance Window 2</p> <p>Date: _____</p>	<ol style="list-style-type: none"> Record the name of SOAM NE site and its server's hostnames to be upgraded during the Maintenance Window 2 in the spaces provided. Mark the associated checkbox as each server upgrade is completed. <p>SOAM NE site name: _____</p> <p><input type="checkbox"/> Active SOAM Server: _____</p> <p><input type="checkbox"/> Standby SOAM Server: _____</p> <p><input type="checkbox"/> DP 1 Server: _____ <input type="checkbox"/> DP 6 Server: _____</p> <p><input type="checkbox"/> DP 2 Server: _____ <input type="checkbox"/> DP 7 Server: _____</p> <p><input type="checkbox"/> DP 3 Server: _____ <input type="checkbox"/> DP 8 Server: _____</p> <p><input type="checkbox"/> DP 4 Server: _____ <input type="checkbox"/> DP 9 Server: _____</p> <p><input type="checkbox"/> DP 5 Server: _____ <input type="checkbox"/> DP 10 Server: _____</p>

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.



	<h2 style="color: red;">CAUTION</h2>	<p>If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes.</p>
	<h2 style="color: red;">WARNING</h2>	<p>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.</p>

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.


	<h2 style="color: red;">WARNING</h2>	<p>The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 6.</p> <p>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.</p> <p>Note: During upgrade some alarms/events may be raised that can be ignored. Alarms are mentioned in step 4 of Appendix A.</p>
---	--------------------------------------	--

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 7 and/or 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 B Health Check Procedures is executed before starting this procedure.

[†] Appendix B 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 TKLCCConfigData File	25
Procedure 4	Full Database Backup (PROV and COMCOL Env for All Servers)	26
Procedure 5	Upgrade the Primary SDS NOAM	41
Procedure 6	Upgrade DR SDS NOAM	50
Procedure 7	Upgrade SOAM with ASU	54
Procedure 9	Upgrade SOAM manually	63
Procedure 32	Workaround to Resolve Syscheck Error for CPU Failure	174
Procedure 10	Accept the Upgrade	65

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. <input type="checkbox"/>	Verify all upgrade requirements have been met.	Requirements are listed in section 3.1 Upgrade Requirements. Verify all upgrade requirements have been met.
2. <input type="checkbox"/>	Verify all administration data needed during upgrade.	Verify all information in section 3.1.2 Logins, Passwords, and Site Information have 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)

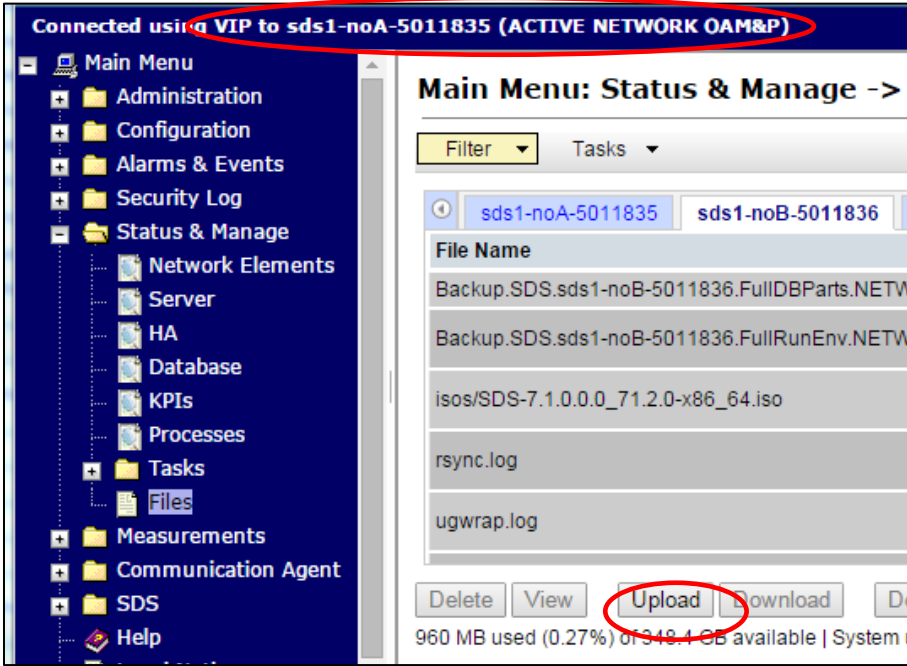
This procedure is part of software upgrade preparation and is used to determine the health and status of the SDS network and servers. This procedure may be executed multiple times, but must also be executed at least once 24-36 hours before starting a maintenance window.

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

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 recommended that the ISO transfers to the target servers be completed before the first scheduled maintenance window.

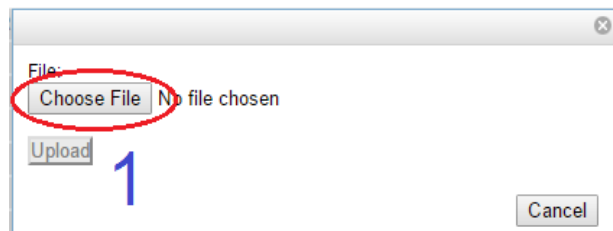
Note: Appendix H Add the SDS ISO to the PMAC Software Repository may be executed at any time after Procedure 2 ISO Administration has been completed.

Procedure 2. ISO Administration		
1.	SDS NOAM GUI: <input type="checkbox"/> Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2.	Primary SDS NOAM VIP (GUI): Connect to the SDS server	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Files. 2. Select the hostname of the active primary SDS server from the list of tabs. 3. Click Upload.  <p>Note: The active primary SDS server displays in the GUI banner as connected to the VIP with a state of ACTIVE NETWORK OAM&P.</p>

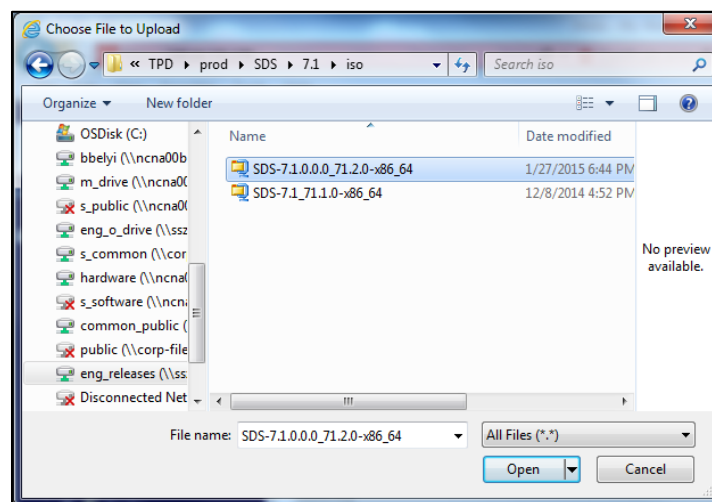
Procedure 2. ISO Administration

3. **Primary SDS NOAM VIP:**
Upload the ISO file

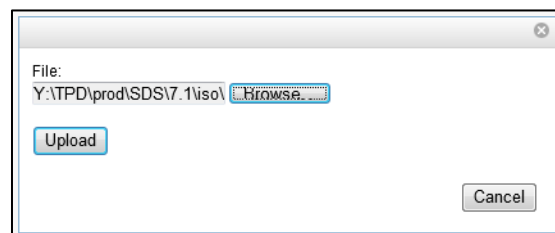
1. Click **Choose File**.



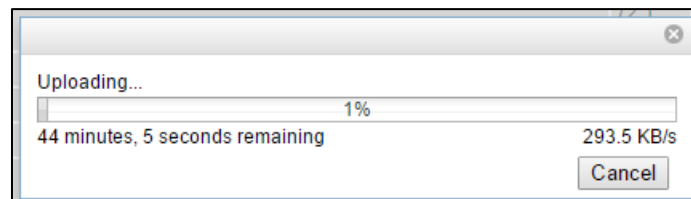
2. Locate the ISO file for the target release and click **Open**.



3. Click **Upload**.



4. Monitor the upload until the file transfer completes.



Note: If transferring 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.

sds1-noA-5011835	sds1-noB-5011836	sds1-qs-5011837	Liberty-SDS-SO-A
File Name	Size	Type	Timestamp
SDS-7.1.0.0.0_71.2.0-x86_64.iso	863.6 MB	iso	2015-02-03 21:09:37 UTC
rsync.log	2.1 KB	log	2015-02-03 00:00:03 UTC
upgrade.log	87.7 KB	log	2015-01-30 17:10:18 UTC
ugwrap.log	1.3 KB	log	2015-01-29 19:46:05 UTC

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 validation to pass.
4. Click **Deploy ISO**.

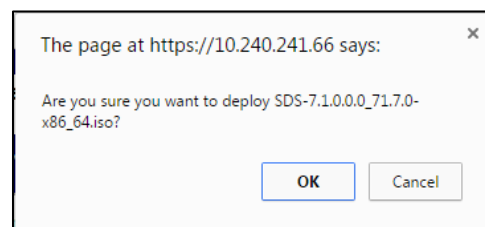
Main Menu: Status & Manage -> Files

Filter Tasks

sds1-noA-5011835	sds1-noB-5011836	sds1-qs-5011837	Liberty-SDS-SO-A	Liberty-
File Name	Size	Type	Timestamp	
rsync.log	2.1 KB	log	2015-02-03 00:00:03 UTC	
SDS-7.1.0.0.0_71.2.0-x86_64.iso	863.6 MB	iso	2015-02-03 21:28:28 UTC	
ugwrap.log	1.3 KB	log	2015-01-29 19:46:05 UTC	
upgrade.log	87.7 KB	log	2015-01-30 17:10:18 UTC	

863.6 MB used (0.24%) of 348.4 GB available | System utilization: 17.9 GB (5.13%) of 348.4 GB available.

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**.

Main Menu: Status & Manage -> Files

Filter Tasks

sds1-noA-5011835 sds1-noB-5011836 sds1-qs-5011837 Liberty-SDS-SO-A

File Name	Size	Type	Timestamp
isos/SDS-7.1.0.0.0_71.2.0-x86_64.iso	863.6 MB	iso	2015-02-03 21:47:30 UTC
rsync.log	2.1 KB	log	2015-02-03 00:00:03 UTC
ugwrap.log	1.3 KB	log	2015-01-29 19:46:05 UTC
upgrade.log	87.7 KB	log	2015-01-30 17:10:18 UTC

Delete View ISO Deployment Report Upload Download Undeploy ISO

863.6 MB used (0.24%) of 348.4 GB available | System utilization: 17.9 GB (5.13%) of 348.4 GB av

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.

Main Menu: Status & Manage -> Files [View]

Main Menu: Status & Manage -> Files [View]
Thu Jul 09 12:32:48 2015 UTC

Deployment report for SDS-7.1.0.0.0_71.7.0-x86_64.iso:


Deployed on 18/18 servers.

```
sds-rlghnc-a: Deployed
sds-rlghnc-b: Deployed
qs-rlghnc: Deployed
sds-mrsvnc-a: Deployed
sds-mrsvnc-b: Deployed
qs-mrsvnc: Deployed
turks-sds-SO-a: Deployed
turks-sds-SO-b: Deployed
turks-DP-01: Deployed
turks-DP-02: Deployed
kauai-sds-SO-a: Deployed
kauai-sds-SO-b: Deployed
kauai-DP-01: Deployed
kauai-DP-02: Deployed
florence-sds-SO-a: Deployed
florence-sds-SO-b: Deployed
florence-DP-01: Deployed
florence-DP-02: Deployed
```

Print Save Back

Note: This completes the ISO administration procedure for source release 7.x and later, skip the remaining steps.

Procedure 2. ISO Administration

- | | | |
|----|---|--|
| 8. |  | Perform Appendix L ISO Link Correction if upgrading from release 7.3, or 7.4 to SDS 8.3. |
|----|---|--|

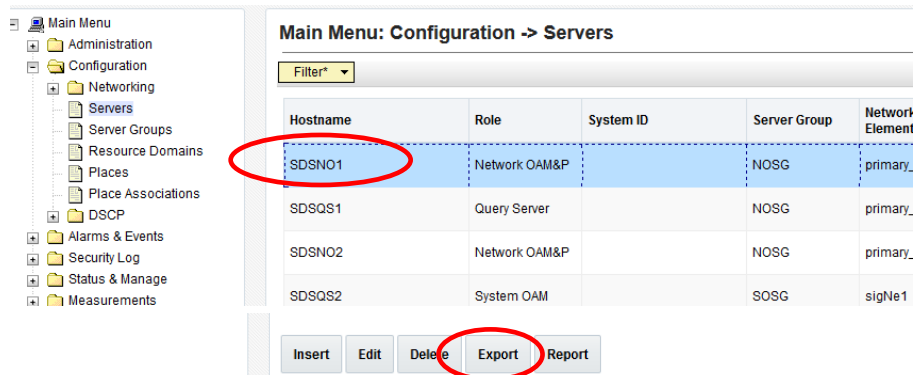
5.6 Back Up TKLCConfigData File

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 | <ol style="list-style-type: none"> Navigate to Configuration > Servers. 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 | <ol style="list-style-type: none"> Access the primary SDS NOAM server command line using ssh or a console.
<code>ssh admusr@<NOAM_VIP></code> Transfer the TKLCConfigData files for all servers in the /var/TKLC/db/filemgmt directory to a remote location.
<code>\$ cd /var/TKLC/db/filemgmt</code>
<code>\$ scp TKLCConfigData.<Sever Hostname>.sh <username>@<remote-server>:<directory></code> |
|----|---|---|

Example:

```
scp TKLCConfigData.SDSDRN01.sh <username>@<remote-server>:<directory>
```

Remember to back up the TKLCConfig data file for **all** servers.

5.7 Perform Health Check (Post ISO Administration)

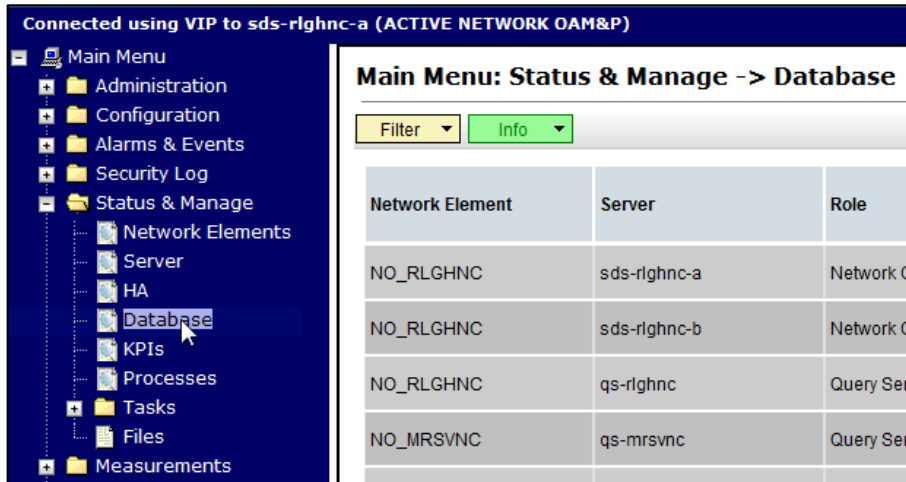
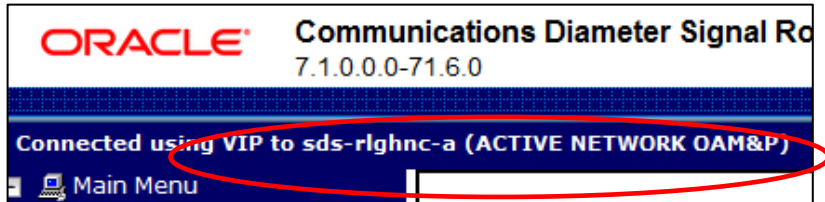
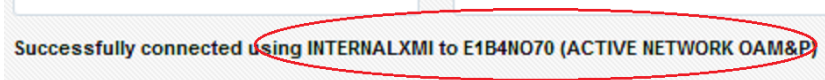
This procedure is part of Software Upgrade Preparation and is used to determine the health and status of the entire SDS network and servers. This may be executed multiple times but must also be executed at least once within the period of 24-36 hours before the start of a maintenance window.

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

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

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.

Main Menu: Status & Manage -> Database

Filter Info

Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	S
NO_RLGHNC	sds-righnc-a	Network OAM&P	Active	OOS	N
NO_RLGHNC	sds-righnc-b	Network OAM&P	Standby	OOS	N

2. Click **Backup**.

port Inhibit Replication Backup... Compare... Restore

4. **Primary SDS NOAM VIP:** Back up the provisioning data

1. Unmark the **Configuration** checkbox.

2. Type a **Comment**.

Main Menu: Status & Manage -> Database [Backup]

Database Backup

Field	Value	De
Server: sds-righnc-a		
Select data for backup	<input checked="" type="checkbox"/> Provisioning <input type="checkbox"/> Configuration	Se
Compression	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none *	Se
Archive Name	Backup.sds.sds-righnc-a.Provisioning.NETWORK_OAMP.20150707_18520 *	
Comment	PreUpgrade to 71.7.0	

Ok Cancel

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.

Main Menu: Status & Manage -> Database [Backup]

Info

Info

• Pre-Validation passed - Data NOT committed ...

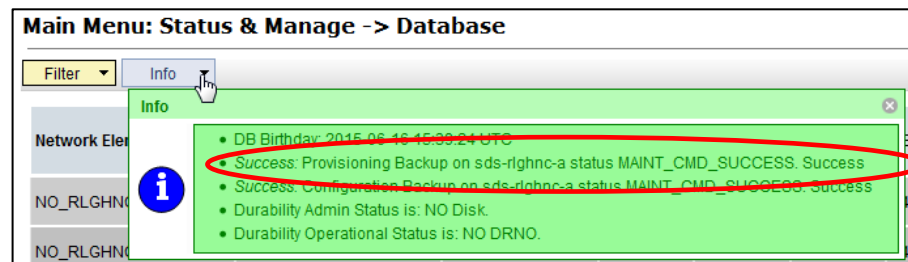
Server: sds-righnc-a

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**.



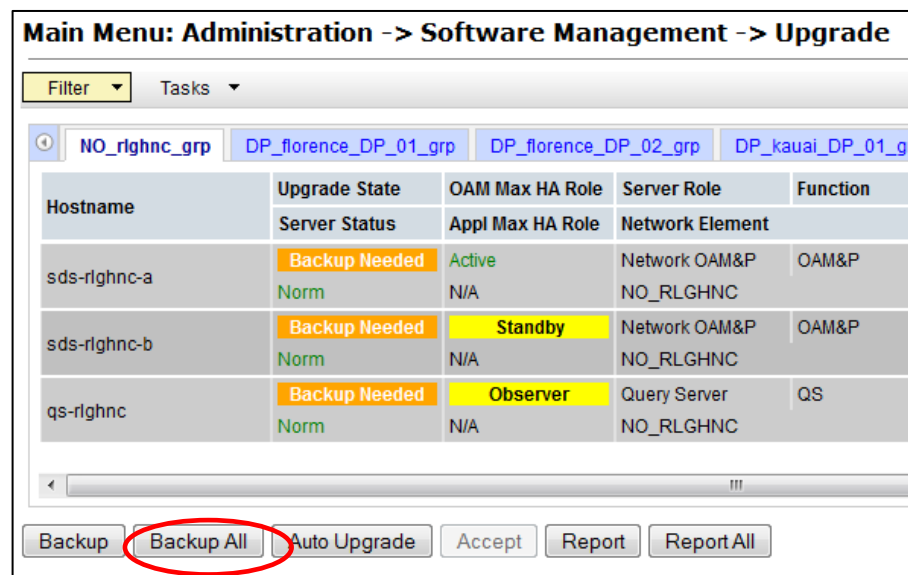
If a status of **MAINT_IN_PROGRESS** is received, then **refresh** the Info message by navigating to **Status & Manage > Database** and clicking on the **Info** tab again.

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**.

Main Menu: Administration -> Software Management -> Upg

Network element	Action	Server(s) in the proper state for backup
NO_RLGHNC	<input checked="" type="checkbox"/> Back up	sds-rlghnc-a sds-rlghnc-b qs-rlghnc
NO_MRSVNC	<input checked="" type="checkbox"/> Back up	sds-mrsvnc-a sds-mrsvnc-b qs-mrsvnc
SO_TURKS	<input checked="" type="checkbox"/> Back up	turks-sds-SO-a turks-sds-SO-b turks-DP-01 turks-
SO_KAUAI	<input checked="" type="checkbox"/> Back up	kauai-sds-SO-a kauai-sds-SO-b kauai-DP-01 kau
SO_FLORENCE	<input checked="" type="checkbox"/> Back up	florence-sds-SO-a florence-sds-SO-b florence-DP

Full backup options		
Database parts exclusion	<input checked="" type="radio"/> Exclude <input type="radio"/> Do not exclude	Select "Exclude" to perform a full backup of the COM /usr/TKLC/appworks/etc/exclude_parts.d/. Select "Do not exclude" to perform a full backup of th take longer and produce larger backup files in /var/T

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.

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks				
NO_rlgnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_g				
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function
	Server Status	Appl Max HA Role	Network Element	
sds-rlghnc-a	Backup In Progress Norm	Active N/A	Network OAM&P NO_RLGHNC	OAM&P
sds-rlghnc-b	Backup In Progress Norm	Standby N/A	Network OAM&P NO_RLGHNC	OAM&P
qs-rlghnc	Backup In Progress Norm	Observer N/A	Query Server NO_RLGHNC	QS

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks				
NO_rlgnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_g				
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function
	Server Status	Appl Max HA Role	Network Element	
sds-rlghnc-a	Ready Norm	Active N/A	Network OAM&P NO_RLGHNC	OAM&P
sds-rlghnc-b	Ready Norm	Standby N/A	Network OAM&P NO_RLGHNC	OAM&P
qs-rlghnc	Ready Norm	Observer N/A	Query Server NO_RLGHNC	QS

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.

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks				
NO_rlgnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_g				
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function
	Server Status	Appl Max HA Role	Network Element	
florence-DP-01	Ready Norm	Active OOS	MP SO_FLORENCE	SDS

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.

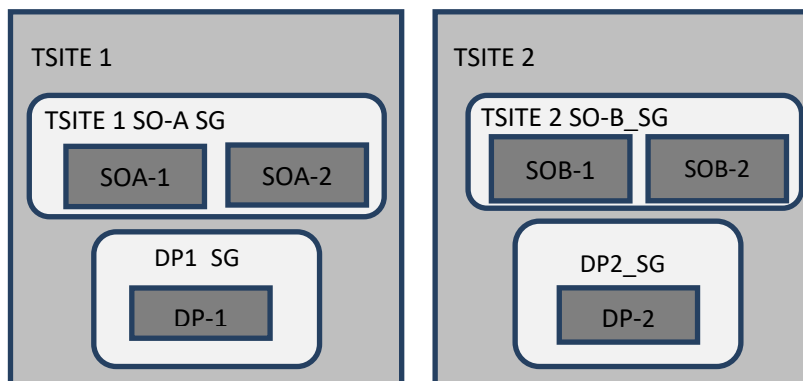


Figure 3. Upgrade Perspective of SDS Site Topology

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).

Main Menu: Administration -> Software Management -> Upgrade

Filter*

Tasks*

NOSG

DRNOSG

SOSG

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SDS-QS	Ready	Observer	Query Server	QS	8.1.0.0.0-81.15.2
	Norm	N/A	NO_DSR_VM_NE		
SDS-NO	Ready	Active	Network OAM&P	OAM&P	8.1.0.0.0-81.15.2
	Err	N/A	NO_DSR_VM_NE		
SDS-NO2	Ready	Standby	Network OAM&P	OAM&P	8.1.0.0.0-81.15.2
	Norm	N/A	NO_DSR_VM_NE		

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.

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)	Ready (2/2)	8.1.0.0.0-81.15.2 (2/2)	
DPSG2	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0.0-81.15.2 (1/1)	
DPSG1	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0.0-81.15.2 (1/1)	
DPSG4	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0.0-81.15.2 (1/1)	
DPSG3	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0.0-81.15.2 (1/1)	

Backup Backup All Checkup Checkup All Site Upgrade Site Accept Report Report All

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.

Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]

Info* ▼

Cycle	Action	Servers															
1	Upgrade	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e6f2ff;"> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> </thead> <tbody> <tr> <td>SOSG</td><td>SDS-SO2 - Standby</td><td>SDS</td><td>OAM (Bulk)</td><td>8.1.0.0.0-81.15.2</td></tr> </tbody> </table>	Server Group	Server	Function	Method	Version	SOSG	SDS-SO2 - Standby	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2					
Server Group	Server	Function	Method	Version													
SOSG	SDS-SO2 - Standby	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2													
2	Upgrade	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e6f2ff;"> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> </thead> <tbody> <tr> <td>SOSG</td><td>SDS-SO - Active</td><td>SDS</td><td>OAM (Bulk)</td><td>8.1.0.0.0-81.15.2</td></tr> </tbody> </table>	Server Group	Server	Function	Method	Version	SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2					
Server Group	Server	Function	Method	Version													
SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2													
3	Upgrade	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e6f2ff;"> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> </thead> <tbody> <tr> <td>DPSG1</td><td>SDS-DP1</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0.0-81.15.2</td></tr> <tr> <td>DPSG2</td><td>SDS-DP2</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0.0-81.15.2</td></tr> </tbody> </table>	Server Group	Server	Function	Method	Version	DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2	DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
4	Upgrade	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e6f2ff;"> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> </thead> <tbody> <tr> <td>DPSG3</td><td>SDS-DP3</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0.0-81.15.2</td></tr> <tr> <td>DPSG4</td><td>SDS-DP4</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0.0-81.15.2</td></tr> </tbody> </table>	Server Group	Server	Function	Method	Version	DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2	DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													

Upgrade Settings

Upgrade ISO

SDS-8.1.0.0.0_81.16.0-x86_64.iso ▼

Select the desired upgrade ISO media file.

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.

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)	8.1.0.0-81.15.2 (2/2)
DPSG1	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG4	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (1/1)

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).

Main Menu: Administration -> Software Management -> Upgrade

Filter* Tasks Thu M

NOSG DRNOSG SOSG

Entire Site SOSG DPSG1 DPSG2 DPSG3 DPSG4

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version	Start Time	Finish Time
	Server Status	Appl HA Role	Network Element		Upgrade ISO	Status Message	
SDS-SO2	Upgrading	Standby	System OAM	OAM	8.1.0.0-81.15.2	2017-05-25 04:50:10 EDT	
	Warn	N/A	SO_DSR_VM_NE		SDS-8.1.0.0_81.16.0-x86_64.iso	Upgrade is in progress	
SDS-SO	Pending	Active	System OAM	OAM	8.1.0.0-81.15.2		
	Norm	N/A	SO_DSR_VM_NE		SDS-8.1.0.0_81.16.0-x86_64.iso	Pending Upgrade	

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).

Main Menu: Administration -> Software Management -> Upgrade

Filter* Tasks

NOSG DRNOSG SOSG

Entire Site SOSG DPSG1 DPSG2 DPSG3 DPSG4

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version	Start Time	Finish Time
	Server Status	Appl HA Role	Network Element		Upgrade ISO	Status Message	
SDS-SO2	Accept or Reject	Standby	System OAM	OAM	8.1.0.0-81.16.0	2017-05-25 04:50:10 EDT	2017-05-25 05:13:03 EDT
	Warn	N/A	SO_DSR_VM_NE		SDS-8.1.0.0_81.16.0-x86_64.iso	Success: Server upgrade is complete	
SDS-SO	Ready	Active	System OAM	OAM	8.1.0.0-81.15.2		
	Norm	N/A	SO_DSR_VM_NE				

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.

Main Menu: Administration -> General Options Wed May 24 15:45:45 20

General options settings

Site Upgrade Bulk Availability *	<input type="text" value="1"/>	<p>Site based upgrade availability for bulk upgrade of MP groups. (0 = none, 1 = 50%, 2 = 66%, 3 = 75%).</p> <p>** Cannot be changed while any site upgrade is running. **</p> <p>[Default = 1; Range = 0-3] [A value is required.]</p>
Site Upgrade SOAM Method *	<input type="text" value="1"/>	<p>Site based upgrade SOAM method. (0 = serial, 1 = bulk).</p> <p><i>Note: Bulk upgrade will upgrade all non-active SOAM servers together.</i></p> <p>** Cannot be changed while any site upgrade is running. **</p> <p>[Default = 1; Range = 0-1] [A value is required.]</p>

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.

Main Menu: Status & Manage -> Tasks -> Active Tasks

Filter* Thu May 25 04:52:51 2017 EDT

SDS-NO	SDS-NO2	SDS-QS	SDS-DRNO	SDS-DRNO2	SDS-DRQS	SDS-SO	SDS-SO2	SDS-SO3	SDS-DP1	SDS-DP2	SDS-DP3	SDS-DP4
ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress					
3	SDS-SO2 Server Upgrade (in SOSG Server Group Upgrade)	running	2017-05-25 04:50:01 EDT	2017-05-25 04:52:00 EDT	0	Upgrade is in progress	17%					
2	SOSG Server Group Upgrade (in SOSG Site Upgrade)	running	2017-05-25 04:49:52 EDT	2017-05-25 04:50:01 EDT	0	Upgrade(s) started.	5%					
1	SOSG Site Upgrade	running	2017-05-25 04:49:43 EDT	2017-05-25 04:49:52 EDT	0	Upgrade(s) started.	5%					
0	Pre-upgrade full backup	completed	2017-05-15 02:43:27 EDT	2017-05-15 02:43:52 EDT	0	Full backup on SDS-NO	100%					

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.

Main Menu: Status & Manage -> Tasks -> Active Tasks Thu May 25 04:53:29 2017 EDT

Filter* Thu May 25 04:53:29 2017 EDT

SDS-NO	SDS-NO2	SDS-QS	SDS-DRNO	SDS-DRNO2	SDS-DRQS	SDS-SO	SDS-SO2	SDS-SO3	SDS-DP1	SDS-DP2	SDS-DP3	SDS-DP4
ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress					
3	SDS-SO2 Server Upgrade (in SOSG Server Group Upgrade)	running	2017-05-25 04:50:01 EDT	2017-05-25 04:53:00 EDT	0	Upgrade is in progress	18%					
2	SOSG Server Group Upgrade (in SOSG Site Upgrade)	running	2017-05-25 04:49:52 EDT	2017-05-25 04:50:01 EDT	0	Upgrade(s) started.	5%					
1	SOSG Site Upgrade	completed	2017-05-25 04:49:43 EDT	2017-05-25 04:53:27 EDT	0	Site upgrade task cancelled by user.	5%					
0	Pre-upgrade full backup	completed	2017-05-15 02:43:27 EDT	2017-05-15 02:43:52 EDT	0	Full backup on SDS-NO	100%					

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.

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)	Ready (1/2) Accept or Reject (1/2)	8.1.0.0-81.15.2 (1/2), 8.1.0.0-81.16.0 (1/2)
DPSG1	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG4	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG3	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG2	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)

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.

Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]

Info*

Cycle	Action	Servers															
1	Upgrade	<table> <tr> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> <tr> <td>SOSG</td><td>SDS-SO - Active</td><td>SDS</td><td>OAM (Bulk)</td><td>8.1.0.0-81.15.2</td></tr> </table>	Server Group	Server	Function	Method	Version	SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0-81.15.2					
Server Group	Server	Function	Method	Version													
SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0-81.15.2													
2	Upgrade	<table> <tr> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> <tr> <td>DPSG1</td><td>SDS-DP1</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0-81.15.2</td></tr> <tr> <td>DPSG2</td><td>SDS-DP2</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0-81.15.2</td></tr> </table>	Server Group	Server	Function	Method	Version	DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0-81.15.2	DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0-81.15.2													
DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0-81.15.2													
3	Upgrade	<table> <tr> <th>Server Group</th><th>Server</th><th>Function</th><th>Method</th><th>Version</th></tr> <tr> <td>DPSG3</td><td>SDS-DP3</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0-81.15.2</td></tr> <tr> <td>DPSG4</td><td>SDS-DP4</td><td>SDS</td><td>Bulk (50% availability)</td><td>8.1.0.0-81.15.2</td></tr> </table>	Server Group	Server	Function	Method	Version	DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0-81.15.2	DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0-81.15.2													
DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0-81.15.2													

Upgrade Settings

Upgrade ISO: SDS-8.1.0.0-81.16.0-x86_64.iso Select the desired upgrade ISO media file.

Ok Cancel

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.

Main Menu: Status & Manage -> Tasks -> Active Tasks

Filter

NO1	NO2	SO1	SO2	DP1	DP2
ID	Name	Status	Start Time	Update Time	
2	SO1 Server Upgrade (in SO_SG Server Group Upgrade)	running	2015-03-02 11:44:42 EST	2015-03-02 11:54:00 EST	
1	SO_SG Server Group Upgrade	running	2015-03-02 11:44:32 EST	2015-03-02 11:47:47 EST	
0	Pre-upgrade full backup	completed	2015-02-27 19:59:06 EST	2015-02-27 20:00:46 EST	

Pause

Restart

Cancel

Delete

Report

Delete All Completed

Delete All Exception

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.

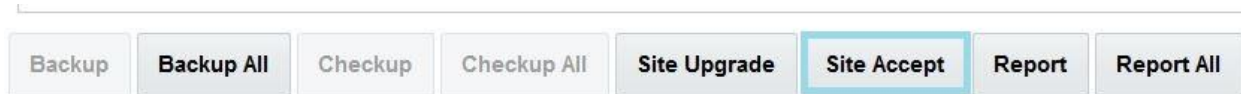


Figure 16. Site Accept Button

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**.

Main Menu: Administration -> Software Management -> Upgrade [Site Accept]

Server group	<input checked="" type="checkbox"/> Action	Server(s) which are Pending Accept
SOSG	<input checked="" type="checkbox"/> Accept upgrade	SDS-SO2

Ok Cancel

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 O for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix B. 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 B.

☐ Execute Appendix M Increase Maximum Number of Open Files.

8.2 Upgrade the Primary SDS NOAM

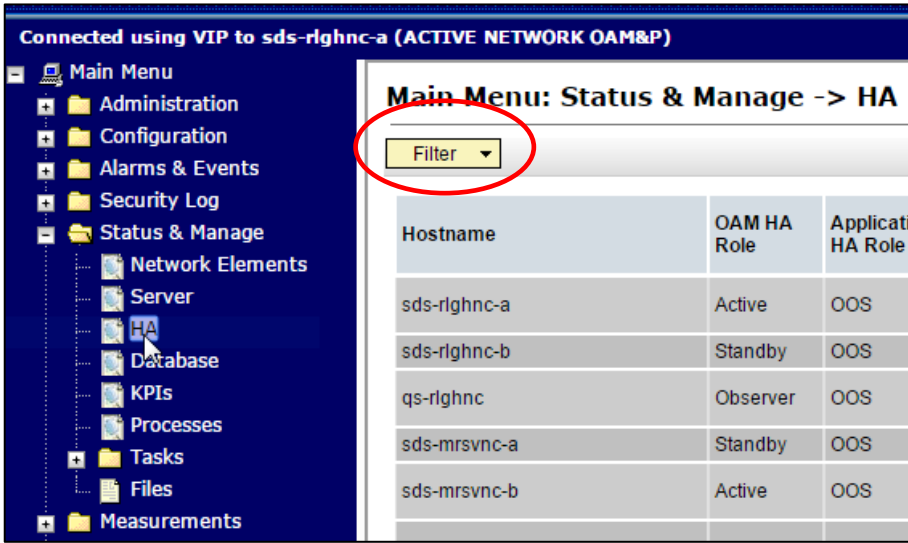
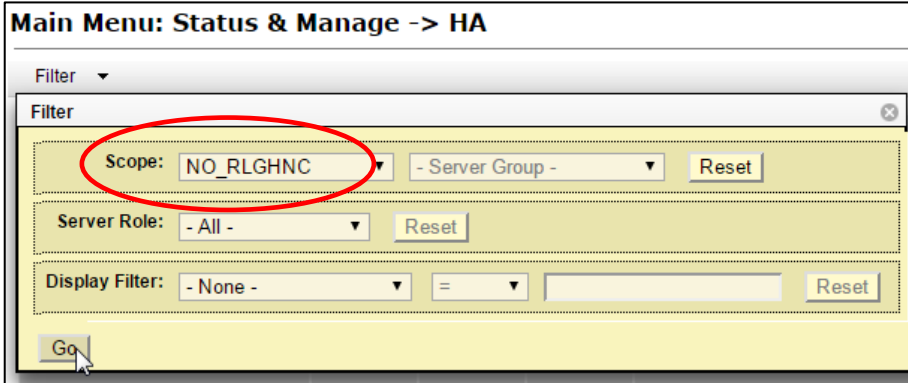
This procedure is used to upgrade the SDS NOAM servers.



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	<p>1. Navigate to Status & Manage > HA.</p> <p>2. Click Filter.</p> 
3.	Primary SDS NOAM VIP GUI: Locate the primary SDS NOAM NE	<p>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.</p> <p>2. Click Go.</p> 

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	S
sds-rlghnc-a	Active	OOS	Active	sds-rlghnc-b	NO_RLGHNC	N
sds-rlghnc-b	Standby	OOS	Active	sds-rlghnc-a	NO_RLGHNC	N
qs-rlghnc	Observer	OOS	Observer	sds-rlghnc-a sds-rlghnc-b	NO_RLGHNC	Q

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
NAT Hosts

Main Menu: SDS -> Configuration -> Options
Apply

Variable	
Display Command Output	<input checked="" type="checkbox"/>
Allow Connections	<input checked="" type="checkbox"/>
Max Transaction Size	50
Log Provisioning Messages	<input checked="" type="checkbox"/>

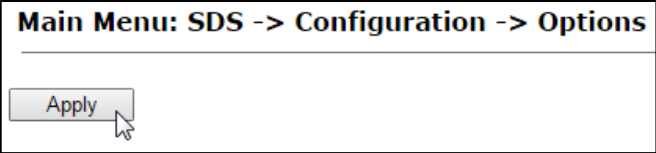
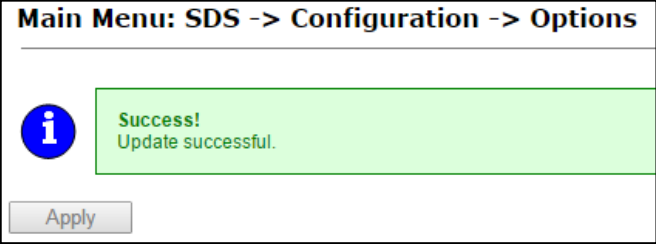
2. Locate the **Remote Import Enabled** checkbox and record the pre-upgrade state.

Transaction Durability Timeout	5 seconds
Remote Import Enabled	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
Remote Import Mode	Non-Blocking ▾

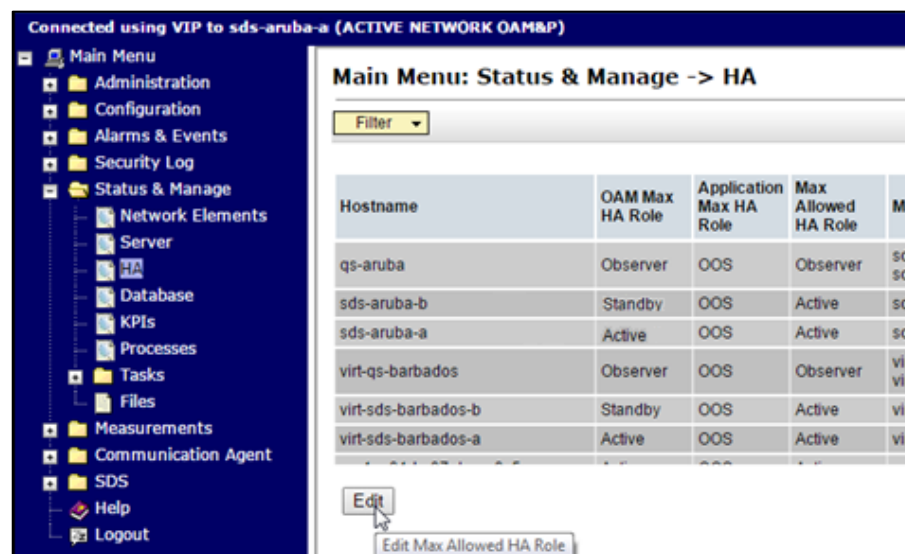
Procedure 5. Upgrade the Primary SDS NOAM		
6. <input type="checkbox"/>	Primary SDS NOAM VIP: Apply change and verify	<p>1. Click Apply.</p>  <p>2. Verify a successful response in the banner.</p> 
7. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the Standby Primary SDS NOAM server	Upgrade the 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. <input type="checkbox"/>	Primary SDS NOAM VIP (CLI): Access the active primary SDS NOAM	<p>Use the VIP address to log into the active primary SDS NOAM with the admusr account.</p> <pre>CentOS release 5.7 (Final) Kernel 2.6.18-274.7.1.el5prere15.0.0_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</pre>

Procedure 5. Upgrade the Primary SDS NOAM		
9. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify status	<p>1. Verify the DbReplication status is Active for the Standby Primary SDS NOAM and Query Server, if equipped.</p> <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> <p>2. If a DbReplication status is received as Audit, then repeat the command until Active is returned.</p> <p>Important: Do not proceed until the status is Active.</p> <p>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).</p> <p>3. Repeat the step until the status is Active for all the mentioned servers.</p> <p>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:</p> <ul style="list-style-type: none"> • Standby Primary SDS NOAM • Query Server • Active DR SDS NOAM • Standby DR SDS NOAM <p>4. If required, contact My Oracle Support (MOS) for any assistance.</p>
10. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	<p>Exit the CLI for the Active Primary SDS NOAM.</p> <pre>[admusr@sds-rlghnc-a filemgmt]\$ exit logout</pre>
11. <input type="checkbox"/>	Access the primary SDS NOAM GUI	<p>Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.</p>

Procedure 5. Upgrade the Primary SDS NOAM

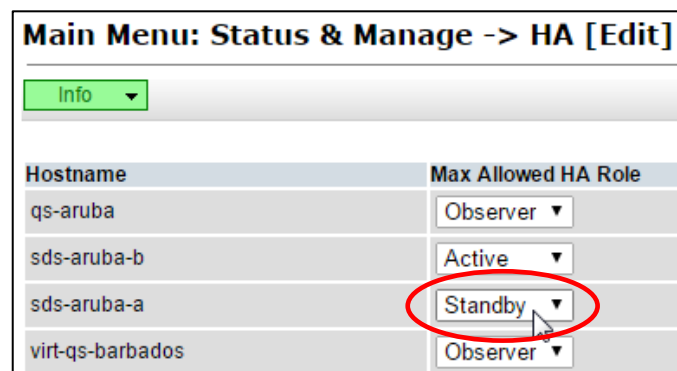
12. **Primary SDS NOAM VIP: Edit server**

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**.



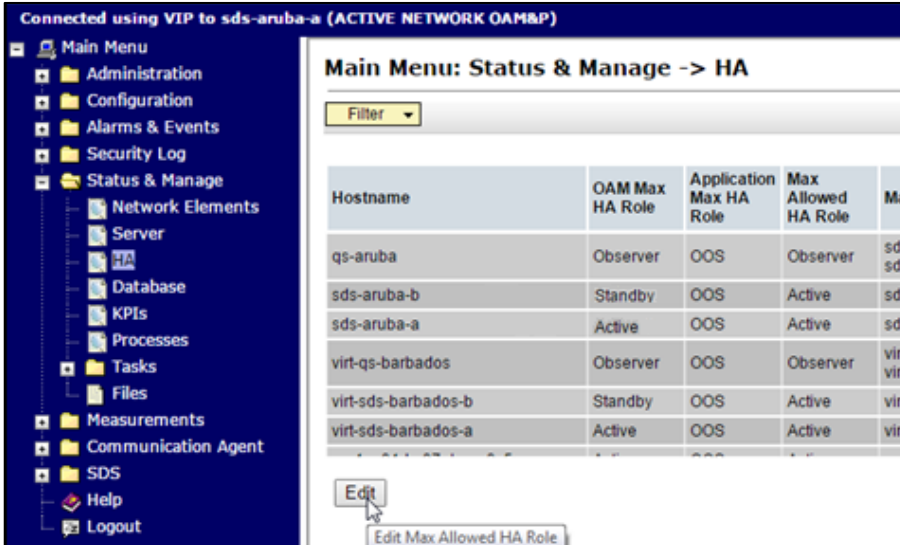
2. Click **OK**.
The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the standby server.
3. If not automatically logged out of the GUI, click **Logout** to log out of the SDS NOAM GUI.

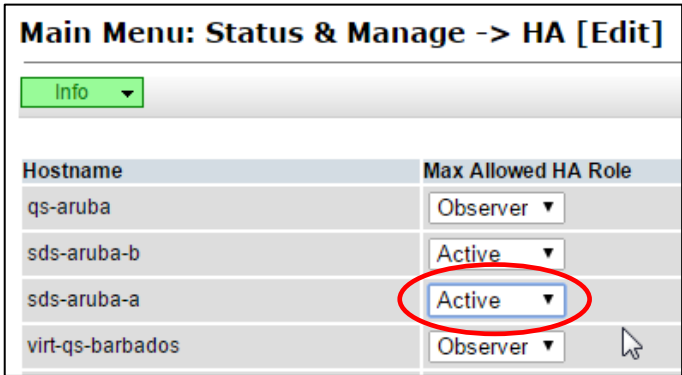


Procedure 5. Upgrade the Primary SDS NOAM

14.	Primary SDS NOAM VIP (GUI): Clear cached data	<p>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:</p> <ol style="list-style-type: none"> 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. <p>Note: Do NOT proceed until the browser cache has been cleared.</p>
-----	--	---

15.	SDS NOAM GUI: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
-----	----------------------------	--


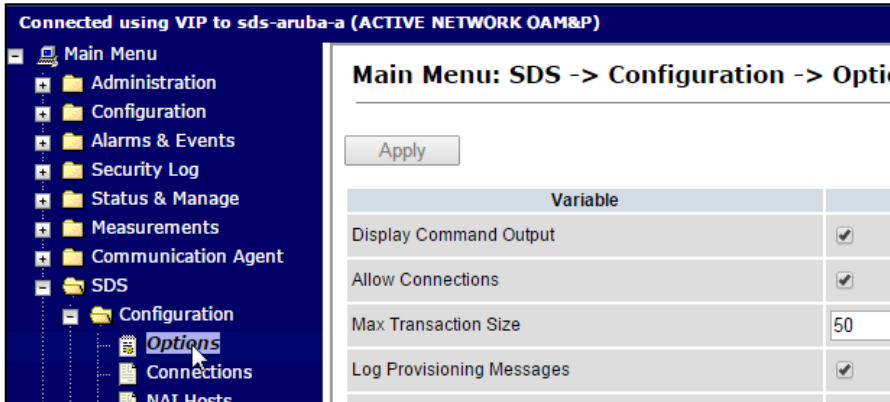
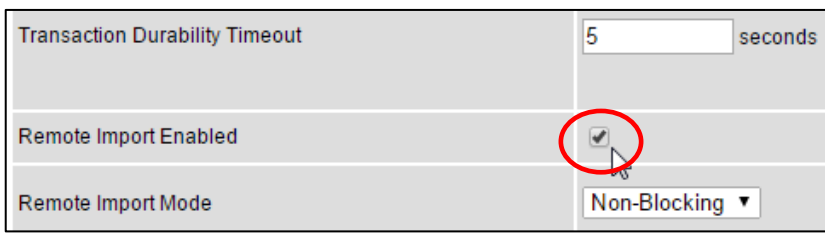
16.	Primary SDS NOAM VIP: Edit server	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA. 2. Click Edit. 
-----	--	---

17.	Primary SDS NOAM VIP: Change Max Allowed HA Role status	<ol style="list-style-type: none"> 1. Select the Standby Primary SDS NOAM server and change a Max Allowed HA Role value from Standby to Active.  <ol style="list-style-type: none"> 2. Click OK.
-----	---	---

Procedure 5. Upgrade the Primary SDS NOAM

18. <input type="checkbox"/>	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. <table><tr><th>Hostname</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Max Allowed HA Role</th><th>Mat</th></tr><tr><td>qs-aruba</td><td>Observer</td><td>OOS</td><td>Observer</td><td>sds</td></tr><tr><td>sds-aruba-b</td><td>Active</td><td>OOS</td><td>Active</td><td>sds</td></tr><tr><td>sds-aruba-a</td><td>Standby</td><td>OOS</td><td>Active</td><td>sds</td></tr><tr><td>virt-qs-barbados</td><td>Observer</td><td>OOS</td><td>Observer</td><td>virt-</td></tr></table>	Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mat	qs-aruba	Observer	OOS	Observer	sds	sds-aruba-b	Active	OOS	Active	sds	sds-aruba-a	Standby	OOS	Active	sds	virt-qs-barbados	Observer	OOS	Observer	virt-
Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mat																							
qs-aruba	Observer	OOS	Observer	sds																							
sds-aruba-b	Active	OOS	Active	sds																							
sds-aruba-a	Standby	OOS	Active	sds																							
virt-qs-barbados	Observer	OOS	Observer	virt-																							
19. <input type="checkbox"/>	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 N 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.																											
20. <input type="checkbox"/>	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. <input type="checkbox"/>	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 N.5 for more details.																									
22. <input type="checkbox"/>	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 29 for remote import.																									

Procedure 5. Upgrade the Primary SDS NOAM		
23. <input type="checkbox"/>	Primary SDS NOAM VIP (CLI): Login	<p>Using the VIP address, log into the Active Primary SDS NOAM with the admusr account.</p> <pre>CentOS release 5.7 (Final) Kernel 2.6.18-274.7.1.el5prere15.0.0_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/awpcom mon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent- gui:/usr/TKLC/comagent:/usr/TKLC/sds PRODPATH=/opt/comcol/prod RUNID=00</pre>
24. <input type="checkbox"/>	Primary SDS NOAM VIP (CLI): Verify status	<ol style="list-style-type: none"> Verify the DbReplication status is Active for the Standby Primary SDS NOAM, Query Server, Active DR SDS NOAM, and Standby NOAM servers (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> <ol style="list-style-type: none"> Repeat the step until the status is Active for all mentioned servers. <p>IMPORTANT</p> <p>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.</p> <p>Servers are:</p> <ul style="list-style-type: none"> • Standby Primary SDS NOAM • Query Server • Active DR SDS NOAM • Standby DR SDS NOAM <ol style="list-style-type: none"> If required, contact My Oracle Support (MOS) for any assistance.
25. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	<p>Exit the CLI for the Active Primary SDS NOAM.</p> <pre>[admusr@sds-rlghnc-a filemgmt]\$ exit logout</pre>

Procedure 5. Upgrade the Primary SDS NOAM		
26. <input type="checkbox"/>	Primary SDS NOAM VIP (CLI): Verify status 	<ol style="list-style-type: none"> 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).
27. <input type="checkbox"/>	Primary SDS VIP: CmHA restart	<p>If the server in topology shows as an Out of Service state, perform a CmHA restart; otherwise, proceed to the next step.</p> <p>Refer to Appendix N for more details.</p> <p>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.</p>
28. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify status	<p>Perform a replication check as explained in step 24.</p> <p>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.</p>
29. <input type="checkbox"/>	Primary SDS NOAM VIP: Re-enable provisioning Remote Import (if applicable)	<p>Re-enable the Remote Import Enabled checkbox if the checkbox recorded in step 5 of this procedure was Checked.</p> <p>If the Remote Import Enabled checkbox recorded in step 5 of this procedure was NOT CHECKED, then this procedure is complete.</p> <ol style="list-style-type: none"> 1. Navigate to SDS > Configuration > Options.  <ol style="list-style-type: none"> 2. Locate the Remote Import Enabled checkbox and mark it. 

Procedure 5. Upgrade the Primary SDS NOAM

30. ☐ **Primary SDS NOAM VIP:**
Apply change and verify

1. Click **Apply**.
2. Verify a successful response in the banner.

Main Menu: SDS -> Configuration -> Options

Success!
Update successful.

Apply

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**.

Connected using VIP to sds-rlghnc-a (ACTIVE NETWORK OAM&P)

Main Menu

- Administration
- Configuration
- Alarms & Events
- Security Log
- Status & Manage
 - Network Elements
 - Server
 - HA
 - Database
 - KPIs
 - Processes
- Tasks
- Files
- Measurements

Main Menu: Status & Manage -> HA

Filter

Hostname	OAM HA Role	Applicat HA Role
sds-rlghnc-a	Active	OOS
sds-rlghnc-b	Standby	OOS
qs-rlghnc	Observer	OOS
sds-mrsvnc-a	Standby	OOS
sds-mrsvnc-b	Active	OOS

Procedure 6. Upgrade DR SDS NOAM

3. <input type="checkbox"/>	Primary SDS NOAM VIP: List servers	<div>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.</div> <div>2. Click Go.</div> <div><div>Filter</div><div><div>Scope: <div>sds_noamp</div> <div>- Server Group -</div> <div>Reset</div></div><div>Server Role: <div>- All -</div> <div>Reset</div></div><div>Display Filter: <div>- None -</div> <div>=</div> <div></div> <div>Reset</div></div><div><div>Go</div></div></div></div>																												
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Identify servers and record server names	<div>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.</div> <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> <div>Active DR SDS NOAM: _____</div> <div>Standby DR SDS NOAM: _____</div> <div>DR SDS Query Server (if equipped): _____</div>	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	dts3-sds-a	Active	OOS	Active	dts3-sds-b	sds_noamp	Network OAM&P	dts3-sds-b	Standby	OOS	Active	dts3-sds-a	sds_noamp	Network OAM&P	dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b	sds_noamp	Query Server
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role																								
dts3-sds-a	Active	OOS	Active	dts3-sds-b	sds_noamp	Network OAM&P																								
dts3-sds-b	Standby	OOS	Active	dts3-sds-a	sds_noamp	Network OAM&P																								
dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b	sds_noamp	Query Server																								
5. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the standby DR SDS server	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.																												
Note: The next two steps of this procedure can be executed in parallel using the Upgrade Server option.																														
6. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the active DR SDS server	<div>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.</div> <div>Important: This causes an HA activity failover to the mate primary SDS NOAM server. This happens a couple minutes after initiating the upgrade.</div>																												
7. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the DR Query server	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.																												

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 B.

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

Refer 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 — Automated vs. Manual Upgrade

Automated	Manual
<p>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.</p> <p>Automated Site Upgrade can be used to upgrade the SOAM and DP servers.</p>	<p>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.</p>
<p>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.</p>	
<p>The Automated Site Upgrade procedures are in section 9.1.</p>	<p>The manual site upgrade procedures are in section 9.2.</p>

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 O for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix B. 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 B.

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 maintenance 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.

Main Menu: Administration -> Software Management -> Upgrade

Filter* Tasks

NO SG DRNOSG SOSG

Entire Site SOSG DPSG1 DPSG2 DPSG3 DPSG4

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versions
SOSG	SDS	OAM (Bulk)	Ready (2/2)	8.1.0.0-81.15.2 (2/2)
DPSG2	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG1	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG4	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG3	SDS	Bulk (50% availability)	Ready (1/1)	8.1.0.0-81.15.2 (1/1)

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.

Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]

Info*

Cycle	Action	Servers															
1	Upgrade	<table> <thead> <tr> <th>Server Group</th> <th>Server</th> <th>Function</th> <th>Method</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>SOSG</td> <td>SDS-SO2 - Standby</td> <td>SDS</td> <td>OAM (Bulk)</td> <td>8.1.0.0.0-81.15.2</td> </tr> </tbody> </table>	Server Group	Server	Function	Method	Version	SOSG	SDS-SO2 - Standby	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2					
Server Group	Server	Function	Method	Version													
SOSG	SDS-SO2 - Standby	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2													
2	Upgrade	<table> <thead> <tr> <th>Server Group</th> <th>Server</th> <th>Function</th> <th>Method</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>SOSG</td> <td>SDS-SO - Active</td> <td>SDS</td> <td>OAM (Bulk)</td> <td>8.1.0.0.0-81.15.2</td> </tr> </tbody> </table>	Server Group	Server	Function	Method	Version	SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2					
Server Group	Server	Function	Method	Version													
SOSG	SDS-SO - Active	SDS	OAM (Bulk)	8.1.0.0.0-81.15.2													
3	Upgrade	<table> <thead> <tr> <th>Server Group</th> <th>Server</th> <th>Function</th> <th>Method</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>DPSG1</td> <td>SDS-DP1</td> <td>SDS</td> <td>Bulk (50% availability)</td> <td>8.1.0.0.0-81.15.2</td> </tr> <tr> <td>DPSG2</td> <td>SDS-DP2</td> <td>SDS</td> <td>Bulk (50% availability)</td> <td>8.1.0.0.0-81.15.2</td> </tr> </tbody> </table>	Server Group	Server	Function	Method	Version	DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2	DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG1	SDS-DP1	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
DPSG2	SDS-DP2	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
4	Upgrade	<table> <thead> <tr> <th>Server Group</th> <th>Server</th> <th>Function</th> <th>Method</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>DPSG3</td> <td>SDS-DP3</td> <td>SDS</td> <td>Bulk (50% availability)</td> <td>8.1.0.0.0-81.15.2</td> </tr> <tr> <td>DPSG4</td> <td>SDS-DP4</td> <td>SDS</td> <td>Bulk (50% availability)</td> <td>8.1.0.0.0-81.15.2</td> </tr> </tbody> </table>	Server Group	Server	Function	Method	Version	DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2	DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2
Server Group	Server	Function	Method	Version													
DPSG3	SDS-DP3	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													
DPSG4	SDS-DP4	SDS	Bulk (50% availability)	8.1.0.0.0-81.15.2													

Upgrade Settings

Upgrade ISO SDS-8.1.0.0.0_81.16.0-x86_64.iso Select the desired upgrade ISO media file.

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.

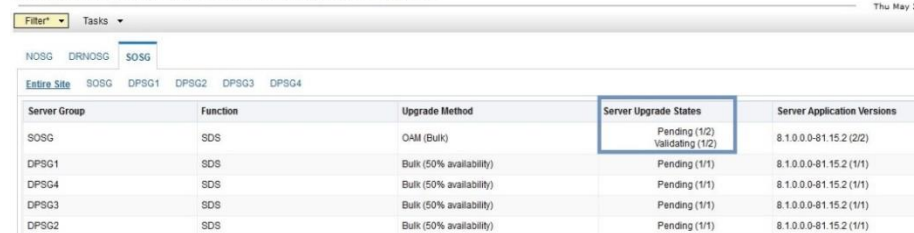
See step 4 of this procedure for instructions if the upgrade fails or if execution time exceeds 60 minutes.

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



Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versions
SOSG	SDS	OAM (Bulk)	Pending (1/2) Validating (1/2)	8.1.0.0-81.15.2 (2/2)
DPSG1	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG4	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG3	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (1/1)
DPSG2	SDS	Bulk (50% availability)	Pending (1/1)	8.1.0.0-81.15.2 (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)

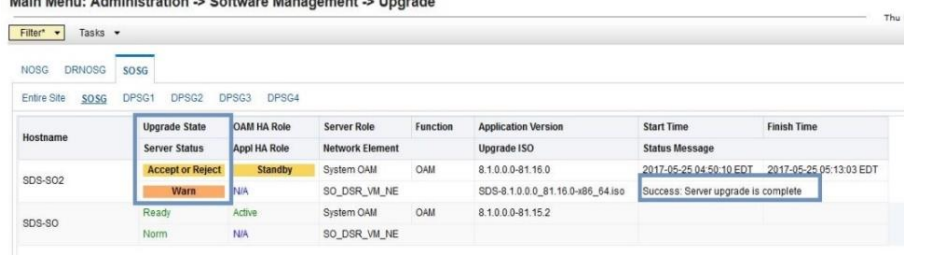
Alarm ID = 31114 (DB Replication over SOAP has failed)

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 O of this document and provide these files. Refer to Appendix I for failed server recovery procedures.

Procedure 7. Upgrade SOAM

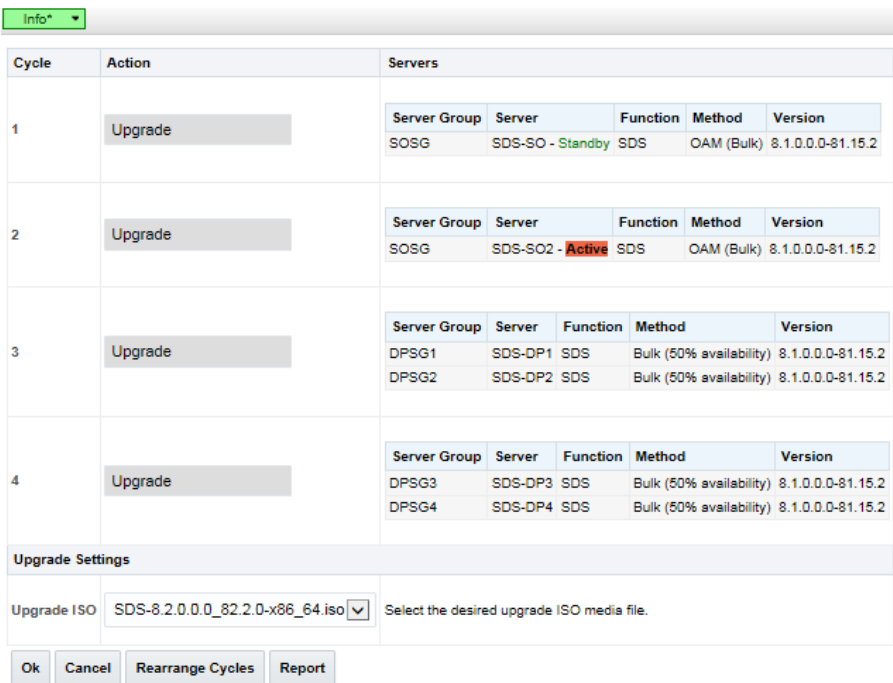
4.	Active NOAM VIP: View In-Progress Status (monitor)	<p>Upon completion of a successful upgrade, every server in the site is in the Accept or Reject state.</p> <p>Main Menu: Administration -> Software Management -> Upgrade</p> 
5.	Server CLI: If the upgrade of a server fails	<p>If the upgrade of a server fails, access the server command line (using SSH or a console), and collect the following files:</p> <ul style="list-style-type: none"> /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/platcfg.log <p>It is recommended to contact My Oracle Support (MOS) by referring to Appendix O of this document and provide these files. Refer to Appendix C Upgrade Server Administration on SDS 7.x for failed server recovery procedures.</p>
6.	Server CLI: Update the tuned profile	<p>After successful upgrade has been verified above, access each of the servers on command line (using SSH or console), and update the tuned profile:</p> <pre>\$ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh</pre> <p>Verify whether tuned profile has been successfully set to comcol_app:</p> <pre>\$ sudo tuned-adm active</pre> <p>Sample Output:</p> <pre>[admusr@SOAM1 ~]\$ sudo tuned-adm active Current active profile: comcol_app Service tuned: enabled, running Service ktune: enabled, running [admusr@SOAM1 ~]\$</pre>

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

1.	Active NOAM VIP: Rearrange the upgrade cycle as needed	<p>Click Rearrange Cycles.</p> <p>Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]</p> 
2.	Active NOAM VIP: Rearrange servers in cycles	<p>1. Click Rearrange Cycles on the Upgrade screen to rearrange servers.</p>

Procedure 8. Rearrange Automated Site Upgrade Cycles

Main Menu: Administration -> Software Management -> Upgrade [Rearrange Cycles]

Cycle	Available Server	Free Pool							
1	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00SOAM00</td> <td> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> </tbody> </table>	Server	Action	DsrSite00SOAM00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>				
Server	Action								
DsrSite00SOAM00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>								
2	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00IPFE00</td> <td rowspan="5"> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> <tr> <td>DsrSite00SS7MP00</td> </tr> <tr> <td>DsrSite00SS7MP01</td> </tr> <tr> <td>DsrSite00STPMP01</td> </tr> <tr> <td>DsrSite00DAM02</td> </tr> </tbody> </table>	Server	Action	DsrSite00IPFE00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>	DsrSite00SS7MP00	DsrSite00SS7MP01	DsrSite00STPMP01	DsrSite00DAM02
Server	Action								
DsrSite00IPFE00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>								
DsrSite00SS7MP00									
DsrSite00SS7MP01									
DsrSite00STPMP01									
DsrSite00DAM02									
3	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00IPFE01</td> <td rowspan="5"> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> <tr> <td>DsrSite00SS7MP02</td> </tr> <tr> <td>DsrSite00SS7MP03</td> </tr> <tr> <td>DsrSite00STPMP00</td> </tr> <tr> <td>DsrSite00DAM02</td> </tr> </tbody> </table>	Server	Action	DsrSite00IPFE01	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>	DsrSite00SS7MP02	DsrSite00SS7MP03	DsrSite00STPMP00	DsrSite00DAM02
Server	Action								
DsrSite00IPFE01	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>								
DsrSite00SS7MP02									
DsrSite00SS7MP03									
DsrSite00STPMP00									
DsrSite00DAM02									

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

Main Menu: Administration -> Software Management -> Upgrade [Rearrange Cycles]

Cycle	Available Server	Free Pool				
1	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00SOAM00</td> <td> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> </tbody> </table>	Server	Action	DsrSite00SOAM00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>	<div>DsrSite00SS7MP02 DsrSite00SS7MP01</div>
Server	Action					
DsrSite00SOAM00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>					
2	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00IPFE00 DsrSite00SS7MP00 DsrSite00STPMP01 DsrSite00DAMP02 DsrSite00DAMP00</td> <td> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> </tbody> </table>	Server	Action	DsrSite00IPFE00 DsrSite00SS7MP00 DsrSite00STPMP01 DsrSite00DAMP02 DsrSite00DAMP00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>	
Server	Action					
DsrSite00IPFE00 DsrSite00SS7MP00 DsrSite00STPMP01 DsrSite00DAMP02 DsrSite00DAMP00	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>					
3	<table border="1"> <thead> <tr> <th>Server</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>DsrSite00IPFE01 DsrSite00SS7MP03 DsrSite00STPMP00 DsrSite00DAMP03</td> <td> <input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/> </td> </tr> </tbody> </table>	Server	Action	DsrSite00IPFE01 DsrSite00SS7MP03 DsrSite00STPMP00 DsrSite00DAMP03	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>	
Server	Action					
DsrSite00IPFE01 DsrSite00SS7MP03 DsrSite00STPMP00 DsrSite00DAMP03	<input type="button" value="Add To Cycle"/> <input type="button" value="Remove From Cycle"/>					

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**.

Main Menu: Administration -> Software Management -> Upgrade [Rearrange Cycles]

The screenshot shows a web-based interface for managing upgrade cycles. At the top, there is a header bar with a 'Remove From Cycle' button. Below this, there is a list of servers, each with a 'Server' column and an 'Action' column. The servers are numbered 2 through 6. Each server entry has a list of server IDs in the 'Server' column and 'Add To Cycle' and 'Remove From Cycle' buttons in the 'Action' column. At the bottom of the window, there are three buttons: 'Ok', 'Cancel', and 'Add Cycle'.

Server	Action
2 DsrSite001PFE00 DsrSite00SS7MP00 DsrSite00STMP01 DsrSite00DAMP02 DsrSite00NAAMP00	Add To Cycle Remove From Cycle
3 DsrSite001PFE01 DsrSite00SS7MP03 DsrSite00STMP00 DsrSite00DAMP03	Add To Cycle Remove From Cycle
4 DsrSite00SS7MP02	Add To Cycle Remove From Cycle
5 DsrSite00SS7MP01	Add To Cycle Remove From Cycle
6	Add To Cycle Remove From Cycle

Ok Cancel 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 B.

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 O for information on contacting My Oracle Support (MOS).

Before upgrading, users must perform the system Health Check in Appendix B. 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 B.

9.2.2 Upgrade SOAM

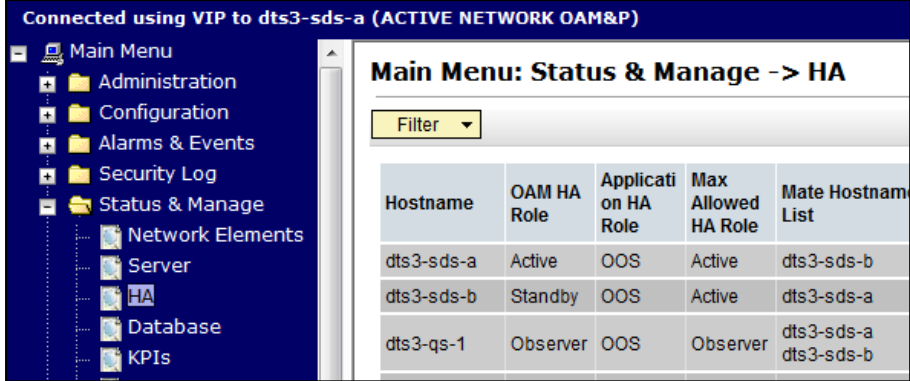
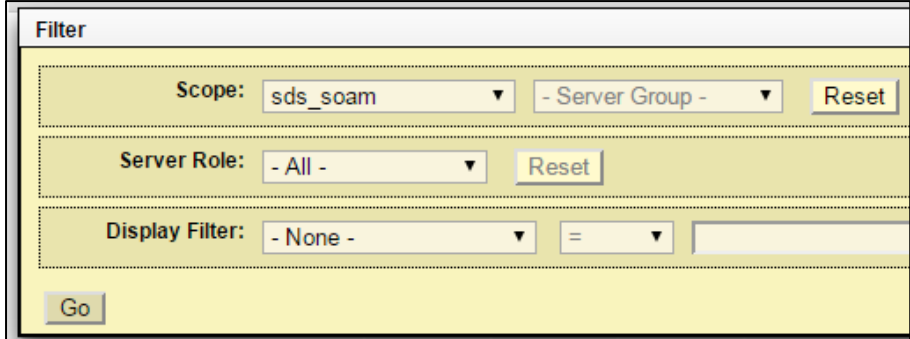
The following procedure details how to upgrade SDS SOAM sites.



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 maintenance window.

Procedure 9. Upgrade SOAM

1. <input type="checkbox"/>	SDS NOAM GUI: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. <input type="checkbox"/>	Primary SDS NOAM VIP (GUI): Record name of the SOAM NE site	<p>1. Navigate to Status & Manage > HA.</p> <p>2. Click Filter.</p>  <p>3. Using the information provided in section 3.1.2 Logins, Passwords, and Site Information, record the name of the SOAM NE site.</p> <p>SOAM NE: _____</p>
3. <input type="checkbox"/>	Primary SDS NOAM VIP: List servers	<p>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.</p> <p>2. Click Go.</p> 

Procedure 9. Upgrade SOAM

4. <input type="checkbox"/>	Primary SDS NOAM VIP: Identify servers and record server names	<div>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.</div> <table><tr><th>Hostname</th><th>OAM HA Role</th><th>Applicati on 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> <div>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: _____</div>	Hostname	OAM HA Role	Applicati on 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
Hostname	OAM HA Role	Applicati on 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																								
5. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the Standby SOAM server	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).																												
6. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade the Active SOAM server	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.																												
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.																														
7. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade up to ½ of the installed DP servers in parallel	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 using the Upgrade Server option for each DP server as described in Appendix D Upgrade Server Administration on SDS 8.x.																												
8. <input type="checkbox"/>	Primary SDS NOAM VIP: Upgrade all remaining DP servers	Upgrade all remaining DP Servers in this SOAM NE site (as identified and recorded in step 4 of this procedure) in parallel using the Upgrade Server option for each DP server as described in Appendix D Upgrade Server Administration on SDS 8.x..																												

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 B.

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!!!**

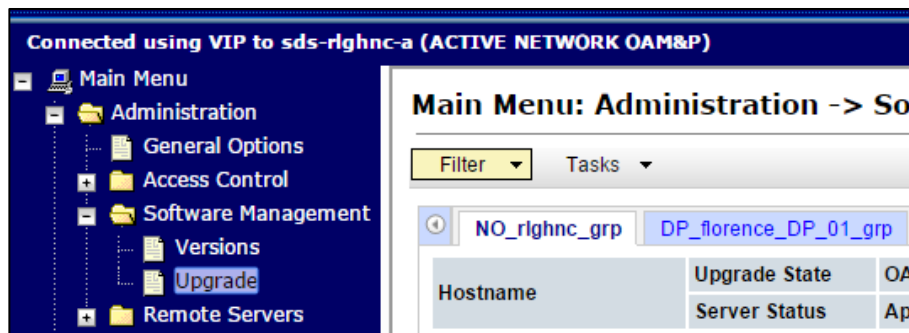
Procedure 10. Accept the Upgrade

- | | | |
|--------------------------|----------------------|--|
| 1. | SDS NOAM GUI: | Use the VIP address to access the primary SDS NOAM GUI as described in |
| <input type="checkbox"/> | Login | Appendix A. |

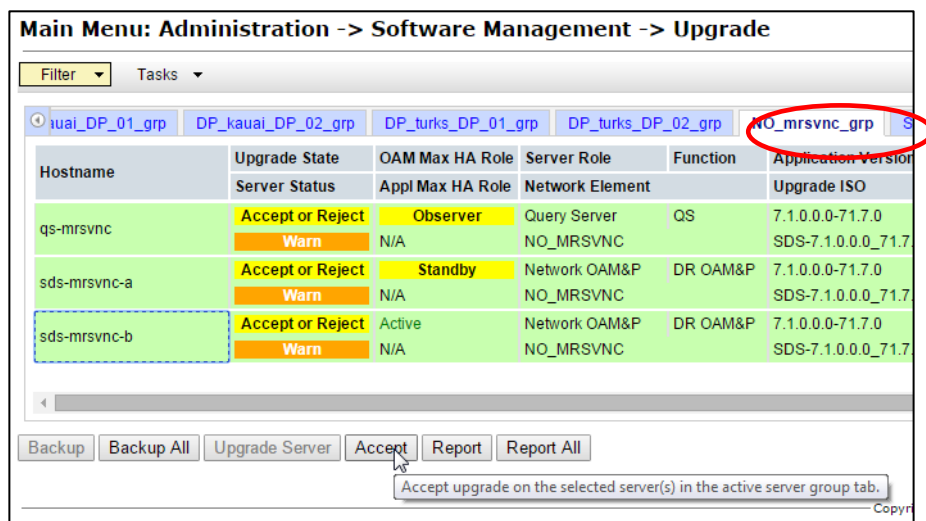
Procedure 10. Accept the Upgrade

2. **Primary SDS NOAM VIP:**
Accept the upgrade

1. Navigate to **Administration > Software Management > Upgrade.**



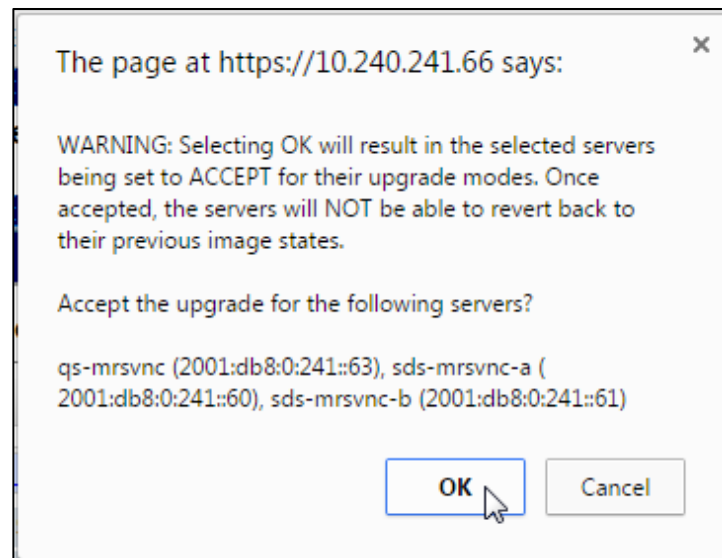
2. Select the Server Group tab containing the server(s) to **Accept** the upgrade.
3. Press and hold the **Ctrl** key to select multiple server(s) in the server group.
4. Click **Accept**.



Procedure 10. Accept the Upgrade

3. ☐ **Primary SDS NOAM VIP:**
Monitor status

Click **OK** to confirm.



The **Upgrade State** changes to **Accepting**.

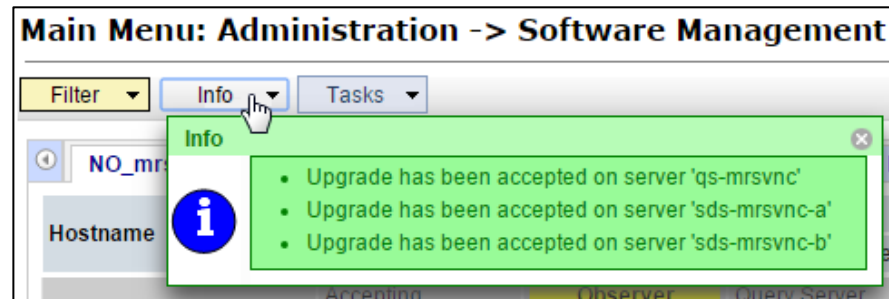
Main Menu: Administration -> Software Management -> Upgrade

Filter Info Tasks

NO_mrsvnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_g

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function
	Server Status	Appl Max HA Role	Network Element	
qs-mrsvnc	Accepting Norm	Observer	Query Server	QS
sds-mrsvnc-a	Accepting Warn	Standby	Network OAM&P	DR OAM&P
sds-mrsvnc-b	Accepting Warn	Active	Network OAM&P	DR OAM&P

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**.

Main Menu: Administration -> Software Management -> Upgrade

Filter Info Tasks

NO_mrsvnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_grp

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	
	Server Status	Appl Max HA Role	Network Element		
qs-mrsvnc	Backup Needed	Observer	Query Server	QS	7
	Norm	N/A	NO_MRSVNC		
sds-mrsvnc-a	Backup Needed	Standby	Network OAM&P	DR OAM&P	7
	Norm	N/A	NO_MRSVNC		
sds-mrsvnc-b	Backup Needed	Active	Network OAM&P	DR OAM&P	7
	Norm	N/A	NO_MRSVNC		

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**.

Connected using VIP to sds-rghnc-a (ACTIVE NETWORK OAM&P)

Main Menu

- Administration
- Configuration
- Alarms & Events
 - View Active
 - View History
 - View Trap Log
- Security Log
- Status & Manage
- Measurements

Main Menu: Alarms & Events -> View A

Filter Tasks Graph

NO_mrsvnc_grp NO_rghnc_grp SO_florence_grp

Seq #	Event ID	Timestamp
	Alarm Text	

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 O 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 O 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 example, 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. <input type="checkbox"/>	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**.

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List
dts3-sds-a	Active	OOS	Active	dts3-sds-b
dts3-sds-b	Standby	OOS	Active	dts3-sds-a
dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b

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.

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

Record the names of SOAM NE site servers:

Active SOAM Server: _____

Standby SOAM Server: _____

DP 1 Server: _____ DP 6 Server: _____


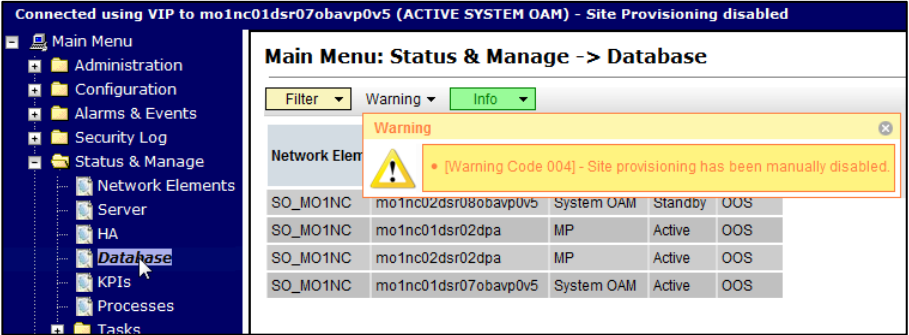

DP 2 Server: _____ DP 7 Server: _____

DP 3 Server: _____ DP 8 Server: _____


DP 4 Server: _____ DP 9 Server: _____

DP 5 Server: _____ DP 10 Server: _____

Procedure 11. Back Out the SOAM

5. <input type="checkbox"/>	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. <input type="checkbox"/>	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. <input type="checkbox"/>	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: <ul style="list-style-type: none"> 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. <input type="checkbox"/>	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. <input type="checkbox"/>	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
10. <input type="checkbox"/>	(Optional) SOAM VIP (GUI): Enable site provisioning Note: Use this step, in case Site Provisioning is Disabled.	1. Navigate to Status & Manage > Database .  2. Click Enable Site Provisioning .  3. Click OK to confirm.

Procedure 11. Back Out the SOAM

11. <input type="checkbox"/>	SOAM VIP: Log out	Click Logout to log out of the SOAM GUI. 
12. <input type="checkbox"/>	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. <input type="checkbox"/>	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 B, 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. <input type="checkbox"/>	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. <input type="checkbox"/>	Primary SDS NOAM VIP: Record name of DR SDS NE site	<div>1. Navigate to Status & Manage > HA.</div> <div>2. Click Filter.</div> <div><div>Connected using VIP to dts3-sds-a (ACTIVE NETWORK OAM&P)</div><div><div><div>Main Menu<ul style="list-style-type: none">AdministrationConfigurationAlarms & EventsSecurity LogStatus & Manage<ul style="list-style-type: none">Network Elements<ul style="list-style-type: none">ServerHADatabaseKPIs</div><div><div>Main Menu: Status & Manage -> HA</div><div>Filter</div><table><thead><tr><th>Hostname</th><th>OAM HA Role</th><th>Applicati on HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostnam List</th></tr></thead><tbody><tr><td>dts3-sds-a</td><td>Active</td><td>OOS</td><td>Active</td><td>dts3-sds-b</td></tr><tr><td>dts3-sds-b</td><td>Standby</td><td>OOS</td><td>Active</td><td>dts3-sds-a</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></tr></tbody></table></div></div></div></div>	Hostname	OAM HA Role	Applicati on HA Role	Max Allowed HA Role	Mate Hostnam List	dts3-sds-a	Active	OOS	Active	dts3-sds-b	dts3-sds-b	Standby	OOS	Active	dts3-sds-a	dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b								
Hostname	OAM HA Role	Applicati on HA Role	Max Allowed HA Role	Mate Hostnam List																										
dts3-sds-a	Active	OOS	Active	dts3-sds-b																										
dts3-sds-b	Standby	OOS	Active	dts3-sds-a																										
dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b																										
3. <input type="checkbox"/>	Primary SDS NOAM VIP: List servers	<div>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.</div> <div>2. Click Go.</div> <div><div>Filter</div><div><div>Scope: sds_noamp - Server Group - Reset</div><div>Server Role: - All - Reset</div><div>Display Filter: - None - = Reset</div><div>Go</div></div></div>																												
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Identify servers and record server names	<div>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.</div> <table><thead><tr><th>Hostname</th><th>OAM HA Role</th><th>Appli catio n HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th></tr></thead><tbody><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></tbody></table> <div>Record the names of primary DR SDS NE site servers: Active DR SDS NOAM: _____ Standby DR SDS NOAM: _____ DR SDS Query Server (if equipped): _____</div>	Hostname	OAM HA Role	Appli catio n HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	dts3-sds-a	Active	OOS	Active	dts3-sds-b	sds_noamp	Network OAM&P	dts3-sds-b	Standby	OOS	Active	dts3-sds-a	sds_noamp	Network OAM&P	dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b	sds_noamp	Query Server
Hostname	OAM HA Role	Appli catio n HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role																								
dts3-sds-a	Active	OOS	Active	dts3-sds-b	sds_noamp	Network OAM&P																								
dts3-sds-b	Standby	OOS	Active	dts3-sds-a	sds_noamp	Network OAM&P																								
dts3-qs-1	Observer	OOS	Observer	dts3-sds-a dts3-sds-b	sds_noamp	Query Server																								
5. <input type="checkbox"/>	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. <input type="checkbox"/>	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. <input type="checkbox"/>	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. <input type="checkbox"/>	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 B, 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.



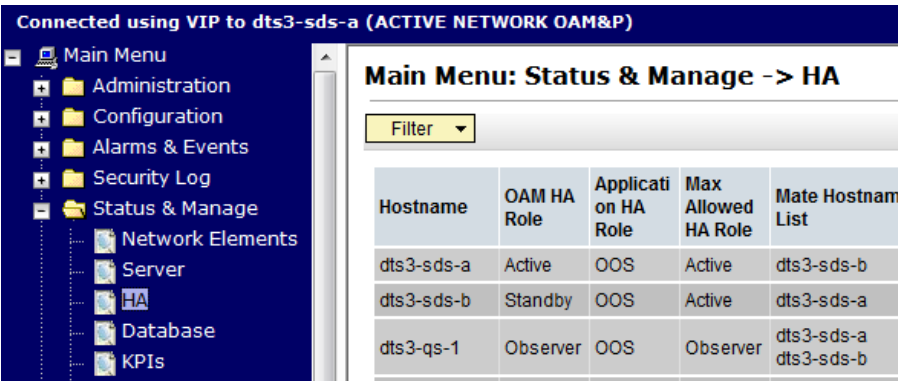
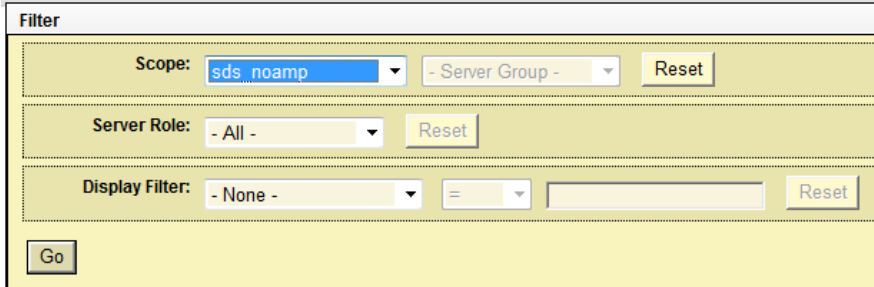
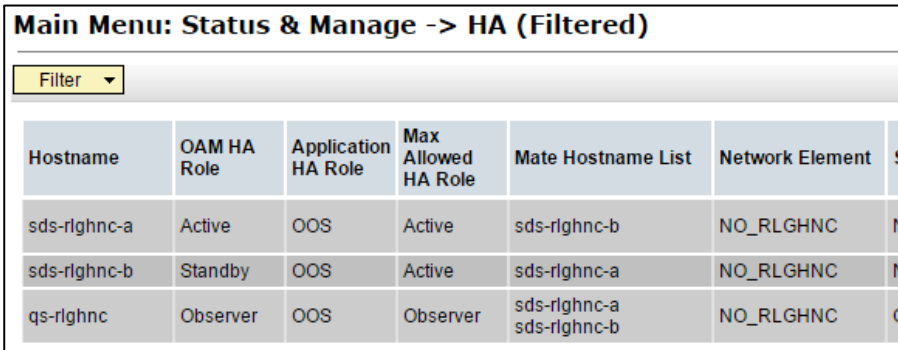
WARNING

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. <input type="checkbox"/>	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. <input type="checkbox"/>	Primary SDS NOAM VIP	<ol style="list-style-type: none"> Navigate to Status & Manage > HA. Click Filter. 
3. <input type="checkbox"/>	Primary SDS NOAM VIP: Locate the primary SDS NOAM NE	<ol style="list-style-type: none"> Using the information provided in section 3.1.2, Logins, Passwords, and Site Information, select the primary SDS Network Element from the Scope field. Click Go. 
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Identify servers and record server names	<p>Identify each server by Hostname, Server Role, and OAM HA Role and record the name of each server.</p>  <p>Active Primary SDS NOAM: _____</p> <p>Standby Primary SDS NOAM: _____</p> <p>Primary SDS Query Server (if equipped): _____</p>

Procedure 13. Back Out Primary SDS NOAM

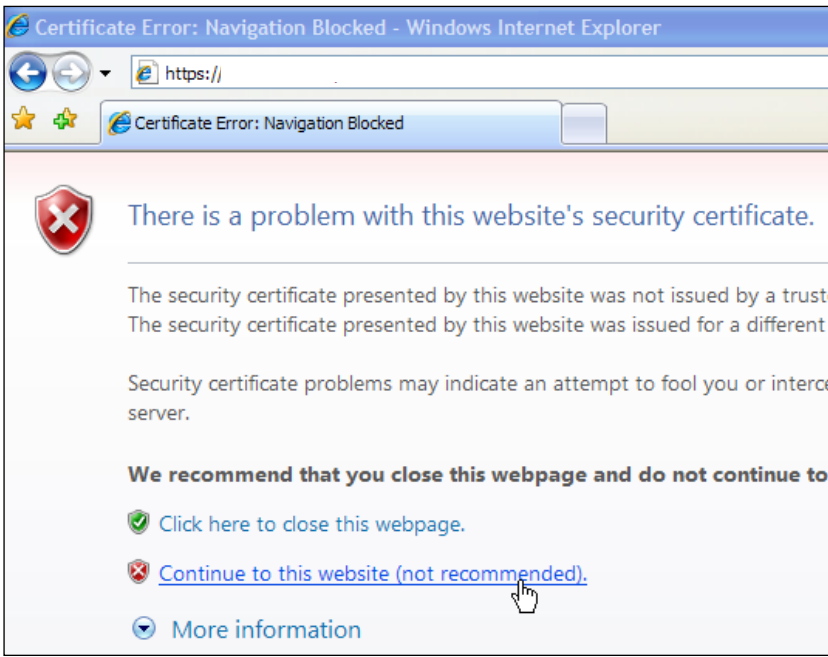
5. <input type="checkbox"/>	Primary SDS NOAM VIP: Downgrade the Standby Primary SDS NOAM server	Downgrade Standby Primary SDS NOAM server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server .
6. <input type="checkbox"/>	Primary SDS NOAM VIP (CLI): Access the active primary SDS NOAM	<p>Use the VIP address to log into the active primary SDS NOAM with the admusr account.</p> <pre>CentOS release 5.7 (Final) Kernel 2.6.18-274.7.1.el5prere15.0.0_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/awpcom mon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent- gui:/usr/TKLC/comagent:/usr/TKLC/sds PRODPATH=/opt/comcol/prod RUNID=00 [admusr@sds-rlghnc-a ~]\$</pre>

Procedure 13. Back Out Primary SDS NOAM		
7. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify status	<p>1. Verify the DbReplication status is Active for the Standby Primary SDS NOAM and Query Server, if equipped.</p> <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> <p>2. If a DbReplication status is Audit is received, then repeat the command until Active is returned.</p> <p>Important: Do not proceed until the status is Active.</p> <p>Check Replication is showing Active for Standby Primary SDS NOAM, Query Server, Active DR SDS NOAM and Standby DR SDS NOAM (if equipped).</p> <p>3. Repeat the step until the status is Active for all the mentioned servers.</p> <p>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:</p> <ul style="list-style-type: none"> • Standby Primary SDS NOAM • Query Server • Active DR SDS NOAM • Standby DR SDS NOAM <p>4. If required, contact My Oracle Support (MOS) for any assistance.</p>
8. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	<p>Exit the CLI for the Active Primary SDS NOAM.</p> <pre>[admusr@sds-rlghnc-a filemgmt]\$ exit logout</pre>
Note: The next 2 steps of this procedure may be executed in parallel.		
9. <input type="checkbox"/>	Primary SDS NOAM VIP: Downgrade Primary SDS Query server	Downgrade Primary Query server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server .
10. <input type="checkbox"/>	Primary SDS NOAM VIP: Downgrade Primary SDS Active server.	<p>Downgrade Active Primary SDS NOAM server (as identified and recorded in step 4 of this procedure) using Appendix E Back Out a Single Server.</p> <p>Important: This causes an HA activity failover to the mate primary SDS NOAM server. This occurs within a few minutes of initiating the upgrade.</p>


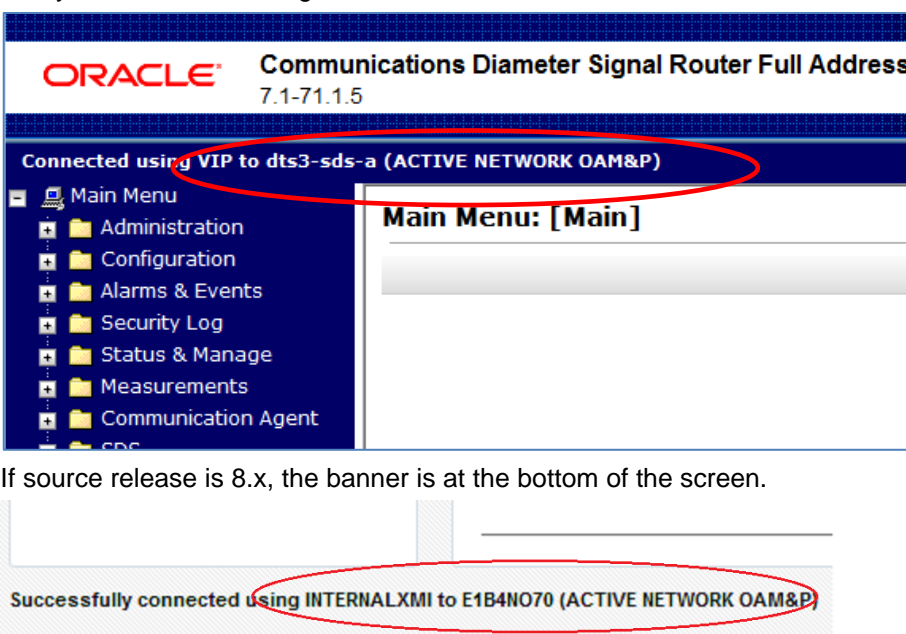
Procedure 13. Back Out Primary SDS NOAM		
11. <input type="checkbox"/>	Allow system to auto-clear temporary alarm states	Wait up to 10 minutes for Alarms associated with server backout to auto-clear. Important: If PDB Relay was recorded as Enabled in Appendix E , step 7 then Event 14189 (pdbRelay Time 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. <input type="checkbox"/>	Execute Health Check	Execute Health Check procedures (Post Backout) as specified in Appendix B, 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. <input type="checkbox"/>	OAM VIP (GUI): Log into the OAM site	<p>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).</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p>  <p>Note: Not applicable for cloud deployments</p>

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

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

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 N.3 Resolve Syscheck Error for CPU Failure.

If the **31201 - Process Not Running** alarm displays, for instance, as cmsoapa, then execute N.4 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:

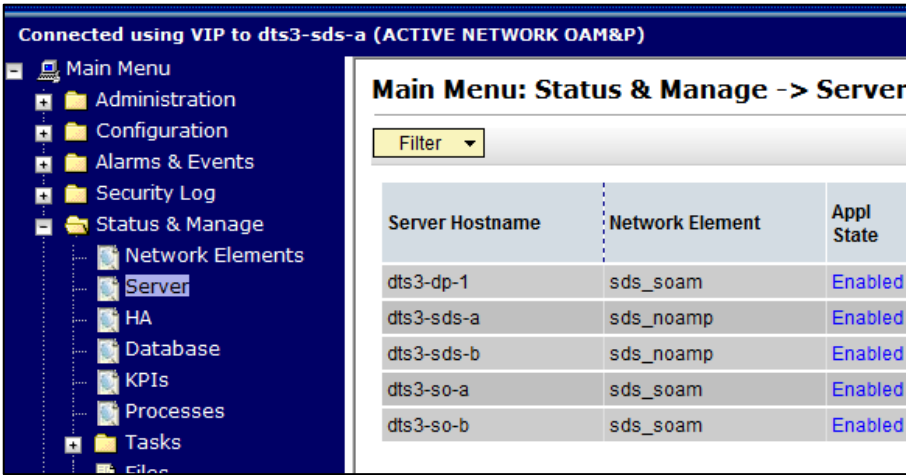
```
$ sudo mkdir -p
/var/TKLC/db/filemgmt/restoretemp

$ 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. <input type="checkbox"/>	SDS NOAM GUI: Login	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
2. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify status	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Verify Server Status is Normal (Normal) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).</p>

Procedure 15. Health Check Procedure

Server Hostname	Network Element	Appl State	Alm	DB	Reporting Status	Proc
dts3-dp-1	sds_soam	Enabled	Norm	Norm	Norm	Norm
dts3-sds-a	sds_noamp	Enabled	Err	Norm	Norm	Norm
dts3-sds-b	sds_noamp	Enabled	Norm	Norm	Norm	Norm
dts3-so-a	sds_soam	Enabled	Norm	Norm	Norm	Norm
dts3-so-b	sds_soam	Enabled	Norm	Norm	Norm	Norm

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.

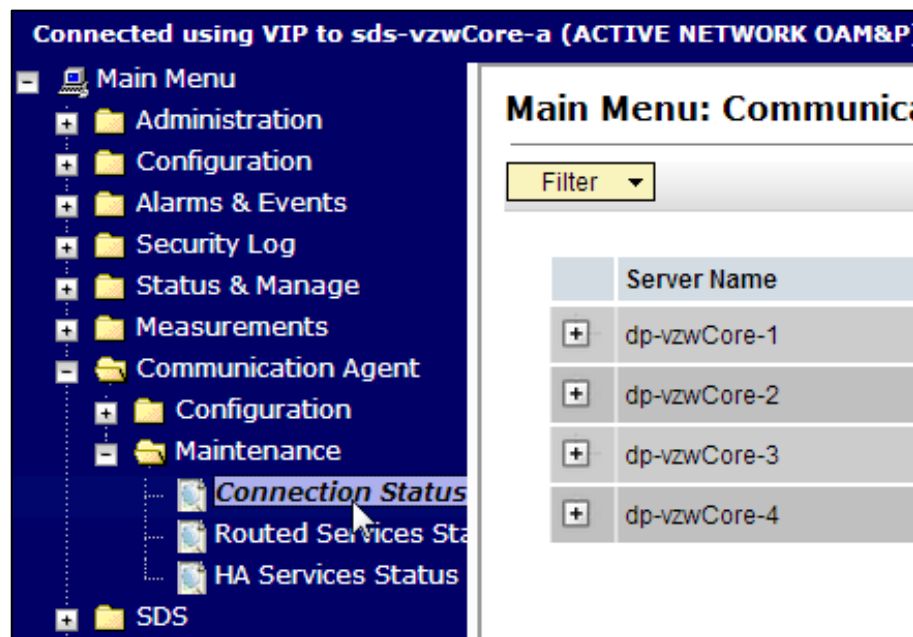
If 31201 - Process Not Running alarm is getting raised for Instance as cmsoapa then execute N.4 Fix cmsoapa Restart to solve this issue.

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)

Procedure 15. Health Check Procedure**Main Menu: Communication Agent -> Maintenance**

Filter			
	Server Name	Automatic Connections Count	Configured Connections Count
+	dp-vzwCore-1	3 of 3 InService	7 of 7 InService
+	dp-vzwCore-2	3 of 3 InService	7 of 7 InService
+	dp-vzwCore-3	3 of 3 InService	7 of 7 InService
+	dp-vzwCore-4	3 of 3 InService	7 of 7 InService

Note: DPs show a **Configured Connections Count** of 1 of 2 InService for Active/Standby configurations. This is normal and can be ignored.

4.



Primary SDS NOAM VIP: View alarm status

Navigate to **Alarms & Events > View Active**.

Main Menu: Alarms & Events -> View Active

Seq #	Event ID	Timestamp	Severity	Pr
38	14101	2015-01-16 22:21:56.707 EST	MAJOR	SD
No Remote Connections				

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:

Procedure 15. Health Check Procedure

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.

5.



Primary SDS NOAM VIP:
 Create Alarms and Events report

1. Click **Export**.



2. Click **OK**.

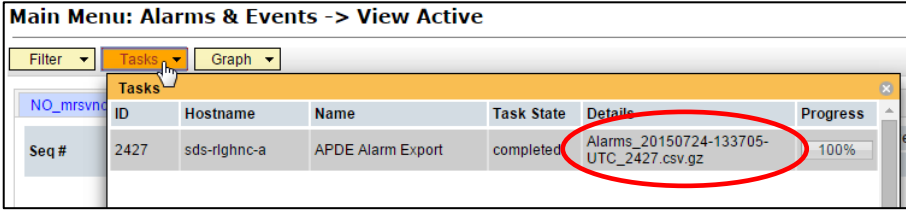

Main Menu: Alarms & Events -> View Active [Export]

Attribute	Value	Description
Export Frequency	<input checked="" type="radio"/> Once <input type="radio"/> Fifteen Minutes <input type="radio"/> Hourly <input type="radio"/> Daily <input type="radio"/> Weekly	Select how often the data will be writ immediately. Note that the Fifteen Mi when provisioning is enabled. [Defau
Task Name	APDE Alarm Export *	Periodic export task name. [Required alphanumeric, minus sign, and space character must not be a minus sign.]
Description		Periodic export task description. [Opt alphanumeric, minus sign, and space character must not be a minus sign.]
Minute	0	Select the minute of each hour when hourly or fifteen minutes. [Default = 0
Time of Day	12:00 AM	Select the time of day when the data weekly. Select from 15-minute incren AM/PM.]
Day of Week	<input checked="" type="radio"/> Sunday <input type="radio"/> Monday <input type="radio"/> Tuesday <input type="radio"/> Wednesday <input type="radio"/> Thursday <input type="radio"/> Friday <input type="radio"/> Saturday	Select the day of week when the data [Default: Sunday.]

Ok
Cancel

The name of the exported alarms CSV file displays in the Tasks tab.

Procedure 15. Health Check Procedure

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

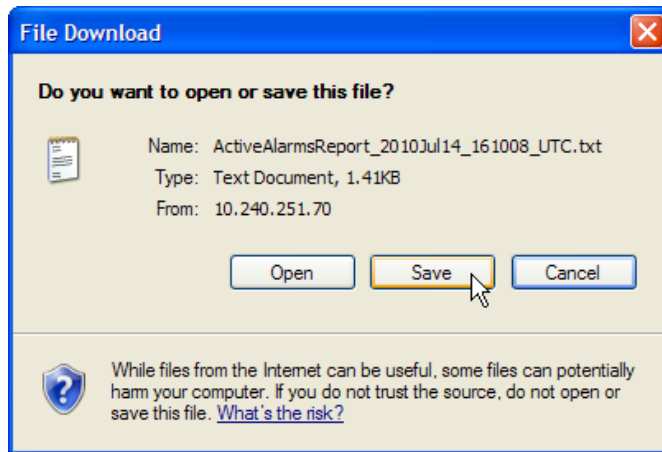
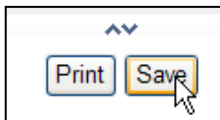
Procedure 15. Health Check Procedure

Main Menu: Alarms & Events -> View Active [Report]

Main Menu: Alarms & Events -> View A
Thu Feb 02 15:59:31 2012

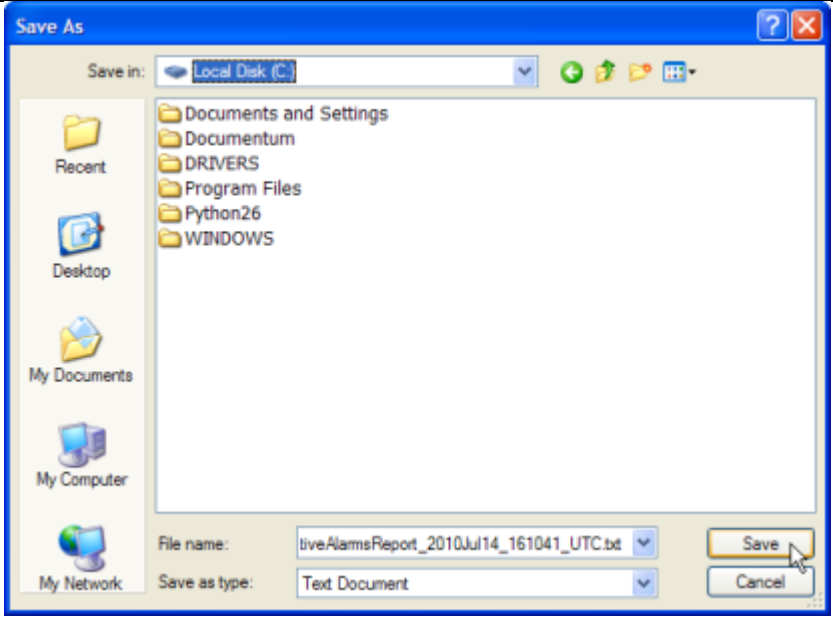
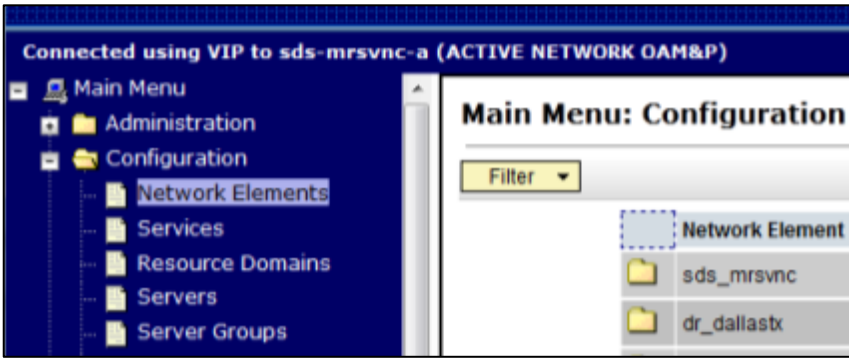
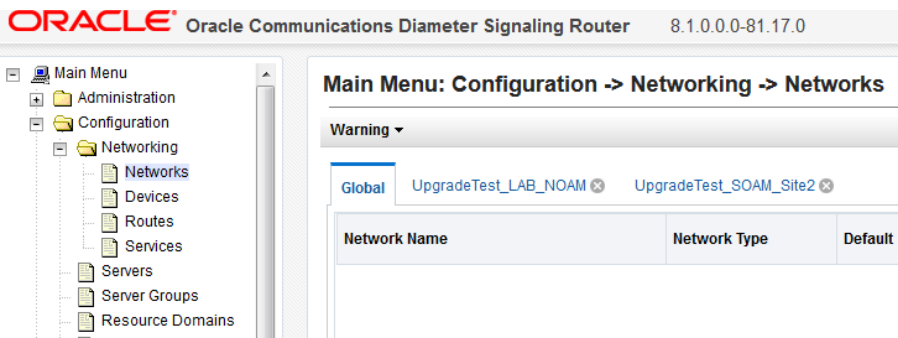
TIMESTAMP: 2012-02-02 15:36:05.350 UTC
 NETWORK_ELEMENT: NO_MRSVNC
 SERVER: sds-mrsvnc-a
 SEQ_NUM: 2099
 EVENT_NUMBER: 14101
 SEVERITY: MAJOR
 PRODUCT: SDS
 PROCESS: xds
 TYPE: PROV
 INSTANCE: No XML client connection
 NAME: No Remote Connections
 DESCR: No remote provisioning clients are connect
 REP INFO:

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

		
<p>8.</p> <p><input type="checkbox"/></p>	<p>Primary SDS NOAM VIP: Create Network Element report</p>	<p>1. Before 8.x, navigate to Configuration > Network Elements.</p>  <p>If the release is 8.x, navigate to Configuration > Networking > Networks.</p>  <p>2. Click Report.</p>

Procedure 15. Health Check Procedure

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

The **Network Element Report** is generated.

Main Menu: Configuration -> Network Elements [Report]

===== sds Network Element Report =====

Report Generated: Wed Feb 01 15:45:11 2012 UTC
 From: Active NETWORK_OAMP on host sds-mrsvnc-a
 Report Version: 3.0.0-3.0.0_10.8.1
 User: guidadmin

----- Network Elements Summary -----

NE Name: sds_mrsvnc

NE Name: dr_dallestx


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.

File Download

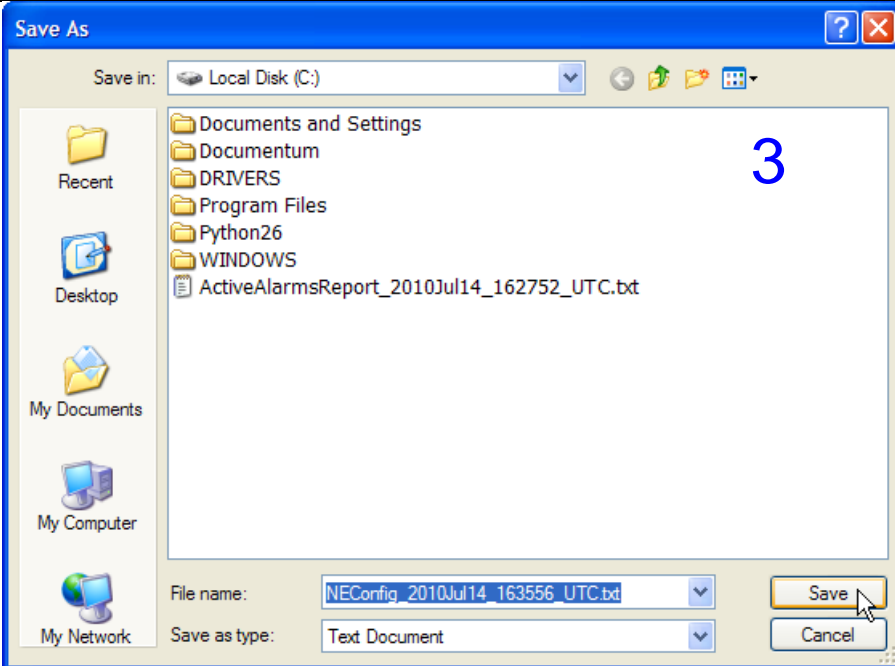
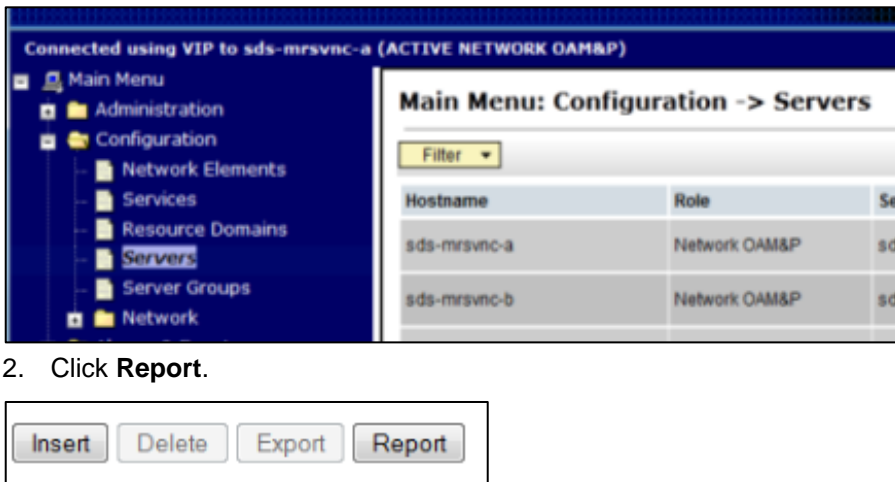
Do you want to open or save this file?

 Name: NEConfig_2010Jul14_163556.UTC.txt
 Type: Text Document
 From: 10.240.251.70

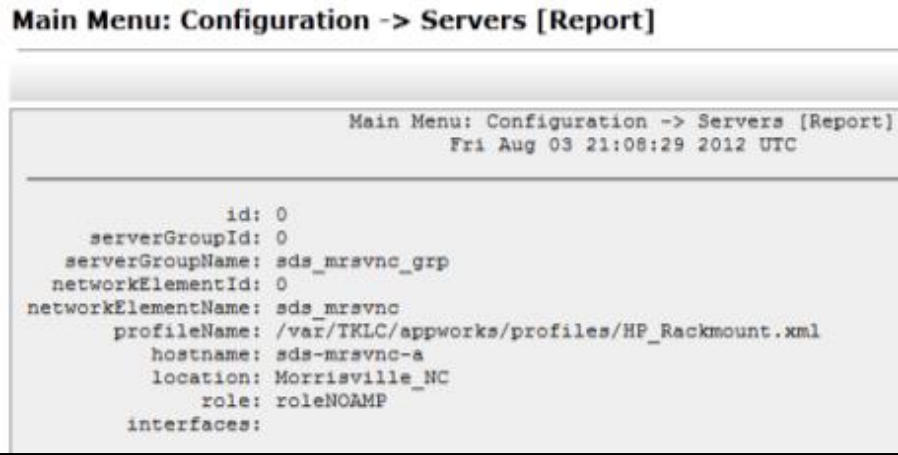

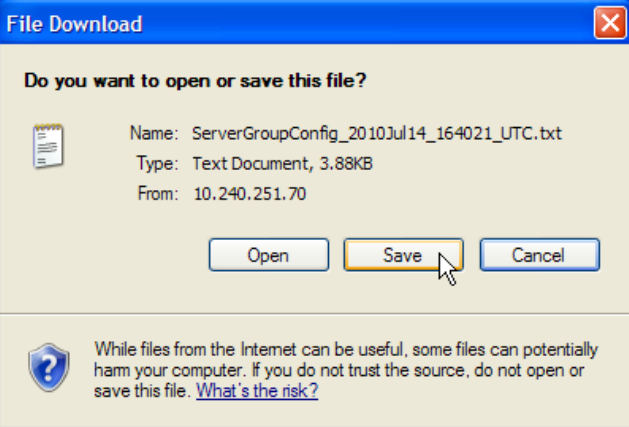
 While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

2. Select a directory on a local disk drive to store the **Network Element** report and click **Save**.

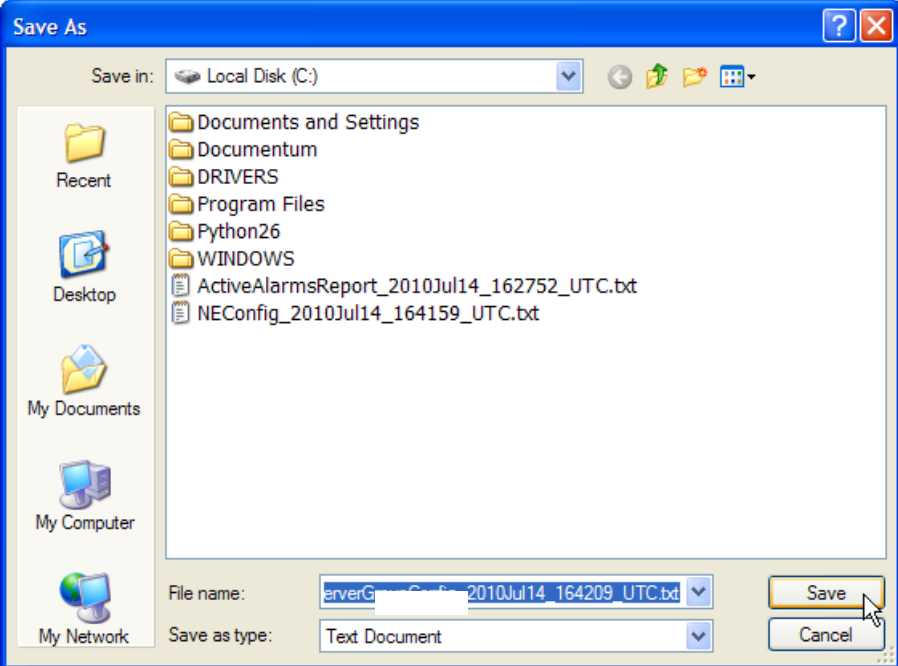
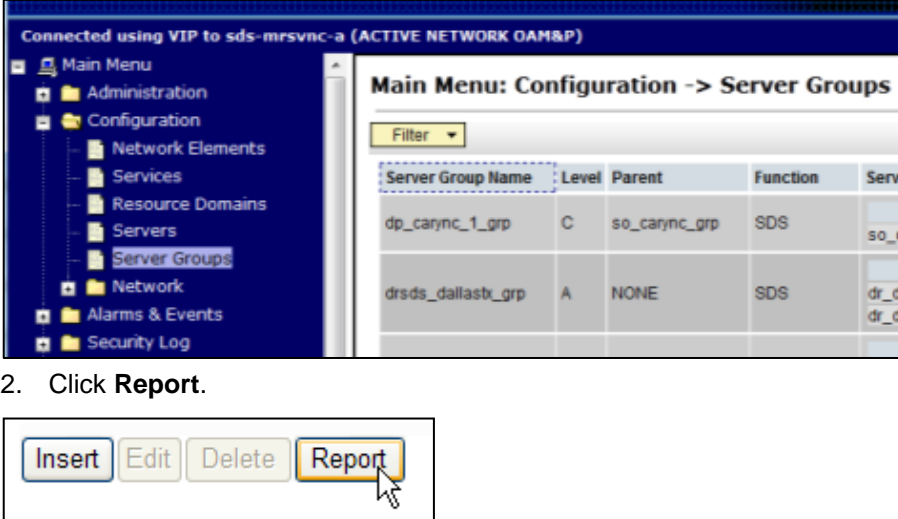
Procedure 15. Health Check Procedure

		
<p>10.</p> <p><input type="checkbox"/></p>	<p>Primary SDS NOAM VIP: Create Servers the report</p>	<p>1. Navigate to Configuration > Servers.</p>  <p>2. Click Report.</p>


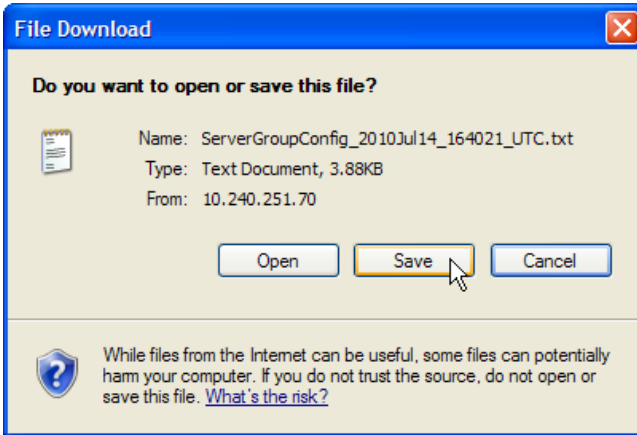
Procedure 15. Health Check Procedure

		 <pre> Main Menu: Configuration -> Servers [Report] Fri Aug 03 21:08:29 2012 UTC id: 0 serverGroupId: 0 serverGroupName: sds_mrsvnc_grp networkElementId: 0 networkElementName: sds_mrsvnc profileName: /var/TKLC/appworks/profiles/HP_Rackmount.xml hostname: sds-mrsvnc-a location: Morrisville_NC role: roleNOAMP interfaces: </pre>
11. <input type="checkbox"/>	Primary SDS NOAM VIP: Save the Servers report	<ol style="list-style-type: none"> Click Save on the Servers report and click Save on the File Download screen. <div data-bbox="500 798 760 961">  </div> <div data-bbox="500 972 1125 1396">  <p>File Download</p> <p>Do you want to open or save this file?</p> <p>Name: ServerGroupConfig_2010Jul14_164021_UTC.txt Type: Text Document, 3.88KB From: 10.240.251.70</p> <p>Open Save Cancel</p> <p>While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?</p> </div> Select a directory on a local disk drive to store the Servers report and click Save.

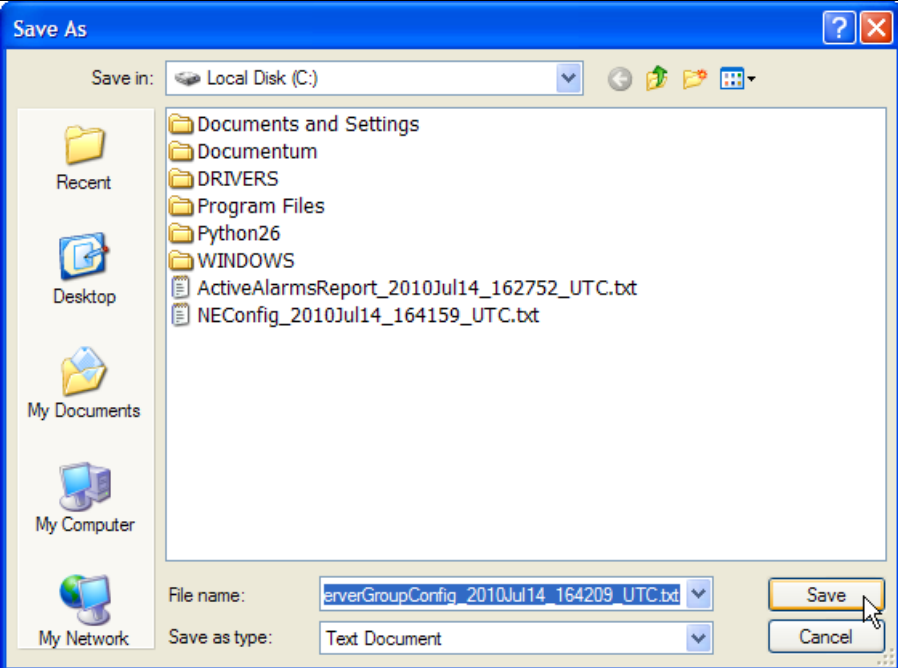
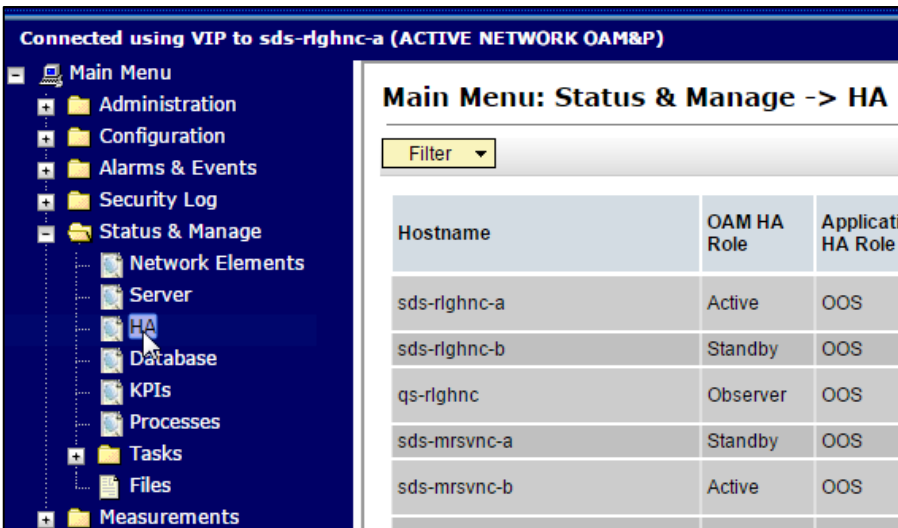
Procedure 15. Health Check Procedure

		
<p>12. <input type="checkbox"/></p>	<p>Primary SDS NOAM VIP: Create Server Groups the report</p>	<p>1. Navigate to Configuration > Server Groups.</p>  <p>2. Click Report.</p>

Procedure 15. Health Check Procedure

		<p>Main Menu: Configuration -> Server Groups [Report]</p> <pre> ===== sds Server Group Report ===== Report Generated: Wed Feb 01 15:47:01 2012 UTC From: Active NETWORK_OAMP on host sds-arsvnc-a Report Version: 3.0.0-3.0.0_10.8.1 User: guiadmin ----- Server Groups Summary sds_arsvnc_grp NE Name: sds_arsvnc Level: A Parent: NONE Function: SDS Virtual IP Address: 010.250.055.125 </pre>
<p>13. <input type="checkbox"/></p>	<p>Primary SDS NOAM VIP: Save the Server Groups report</p>	<p>1. Click Save on the Server Groups report and click Save on the File Download screen.</p> <div data-bbox="495 898 760 1066">  </div> <div data-bbox="492 1071 1125 1503">  </div> <p>2. Select a directory on a local disk drive to store the active Server Groups report and click Save.</p>

Procedure 15. Health Check Procedure

																				
<p>14. <input type="checkbox"/></p>	<p>Provide saved report files to My Oracle Support (MOS)</p>	<p>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:</p> <ul style="list-style-type: none"> • 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) 																		
<p>15. <input type="checkbox"/></p>	<p>Primary SDS NOAM VIP: Verify OAM HA Role status</p>	<p>1. Navigate to Status & Manage > HA.</p>  <table border="1"> <thead> <tr> <th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th></tr> </thead> <tbody> <tr> <td>sds-rhghnc-a</td><td>Active</td><td>OOS</td></tr> <tr> <td>sds-rhghnc-b</td><td>Standby</td><td>OOS</td></tr> <tr> <td>qs-rhghnc</td><td>Observer</td><td>OOS</td></tr> <tr> <td>sds-mrsvnc-a</td><td>Standby</td><td>OOS</td></tr> <tr> <td>sds-mrsvnc-b</td><td>Active</td><td>OOS</td></tr> </tbody> </table> <p>2. Verify the OAM HA Role for all servers shows either Active or Standby.</p>	Hostname	OAM HA Role	Application HA Role	sds-rhghnc-a	Active	OOS	sds-rhghnc-b	Standby	OOS	qs-rhghnc	Observer	OOS	sds-mrsvnc-a	Standby	OOS	sds-mrsvnc-b	Active	OOS
Hostname	OAM HA Role	Application HA Role																		
sds-rhghnc-a	Active	OOS																		
sds-rhghnc-b	Standby	OOS																		
qs-rhghnc	Observer	OOS																		
sds-mrsvnc-a	Standby	OOS																		
sds-mrsvnc-b	Active	OOS																		

Procedure 15. Health Check Procedure

Main Menu: Status & Manage -> HA

Filter ▾

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role
sds-rlghnc-a	Active	OOS	Active	sds-rlghnc-b	NO_RLGHNC	Network OAM&P
sds-rlghnc-b	Standby	OOS	Active	sds-rlghnc-a	NO_RLGHNC	Network OAM&P
qs-rlghnc	Observer	OOS	Observer	sds-rlghnc-a sds-rlghnc-b	NO_RLGHNC	Query Server
sds-mrsvnc-a	Standby	OOS	Active	sds-mrsvnc-b	NO_MRSVNC	Network OAM&P
sds-mrsvnc-b	Active	OOS	Active	sds-mrsvnc-a	NO_MRSVNC	Network OAM&P
qs-mrsvnc	Observer	OOS	Observer	sds-mrsvnc-a sds-mrsvnc-b	NO_MRSVNC	Query Server
turks-sds-SO-a	Standby	OOS	Active	turks-sds-SO-b	SO_TURKS	System OAM
turks-sds-SO-b	Active	OOS	Active	turks-sds-SO-a	SO_TURKS	System OAM
turks-DP-01	Active	OOS	Active		SO_TURKS	MP
turks-DP-02	Active	OOS	Active		SO_TURKS	MP
kauai-sds-SO-a	Standby	OOS	Active	kauai-sds-SO-b	SO_KAUAI	System OAM

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.

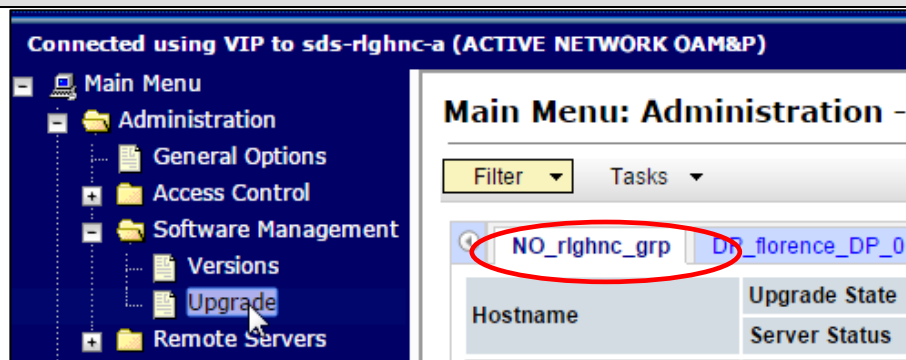
Appendix C. Upgrade Server Administration on SDS 7.x

 STOP	<p>Unless executing parallel upgrades, DO NOT PROCEED until the Upgrade State is Accept or Reject.</p> <p>If an upgrade failure is experienced (that is, Upgrade State = Failed), refer to Appendix I Recover from a Failed Upgrade.</p>
---	---

Procedure 16. Upgrade Server Administration on SDS 7.x

1.	<input type="checkbox"/> Access the primary SDS NOAM GUI	<p>Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.</p>
2.	<input type="checkbox"/> Primary SDS NOAM VIP: Verify status and application version	<ol style="list-style-type: none"> Navigate to Administration > Software Management > Upgrade. Select the Server Group tab for the server(s) to be upgraded.

Procedure 16. Upgrade Server Administration on SDS 7.x



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.

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks

NO_rlgnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_grp

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
sds-rlghnc-a	Ready Norm	Active N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.6.0
sds-rlghnc-b	Ready Norm	Standby N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.6.0
qs-rlghnc	Ready Norm	Observer N/A	Query Server NO_RLGHNC	QS	7.1.0.0.0-71.6.0



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.

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**.

Procedure 16. Upgrade Server Administration on SDS 7.x

Main Menu: Administration -> Software Management -> Upgrade

Filter ▾ Tasks ▾

NO_rlgnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_grp

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Vers
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
sds-rlghnc-a	Ready Norm	Active N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.7.0
sds-rlghnc-b	Ready Norm	Standby N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.7.0
qs-rlghnc	Ready Norm	Observer N/A	Query Server NO_RLGHNC	QS	7.1.0.0.0-71.7.0

Backup Backup All Upgrade Server Accept Report Report All

Initiate upgrade on the selected server(s) or all servers in the active s

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

Main Menu: Administration -> Softw. Management -> Upgrade [I

Info ▾

Hostname	Action	Status
sds-rlghnc-b	Upgrade	OAM Max HA Role Standby Network Element NO_RLGHNC

Upgrade Settings

Upgrade ISO SDS-7.1.0.0.0_71.8.0-x86_64.iso Select the desired upgrade ISO media file.

Ok Cancel

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** only!
WARNING
DO NOT use the **Auto Upgrade**

1. Click **Auto Upgrade**.
Note: Do NOT select any servers with this option.

Procedure 16. Upgrade Server Administration on SDS 7.x

option when upgrading the primary SDS NOAM server group.

Primary SDS NOAM VIP:
Upgrade servers

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks

uai_DP_01_grp DP_kauai_DP_02_grp DP_turks_DP_01_grp DP_turks_DP_02_grp NO_mrs

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
qs-mrsvnc	Ready	Observer	Query Server	QS	7.1.0.0.0-71.7.0
sds-mrsvnc-a	Norm	N/A	NO_MRSVNC		
sds-mrsvnc-a	Ready	Standby	Network OAM&P	DR OAM&P	7.1.0.0.0-71.7.0
sds-mrsvnc-a	Norm	N/A	NO_MRSVNC		
sds-mrsvnc-b	Ready	Active	Network OAM&P	DR OAM&P	7.1.0.0.0-71.7.0
sds-mrsvnc-b	Norm	N/A	NO_MRSVNC		

Backup Backup All Auto Upgrade Accept Report Report All

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.).

Main Menu: Administration -> Software Management -> Upgrade

Info

Hostname	Action	Status
qs-mrsvnc	Upgrade	OAM Max HA Role: Observer Network Element: NO_MRSVNC
sds-mrsvnc-a	Upgrade	OAM Max HA Role: Standby Network Element: NO_MRSVNC
sds-mrsvnc-b	Auto upgrade	OAM Max HA Role: Active Network Element: NO_MRSVNC (This server will upgrade after all Standby servers are upgraded)

Upgrade Settings

Server group upgrade mode.

Mode: ☒ Bulk ☐ Serial ☐ Grouped Bulk

Upgrade ISO: SDS-7.1.0.0.0_71.8.0-x86_64.iso

Ok Cancel


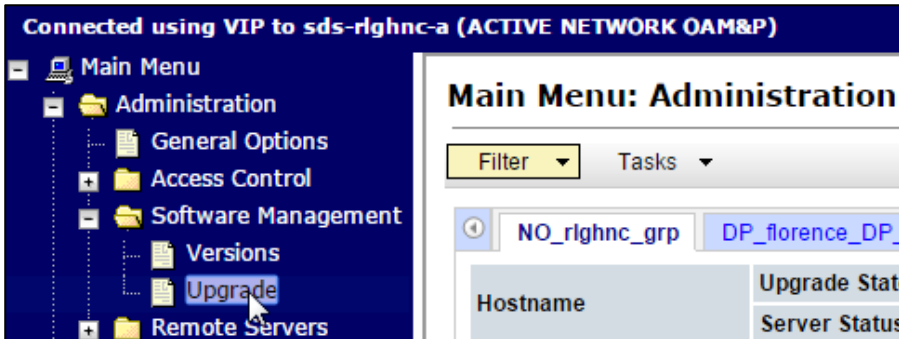
Note: During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all the NOAM and DR-NOAM servers have been upgraded.

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. <input type="checkbox"/>	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. <input type="checkbox"/>	Primary SDS NOAM VIP: Log out	Click Logout to log out of the SDS NOAM GUI. 
7. <input type="checkbox"/>	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: <ol style="list-style-type: none"> 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. <p>Note: Do NOT proceed until the browser cache has been cleared.</p>
8. <input type="checkbox"/>	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
9. <input type="checkbox"/>	Primary SDS NOAM VIP: Monitor status	<ol style="list-style-type: none"> 1. Navigate to Administration > Software Management > Upgrade.  2. Monitor the Upgrade State and the Status Message for the servers being upgraded.

Procedure 16. Upgrade Server Administration on SDS 7.x

Main Menu: Administration -> Software Management -> Upgrade

Filter Status Tasks

Status

- One or more server upgrades started

Hostname	Server Status	Appl Max HA Role	Network Element	Function	Application Version	Start Time	Message
sds-rlghnc-a	Ready Err	Active N/A	Network OAM&P	OAM&P	7.1.0.0-71.7.0		
sds-rlghnc-b	Upgrading Unk	OOS N/A	Network OAM&P	OAM&P	7.1.0.0-71.8.0 SDS-7.1.0.0-71.8.0-x86_64.iso	2015-08-06 12:22:37 UTC	Upgrade is in progress
qs-rlghnc	Ready Err	Observer N/A	Query Server	QS	7.1.0.0-71.7.0		

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 or 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.

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.

Procedure 16. Upgrade Server Administration on SDS 7.x

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

Appendix D. Upgrade Server Administration on SDS 8.x

	CAUTION	<p>Unless executing parallel upgrades, DO NOT PROCEED until the Upgrade State is Accept or Reject.</p> <p>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:</p> <pre>\$ 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</pre> <p>If an upgrade failure is experienced (that is, Upgrade State = Failed), refer to Appendix I Recover from a Failed Upgrade</p>
---	----------------	--

Procedure 17. Upgrade Server Administration on SDS 8.x

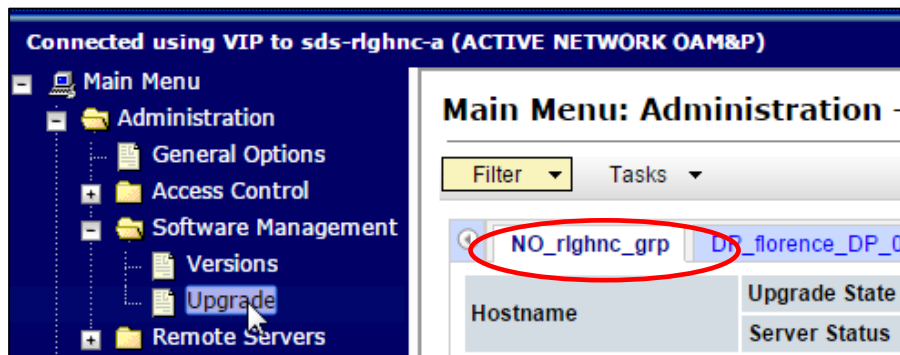
1. <input type="checkbox"/>	Access the primary SDS NOAM GUI	Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.
--------------------------------	---------------------------------	--

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.

Main Menu: Administration -> Software Management -> Upgrade					
Filter	Tasks				
NO_rlgnc_grp	DP_florence_DP_01_grp	DP_florence_DP_02_grp	DP_kauai_DP_01_grp		
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
sds-rlghnc-a	Ready	Active	Network OAM&P	OAM&P	7.1.0.0-71.6.0
	Norm	N/A	NO_RLGHNC		
sds-rlghnc-b	Ready	Standby	Network OAM&P	OAM&P	7.1.0.0-71.6.0
	Norm	N/A	NO_RLGHNC		
qs-rlghnc	Ready	Observer	Query Server	QS	7.1.0.0-71.6.0
	Norm	N/A	NO_RLGHNC		



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**.

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks

NO_rlghnc_grp DP_florence_DP_01_grp DP_florence_DP_02_grp DP_kauai_DP_01_grp

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Vers
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
sds-rlghnc-a	Ready Norm	Active N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.7.0
sds-rlghnc-b	Ready Norm	Standby N/A	Network OAM&P NO_RLGHNC	OAM&P	7.1.0.0.0-71.7.0
qs-rlghnc	Ready Norm	Observer N/A	Query Server NO_RLGHNC	QS	7.1.0.0.0-71.7.0

Backup Backup All Upgrade Server Accept Report Report All

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

Main Menu: Administration -> Softw. Management -> Upgrade [I

Info

Hostname	Action	Status
sds-rlghnc-b	Upgrade	OAM Max HA Role Standby Network Element NO_RLGHNC

Upgrade Settings

Upgrade ISO SDS-7.1.0.0.0_71.8.0-x86_64.iso Select the desired upgrade ISO media file.

Ok Cancel

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!

WARNING
DO NOT use the

1. Click **Auto Upgrade**.

Note: Do NOT select any servers with this option.

Procedure 17. Upgrade Server Administration on SDS 8.x

Auto Upgrade option when upgrading the primary SDS NOAM server group.

Primary SDS NOAM VIP:
Upgrade servers

Main Menu: Administration -> Software Management -> Upgrade

Filter Tasks

uai_DP_01_grp DP_kauai_DP_02_grp DP_turks_DP_01_grp DP_turks_DP_02_grp NO_mrsv

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Versi
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
qs-mrsvnc	Ready Norm	Observer	Query Server	QS	7.1.0.0.0-71.7.0
sds-mrsvnc-a	Ready Norm	Standby	Network OAM&P	DR OAM&P	7.1.0.0.0-71.7.0
sds-mrsvnc-b	Ready Norm	Active	Network OAM&P	DR OAM&P	7.1.0.0.0-71.7.0

Backup Backup All Auto Upgrade Accept Report Report All

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.).

Main Menu: Administration -> Software Management -> Upgr

Info

Hostname	Action	Status
qs-mrsvnc	Upgrade	OAM Max HA Role: Observer Network Eleme: NO_MRSVNC
sds-mrsvnc-a	Upgrade	OAM Max HA Role: Standby Network Eleme: NO_MRSVNC
sds-mrsvnc-b	Auto upgrade	OAM Max HA Role: Active Network Eleme: NO_MRSVNC (This server will upgrade after all Standby servers)

Upgrade Settings

Mode: ☒ Bulk ☐ Serial ☐ Grouped Bulk

Upgrade ISO: SDS-7.1.0.0.0_71.8.0-x86_64.iso

Server group upgrade mode.
Select "Bulk" to upgrade all non-active servers.
Select "Serial" to upgrade servers one by one.
Select "Grouped Bulk" to upgrade all servers in a group.
In all modes, the active OAM server will be upgraded last.
HA groups are created according to the upgrade mode.
The non-active HA role order is spare, standby, then query.

Ok Cancel

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

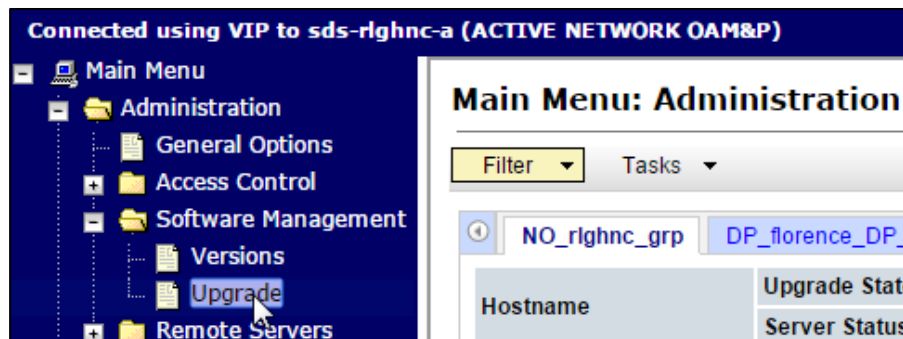
If upgrading the formerly active primary SDS NOAM server (that is 2nd NOAM to be upgraded), then continue with the next step of this procedure; otherwise, SKIP to step 9 of this procedure.

5. <input type="checkbox"/>	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. <input type="checkbox"/>	Primary SDS NOAM VIP: Log out	Click Logout to log out of the SDS NOAM GUI. 
7. <input type="checkbox"/>	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: <ol style="list-style-type: none"> 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. <p>Note: Do NOT proceed until the browser cache has been cleared.</p>
8. <input type="checkbox"/>	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.

Main Menu: Administration -> Software Management -> Upgrade

Filter Status Tasks

Status

- One or more server upgrades started

Hostname	Server Status	Appl Max HA Role	Network Element	Function	Application Version	Start Time	Status Message
sds-rlghnc-a	Ready	Active	Network OAM&P	OAM&P	7.1.0.0.0-71.7.0		
sds-rlghnc-b	Upgrading	OOS	Network OAM&P	OAM&P	7.1.0.0.0-71.8.0	2015-08-06 12:22:37 UTC	Upgrade is in progress
qs-rlghnc	Ready	Observer	Query Server	QS	7.1.0.0.0-71.7.0		

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

Appendix E. Back Out a Single Server


Procedure 18. Back Out a Single Server

1. <input type="checkbox"/>	Primary SDS NOAM VIP: Ensure the server to be downgraded is in the Accept or Reject state	<ol style="list-style-type: none"> 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. <input type="checkbox"/>	Primary SDS NOAM VIP: Set the Max Allowed HA Role to Standby	<ol style="list-style-type: none"> 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

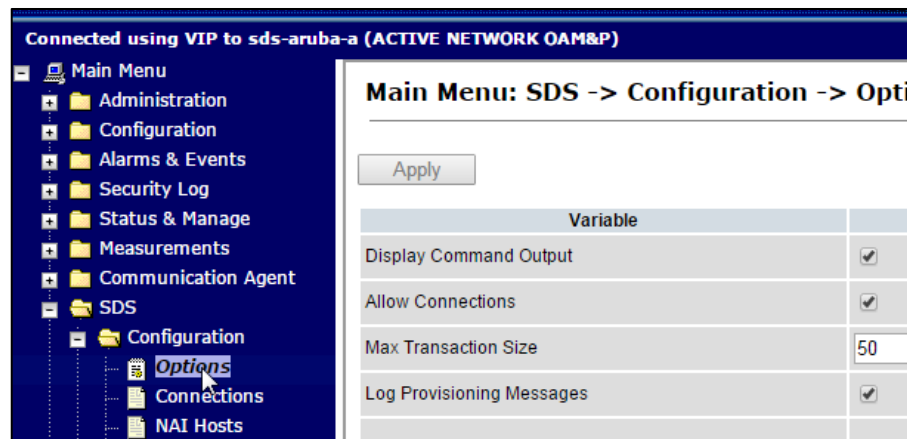
If downgrading the active primary SDS NOAM server, then continue with the next step of this procedure; otherwise, skip to step 7 of this procedure.

Procedure 18. Back Out a Single Server		
3. <input type="checkbox"/>	Primary SDS NOAM VIP: If downgrading the active primary SDS NOAM server, an HA failover occurs	<p>The user's GUI session ends as the active primary SDS server goes through HA failover and becomes the Standby server.</p> <p>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 N to have the NOAMP HA fail over.</p>
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Log out	<p>Click Logout to log out of the SDS NOAM GUI.</p> 
5. <input type="checkbox"/>	Primary SDS NOAM VIP: Clear cached data	<p>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:</p> <ol style="list-style-type: none"> 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. <p>Note: Do NOT proceed until the browser cache has been cleared.</p>
6. <input type="checkbox"/>	Access the primary SDS NOAM GUI	<p>Use the VIP address to access the primary SDS NOAM GUI as described in Appendix A.</p>

Procedure 18. Back Out a Single Server

7. **Primary SDS NOAM VIP:**
Record PDB Relay Enabled state

1. Navigate to **SDS > Configuration > Options.**



Connected using VIP to sds-aruba-a (ACTIVE NETWORK OAM&P)

Main Menu: SDS -> Configuration -> Options

Variable	
Display Command Output	<input checked="" type="checkbox"/>
Allow Connections	<input checked="" type="checkbox"/>
Max Transaction Size	50
Log Provisioning Messages	<input checked="" type="checkbox"/>

2. Locate the **PDB Relay Enabled** checkbox and record if it is checked or not checked.

Remote Audit Number Range Limit	1000 numbers
PDB Relay Enabled	<input checked="" type="checkbox"/>
PDB Relay Primary Remote System VIP Address	10.240.40.6

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 11 of this procedure.

Procedure 18. Back Out a Single Server

8. <input type="checkbox"/>	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.el5prere15.0.0_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. <input type="checkbox"/>	Primary SDS NOAM VIP: Set the pdbRelayTimeStamp to 0	[admusr@sds-rlghnc-b ~]\$ sudo iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp' "
10. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	Exit the CLI for the active primary SDS NOAM. [admusr@sds-rlghnc-b ~]\$ exit logout
11. <input type="checkbox"/>	Primary SDS NOAM VIP: Stop the software	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Server. 2. Select the server(s) to be backed out and click Stop. 3. Click OK to confirm. 4. Verify the Appl State updates to Disabled.
12. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify the server(s) are backout ready	<ol style="list-style-type: none"> 1. Navigate to Administration > Software Management > Upgrade. 2. Select the tab for the server group containing the server(s) to be backed out. <p>Note: It may take a couple minutes for the grid to update.</p> <ol style="list-style-type: none"> 3. Verify the Upgrade State displays as Backout Ready. <p>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.</p>

Procedure 18. Back Out a Single Server

13. <input type="checkbox"/>	Server CLI: SSH to the server(s) to be backed out	<p>Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.</p> <pre>ssh <NOAM XMI IP address></pre> <p>login as: admusr</p> <p>password: <enter password></p> <p>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.</p>
14. <input type="checkbox"/>	Server CLI: Execute the backout	<p>Execute the backout using the reject script:</p> <pre>\$ sudo /var/TKLC/backout/reject</pre> <p>*** TRUNCATED OUTPUT ***</p> <pre>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</pre> <p>Answer y to continue the backout.</p> <p>The server reboots and the user is automatically logged out.</p>
15. <input type="checkbox"/>	Server CLI: SSH to the server(s) to be backed out	<p>Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.</p> <pre>ssh <NOAM XMI IP address></pre> <p>login as: admusr</p> <p>password: <enter password></p>

Procedure 18. Back Out a Single Server

16. <input type="checkbox"/>	Server CLI: Verify the Backout	<p>Examine the upgrade logs in the /var/TKLC/log/upgrade directory and verify no errors are reported.</p> <pre>\$ grep ERROR /var/TKLC/log/upgrade/upgrade.log</pre> <p>Note: The following errors can be ignored:</p> <ul style="list-style-type: none"> • DEBUG: 'iq' 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/hpacuccli 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 • 1526453748::ERROR: Cannot reduce filemgmt enough to leave room for dual image upgrade <p>If the backout was not successful, because other errors were recorded in the logs, then contact My Oracle Support (MOS) for further instructions.</p> <p>If the backout was successful (no errors or failures), then continue with the remaining steps.</p>
---------------------------------	---	--

Procedure 18. Back Out a Single Server

17. <input type="checkbox"/>	Server CLI: Restore the COMCOL Full DB/Run environment	<p>Execute the backout_restore utility to restore the full database run environment.</p> <pre>\$ sudo /var/tmp/backout_restore</pre> <p>*** TRUNCATED OUTPUT ***</p> <p>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.</p> <p>Are you sure you want to proceed? (y n): y</p> <p>Answer y to continue the restore.</p> <p>Note: The COMCOL restore process may take several minutes to complete.</p> <p>If the restore was successful, the following displays:</p> <p>Success: Full restore of COMCOL run env has completed.</p> <p>If an error is encountered and reported by the utility, then work with My Oracle Support (MOS) for further instructions.</p> <p>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.</p>
18. <input type="checkbox"/>	Server CLI: Reboot the server	<pre>\$ sudo init 6</pre> <p>This step can take several minutes and terminates the SSH session.</p>
19. <input type="checkbox"/>	Server CLI: SSH to the server(s) that was backed out	<p>Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.</p> <pre>ssh <NOAM XMI IP address></pre> <pre>login as: admusr</pre> <pre>password: <enter password></pre>

Procedure 18. Back Out a Single Server

20. **Server CLI:**
☐ Restore softlink
 for ComAgent
 directory

```
[admusr@HPC-NO1 ~]$ cd /var/TKLC/appworks/library
$ sudo ln -s /usr/TKLC/comagent-gui/gui/ Comagent
```

Verify if the ComAgent link has been restored:

```
[admusr@HPC-NO1 library]$ ls -ltr
total 56
drwxr-xr-x  7 awadmin awadm 4096 Aug 25  2017 Diameter
lrwxrwxrwx  1 root    root    47 Dec 15  02:05 Zend ->
/usr/TKLC/plat/www/zend-framework/library/Zend/
lrwxrwxrwx  1 root    root    21 Dec 15  02:07 Awps7 ->
/usr/TKLC/awps7/gui/
lrwxrwxrwx  1 root    root    29 Dec 15  02:07 TransportMgr ->
/usr/TKLC/awpttransportmgr/gui
lrwxrwxrwx  1 root    root    38 Dec 15  02:07 Exgstack ->
/usr/TKLC/awpttransportmgr/gui/Exgstack
drwxr-xr-x  3 awadmin awadm 4096 Dec 31  15:58 Rbar
drwxr-xr-x  4 awadmin awadm 4096 May 22  10:42 AWCLI
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Radius
drwxr-xr-x  4 awadmin awadm 4096 May 22  10:44 Dca
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Fabr
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Gla
drwxr-xr-x  2 awadmin awadm 4096 May 22  10:44 Loadgen
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Mapiwf
drwxr-xr-x  6 awadmin awadm 4096 May 22  10:44 Pdra
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Sbr
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:44 Vstp
lrwxrwxrwx  1 root    root    18 May 22  10:44 Ipfe -> /usr/TKLC/ipfe/gui
drwxr-xr-x  3 awadmin awadm 4096 May 22  10:45 Csbr
drwxr-xr-x 17 awadmin awadm 4096 May 22  10:45 AppWorks
lrwxrwxrwx  1 root    root    27 May 22  11:47 Comagent ->
/usr/TKLC/comagent-gui/gui/
```

If the output is received as highlighted in red, the softlink for Comagent directory has been restored.

Procedure 18. Back Out a Single Server

21. <input type="checkbox"/>	Server CLI: Verify the httpd service has restarted	<ol style="list-style-type: none"> 1. If this is an NO or SO, verify httpd service is running. <pre>\$ sudo service httpd status</pre> <pre>httpd (pid xxxx) is running...</pre> <p>Note: The process IDs are variable so the actual number value can be ignored.</p> 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: <ol style="list-style-type: none"> 3. Check the ownership of the file: <pre>ls -ltr /home/awadmin/.ssh/</pre> <p>The file permission should be defined as shown:</p> <pre>[admusr@HPC-NO1 ~]\$ sudo ls -ltr /home/awadmin/.ssh/</pre> <pre>total 20</pre> <pre>-rw----- 1 awadmin awadm 1281 Sep 27 16:19 config</pre> <pre>-rw-r----- 1 awadmin awadm 605 Nov 18 13:20 id_dsa.pub</pre> <pre>-rw----- 1 awadmin awadm 668 Nov 18 13:20 id_dsa</pre> <pre>-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: <pre>sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa</pre> 5. Verify file ownership is changed to awadmin awadm.
22. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify the server(s) application version and upgrade state	<ol style="list-style-type: none"> 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. <p>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.</p>

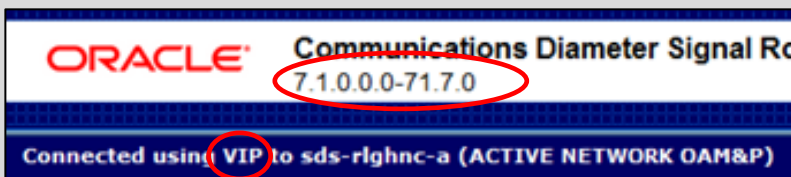
For primary active SDS at release 7.3 or later:

- 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 28 of this procedure.



CAUTION

Note: The primary active SDS release displays on the NOAM GUI banner (using the VIP).



Procedure 18. Back Out a Single Server		
23. <input type="checkbox"/>	Primary SDS NOAM VIP: Set the Max Allowed HA Role to Active	<p>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.</p> <ol style="list-style-type: none"> 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.
24. <input type="checkbox"/>	Primary SDS NOAM VIP: Restart the software	<ol style="list-style-type: none"> 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.
25. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify the Upgrade State	<ol style="list-style-type: none"> 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).
26. <input type="checkbox"/>	Primary SDS NOAM VIP: Stop the software (if necessary)	<p>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.</p> <ol style="list-style-type: none"> 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.
27. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify the server(s) Upgrade State	<ol style="list-style-type: none"> 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 23 of this procedure.

Procedure 18. Back Out a Single Server

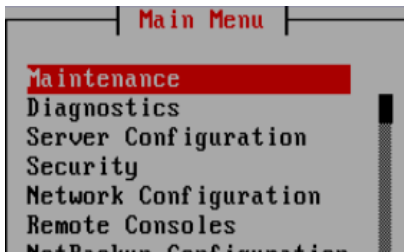

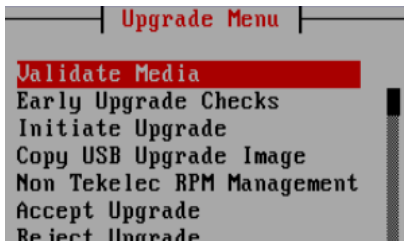
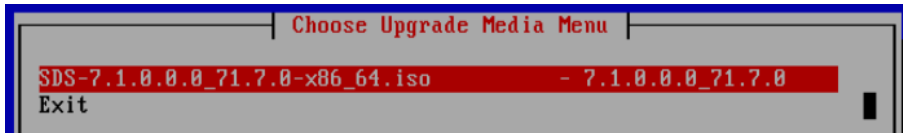
28. <input type="checkbox"/>	Primary SDS NOAM VIP: Complete the backout action (if necessary)	<p>If the server(s) that was backed out displays an Upgrade State of Ready or Success, then</p> <ol style="list-style-type: none"> 1. Select the server(s) that was backed out and click Complete. Leave the Action set to its default value of Complete. 2. Click OK to confirm the action. <p>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.</p> <p>The user may see the following SOAP error display on the GUI banner.</p> <p>SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]</p> <p>It is safe to ignore this error message.</p>
---------------------------------	--	---

Appendix F. Manually Perform ISO Validation

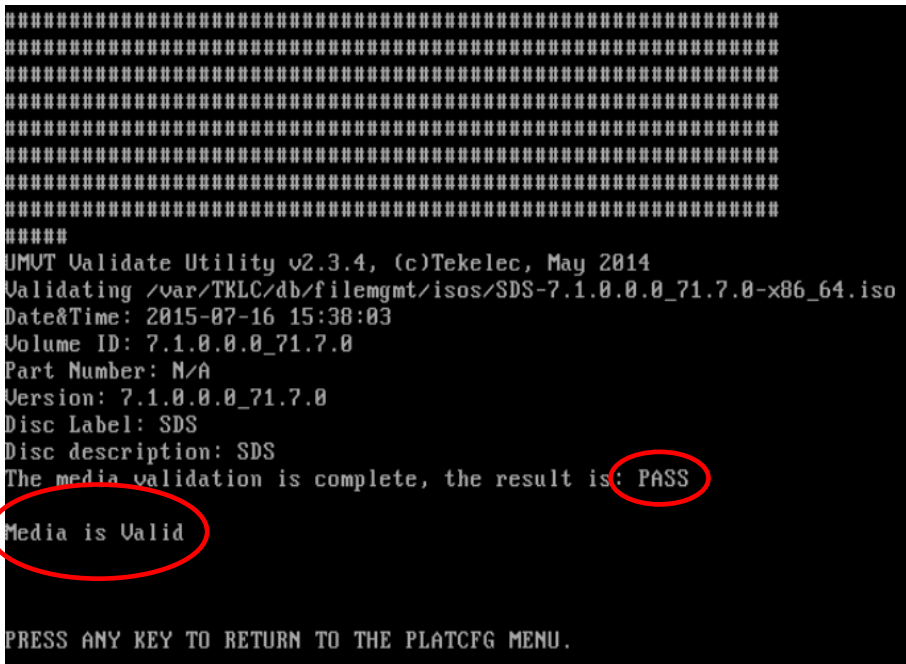
Note: This a procedure assumes that the **ISO** file to be validated has already been uploaded to the server in question and is present in the `/var/TKLC/db/filemgmt/`, `/var/TKLC/db/filemgmt/isos/` or `/var/TKLC/upgrade/` directory.

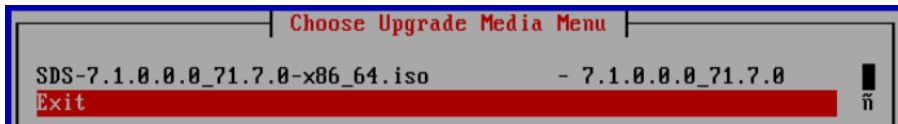
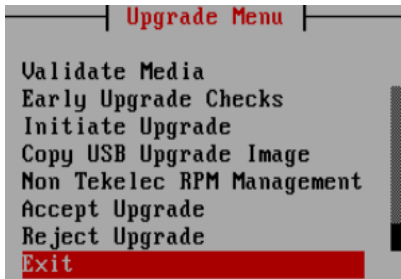
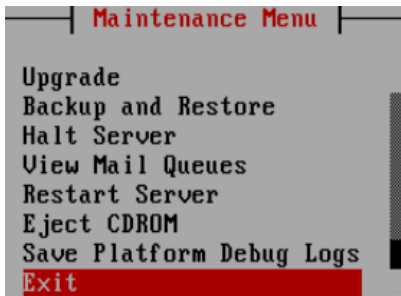
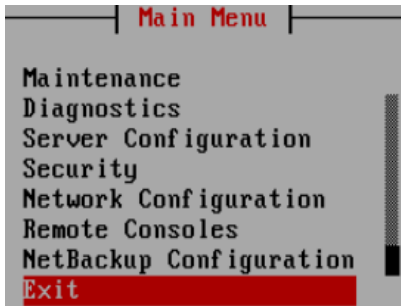
Procedure 19. Manually Perform ISO Validation

1. <input type="checkbox"/>	Primary SDS NOAM VIP: Access the active primary SDS NOAM	<p>Use the VIP address to log into the active primary SDS NOAM with the admusr account.</p> <p>CentOS release 5.7 (Final) Kernel 2.6.18-274.7.1.el5prere15.0.0_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</p>
2. <input type="checkbox"/>	Primary SDS NOAM VIP: Verify ISO file is in the <code>/var/TKLC/upgrade/</code> directory.	<ol style="list-style-type: none"> 1. Verify the ISO file is located in the <code>/var/TKLC/upgrade/</code> 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 <code>var/TKLC/upgrade/</code> 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/

Procedure 19. Manually Perform ISO Validation		
3. <input type="checkbox"/>	Primary SDS NOAM VIP: Become the platcfg user	<p>Become the platcfg user by using the su command.</p> <p>For password information, refer to Table 3. Logins, Passwords, and Site Information, if necessary.</p> <pre>[admusr@sds-rlghnc-a ~]\$ su - platcfg Password: <platcfg_password></pre>
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Select the ISO file	<p>1. From the platcfg menu, select Maintenance and press Enter.</p>  <p>2. Select Upgrade and press Enter.</p>  <p>3. Select Validate Media and press Enter.</p>  <p>Select Choose Upgrade Media Menu, select the target ISO file, and press Enter.</p> 

Procedure 19. Manually Perform ISO Validation

<p>5.</p> <p><input type="checkbox"/></p>	<p>Primary SDS</p> <p>NOAM VIP:</p> <p>Verify ISO media</p>	<p>1. Verify ISO media is Valid.</p>  <pre> ##### UMUT Validate Utility v2.3.4, (c)Tekelec, May 2014 Validating /var/TKLC/db/filemgmt/isos/SDS-7.1.0.0_71.7.0-x86_64.iso Date&Time: 2015-07-16 15:38:03 Volume ID: 7.1.0.0_71.7.0 Part Number: N/A Version: 7.1.0.0_71.7.0 Disc Label: SDS Disc description: SDS The media validation is complete, the result is: PASS Media is Valid PRESS ANY KEY TO RETURN TO THE PLATCFG MENU. </pre> <p>2. Press Enter to return to the platcfg menu.</p>
---	---	---

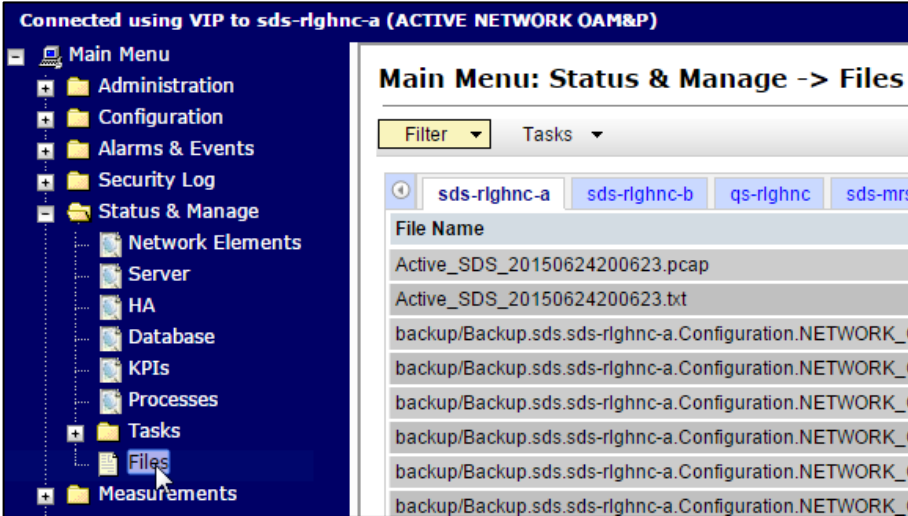
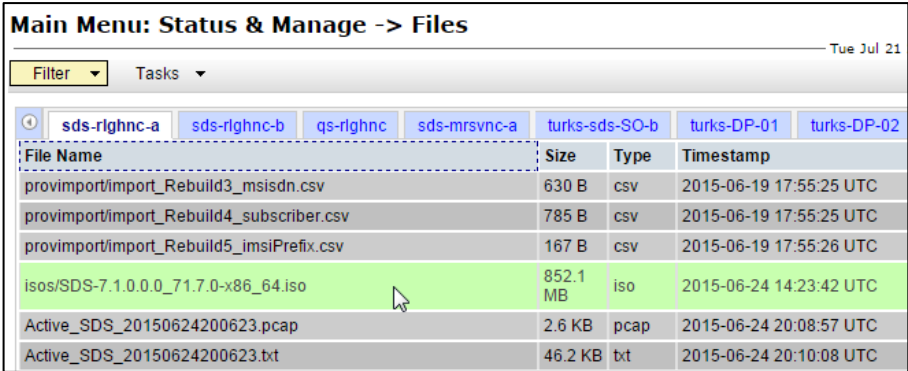
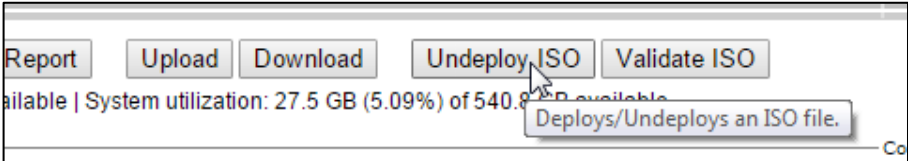
Procedure 19. Manually Perform ISO Validation		
6. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit from menus	<p>1. Select Exit and press Enter.</p>  <p>2. Select Exit and press Enter.</p>  <p>3. Select Exit and press Enter.</p>  <p>4. Select Exit and press Enter.</p> 
7. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	<p>Exit the CLI for the Active Primary SDS NOAM.</p> <pre>[admusr@sds-rlghnc-a ~]\$ exit logout</pre>
8. <input type="checkbox"/>	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**.

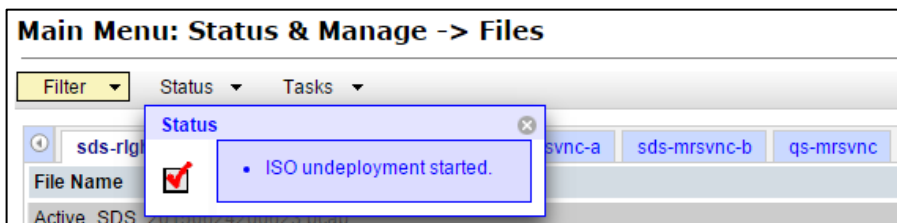
Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance)

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	<p>1. Navigate to Status & Manage > Files.</p>  <p>2. Select the ISO file for the target release.</p>  <p>3. Click Undeploy ISO.</p>  <p>4. Click OK.</p>

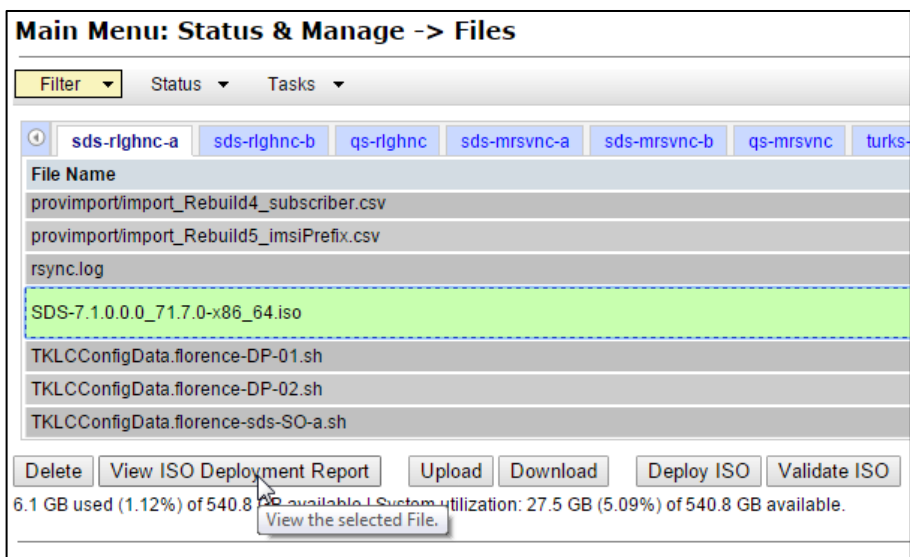
Procedure 20. Undeploy an ISO File (Post Upgrade Acceptance)

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)

		<div data-bbox="492 247 1328 934"> <p>Main Menu: Status & Manage -> Files [View]</p> <hr/> <p>Main Menu: Status & Manage -> Files [View] Tue Jul 21 20:08:34 2015 UTC</p> <p>Deployment report for SDS-7.1.0.0.0_71.7.0-x86_64.iso:</p> <p>Deployed on 0/18 servers.</p> <pre>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</pre> </div> <p>4. Repeat until the ISO displays Not Deployed on all servers in the topology.</p>
--	--	---

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.

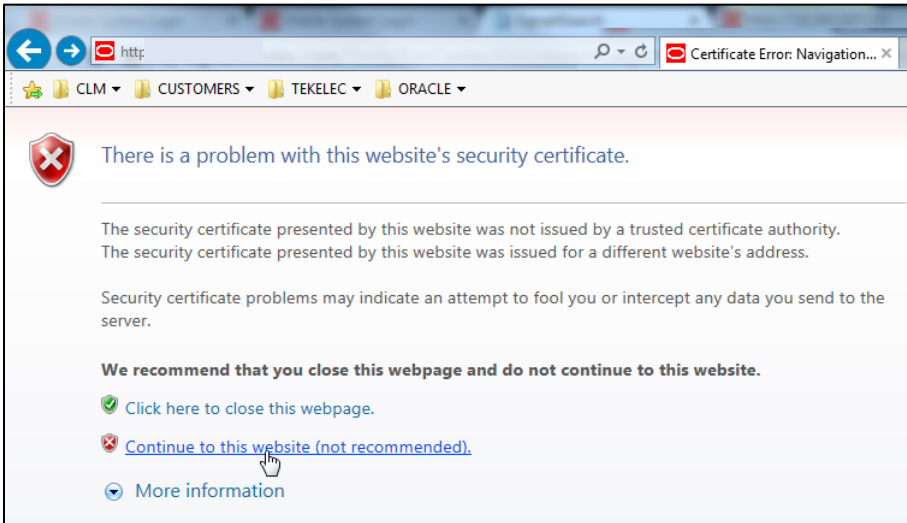

This procedure must be done once for each PMAC at each DSR signaling site that contains SDS SOAM/DP servers.

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

1. <input type="checkbox"/>	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.el5prere15.0.0_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/awpcom mon:/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. <input type="checkbox"/>	Primary SDS NOAM VIP: Access 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. <input type="checkbox"/>	Primary SDS NOAM VIP: Identify ISO file and copy it	<p>1. Identify the exact name of the target ISO file.</p> <pre>[admusr@sds-rlghnc-a filemgmt]\$ ls -l *.iso</pre> <pre>-rw-rw-r-- 1 awadmin awadm 893536256 Jun 24 14:23 SDS-8.0.0.0.0_80.22.0-x86_64.iso</pre> <p>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.</p> <pre>\$ scp -p SDS-8.0.0.0.0_80.22.0-x86_64.iso admusr@10.240.246.7:/var/TKLC/upgrade/</pre> <pre>FIPS integrity verification test failed.</pre> <pre>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.</pre> <pre>Are you sure you want to continue connecting (yes/no)? yes</pre> <pre>Warning: Permanently added '10.240.246.7' (RSA) to the list of known hosts.</pre> <pre>Password: <admusr_password></pre> <pre>SDS-8.0.0.0.0_80.22.0-x86_64.iso 100% 852MB 11.2MB/s 01:16</pre>
4. <input type="checkbox"/>	Primary SDS NOAM VIP: Exit CLI	Exit the CLI for the Active Primary SDS NOAM . [admusr@sds-rlghnc-a filemgmt]\$ exit logout

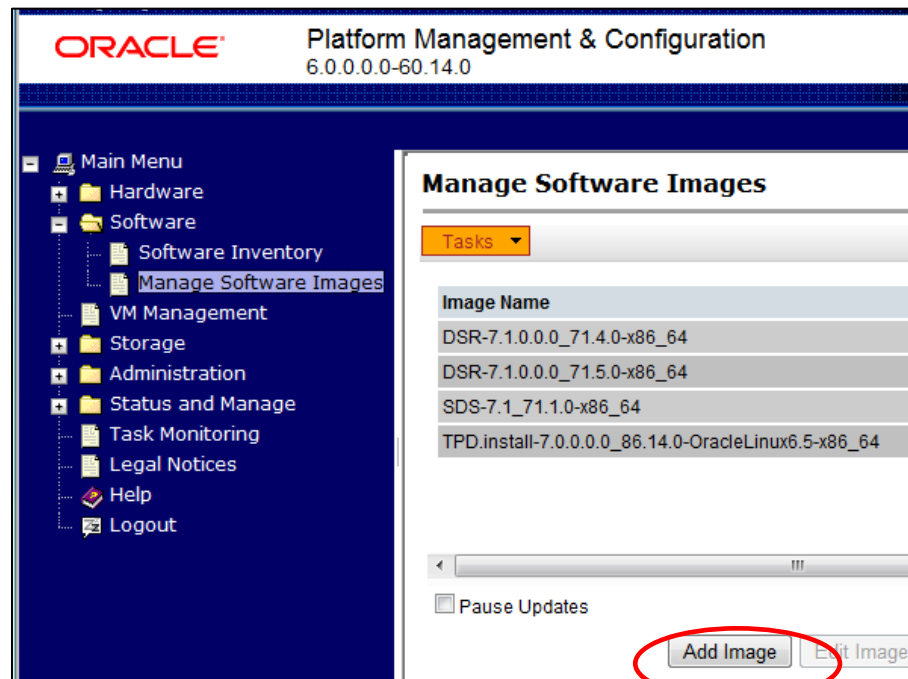
Procedure 21. Add the SDS ISO to the PMAC Software Repository

5.	PMAC Server (GUI): Log into the Platform Management and Configuration application	<p>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.</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p> 
6.	PMAC Server: Login	<p>Login using the default user and password.</p> 

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**.

Add Software Image

Images may be added from any of these sources:

- Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
- USB media attached to the PM&C's host (Refer to Note)
- External mounts. Prefix the directory with "extfile://".
- These local search paths:
 - /var/TKLC/upgrade/*.iso
 - /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso

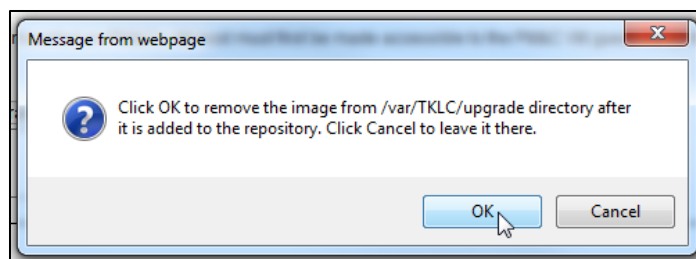
Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM in [VM Management](#).

Path: /var/TKLC/upgrade/SDS-7.1.0.0.0_71.7.0-x86_64.iso

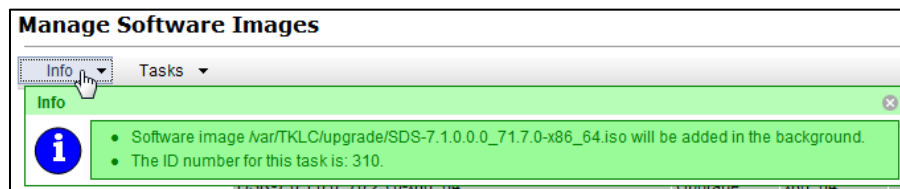
Description: SDS 71.7.0

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.

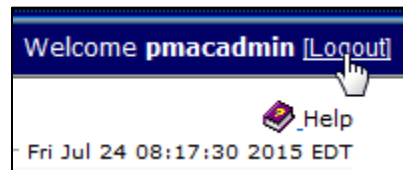
Manage Software Images						
Tasks						
ID	Task	Target	Status	State	Start Time	
310	Add Image		Done: SDS-7.1.0.0.0_71.7.0-x86_64	COMPLETE	2015-07-24 07:54:0	
255	Add Image		Done: DSR-7.1.0.0.0_71.20.0-x86_64	COMPLETE	2015-07-24 11:42:3	
254	Add Image		Done: TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64	COMPLETE	2015-07-24 11:41:5	

The new software displays in the list when complete.

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_62.36.0-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

10. **PMAC Server:**
Log out

Click **Logout**.



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.

Procedure 22. Recover from a Failed Upgrade

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.

Connected using VIP to sds-rlghnc-b (ACTIVE NETWORK OAM&P)

Main Menu: Administration -> Software Manag

Filter Tasks

DP_freeport_DP_02_grp NO_mrsnc_grp SO_florence_grp

Hostname	Upgrade State	Server Status	OAM Max HA Role	Appl Max HA Role	Netw
qs-mrsvnc	Accept or Reject	Warn	Observer		Quer
sds-mrsvnc-a	Failed	Err	N/A	Standby	Netw
sds-mrsvnc-b	Accept or Reject	Warn	Active	N/A	Netw



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**.

Connected using VIP to sds-rlghnc-b (ACTIVE NETWORK OAM&P)

Main Menu

- Administration
- Configuration
- Alarms & Events
- Security Log
- Status & Manage
 - Network Elements
 - Server
 - HA
 - Database
 - KPIs
 - Processes
 - Tasks
 - Active Tasks
 - Scheduled Tasks
 - Files
 - Measurements

Main Menu: Status & Manage -> Tasks ->

Filter

sds-rlghnc-a sds-rlghnc-b qs-rlghnc sds-mrsvnc

ID	Name	Status
347	APDE Remote Server Copy	completed
346	sds-mrsvnc-a Server Upgrade (in NO_mrsvnc_grp Server Group Upgrade)	exception
345	RLGHNC PROV Export	completed
344	RLGHNC OAM.SYSTEM Export	completed
	sds-mrsvnc-b Server Upgrade (in	

2. From the **Filter** option, enter the following filter values:

Network Element: **All**

Display Filter: **Name Like *upgrade***

3. Click **Go**.

Main Menu: Status & Manage -> Tasks -> Active Tasks

Filter

Filter

Network Element: - All -

Display Filter: Name

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**.

Main Menu: Status & Manage -> Tasks -> Active Tasks

Filter ▼

ID	Name	Status	Start Time
346	sds-mrsvnc-a Server Upgrade (in NO_mrsvnc_grp Server Group Upgrade)	exception	2015-08-26 15:02:04
343	sds-mrsvnc-b Server Upgrade (in NO_mrsvnc_grp Server Group Upgrade)	completed	2015-08-26 14:46:03
342	qs-mrsvnc Server Upgrade (in NO_mrsvnc_grp Server Group Upgrade)	completed	2015-08-26 14:46:03
341	NO_mrsvnc_grp Server Group Upgrade	paused	2015-08-26 14:45:58
337	qs-rlghnc Server Upgrade	completed	2015-08-26 13:55:58
336	sds-rlghnc-a Server Upgrade	completed	2015-08-26 13:54:46
309	sds-rlghnc-a Server Upgrade	completed	2015-08-25 14:04:30

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**

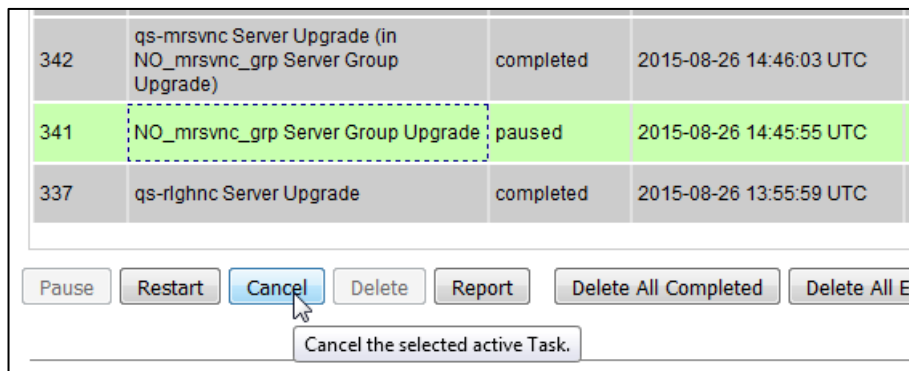
Before clicking **Cancel** for the server group upgrade task, ensure the upgrade status of the individual servers in that particular server group should have status as completed or exception (that is, failed for some reason).

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.

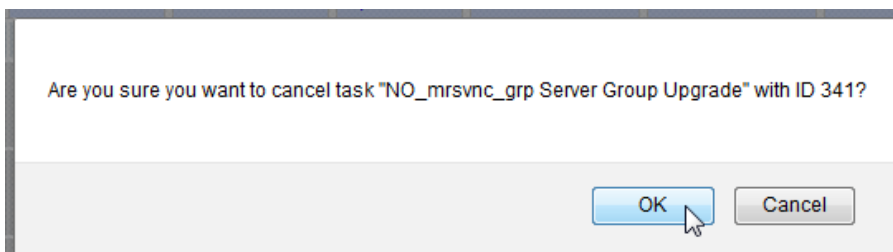


342	qs-mrsvnc Server Upgrade (in NO_mrsvnc_grp Server Group Upgrade)	completed	2015-08-26 14:46:03 UTC
341	NO_mrsvnc_grp Server Group Upgrade	paused	2015-08-26 14:45:55 UTC
337	qs-rghnc Server Upgrade	completed	2015-08-26 13:55:59 UTC

Buttons: Pause, Restart, Cancel, Delete, Report, Delete All Completed, Delete All E

Cancel the selected active Task.

3. Click **OK** on the confirmation screen to confirm the cancellation.

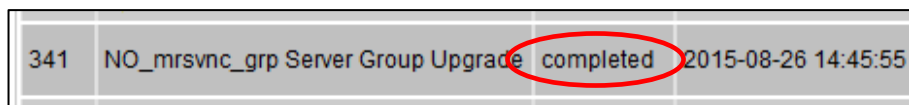


Are you sure you want to cancel task "NO_mrsvnc_grp Server Group Upgrade" with ID 341?

Buttons: OK, Cancel

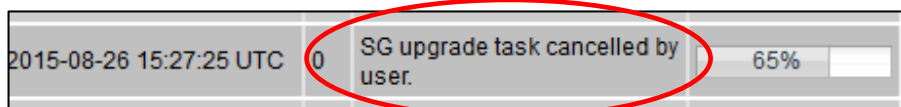
6. **Primary SDS NOAM VIP:**
Verify the Server Group Upgrade task is cancelled

1. On the Active Tasks screen, verify the Status changed from **paused** to **completed**.



341	NO_mrsvnc_grp Server Group Upgrade	completed	2015-08-26 14:45:55
-----	------------------------------------	-----------	---------------------

2. Verify the Result Details column now states "SG upgrade task cancelled by user."



2015-08-26 15:27:25 UTC	0	SG upgrade task cancelled by user.	65%
-------------------------	---	------------------------------------	-----

Procedure 22. Recover from a Failed Upgrade

7. <input type="checkbox"/>	Failed Server (CLI): Access the failed server	<p>Use the XMI address to log into the failed server with the admusr account.</p> <pre>CentOS release 5.7 (Final) Kernel 2.6.18-274.7.1.el5prere15.0.0_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</pre>
8. <input type="checkbox"/>	Failed Server (CLI): Inspect the upgrade.log file	<p>Identify the reason for the failure in the upgrade.log file.</p> <pre>[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::</pre>

Procedure 22. Recover from a Failed Upgrade

9. <input type="checkbox"/>	Failed Server (CLI): Inspect the earlyChecks.log file	<p>Identify the reason for the failure in the earlyChecks.log file.</p> <pre>[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!</pre>
<div data-bbox="191 865 308 982"></div> <div data-bbox="337 890 578 940">CAUTION</div>		<ul style="list-style-type: none"> 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 O. DO NOT PROCEED THE NEXT STEP UNTIL THE ALARM CONDITION HAS BEEN CLEARED!
10. <input type="checkbox"/>	Failed Server (CLI): Verify platform alarms are cleared from the failed server	<p>Use the alarmMgr utility to verify all platform alarms have been cleared from the system.</p> <pre>[admusr@sds-mrsvnc-b ~]\$ alarmMgr -alarmStatus</pre>
11. <input type="checkbox"/>	Failed Server (CLI): Exit CLI	<p>Exit the CLI for the failed server.</p> <pre>[admusr@sds-mrsvnc-a ~]\$ exit logout</pre>
12. <input type="checkbox"/>	Primary SDS NOAM VIP (GUI): Execute the server upgrade again.	<p>Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option.</p> <p>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.</p>

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.

J.1 Add SDS Software Images to PMAC Server

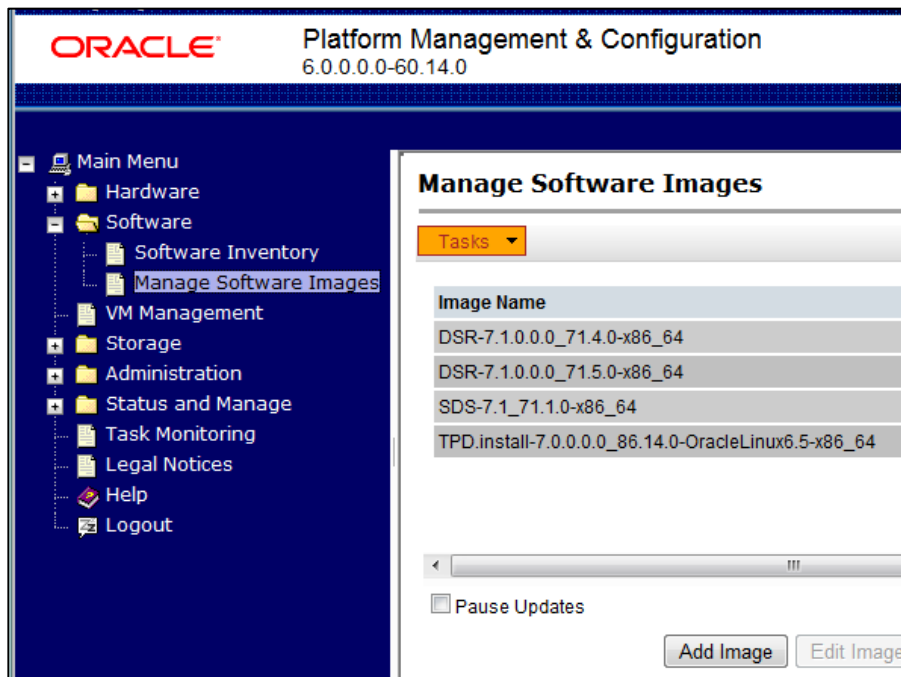
Procedure 23. Add SDS Software Images to PMAC Server		
1. <input type="checkbox"/>	Active SDS VIP (CLI): Login	From the command prompt, log into the server as the admusr . login: admusr Using keyboard-interactive authentication. Password: <admusr_password>
2. <input type="checkbox"/>	Active SDS VIP (CLI): Change directories	cd to the /var/TKLC/upgrade/ directory. \$ cd /var/TKLC/upgrade/
3. <input type="checkbox"/>	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. <input type="checkbox"/>	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. <input type="checkbox"/>	PMAC Server (GUI): Log into the Platform Management and Configuration application	<p>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.</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p> 
6. <input type="checkbox"/>	PMAC Server: Login	<p>Login using the default user and password.</p> 

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**.

Add Software Image

Images may be added from any of these sources:

- Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
- USB media attached to the PM&C's host (Refer to Note)
- External mounts. Prefix the directory with "extfile://".
- These local search paths:
 - /var/TKLC/upgrade/*.iso
 - /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso

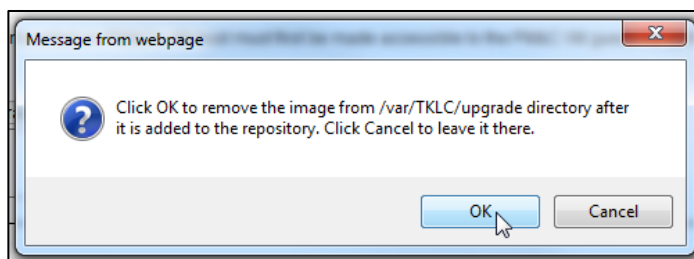
Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the P
[VM Management](#).

Path: /var/TKLC/upgrade/SDS-7.1.0.0.0_71.9.0-x86_64.iso

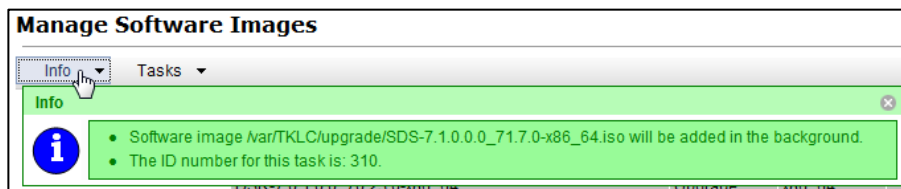
Description:

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.

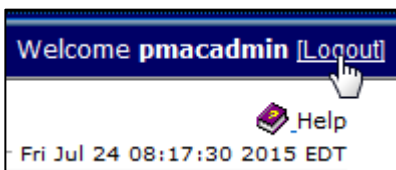
ID	Task	Target	Status	Running Time	Start Time	Progress
773	Add Image		Extracting/Verifying image source.	0:00:00	2011-12-05 16:32:50	11%
762	Add Image		Done: 872-2329-103-3.0.0_30.14.0-DSR-x86_64	0:00:05	2011-12-05 09:38:36	100%
739	Add Image		Done: 872-2329-101-3.0.0_30.12.1-DSR-x86_64	0:00:06	2011-11-30 16:51:57	100%
729	Add Image		Done: 872-2329-102-3.0.0_30.13.0-DSR-x86_64	0:00:06	2011-11-25 07:51:00	100%

The new software image displays in the list when complete.

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_64	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

10. **PMAC Server:**
Log out

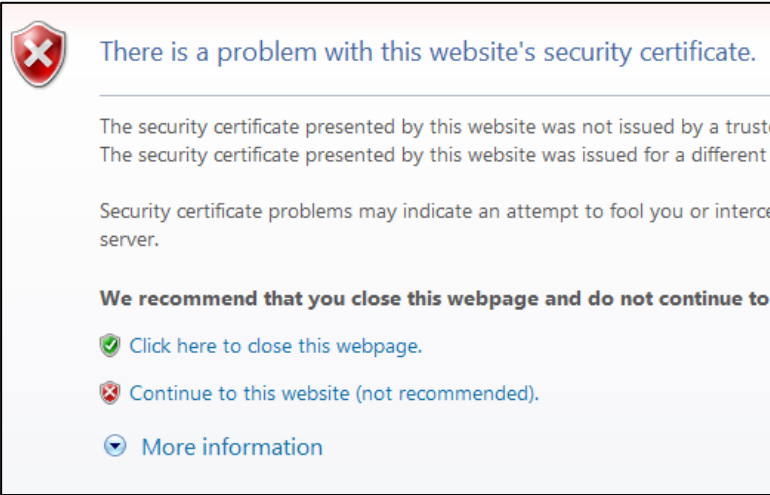

Click **Logout**.



11. **SDS Health Check**

Execute SDS Health Check procedures as specified in Appendix B.

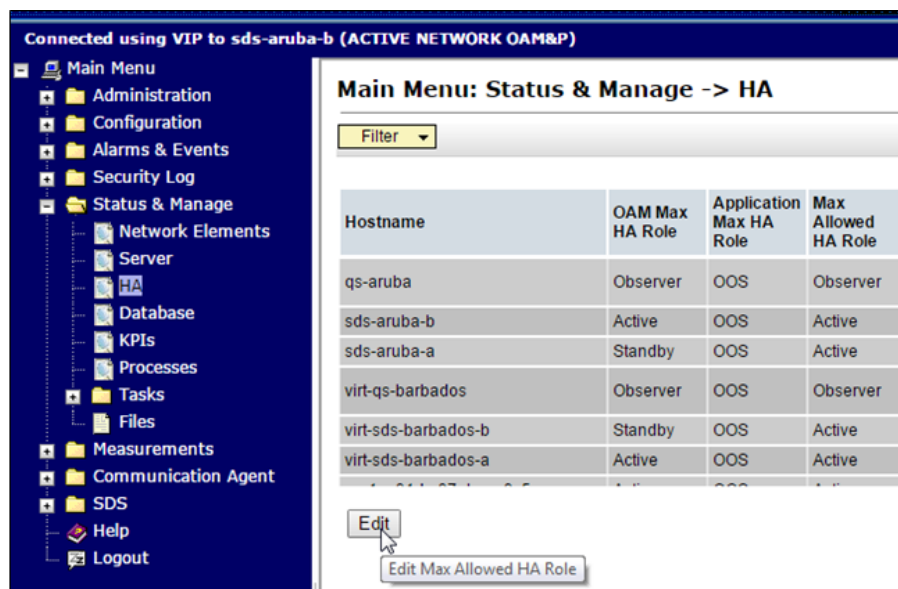
J.2 Remove the SDS SOAM VM from the SOAM Server Group

Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group		
1. <input type="checkbox"/>	Primary NOAM VIP: Log into the NOAM VIP address	<p>Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the NOAM VIP address.</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p> 
2. <input type="checkbox"/>	Primary NOAM VIP: Login	<p>Login using the default user and password.</p> 

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

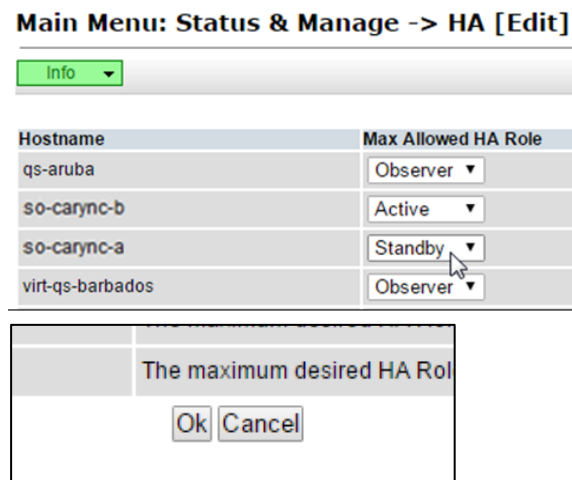
3. ☐ **Primary SDS NOAM VIP:** Edit an HA role

1. Navigate to **Status & Manage > HA**.
2. Click **Edit**.



4. ☐ **Primary SDS NOAM VIP:** Change the SOAM server HA role to Standby

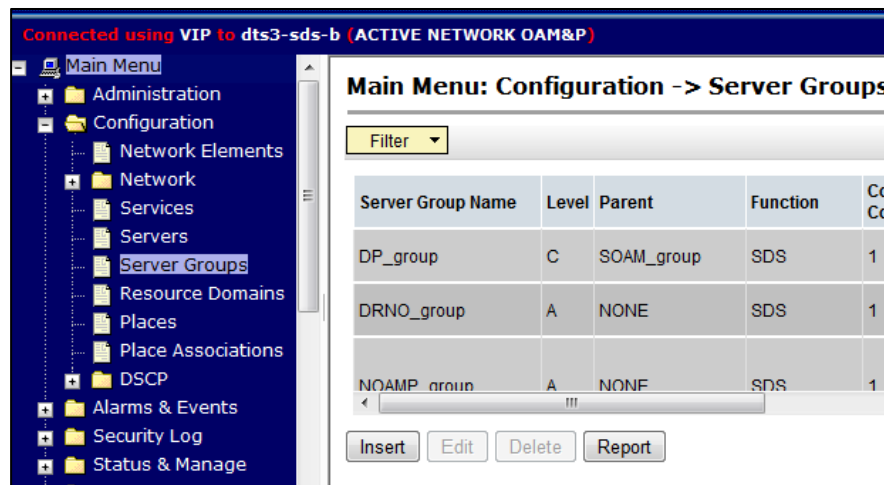
1. Select the active primary SDS SOAM server and change the **Max Allowed HA Role** to **Standby**.
2. Click **OK**.



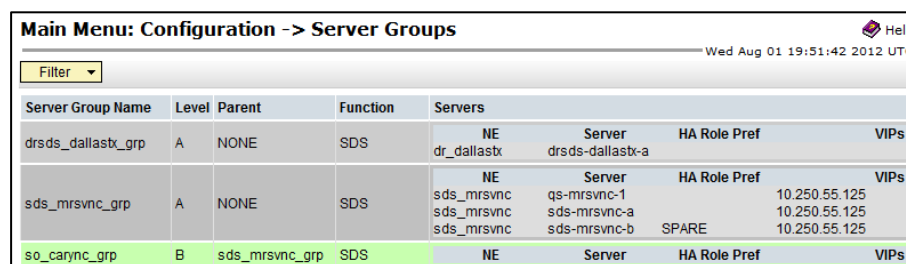
Procedure 24. Remove the SDS SOAM VM from the SOAM Server Group

5. **Primary NOAM VIP:** Edit the SOAM server

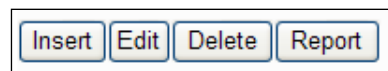
1. Navigate to **Configuration > Server Groups**.



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.

Main Menu: Configuration -> Server Groups [Edit] Wed Aug 01 19:55:49 2012

Field	Value	Description
Server Group Name	so_carync_grp *	Unique identifier used to label a Server Group. [Default = n/a. Range = A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]
Level	B *	Select one of the Levels supported by the system
Parent	sds_mrsync_grp *	Select an existing Server Group or NONE
Function	SDS *	Select one of the Functions supported by the system
NTP Server 1		The IP Address of a reachable NTP server to be used for clock synchronization. Configurable for level A only. [Range = A valid IP address or blank]
NTP Server 2		The IP Address of a backup NTP server (optional). Configurable for level A only. [Range = A valid IP address or blank]
so_carync		
Server	SG Inclusion	Preferred HA Role
so-carync-a	<input type="checkbox"/> Include in SG	<input type="checkbox"/> Preferred Spare
so-carync-b	<input type="checkbox"/> Include in SG	<input type="checkbox"/> Preferred Spare
VIP Assignment		
VIP Address		Add
Ok Apply Cancel		

2. When the **Pre-Validation passed** message displays, click **Apply**.

Main Menu: Configuration -> Server Groups [Edit]

Info

Info

• Pre-Validation passed - Data NOT committed ...

Network Element

so_carync

Select the Network Element

7. **Primary NOAM VIP:** Log out

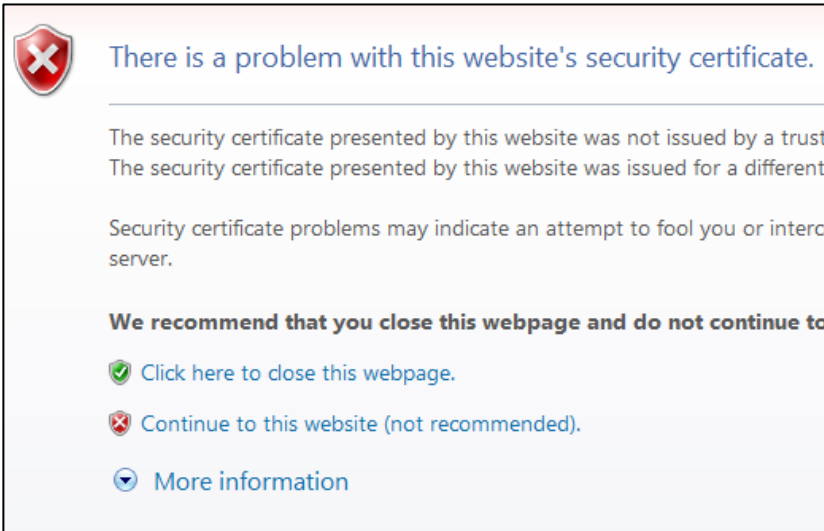
Click **Logout** to log out of the SDS GUI.

Welcome **guiadmin** [Logout]

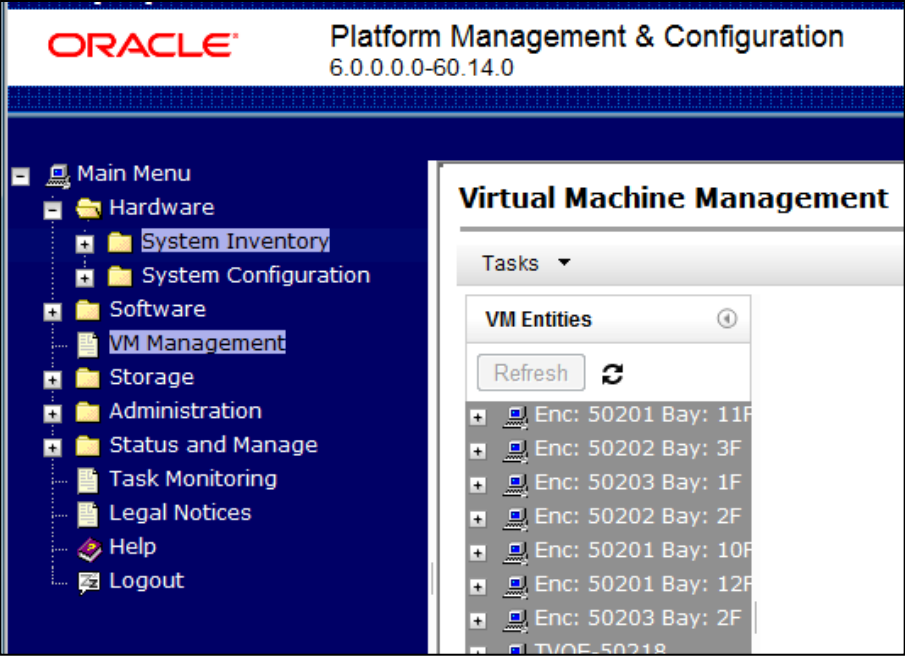
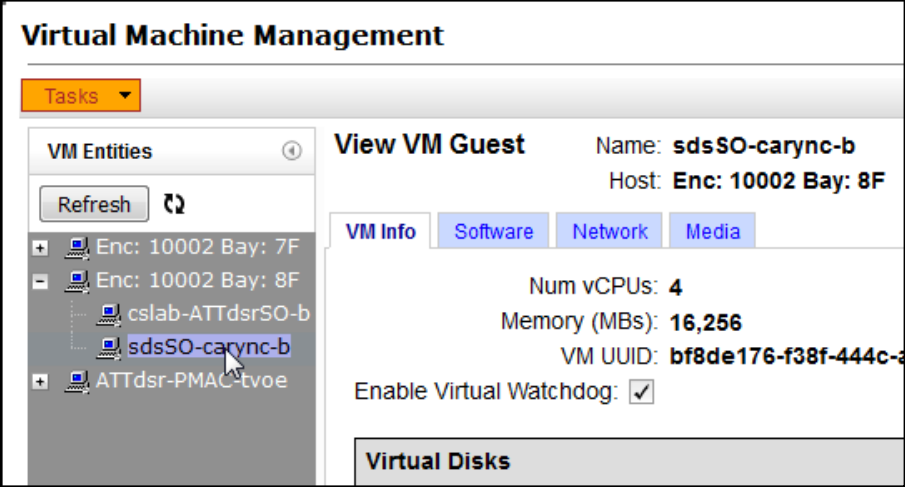
Help

Fri Nov 18 14:43:32 2011 UTC

J.3 Delete Existing SOAM VM and Recreate SDS SOAM VM with New Profile

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile		
1. <input type="checkbox"/>	PMAC Server (GUI): Log into the Platform Management and Configuration application	<p>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.</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p> 
2. <input type="checkbox"/>	PMAC Server: Login	<p>Login using the default user and password.</p> 

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

<p>3.</p> <p><input type="checkbox"/></p>	<p>PMAC Server GUI: Access VM Management screen</p>	<p>Navigate to VM Management.</p> 
<p>4.</p> <p><input type="checkbox"/></p>	<p>PMAC Server GUI: Select the 1B subscriber profile</p>	<ol style="list-style-type: none"> 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. 



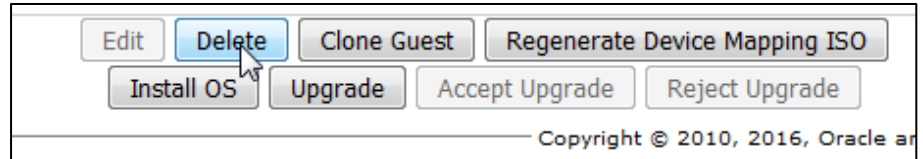
CAUTION

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.

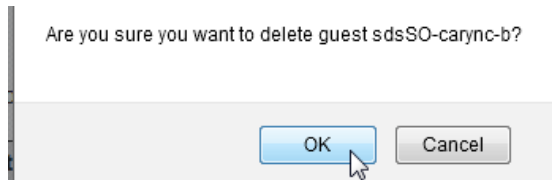
Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

5. **PMAC Server**
☐ **GUI:** Delete the VM

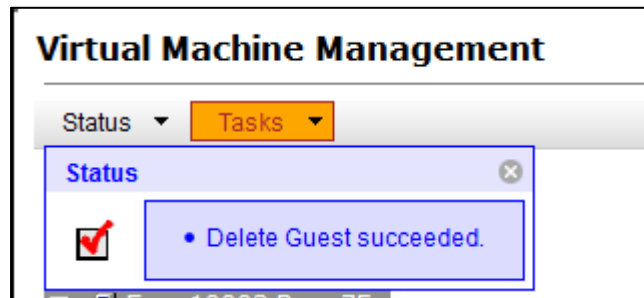
1. Click **Delete**.



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**.

Virtual Machine Management Tue Dec 23

Tasks ▾

VM Entities ⌵

Refresh ↻

- Enc: 50201 Bay: 11F
- Enc: 50202 Bay: 3F
- Enc: 50203 Bay: 1F
- Enc: 50202 Bay: 2F
- Enc: 50201 Bay: 10F
- Enc: 50201 Bay: 12F
- Enc: 50203 Bay: 2F
- TVOE-50218
- Enc: 50202 Bay: 8F
- Enc: 50201 Bay: 9F

Pause Updates ☐

View VM Host Name: **hostnameb22b**
Enc/Bay: **50201/11F**

VM Info Software Network Media

Guests

Name	Status
DTS3_SOAM_A	Running

Bridges

Device
control
imi
xmi

Storage Pools

Name	Capacity MB	Allocation MB	Ava
vgguests	266304	112640	

Create Guest

3. Click **Import Profile**.

Virtual Machine Management

Info ▾

VM Entities ⌵

- Enc: 50101 Bay: 11F
 - DSR_NOAMP_A
- Enc: 50101 Bay: 12F
 - DSR_NOAMP_B

Create VM Guest

Name:

Host: **Enc: 50101 Bay: 12F** ▾

VM Info

Num vCPUs: ⬆ ⬇ ⬆ VM UUID:

Memory (MBs): ⬆ ⬇ ⬆

Virtual Disks

Prim	Size (MB)	Host Pool	Host Vol Name
<input checked="" type="checkbox"/>	12288	vgguests	

Virtual NICs Add Delete

Host Bridge	Guest Dev Name
control	control

Create **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 7.3	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.**

Import Profile

ISO/Profile: SDS--3.0.0 10.4.0--872-2358-102--x86 64 => DP SOAM A

Num CPUs:4 Memory (MBs):16384

Virtual Disks:	Prim	Size (MB)	Pool	TPD Dev
	<input checked="" type="checkbox"/>	153600	vgguests	

NICs:	Bridge	TPD Dev
	control	control
	imi	imi
	xmi	xmi

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**.

Virtual Machine Management Help
Mon Dec 05 18:34:24 2011 UTC

VM Entities

- Enc: 50101 Bay: 11F
 - DSR_NOAMP_A
 - Enc: 50101 Bay: 12F
 - DSR_NOAMP_B

Create VM Guest

Name: Host:

VM Info

Num vCPUs: VM UUID:

Memory (MBs):

Virtual Disks

Prim	Size (MB)	Host Pool	Host Vol Name	Guest Dev Name
<input checked="" type="checkbox"/>	153600	vpguests	DP_SOAM_A.img	

Virtual NICs

Host Bridge	Guest Dev Name
control	control
imi	imi
xmi	xmi

Note: If the VM guest creation fails due to a **Host resources are oversubscribed** error, contact My Oracle Support (MOS) as described in Appendix O.

3. Verify the task successfully completes by watching the **Progress** value change to 100%.

Virtual Disks

Prim	Size (MB)	Host Pool	Host Vol Name	Guest Dev Name
<input checked="" type="checkbox"/>	153600	vpguests	DP_SOAM_A.img	PRIMARY

Virtual NICs

Host Bridge	Guest Dev Name	MAC Addr
control	control	52:54:00:15:eb:6c
xmi	xmi	52:54:00:d9:ba:7f

ID	Task	Target	Status	Running Time	Start Time	Progress
767	VirtAction: Create	Enc: 50101 Bay: 11F Guest: DP_SOAM_A	Guest creation completed (DP_SOAM_A)	0:00:04	2011-12-05 13:36:58	100%

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

9. **PMAC Server GUI:** Install the operating system

Click **Install OS**.

Host Bridge	Guest Dev Name	MAC Addr
control	control	52:54:00:15:eb:6c
xmi	xmi	52:54:00:d9:ba:7f

Buttons: Edit, Delete, Install OS, Upgrade, Clone Guest

Tabs: Target, Status, Running Time, Start Time

10. **PMAC Server GUI:** Start the installation of the TPD image

1. Select the TPD image and click **Start Install**.

Image Name	Type	Architecture	Description
TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	official TPD 5.0.0-72.28.0 F
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
TVOE--1.0.0_72.30.0--872-2290-101--x86_64	Bootable	x86_64	latest TVOE ISO

Start Install

2. Click **OK** to confirm.

Windows Internet Explorer

Are you sure you want to install TPD--5.0.0_72.28.0--x86_64 on the listed entities?

Buttons: OK, Cancel

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%.

Main Menu

- Hardware
- System Inventory
- System Configuration
- Software
- VM Management
- Storage
- Administration
- Status and Manage
- Task Monitoring**
- Legal Notices
- Help

Background Task Monitoring

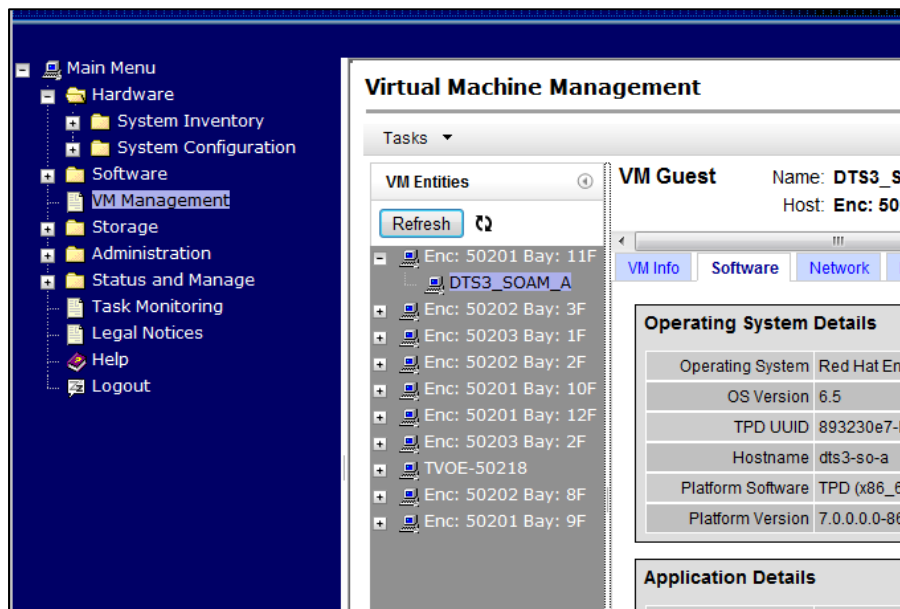
Filter

ID	Task	Target
7239	Upgrade	Enc:50202 Ba
7238	Upgrade	Enc:50202 Ba Guest: DSR S
7237	Upgrade	Enc:50202 Ba Guest: DSR N

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

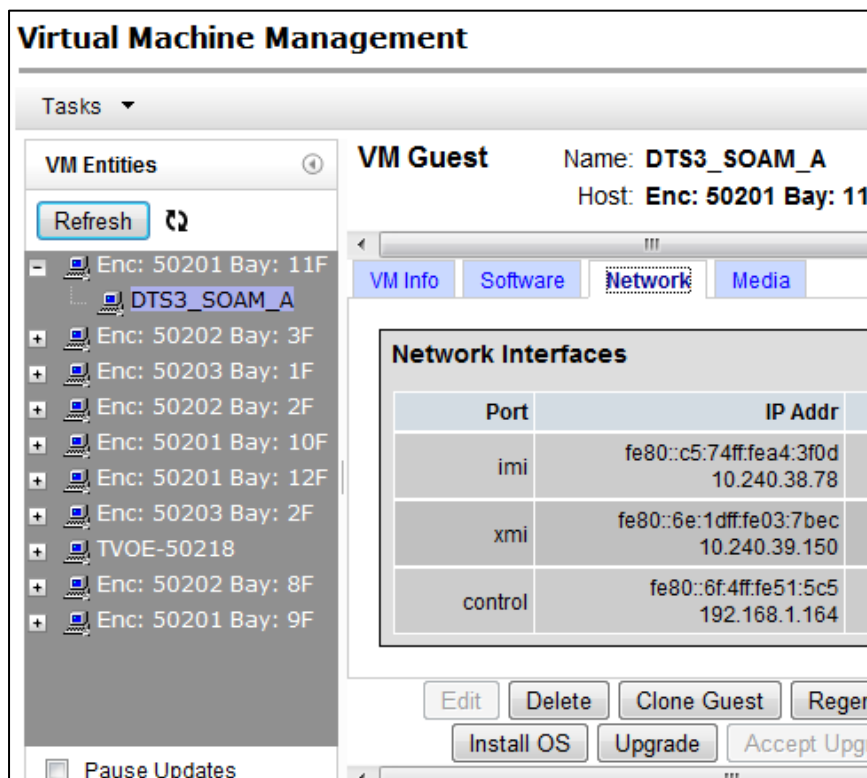
11. **PMAC Server GUI:** Verify installation

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. Select the SDS version from the **Image Name** column and click **Start Software Upgrade**.

Select Image

Image Name	Type	Architecture
DSR-7.1.0.0.0_71.4.0-x86_64	Upgrade	x86_64
DSR-7.1.0.0.0_71.5.0-x86_64	Upgrade	x86_64
SDS-7.1_71.1.0-x86_64	Upgrade	x86_64
TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64	Bootable	x86_64

Start Software Upgrade

2. Click **OK** to confirm.

Message from webpage

Are you sure you want to upgrade to SDS-7.1_71.1.0-x86_64 on the listed entities?

OK Cancel

3. Navigate to **Task Monitoring** to monitor the upgrade.

Background Task Monitoring

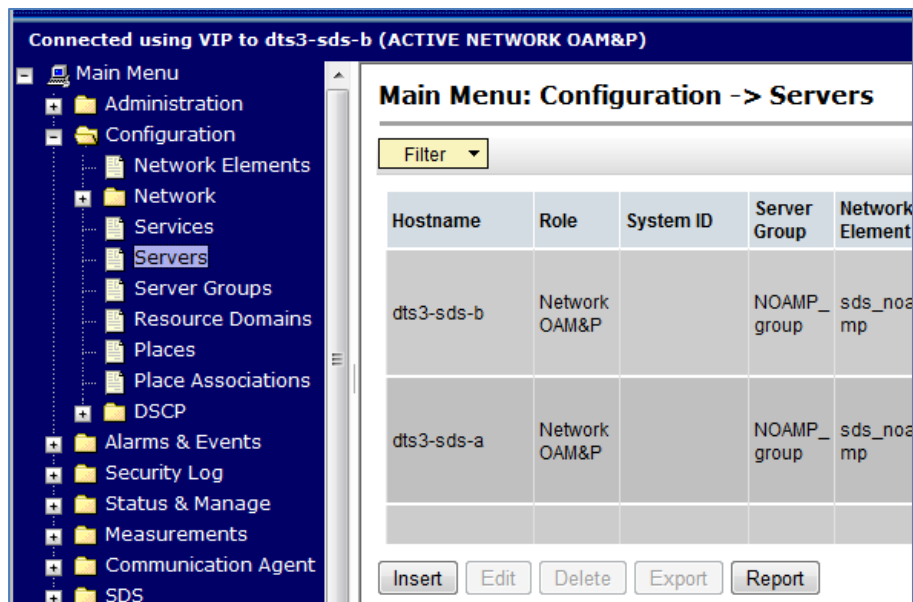
Filter

ID	Task	Target
7239	Upgrade	Enc:50202 Ba
7238	Upgrade	Enc:50202 Ba Guest: DSR S
7237	Upgrade	Enc:50202 Ba Guest: DSR M
7236	Add Image	

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.

Hostname	Role	Server Group	Network Element	Location	Details
sds-mrsync-a	Network OAM&P	sds_mrsync_grp	sds_mrsync	Morrisville_NC	XMI: 10.250.55.124 IMI: 169.254.100.11
sds-mrsync-b	Network OAM&P	sds_mrsync_grp	sds_mrsync	Morrisville_NC	XMI: 10.250.55.128 IMI: 169.254.100.12
qs-mrsync-1	Query Server	sds_mrsync_grp	sds_mrsync	Morrisville_NC	XMI: 10.250.55.127 IMI: 169.254.100.13
drds-dallastx-a	Network OAM&P	drds_dallastx_grp	dr_dallastx	Dallas_TX	XMI: 10.250.55.161 IMI: 169.254.100.14
so-carync-a	System OAM		so_carync	Cary_NC	XMI: 10.240.39.150 IMI: 10.240.38.78

3. Click **Export**.

so-carync-a	System OAM	so_carync	Cary_NC	XMI: 10.240.39.150 IMI: 10.240.38.78
-------------	------------	-----------	---------	---

Insert Delete Export Report ☐ Pause updates

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. <input type="checkbox"/>	SDS VIP CLI: Directory list	Get a directory listing and find the configuration file containing the SOAM server name \$ ls -ltr TKLCCConfigData*.sh *** TRUNCATED OUTPUT *** -rw-rw-rw- 1 root root 2208 Dec 19 16:50 TKLCCConfigData.so-carync-b.sh
19. <input type="checkbox"/>	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> TKLCCConfigData.so-carync-b.sh 100% 1741 1.7KB/s 00:00
20. <input type="checkbox"/>	SDS VIP CLI: Log out of the active NOAM CLI	\$ exit
21. <input type="checkbox"/>	PMAC Server CLI: Login	Use SSH to log into the PMAC guest VM server as the admusr user. login: admusr Password: <admusr_password>
22. <input type="checkbox"/>	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: TKLCCConfigData.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. <input type="checkbox"/>	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. <input type="checkbox"/>	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: TKLCCConfigData.<server_hostname>.sh translates to TKLCCConfigData.sh \$ cp -p /tmp/TKLCCConfigData.so-carync-b.sh /var/tmp/TKLCCConfigData.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. <input type="checkbox"/>	SOAM Guest VM: Monitor for broadcast message sent to the terminal	<p>Note: The time to complete this step varies by server and may take from 3-5 minutes to complete.</p> <p>*** NO OUTPUT FOR ≈ 3-5 MINUTES ***</p> <p>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></p>
26. <input type="checkbox"/>	SOAM Guest VM: Accept upgrade to the application software	<pre>\$ 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</pre>
27. <input type="checkbox"/>	SOAM Guest VM: Verify the desired time zone is currently in use	<pre>\$ date Mon Aug 10 19:34:51 UTC 2015 Configure the time zone (optional) \$ sudo set_ini_tz.pl <time_zone></pre> <p>Note: The following command example sets the time to the UTC (aka GMT) time zone, which is recommended for all sites.</p> <p>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.</p> <pre>\$ sudo set_ini_tz.pl "Etc/UTC"</pre>

Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile		
28. <input type="checkbox"/>	SOAM Guest VM: Reboot the SOAM server	<p>Reboot the SOAM server.</p> <pre>\$ sudo init 6</pre> <p>Sample output:</p> <pre>Connection to xxx.xxx.xxx.xxx closed by remote host. Connection to xxx.xxx.xxx.xxx closed.</pre>
29. <input type="checkbox"/>	PMAC Guest VM: Reboot the SOAM server console	<p>Reboot and reconnect to the SOAM server console from the PMAC server console.</p> <pre>\$ ssh <SDS_SOAM_VM_Control_IP> admusr@xxx.xxx.xxx.xxx's password: <admusr_password></pre>
30. <input type="checkbox"/>	SOAM Guest VM: Verify address	<p>Verify IMI and XMI addresses have been applied.</p> <pre>\$ 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</pre>
31. <input type="checkbox"/>	SOAM Guest VM: Check health of server	<p>Syscheck the current health of the server.</p> <pre>\$ 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</pre>

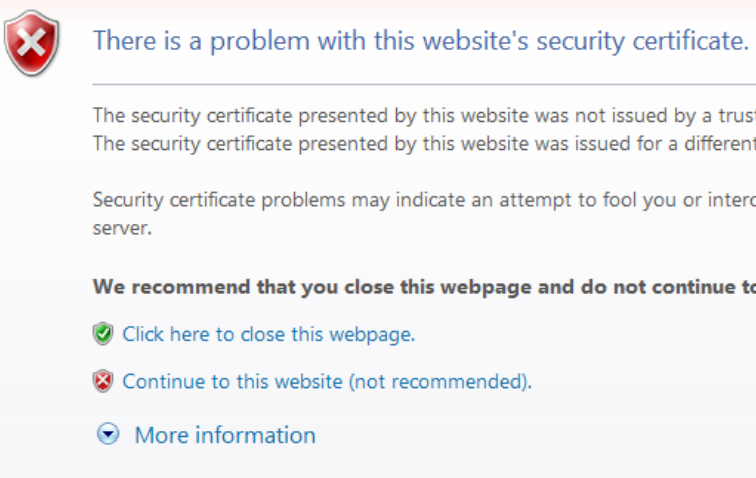



Procedure 25. Recreate the SDS SOAM VM with the 1B Subscriber Profile

32. <input type="checkbox"/>	SOAM Guest VM: PING the XMI IP address	<p>From the SOAM Guest, ping the IMI IP address of the mate SOAM VM Guest.</p> <pre>\$ 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</pre>
33. <input type="checkbox"/>	SOAM Guest VM: PING the XMI IP address	<p>From the SOAM Guest, ping the XMI IP address of the mate SOAM VM Guest.</p> <pre>\$ 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</pre>
34. <input type="checkbox"/>	SOAM Guest VM: PING the gateway	<p>From the SOAM Guest, ping the local XMI gateway address associated with the SOAM NE.</p> <pre>\$ 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</pre>

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

35. <input type="checkbox"/>	SOAM Guest VM: Verify server connectivity	<p>Use the ntpq command to verify the server has connectivity to at least one of the assigned NTP server(s).</p> <p>Note: NTP connectivity is denoted by the presence of an asterisk (*) to the left of one of the remote IP addresses.</p> <pre>\$ 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</pre>
		<p>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.</p>
36. <input type="checkbox"/>	SOAM Guest VM: Exit from the SOAM	<p>Exit from the SOAM command line to return the PMAC server console prompt.</p> <pre>\$ exit</pre>
37. <input type="checkbox"/>	PMAC Guest VM: Exit from the PMAC server	<pre>\$ exit</pre>

J.4 Add the New SOAM VM to the SOAM Server Group**Procedure 26. Place the SDS SOAM VM into the SOAM Server Group**

1. <input type="checkbox"/>	SDS NOAM VIP: Log into the NOAM VIP address	<p>Open an approved Web browser (Internet Explorer 8.0, 9.0, or 10.0) and connect to the SDS NOAM VIP address.</p> <p>If a certificate error is received, click on the Continue to this website (not recommended) link.</p> <div data-bbox="496 1182 1265 1667">  <p>The security certificate presented by this website was not issued by a trust... The security certificate presented by this website was issued for a different...</p> <p>Security certificate problems may indicate an attempt to fool you or interce... server.</p> <p>We recommend that you close this webpage and do not continue to</p> <p> Click here to close this webpage.</p> <p> Continue to this website (not recommended).</p> <p> More information</p> </div>
--------------------------------	--	--

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

<p>2.</p> <p><input type="checkbox"/></p>	<p>SDS NOAM VIP:</p> <p>Login</p>	<p>Login using the default user and password.</p> <div data-bbox="495 289 1263 877">  </div>
---	--	--

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

3. **SDS NOAM VIP:**
☐ Edit the SOAM server

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

Connected using VIP to dts3-sds-b (ACTIVE NETWORK OAM&P)

Main Menu: Configuration -> Server Groups

Filter

Server Group Name	Level	Parent	Function	Con Cou
DP_group	C	SOAM_group	SDS	1
DRNO_group	A	NONE	SDS	1
NOAMP_group	A	NONE	SDS	1

Insert Edit Delete Report

2. Select the SOAM server that was converted to the 1B Subscriber profile.

Main Menu: Configuration -> Server Groups Wed Aug 01 19:51:42 2012 UTC

Filter

Server Group Name	Level	Parent	Function	Servers	NE	Server	HA Role Pref	VIPs
drds_dallastx_grp	A	NONE	SDS	dr_dallastx	drds_dallastx-a			
sds_mrsvnc_grp	A	NONE	SDS	sds_mrsvnc	qs-mrsvnc-1		10.250.55.125	
				sds_mrsvnc	sds-mrsvnc-a		10.250.55.125	
				sds_mrsvnc	sds-mrsvnc-b	SPARE	10.250.55.125	
so_canync_grp	B	sds_mrsvnc_grp	SDS	NE	Server	HA Role Pref	VIPs	

3. Click **Edit**.

Insert Edit Delete Report

Note: You may need to scroll to see the **Edit** button.

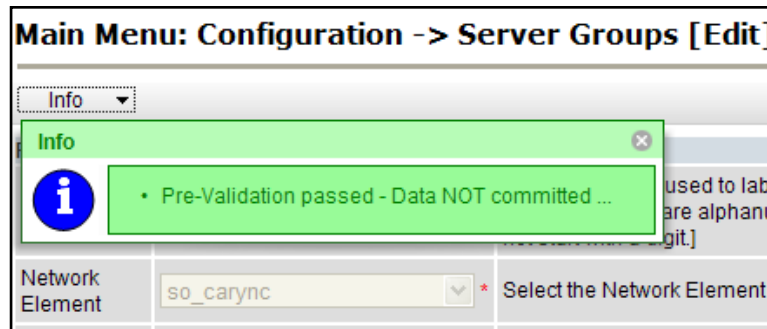
Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

4. **SDS NOAM VIP:**
☐ Ready server for pre-validation

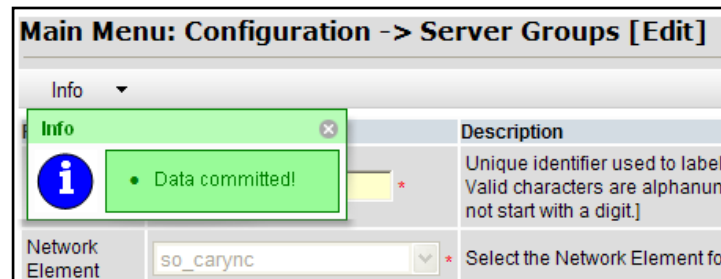
1. Mark the **SG Inclusion** checkbox for the server.

so_carync		
Server	SG Inclusion	Preferred HA Role
so-carync-a	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Preferred Spare
so-carync-b	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Preferred Spare

2. When the **Pre-Validation passed** message displays, click **Apply**.



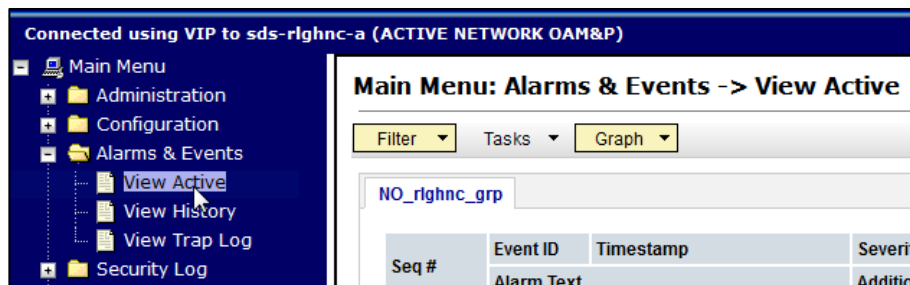
The Info banner changes to **Data committed**.



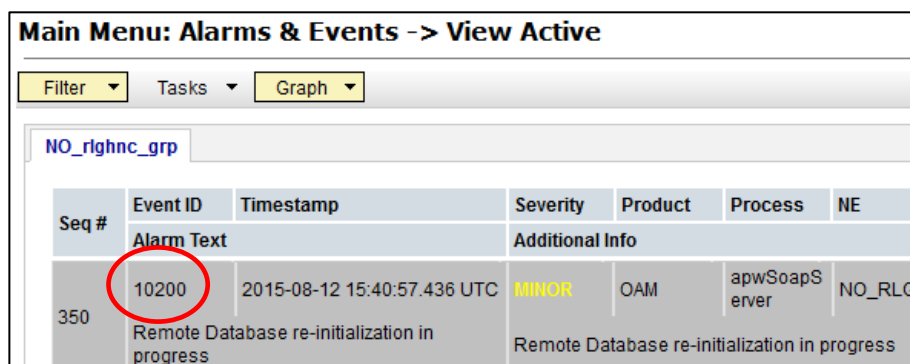
Procedure 26. Place the SDS SOAM VM into the SOAM Server Group

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**.

Connected using VIP to dts3-sds-a (ACTIVE NETWORK OAM&P)

- Main Menu
- Administration
- Configuration
- Alarms & Events
- Security Log
- Status & Manage
 - Network Elements
 - Server**
 - HA
 - Database
 - KPIs
 - Processes
 - Tasks
 - Files

Main Menu: Status & Manage -> Server

Filter ▼

Server Hostname	Network Element	Appl State
dts3-dp-1	sds_soam	Enabled
dts3-sds-a	sds_noamp	Enabled
dts3-sds-b	sds_noamp	Enabled
dts3-so-a	sds_soam	Enabled
dts3-so-b	sds_soam	Enabled

2. Verify Server Status is Normal (**Norm**) for Database (DB) and **Man** for Processes (Proc).

Main Menu: Status & Manage -> Server Help

Wed Aug 01 21:11:16 2012 UTC

Filter ▼

Network Element	Server Hostname	Appl State	Alm	DB	Reporting Status	Proc
dr_dallastx	drdsd-dallastx-a	Enabled	Norm	Norm	Norm	Norm
sds_mrsvnc	sds-mrsvnc-a	Enabled	Err	Norm	Norm	Norm
sds_mrsvnc	sds-mrsvnc-b	Enabled	Norm	Norm	Norm	Norm
sds_mrsvnc	qs-mrsvnc-1	Enabled	Norm	Norm	Norm	Norm
so_carync	so-carync-b	Disabled	Warn	Norm	Norm	Man
so_carync	so-carync-a	Enabled	Norm	Norm	Norm	Norm

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.

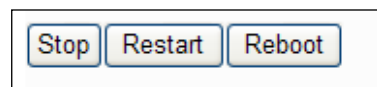
Main Menu: Status & Manage -> Server Help

Wed Aug 01 21:11:16 2012 UTC

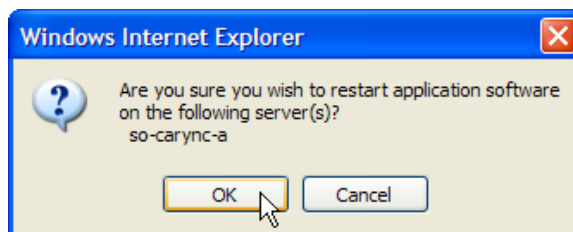
Filter

Network Element	Server Hostname	Appl State	Alm	DB	Reporting Status	Proc
dr_dallastx	drdsds-dallastx-a	Enabled	Norm	Norm	Norm	Norm
sds_mrsvnc	sds-mrsvnc-a	Enabled	Err	Norm	Norm	Norm
sds_mrsvnc	sds-mrsvnc-b	Enabled	Norm	Norm	Norm	Norm
sds_mrsvnc	qs-mrsvnc-1	Enabled	Norm	Norm	Norm	Norm
so_carync	so-carync-b	Disabled	Warn	Norm	Norm	Man
so_carync	so-carync-a	Enabled	Norm	Norm	Norm	Norm

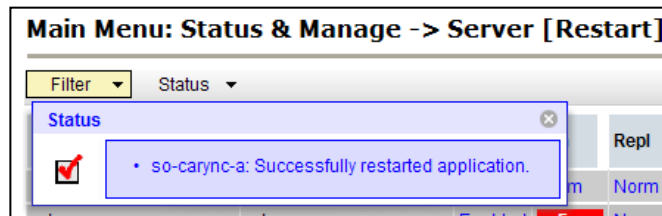
2. Click **Restart**.



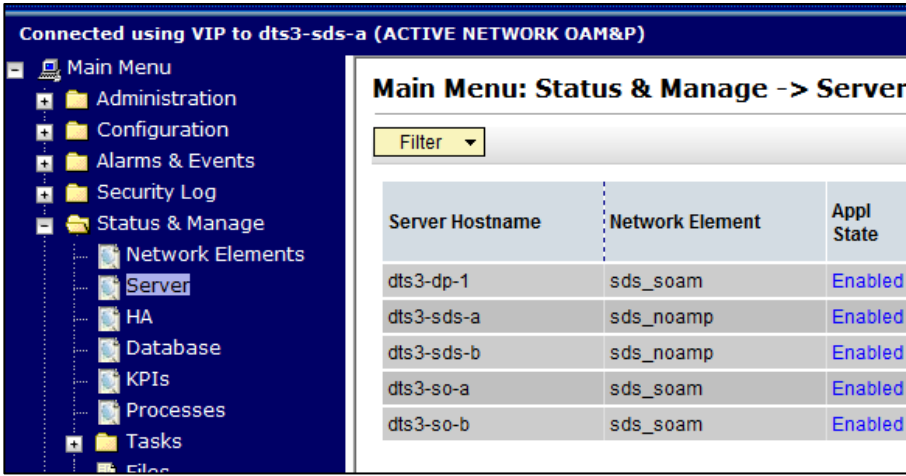
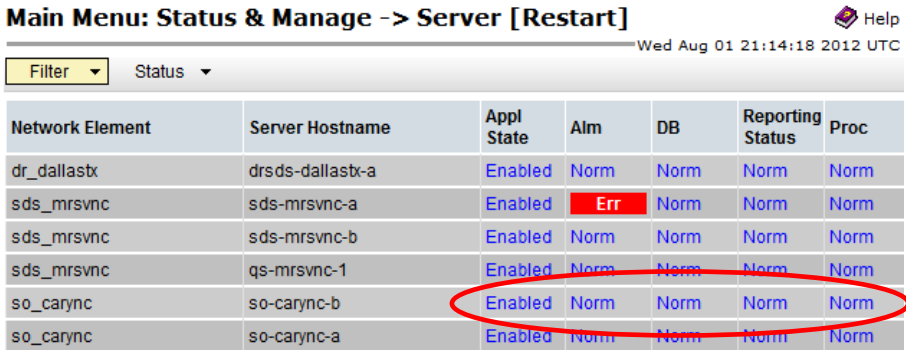

3. Click **OK** to confirm.



A **Successfully restarted application** message displays in the banner.



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

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

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**.

Connected using VIP to sds1-nob-1191036 (ACTIVE NETWORK OAM&P)

Main Menu: Status & Manage -> HA

Filter

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
sds1-noa-1191038	Standby	OOS	Active
sds1-nob-1191036	Active	OOS	Active
sds1-qs-1191034	Observer	OOS	Observer
SDS-SO1-BigRed1	Standby	OOS	Active
SDS-SO2-BigRed1	Active	OOS	Active
SDS-DP1-BigRed1	Active	OOS	Active
SDS-DP2-BigRed1	Standby	OOS	Standby
SDS-DP3-BigRed1	Active	OOS	Active

3. Click **Edit**.

Main Menu: Status & Manage -> HA

Filter

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
sds1-noa-1191038	Standby	OOS	Active
sds1-nob-1191036	Active	OOS	Active
sds1-qs-1191034	Observer	OOS	Observer
SDS-SO1-BigRed1	Standby	OOS	Active
SDS-SO2-BigRed1	Active	OOS	Active
SDS-DP1-BigRed1	Active	OOS	Active
SDS-DP2-BigRed1	Standby	OOS	Standby

Edit

4. Change the Max Allowed HA Role to **Active**.

5. Click **OK**.

Main Menu: Status & Manage -> HA [Edit]

Hostname	Max Allowed HA Role
sds1-noa-1191038	Active
sds1-nob-1191036	Active
sds1-qs-1191034	Observer
SDS-SO1-BigRed1	Active
SDS-SO2-BigRed1	Active
SDS-DP1-BigRed1	Active
SDS-DP2-BigRed1	Active

Ok Cancel

Procedure 27. Manual Completion of Server Upgrade

2. **Primary SDS NOAM VIP:**
Verify the Max Allowed HA Role changes to **Active**

Main Menu: Status & Manage -> HA

Filter	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
	sds1-noa-1191038	Standby	OOS	Active
	sds1-nob-1191036	Active	OOS	Active
	sds1-qs-1191034	Observer	OOS	Observer
	SDS-SO1-BigRed1	Standby	OOS	Active
	SDS-SO2-BigRed1	Active	OOS	Active
	SDS-DP1-BigRed1	Active	OOS	Active
	SDS-DP2-BigRed1	Active	OOS	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**.

Connected using VIP to sds1-nob-1191036 (ACTIVE NETWORK OAM&P)

Main Menu: Status & Manage -> Server

Server Hostname	Network Element	Appl State	Alm
BR2-DP1	BigRed_SOAMP	Enabled	Warn
BR2-SDS-SOA	BigRed_SOAMP	Enabled	Warn
BR2-SDS-SOB	BigRed_SOAMP	Enabled	Warn
SDS-DP1-BigRed1	SO_BigRed1	Enabled	Warn
SDS-DP2-BigRed1	SO_BigRed1	Disabled	Err

Buttons: Stop Restart Reboot NTP Sync Report

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**.

Main Menu: Administration -> Software Management -> Upgrade

Filter	Tasks	Primary_NO_grp	BR1_DP1	BR1_DP2	BR1_DP3	BR1_DP4	BR2_DP1_SG	BR2_SO_SG	BigRed1_SDS_SO	DR_NO_grp
		Hostname	Upgrade State	OAM Max HA Role	Application Version	Start Time	Finish Time			
		Server Status	Server Status	Appl Max HA Role	Upgrade ISO	Status Message				
		SDS-DP2-BigRed1	Accept or Reject	Active	7.2.0.0-72.24.0	2016-06-07 02:01:11 UTC	2016-06-07 02:01:11 UTC			
			Warn	OOS	SDS-7.2.0.0-72.24.0-x86_64	Success: Server upgrade is complete				

Appendix L. ISO Link Correction

This procedure performs the ISO symlink correction and is required when upgrading from Release **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. <input type="checkbox"/>	Verify this procedure should be run	<ul style="list-style-type: none"> Is the topology of servers to be upgraded currently running SDS release 7.3, or 7.4? Has the SDS 8.x ISO been deployed? <p>If Yes to the above questions, then proceed to the next step. If No, this procedure is complete.</p>
2. <input type="checkbox"/>	Active NOAM GUI: Undeploy all unneeded ISO images	<ol style="list-style-type: none"> Navigate to Status & Manage > Files. Select to remove all unneeded old ISO images from the /var/TKLC/upgrade directory. Keep the ISO image file being used for this upgrade. Click Undeploy ISO. This saves space in the /var/TKLC/upgrade directory. 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. Click View ISO Deployment Report.
3. <input type="checkbox"/>	Active NOAM CLI: Log into the active NOAM	<p>Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the active NOAM.</p> <pre>ssh admusr@<NOAM_VIP> password: <enter password></pre>
4. <input type="checkbox"/>	Active NOAM CLI: Mount the ISO image	<p>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.</p> <pre>\$ sudo mount -o loop /var/TKLC/db/filemgmt/isos/SDS-8.0.0.0.0_80.x.y-x86_64.iso /mnt/upgrade</pre>

Procedure 28. ISO Link Correction		
5. <input type="checkbox"/>	Active NOAM CLI: Copy the script	Copy the script from the mounted ISO to /var/tmp to use it. <pre>\$ cp /mnt/upgrade/upgrade/bin/changeLinksToFiles.php /var/tmp</pre>
6. <input type="checkbox"/>	Active NOAM CLI: Unmount the ISO image	Unmount the SDS 8.0 ISO image. <pre>\$ sudo umount /mnt/upgrade</pre>
7. <input type="checkbox"/>	Active NOAM CLI: Verify the script is executable	Make the script executable. <pre>\$ chmod +x /var/tmp/changeLinksToFiles.php</pre> <pre>\$ ls -l /var/tmp/changeLinksToFiles.php</pre> <pre>-r-x----- 1 admusr admgrp 2652 Dec 2 14:07 /var/tmp/changeLinksToFiles.php</pre> <p>In the above example, the x is present for admusr, indicating the script is indeed executable for the user.</p>
8. <input type="checkbox"/>	Active NOAM CLI: Execute the script	Execute the script to change the symlink into a copy of the ISO image file. <pre>\$ /var/tmp/changeLinksToFiles.php</pre> <p>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.</p> <p>Example output for each server in the entire topology.</p> <pre>\$ /var/tmp/changeLinksToFiles.php</pre> <pre>server: NO1</pre> <pre>hostname alias based on service: nol-internalimi</pre> <pre>FIPS integrity verification test failed.</pre> <pre>Warning: Permanently added 'nol-internalimi,192.168.1.11' (RSA) to the list of known hosts.</pre> <pre>found link /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso</pre> <pre>FIPS integrity verification test failed.</pre> <pre>Warning: Permanently added 'nol-internalimi,192.168.1.11' (RSA) to the list of known hosts.</pre> <pre>Remove command succeeded! host: nol-internalimi, file: /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso</pre> <pre>FIPS integrity verification test failed.</pre> <pre>Warning: Permanently added 'nol-internalimi,192.168.1.11' (RSA) to the list of known hosts.</pre> <pre>Copy command succeeded! host: nol-internalimi, file: /var/TKLC/upgrade/SDS-8.0.0.0.0_80.20.0-x86_64.iso</pre> <p>The following expected messages can be ignored:</p> <pre>FIPS integrity verification test failed.</pre> <pre>Warning: Permanently added '<host>-internalimi,<ip address>' (RSA) to the list of known hosts.</pre> <p>If any unexpected failure messages occur, it is recommended to contact My Oracle Support (MOS) for guidance.</p>

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. <input type="checkbox"/>	Active NOAM: Log into the active NOAM and find the process ID of idbsvc	<p>Determine the number of files currently open.</p> <ol style="list-style-type: none"> 1. Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM. <pre>ssh <NOAM XMI IP address> login as: admusr password: <enter password></pre> <p>Note: The static XMI IP address for each server should be available in section 3.1.2.</p> 2. Retrieve the pid of idbsvc. The pid is highlighted in blue in the sample output shown: <pre>\$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2</pre> 3. The number of open files displays with the lsof command. Use the highlighted value in place of XXXX in the lsof command. <pre>\$ sudo lsof -p XXXX wc -l 1278</pre> 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: <pre>\$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd</pre> 6. The number of open files displays with the lsof command. Use the highlighted value in place of XXXX in the lsof command. <pre>\$ sudo lsof -p XXXX wc -l 1280</pre> 7. Record the number of files currently open: _____

Procedure 29. Increase Maximum Number of Open Files

2.	Active NOAM: <input type="checkbox"/> Find out the maximum number of open files permitted in system	<p>Display the maximum number of open files for idbsvc.</p> <ol style="list-style-type: none"> 1. Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command below. <pre>\$ sudo cat /proc/XXXX/limits grep -i open</pre> <pre>Max open files 32768 32768 files</pre> 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. <pre>\$ sudo cat /proc/XXXX/limits grep -i open</pre> <pre>Max open files 1024 4096 files</pre> 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: <input type="checkbox"/> Check if current number of open files (used by idbsvc) is in safe limit	<ul style="list-style-type: none"> • 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. <p>Repeat this procedure (if required) for other NOAM servers.</p>
4.	Active NOAM: <input type="checkbox"/> Check if maximum number of open files for tpdProvd is already set	<ul style="list-style-type: none"> • 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. <p>Repeat this procedure (if required) for other NOAM servers.</p>

Procedure 29. Increase Maximum Number of Open Files		
5. <input type="checkbox"/>	Active NOAM: Increase maximum number of open files	<ol style="list-style-type: none"> Use a text editor with sudo, edit the <code>/etc/init/tpdProvd.conf</code> file to add the following two lines just before the Start the daemon comment line: <pre># increase open file limit limit nofile 32768 32768</pre> Example: <pre># # 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</pre> Save the file and close the editor. <p>Caution: Do not edit any other line in this file. You can back up the file, if required.</p>
6. <input type="checkbox"/>	Active NOAM: Restart the tpdProvd process	<ol style="list-style-type: none"> Type the following command to stop tpdProvd: <pre>\$ sudo initctl stop tpdProvd</pre> Type the following command to restart tpdProvd <pre>\$ sudo initctl start tpdProvd</pre> <p>Sample output: <pre>tpdProvd start/running, process 186743</pre></p>
7. <input type="checkbox"/>	Active NOAM CLI: Recheck the open file maximum limit is set for tpdProvd	<ol style="list-style-type: none"> Retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below: <pre>\$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd</pre> Use the highlighted value in place of XXXX in the cat command below. <pre>\$ sudo cat /proc/XXXX/limits grep -i open Max open files 32768 32768 files</pre> 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 O.

Appendix N. Workarounds

N.1 Resolve Server HA Failover Issue

Procedure 30 resolves the HA failover issue by restarting the cmha process on the server.

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

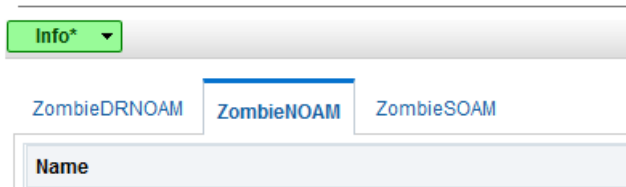
Procedure 30. Workaround to Resolve Server HA Failover Issue		
1. <input type="checkbox"/>	Server CLI: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the NOAM server which is experiencing the HA failover issue : <pre>ssh admusr@<server address> password: <enter password></pre> Answer yes if you are asked to confirm the identity of the server.
2. <input type="checkbox"/>	Server CLI: Resolve HA failover issue(s)	Execute this command: <pre>sudo pm.kill cmha</pre>
3. <input type="checkbox"/>	Repeat, if needed	Repeat procedure on each affected server, if required. Return to procedure/step in upgrade process which pointed to refer this procedure.

N.2 SNMP Configuration

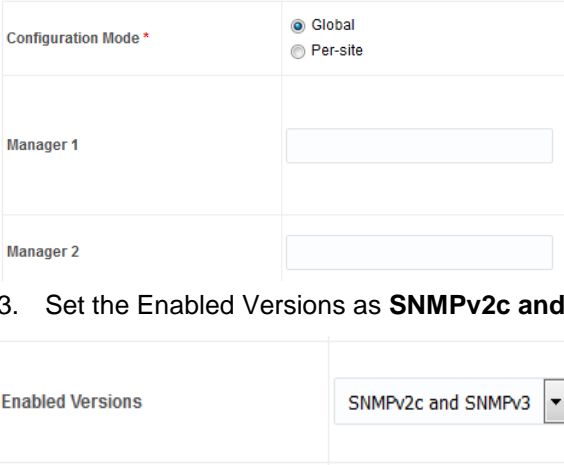
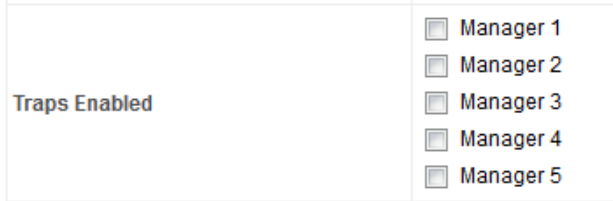

Procedure 31 configures or updates the SNMP with **SNMPv2c** and **SNMPv3** as the enabled versions for SNMP traps configuration, as PMAC does not support SNMPv3.

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 31. Workaround for SNMP Configuration		
1. <input type="checkbox"/>	NOAMP VIP GUI: Login	<ol style="list-style-type: none"> 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: <p>Main Menu: Administration -> Remote Servers</p> 

Procedure 31. Workaround for SNMP Configuration

2. <input type="checkbox"/>	NOAM VIP GUI: Configure/Update system-wide SNMP trap receiver(s)	<ol style="list-style-type: none"> 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 XML 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. <p>SNMP Trap Configuration Insert for ZombieNOAM</p>  <ol style="list-style-type: none"> 3. Set the Enabled Versions as SNMPv2c and SNMPv3. <p>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.  <ol style="list-style-type: none"> 5. Type the SNMP Community Name.  <ol style="list-style-type: none"> 6. Leave all other fields at their default values. 7. Click OK. </p>
3. <input type="checkbox"/>	PMAC GUI: Login	<ol style="list-style-type: none"> 1. If needed, open a web browser and enter: http://<pmac_management_ip> 2. Login as the pmacadmin user.

Procedure 31. Workaround for SNMP Configuration

<p>4. PMAC GUI: <input type="checkbox"/> Update the TVOE host SNMP community string</p>	<ol style="list-style-type: none"> 1. Navigate to Administration > Credentials > SNMP Community String Update. 2. Mark the Use Site Specific Read/Write Community String checkbox. <div data-bbox="516 394 1406 850"> <p>Select Read Only or Read/Write Community String:</p> <p><input type="radio"/> Read Only <input checked="" type="radio"/> Read/Write</p> <p>Check this box if updating servers using the Site Specific SNMP Community String:</p> <p><input checked="" type="checkbox"/> Use Site Specific Read/Write Community String</p> <p>Community String: <input type="text"/></p> <p>Note: The Community String value can be 1 to 31 uppercase, lowercase, or numeric characters.</p> <p><input type="button" value="Update Servers"/></p> </div> 3. Click Update Servers. <div data-bbox="516 955 1406 1060"> <p><small>You are about to update the Read/Write SNMP Credentials on all known supporting TVOE servers and the PM&C guest on the control network of this PM&C. Changing of SNMP Community Strings is only supported across product release versions that support this functionality and attempting to do so with product versions not supporting it may cause the system to become inoperable.</small></p> <p><small>Are you sure you want to continue?</small></p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> 4. Click OK. 5. Return to the procedure step that directed the execution of this procedure.
---	--

N.3 Resolve Syscheck Error for CPU Failure

This procedure resolves the syscheck errors for CPU failure.

Procedure 32. Workaround to Resolve Syscheck Error for CPU Failure

<p>1. <input type="checkbox"/> Log into server using CLI on which syscheck is failing</p>	<p>Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.</p> <pre>ssh admusr@<SERVER_XMI> password: <enter password></pre> <p>Answer yes if you are asked to confirm the identity of the server.</p>
---	---

Procedure 32. Workaround to Resolve Syscheck Error for CPU Failure

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.

N.4 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 33. 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:

ORACLE®

Oracle System Login

Tue Jun 7 13:49:06 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

☐ Change password

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

Procedure 33. Workaround to Fix the cmsoapa Restart

2. <input type="checkbox"/>	NOAM VIP GUI: Identify the servers with the 31201 alarm for the cmsoapa process not running	<ol style="list-style-type: none"> 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. <input type="checkbox"/>	Login into Server using CLI on which cmsoapa is restarting	<p>Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.</p> <pre>ssh admusr@<SERVER_XMI> password: <enter password></pre> <p>Answer yes if you are asked to confirm the identity of the server</p>
4. <input type="checkbox"/>	Server CLI: Execute workaround	<ol style="list-style-type: none"> 1. Execute workaround: <pre>\$ sudo prod.dbdown</pre> 2. After few minutes, when processes are down. Execute prod.start. <pre>\$ sudo prod.start</pre> 3. Repeat the steps on all server(s) where the alarm is, that is, where the cmsoapa process is restarting.

N.5 Fix DNS Issue

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

Procedure 34. Workaround to Fix DNS Issue

1. <input type="checkbox"/>	Verify the QS server transitions to a "A" State	<ol style="list-style-type: none"> 1. Login to QS Server with the admusr account. 2. Execute the command: <pre>[admusr@SG2-SDS-QS ~]\$ sudo prod.state ...prod.state (RUNID=00)... ...getting current state... Current state: A (product under procmgr)</pre> <ol style="list-style-type: none"> 1. If current state is A, stop and continue completing the upgrade. 2. If not, then continue to the next step.
2. <input type="checkbox"/>	Verify the permissions of the /etc/resolv.conf file is 644	<p>Execute:</p> <pre>[admusr@SG2-SDS-QS ~]\$ ll /etc/resolv.conf -rw-r--r-- 1 root root 73 Feb 21 19:47 /etc/resolv.conf</pre>
3. <input type="checkbox"/>	Verify the /etc/resolv.conf file contains the upgraded standby server	<p>Check the file content:</p> <pre>[admusr@SG2-SDS-QS ~]\$ sudo cat /etc/resolv.conf <Primary Server A> <Primary Server B> <Secondary Server B></pre> <p>If not, checkout and edit the file as shown using the steps below</p>

Procedure 34. Workaround to Fix DNS Issue		
4. <input type="checkbox"/>	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. <input type="checkbox"/>	Edit the /etc/resolv.conf file	Edit the conf file: [admusr@SG2-SDS-QS ~]\$ sudo vi /etc/resolv.conf
6. <input type="checkbox"/>	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>
7. <input type="checkbox"/>	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. <input type="checkbox"/>	Clear DNS cache using the nscd command	Clear DNS cache: [admusr@SG2-SDS-QS ~]\$ sudo nscd -i hosts
9. <input type="checkbox"/>	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 O. My Oracle Support (MOS)

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

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown 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 will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
1. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
2. 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.