Oracle® Database

Diameter Signaling Router Diameter SDS Software Upgrade Guide

Release 9.0.2.1.0
G13785-01
August 2024

Oracle Database Diameter Signaling Router Diameter SDS Software Upgrade Guide, Release 9.0.2.1.0

G13785-01

Contents

My Oracle Support

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

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

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms and Terminology

Listed below is an alphabetized list of acronyms and terminologies used in the document:

Table Acronyms

Acronym	Meaning
CLI	Command Line Interface
CSV	Comma-separated Values
DP	Database Processor
DR	Disaster Recovery
GA	General Availability
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IPM	Initial Product Manufacture
ISO	ISO 9660 file system
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
NE	Network Element
NOAM	Network OAM
OAM&P	Operations, Administration, Maintenance and Provisioning
SDS	Subscriber Database Server
SOAM	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
XSI	External Signaling Interface
DIU	Dual Image Upgrade

Table Terminology

Acronym	Definition
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 8.6 to SDS 9.0.x
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 9.x to 9.x
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.

Table (Cont.) Terminology

Acronym	Definition
Back out	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: • Server is forced standby • Server is application disabled (signaling servers do not process any traffic)

Whats New in This Guide

This section introduces the documentation updates for release 9.0.2.1.0.

Release 9.0.2.1.0 - G13785-01, August 2024

Updated SDS upgrade paths in the SDS Supported Upgrade Paths section.

1
Introduction

This document describes methods used and procedures to perform an application software upgrade on in-service Subscriber Data Servers and Subscriber Data Servers Database Processor blades in an Subscriber Data Servers network. The supported upgrade paths are:

> **Note:**
>
> From SDS 9.0.0.0.0 and later, consider ISO as DIU ISO in all occurrences, throughout this document.

```
8.6.x, 9.0, 9.0.1, to 9.0.2
```

X = PI End Cycle

Y = Patches within the PI Cycle

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

This document provides instructions to run any SDS 8.6 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 Acronyms and Terminology

Listed below is an alphabetized list of acronyms and terminologies used in the document:

Table 1-1 Acronyms

Acronym	Meaning
CLI	Command Line Interface
CSV	Comma-separated Values
DP	Database Processor

Table 1-1 (Cont.) Acronyms

Acronym	Meaning
DR	Disaster Recovery
GA	General Availability
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IPM	Initial Product Manufacture
ISO	ISO 9660 file system
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
NE	Network Element
NOAM	Network OAM
OAM&P	Operations, Administration, Maintenance and Provisioning
SDS	Subscriber Database Server
SOAM	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
XSI	External Signaling Interface
DIU	Dual Image Upgrade

Table 1-2 Terminology

Acronym	Definition
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 8.6 to SDS 9.0.x
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 9.x to 9.x
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.
Back out	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.

Table 1-2 (Cont.) Terminology

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

1.2 References

- *SDS Initial Installation and Configuration Guide.*
- *Database Management: Backup and System Restoration*
- *SDS Disaster Recovery Guide*
- *HP Solutions Firmware Upgrade Pack Release Notes, v2.1.5 (or latest 2.1 version)*
- *Platform 7.2 Configuration Guide*

1.3 Activity Logging

While connected to the system, log all the activity using a convention that notates the Customer Name, Site or Node location, Server Host name, and Date. Post upgrade provide all logs to Oracle for archiving.

1.4 Use of Health Checks

The user may run the Health Check Procedures procedure 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.

1.5 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.

1.6 Warnings, Cautions, and Notes

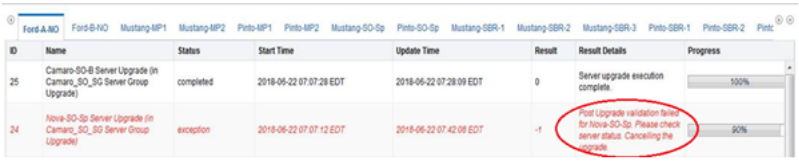
This section presents notices of warnings and cautions that directly relate to the success of the upgrade. It is imperative that each of these notices be read and understood before continuing with the upgrade. If there are any conflicts, issues, or questions related to these notices, it is recommended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

Upgrade Check

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

```
"Post Ugrade validation failed for <server_name>. Please check server status.
Canceling the upgrade."
```

Figure 1-1 Server Status



> **Note:**
>
> **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 run a software upgrade of an in-service Subscriber Data Servers from the source release to the target release.

> **Note:**
>
> Initial Installation is not within the scope of this upgrade document. See the SDS Initial Installation and Configuration Guide for more information.

2.1 SDS Supported Upgrade Paths

The following table provides information about the supported upgrade paths:

Table 2-1 SDS Upgrade Paths

Source Release	Target Release
9.0.0.0.0	9.0.2.1.0
9.0.1.0.0	9.0.2.1.0
9.0.2.0.0	9.0.2.1.0

The supported migration paths for SDS 9.0.2.1.0 are listed in the following table:

Table 2-2 SDS Migration Paths

Source Release (BareMetal)	Target Release (Cloud)
8.4.0.3.0	9.0.2.1.0
8.5.0.2.0	9.0.2.1.0

> **Note:**
>
> For further information on migrating SDS, see SDS BareMetal to Cloud Migration Guide.

3
Upgrade Overview

> **Note:**
>
> If the upgrade is required from 8.6.x VM to 9.0.2, refer to Dual Hop Upgrade from SDS-8.6.x to SDS-9.0.2 Using Ansible section.

This section lists the required materials and information needed to run 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 Upgrade Preparation Overview through Recovery Procedures Overview. 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 run procedures. Detailed steps for each procedure are provided in Upgrade Preparation.

3.1 Upgrade Requirements

> **Note:**
>
> Any third party software that the customer has installed will be removed after an upgrade.

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

- Target-release DIU ISO image file
  Example: SDS-9.0.2.0.0_98.15.0-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.

> **Note:**
>
> For a major upgrade, along with DIU ISO, the tar file and TPD OL7 DIU ISO is required.

- User logins, passwords, IP addresses, and other administration information. For more information, see the Logins, Passwords, and Site Informationsection.
- Direct access to server IMI IP addresses from the user's local workstation is preferable in the case of a back out.

> **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 file name is in the following format:

For example: `SDS-9.0.2.0.0_98.15.0-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 3-1 Logins, Passwords, and Site Information

NE Type	NE Name
Primary SDS site	
DR SDS site	

Table 3-1 (Cont.) Logins, Passwords, and Site Information

NE Type	NE Name
SOAM 1 site	
SOAM 2 site	
SOAM 3 site	
SOAM 4 site	

Table 3-2 Software

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

Table 3-3 Access Information

Access Information	Value
Primary site XMI VIP (GUI)	
DR site XMI VIP	
SDS GUI admin user name 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*	
PMAC user root password*	
PMAC user admusr password*	
PMAC user PMACftpusr password*	
On board administrator GUI admin user name and password	

3.2 MySql User Accounts Password

This section provides the procedure to check for the presence of any forbidden special characters in the mysql passwords for **awadmin** and **root** user accounts.

Mysql password can contain the following:

- Upper case alphabets (A-Z)
- Lower case alphabets (a-z)
- Digits (0-9)
- 21 allowed special characters

Allowed Special Characters

There are a total of 32 special characters on the standard qwerty keyboard. Out of these 32 special characters, 21 characters are supported in the MySql passwords.

The following table provides the list of these 21 allowed special characters.

Table 3-4 Allowed Special Characters

Allowed Special Characters	Name
#	Octothorpe or hash or pound sign
!	Exclamation point
~	Tilde
%	Percent
^	Caret or circumflex
*	Asterisk
_	Underscore
-	Hyphen or dash
+	Plus
=	Equal
?	Question Mark
{	Open Braces
}	Close Braces
(	Open Parenthesis
)	Close Parenthesis
<	Open angle bracket or less than
>	Close angle bracket or greater than
|	Pipe or Vertical bar
.	Dot
,	Comma
;	Semi Colon

Forbidden Special Characters

There are a total of 32 special characters on the standard qwerty keyboard. Out of these 32 special characters, 11 characters are currently not supported in the MySql passwords. Usage of these forbidden special characters in the password will set the incorrect password in the database of MySql Server.

The following table provides the list of these 11 forbidden special characters.

Table 3-5 Forbidden Special Characters

Forbidden Special Characters	Name
@	Ampersat
$	Dollar
&	Ampersand
`	Backtick or backquote or grave accent
\	Backslash
/	Forward slash
[	Open Square Bracket
]	Close Square Bracket

Table 3-5 (Cont.) Forbidden Special Characters

Forbidden Special Characters	Name
`	Single quotation mark or apostrophe
"	Double quotation mark
:	Colon

3.2.1 Sanity Check on MySql Passwords

Perform the following procedure to sanity check MySql passwords.

1. Log in to the source server as `admusr`.

   ```
   Username: admusr
   Password: <current admin user password>
   ```

2. Verify the mysql passwords using the following commands.

   For `awadmin` user account:

   ```
   sudo /usr/TKLC/appworks/bin/aw.wallet credential get mysql default
   ```

   For `root` user account, use the following command:

   ```
   sudo /usr/TKLC/appworks/bin/aw.wallet credential get mysql root
   ```

3. If passwords contain forbidden special characters mentioned in the Table 3-5 table, then reset the mysql password using the allowed special character mentioned in the Table 3-4 table.

> **Note:**
>
> To reset the mysql password, see *Updating the MySQL Password* in *DSR Security Guide*.

3.3 Upgrade Maintenance Windows

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

Upgrade Maintenance Windows

Maintenance Window 1:

The following information has to be recorded in this maintenance window:

1. Record the date of the maintenance window.

2. Record the names of the primary SDS NE site, DR SDS NE site, and server's hostnames to be upgraded during Maintenance Window.
3. Verify and record the following information after each server upgrade is completed:
   - Primary SDS NE site name
     - Primary SDS active server
     - Primary SDS standby server
     - Primary SDS query server
   - DR SDS NE site name
     - DR SDS active server
     - DR SDS standby server
     - DR SDS query server

Upgrade Maintenance Windows

Maintenance Window 2:

The following information has to be recorded in this maintenance window:

1. Record the name of SOAM NE site and its server's host names to be upgraded during the maintenance window .
2. Verify and record the following information after each server upgrade is completed:
   - SOAM NE site name
     - Active SOAM Server
     - Standby SOAM Server
   - DP Server Names
     - DP 1 Server
     - DP 2 Server
     - DP 3 Server
     - DP 4 Server
     - DP 5 Server
     - DP 6 Server
     - DP 7 Server
     - DP 8 Server
     - DP 9 Server
     - DP 10 Server

Keep track of maintenance windows for each SOAM NE site.

3.4 Upgrade Preparation Overview

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

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

> **Note:**
>
> In Upgrade DR SDS NOAM procedure, 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.

Upgrade Preparation Procedures

Table 3-6 Upgrade Preparation Procedures

Procedure Title	Elapsed Time (Hrs:Min)	
	This Step	Cumulative
Required Materials Check	00:15	00:15
ISO Administration	*	*
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.

3.5 Primary SDS Site or DR SDS Site Upgrade Execution Overview

The procedures shown in the following table are performed inside a maintenance window. The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in following table.

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

> **Note:**
>
> During upgrade some alarms/events may be raised that can be ignored. Alarms are mentioned in Access the OAM GUI Using the VIP (NOAM/SOAM).

Table 3-7 Primary SDS or DR SDS Upgrade Procedures Strategy

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

3.6 SOAM Upgrade Execution Overview

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

Table 3-8 SOAM Upgrade Procedures

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

3.7 Post Upgrade Execution Overview

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

Table 3-9 Post Upgrade Procedures

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

3.8 Recovery Procedures Overview

These procedures are customized to the specific situation encountered and therefore do not have well-established time frames. The order of the back out for the primary NOAM NE and DR NOAM NE needs to be followed as shown in the following table.

> **Note:**
>
> Backout is not supported if the upgrade was performed from 8.x to 9.x release

> **Note:**
>
> During back out of servers, there are steps to check the replication status before going to the next server back out. Follow the steps to perform; otherwise, it may result in data loss.

> **Note:**
>
> During the back out some alarms/events may be raised that can be ignored. Alarms are mentioned in step 4 of Health Check Procedures.

Table 3-10 Backout Procedures

Procedure Title	Elapsed Time (Hrs:Min)	
	This Step	Cumulative
Back Out the SOAM	*	*
Back Out the DR SDS NOAM	*	*
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.

Contact My Oracle Supportin needed.

> **Note:**
>
> 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 4-1 SDS Upgrade Matrix

Network Element Type	Procedures							
	1	2	3	4	5	6	7	8
Primary NOAM NE DR NOAM NE (SDS/ Query Server)	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
SOAM NE (SOAM/DP)	Yes	No	No	No	No	No	Yes	Yes

> **Note:**
>
> Run Health Check Procedures before and after completing this procedure.

SDS Upgrade – List of Procedures:

- Required Materials Check
- ISO Administration
- Backup TKLCConfigData
- Full Database Backup (PROV and COMCOL Env for All Servers)

5
Upgrade Preparation

This section provides detailed procedures to prepare a system for upgrade execution. These procedures may be performed 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.

1. Verify if all the upgrade requirements have been met. Requirements are listed in section Upgrade Requirements.Verify all upgrade requirements have been met.
2. Verify if all administration data needed during upgrade. Verify if all information Logins, Passwords, and Site Informationentered is accurate.

5.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the SDS 9.0.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 five 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 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 performed multiple times, it must be run at least once in 24-36 hours before starting a maintenance window.

Run SDS health check procedures as specified in Health Check Procedures.

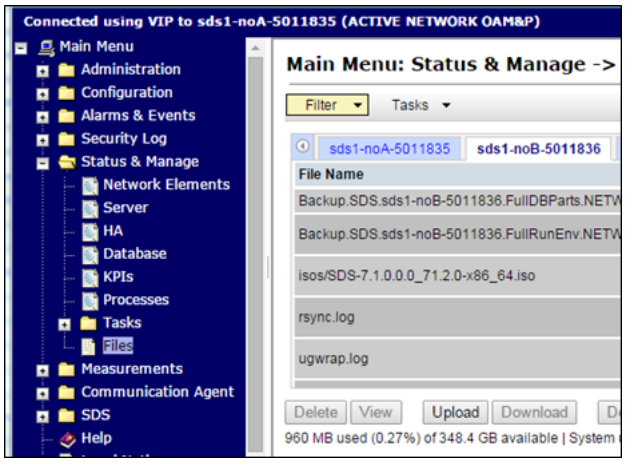
5.4 ISO Administration

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:**
>
> **Add the SDS ISO to the PMAC Software Repository** may be performed at any time after ISO administration procedure has been completed.

1. Log in to the SDS NOAM GUI. Use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP (GUI), connect to the SDS server. Expand **Status & Manage** click **Files**. Select the host name of the active primary SDS server from the list of tabs. Click **Upload**.

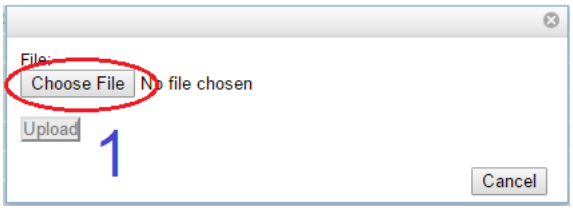
Figure 5-1 Upload



> **Note:**
>
> The active primary SDS server displays in the GUI banner as connected to the VIP with a state of **ACTIVE NETWORK OAM&P**.

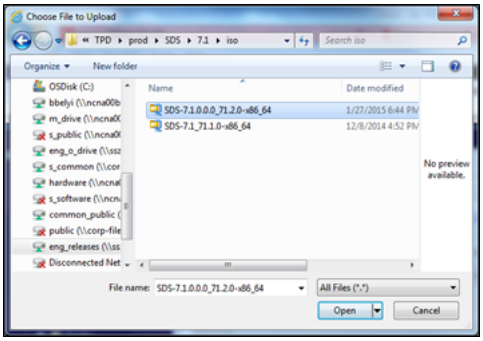
3. Upload the ISO file, click **Choose File**.

Figure 5-2 Choose File



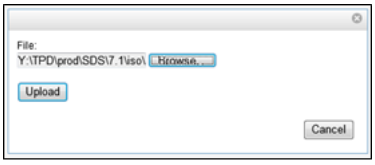
4. Locate the ISO file for the target release and click **Open**.

Figure 5-3 Open



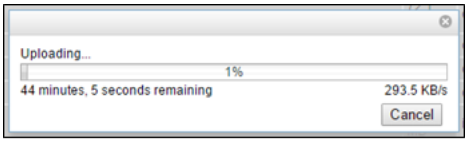
5. Click **Upload**.

Figure 5-4 Upload



6. Monitor the upload until the file transfer completes.

Figure 5-5 File Transfer

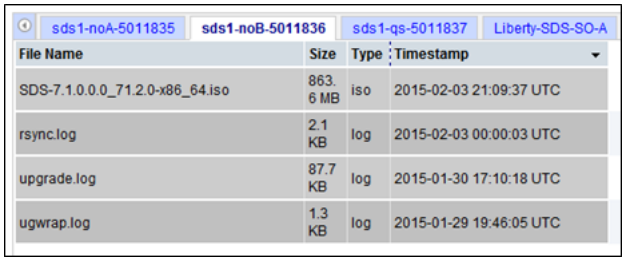


Note:

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.

7. Click the **Timestamp** heading twice to sort the column by most recent files.

Figure 5-6 Timestamp



8. Run the following commands, on Active NOAM CLI.
   a. Run this command on CLI:

      ```
      sudo sed -i '528i\ sleep(300);' /var/TKLC/appworks/services/
      SvrUpgrade.php
      ```

   b. Run this command on CLI:

      ```
      sudo sed -i '/if (array_key_exists("MateHostname", $serverData))/c\ if
      (is_array($serverData) &&
      array_key_exists("MateHostname", $serverData))' /var/TKLC/appworks/
      validator/Sds/HaStatusValidator.php
      ```

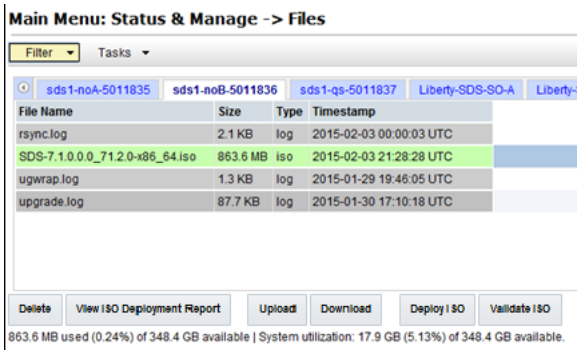
   c. Run this command on CLI:

      ```
      sudo sed -i '310s/validate_cd/validate_cd_tmp/' /var/TKLC/appworks/
      services/FileManagement.php
      ```

> **Note:**
>
> Perform this step only if the base release is 9.0.0.0.0_97.16.0.

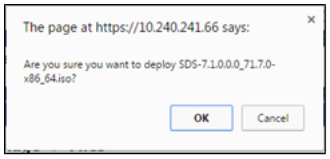
9. Deploy the ISO file to all SDS servers in the network.
   a. Select the ISO file.
   b. Click **Validate ISO**.
   c. Wait for validation to pass.
   d. Click **Deploy ISO**.

Figure 5-7 Deploy ISO



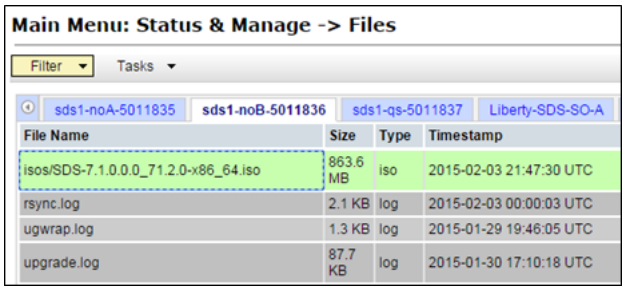
Click **OK**.

Figure 5-8 OK



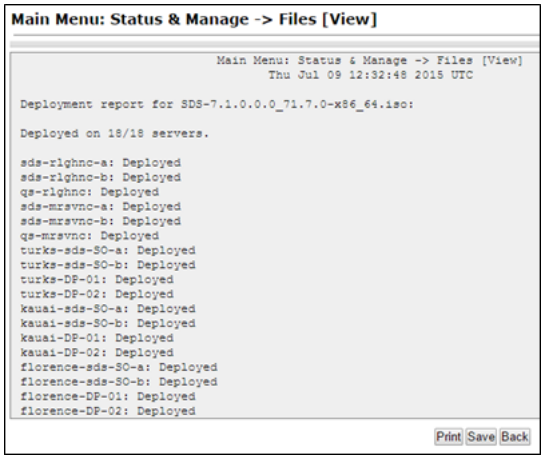
10. Monitor the ISO deployment status, select the ISO file. Click **View ISO Deployment Report**.

Figure 5-9 ISO Deployment Report



11. 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 9 of this procedure until the **ISO** has been **Deployed** to all servers.

Figure 5-10 Report



5.5 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.

1. Login to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP GUI, export servers. Expand **Configuration** click **Servers**. Select each server in the topology and click **Export**.

Figure 5-11 Servers

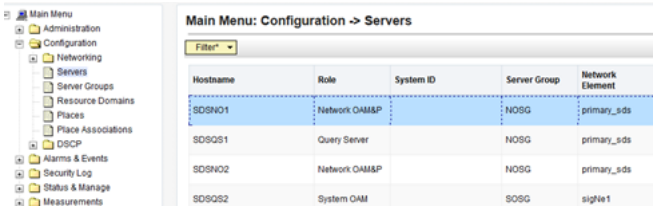


Figure 5-12 Export

> **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. Back up TKLCConfig data and access the CLI of the primary SDS NOAM, access the primary SDS NOAM server command line using ssh or a console.

   ```
   ssh admusr@<NOAM_VIP>
   ```

4. Transfer the `TKLCConfigData` files for all servers in the `/var/TKLC/db/filemgmt` directory to a remote location.

   ```
   $ cd /var/TKLC/db/filemgmt
   $ scp TKLCConfigData.<Sever Hostname>.sh
   <username>@<remote-server>:<directory>
   ```

   For example:

   ```
   scp TKLCConfigData.SDSDRNO1.sh <username>@<remote-
   server>:<directory>
   ```

> **Note:**
>
> Back up the TKLCConfig data file for all servers.

5.6 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 performed multiple times but must also be run at least once within the period of 24-36 hours before the start of a maintenance window.

Run SDS Health Check procedures as specified in Health Check Procedures

5.7 Full Database Back up (PROV and COMCOL ENV for All Servers)

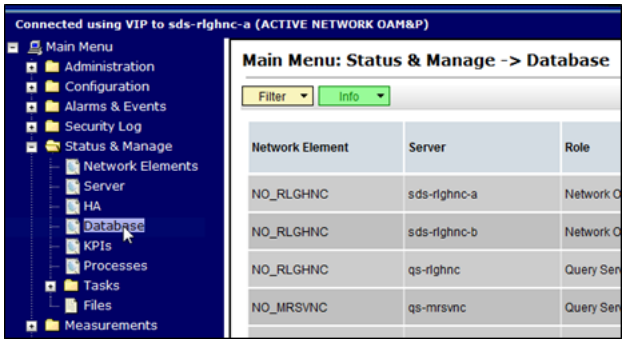
This procedure is part of software upgrade preparation and is used to conduct a full backup of the COMCOL run environment on every server, to be used in the event of a back out or rollback of the new software release.

> **Note:**
>
> For 8.6.x release, backup files are created automatically when ./ majorUpgrade.sh script is used.

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

1. Log in to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM)
2. In the Primary SDS NOAM VIP (GUI), verify the name of the primary active network OAMP SDS server. Expand **Status & Manage** click **Database**.

Figure 5-13 Database



3. Verify the host name of the active primary OAMP SDS server from the GUI banner.

Figure 5-14 Verify host name

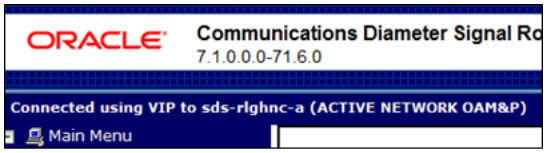
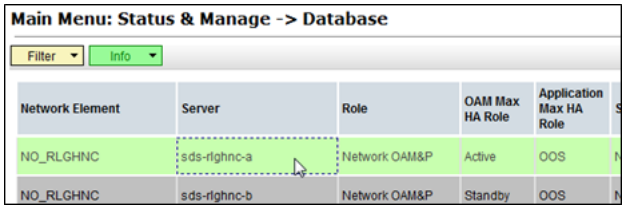


Figure 5-15 Host name

4. In the Primary SDS NOAM VIP, back up the server. Select the SDS server.

Figure 5-16 SDS Server

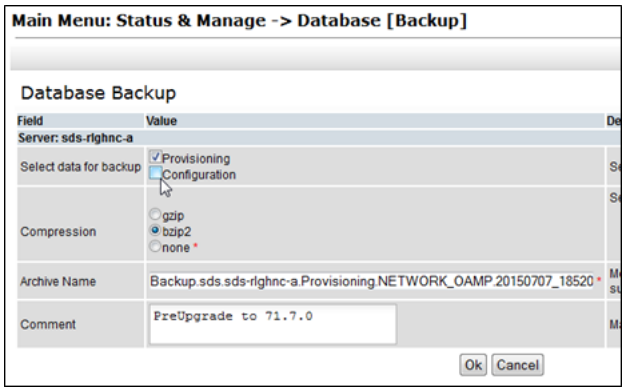


5. Click **Backup**

Figure 5-17 Back up

6. Back up the provisioning data, un-check the **Configuration** check box. Enter a **Comment**.

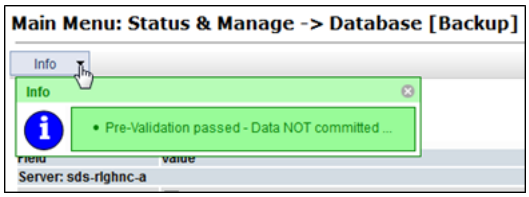
Figure 5-18 Database Back up



> **Note:**
>
> Entering a **Comment** is mandatory.

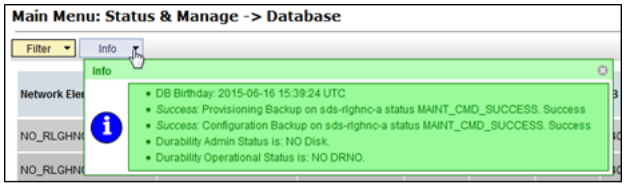
7. Click **Info** to verify if the changes have passed pre-validation.

Figure 5-19 Verify Information



8. Click **OK**.
9. In the Primary SDS NOAM VIP, verify status. Wait for the screen to refresh (for about 1or 2 minutes).Click the **Info** tab to verify the **Provisioning Backup** shows a status of **MAINT_CMD_SUCCESS**.

Figure 5-20 Provisioning Backup



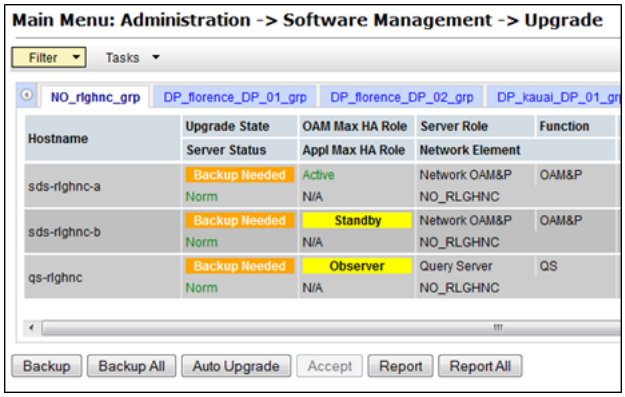
10. If a status of MAINT_IN_PROGRESS is received, then refresh the Info message, expand **Status & Manage** click **Database**. Click on the **Info** tab again.

> **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.

11. In the Primary SDS NOAM VIP, back up the servers. Expand **Administration** select **Software Management** click **Upgrade**. Click **Backup All**.

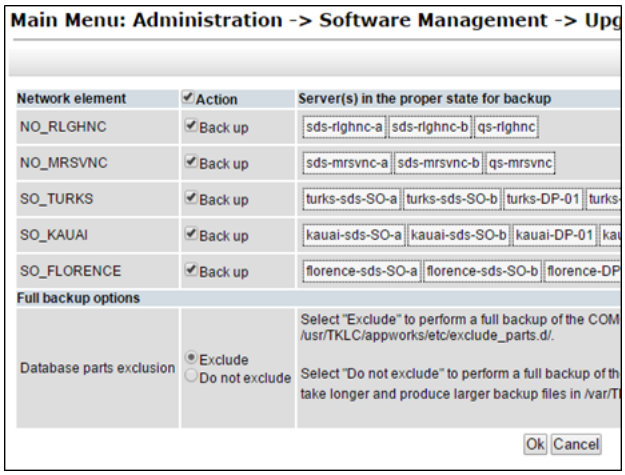
Figure 5-21 Back up Server



> **Note:**
>
> All servers in an Upgrade state are displayed on the screen. Servers in a **Forced Standby** or **OOS** state are not displayed.

12. Select the **Exclude** option. Click **OK**.

Figure 5-22 Exclude Option



13. In the Primary SDS NOAM VIP, monitor progress. Verify the **Upgrade State** of the servers goes from a **Backup in Progress** state to a **Ready** state.

Figure 5-23 Upgrade State

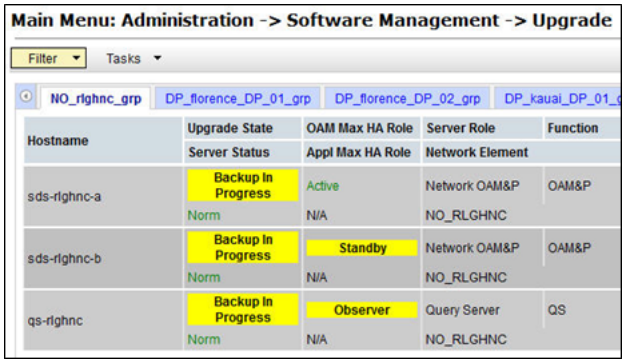
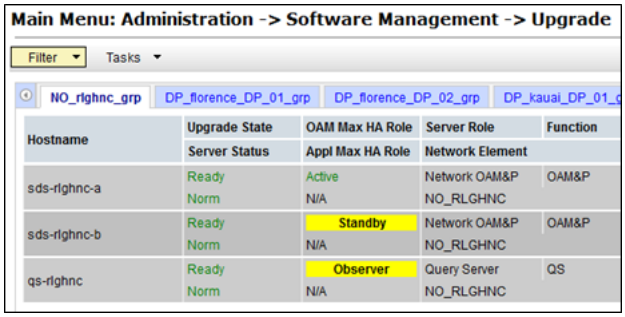


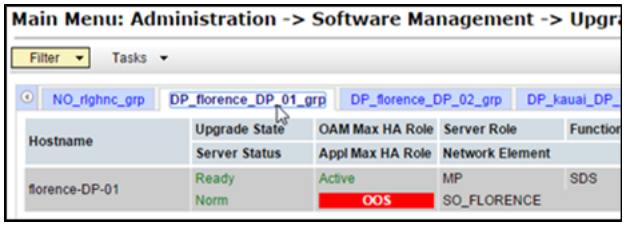
Figure 5-24 Upgrade State Ready



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

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

Figure 5-25 Server Upgrade State



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 (SOAM's 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.

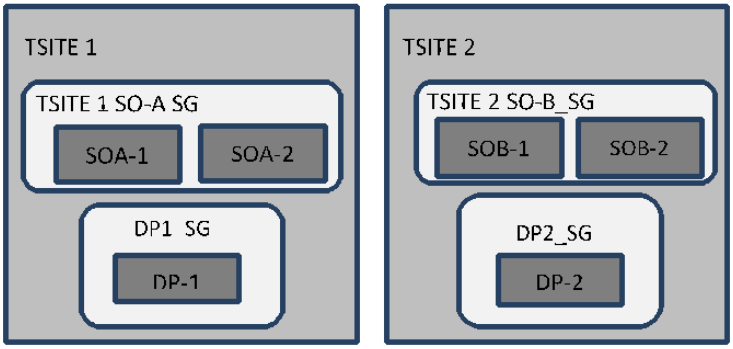
Automated Site Upgrade can be used to upgrade the SOAM and DP servers. However, Auto Site Upgrade cannot be used to upgrade PMAC or TVOE at a site.

With this feature, a site upgrade can be initiated on SO-A SG and all of its sub-servers (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 the sub-servers of SO-A SG (not shown). These upgrades begin in parallel with server upgrade in DP1 SG.

> **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 6-1 Upgrade Perspective of SDS Site Topology

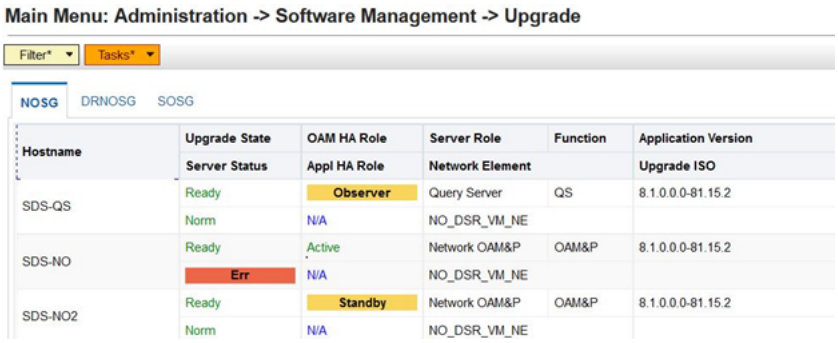


6.1 Site Upgrade Execution

With Auto Site Upgrade, upgrade is initiated by expanding **Administration** selecting **Software Management** and clicking on **Upgrade screen**. On initial entry to this screen, the user is

presented with a tabbed display of the NOAM server group and SOAM sites (Figure 6-2).When the NOAM server group tab is selected (as shown in Figure 6-2), this screen is largely unchanged from the upgrade screen of previous releases. The NOAM server group servers are displayed with the usual assortment of buttons. On this screen, the Auto Upgrade button refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature becomes available once a SOAM server group tab is selected. The SOAM server group tabs correspond to the topological sites (TSites).

Figure 6-2 Site Upgrade — NOAM View



On selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen displays (Figure 6-3). 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 Site Upgrade Options for additional details on bulk availability).
- The **Server Upgrade States** column groups the servers by state, indicating the number of servers in the server group that are in each state.
- The **Server Application Versions** column indicates the current application version, indicating the number of servers in the server group that are at each version.

Figure 6-3 Site Upgrade — Entire Site View

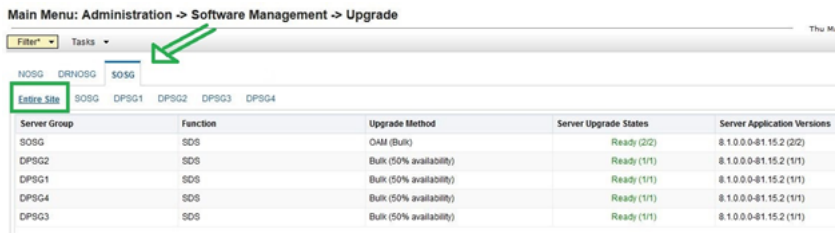


Figure 6-4 Site Upgrade — Entire Site View

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

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

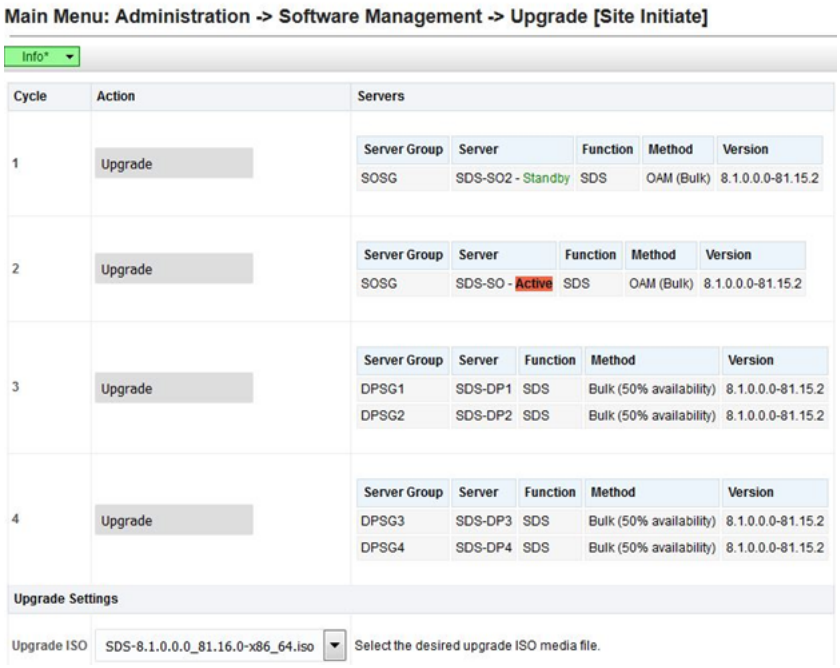
A site is eligible for Auto Site Upgrade when at least one server in the site is upgrade ready.

Click **Site Upgrade** from the **Entire Site** view to display the Upgrade Site Initiate screen (Figure 6-5). The Site Initiate screen shows the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 6-5, 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 Site Upgrade Options.

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

Figure 6-5 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 6-5, Cycle 3 consists of SDS-DP1 and SDS-DP2 and Cycle 4 consists of SDS-DP3 and SDS-DP4.

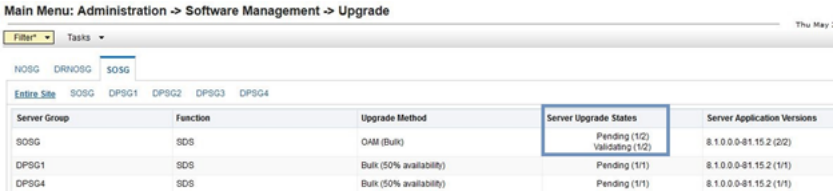
The site upgrade is complete when every server in the site is in the **Accept or Reject** state.

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 Minimum Server Availability.

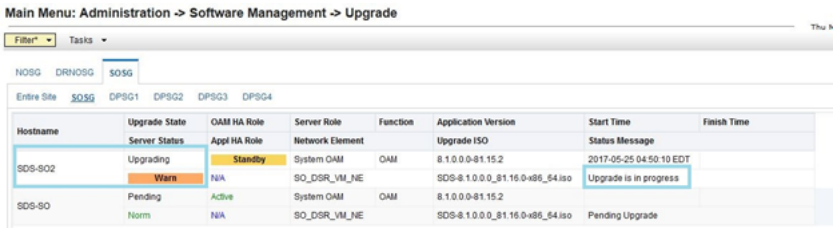
To initiate the site upgrade, a target ISO is selected from the ISO pick list in the **Upgrade Settings** section of the Site Initiate screen (Figure 6-5). Once the **OK** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 6-6). With the **Entire Site** link selected, a summary of the upgrade status for the selected site displays. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. This view can be used to monitor the upgrade status of the overall site. More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.

Figure 6-6 Site Upgrade Monitoring



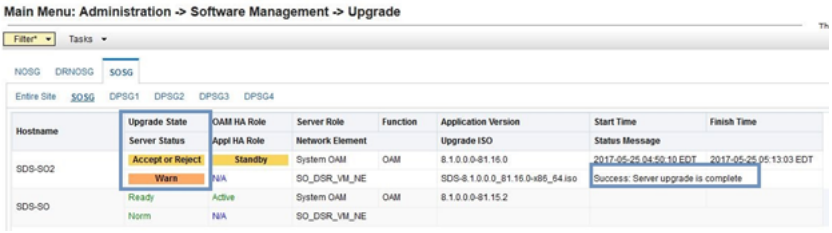
When a server group link is selected on the Upgrade Administration screen, the table rows are populated with the upgrade details of the individual servers within that server group (Figure 6-7).

Figure 6-7 Server Group Upgrade Monitoring



Upon completion of a successful upgrade, every server in the site is in the **Accept or Reject** state (Figure 6-8).

Figure 6-8 Server Group Upgrade Monitoring



See Cancel and Restart Auto Site Upgrade for a description of canceling 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.

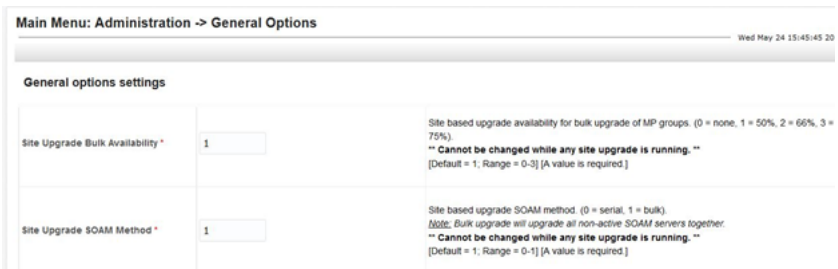
For example, if the specified minimum availability is 50% and there are eight servers of type **X**, then four remain in service while four upgrade. However, if there are nine server of type **X**, then the minimum availability requires that five remain in service while four upgrade. The minimum availability 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 Site Upgrade Options.

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** screen under **General Options**. The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

Figure 6-9 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.

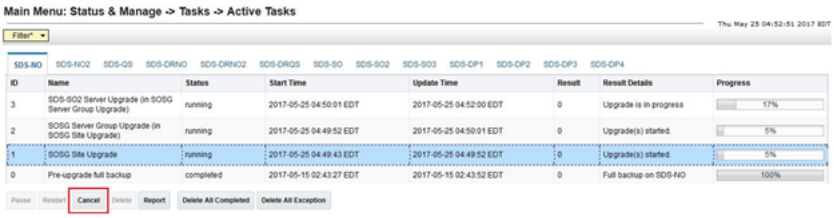
Regardless of the SOAM upgrade method, the active SOAM are always upgraded after the standby SOAM.

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 by navigating to **Status & Manage** select **Tasks** and click **Active Tasks**.

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

Figure 6-10 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 canceled 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 6-11 shows the Active Task screen after a site upgrade has been canceled.

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

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

Figure 6-11 User Canceled the Site Upgrade Tasks

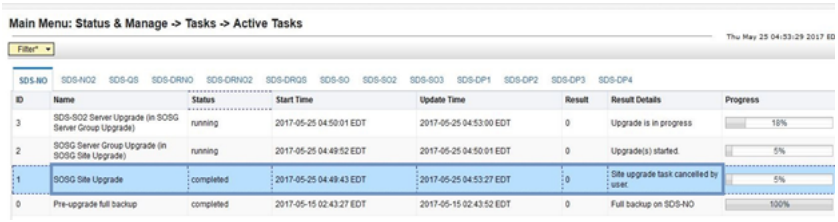
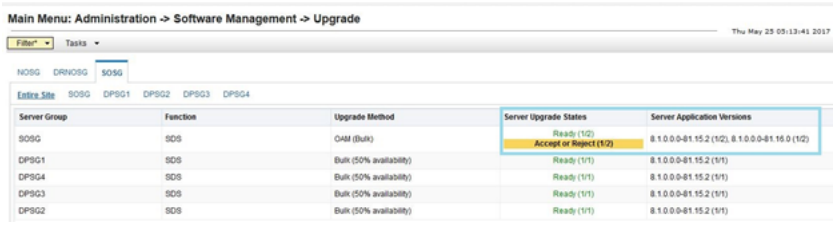


Figure 6-11 represents a site upgrade that was canceled before the site was completely upgraded. The servers that were in progress when the upgrade was canceled continued to upgrade to the target release. These servers are now in the **Accept or Reject** state. The servers that were pending when the upgrade was canceled are now in the **Ready** state, ready to be upgraded.

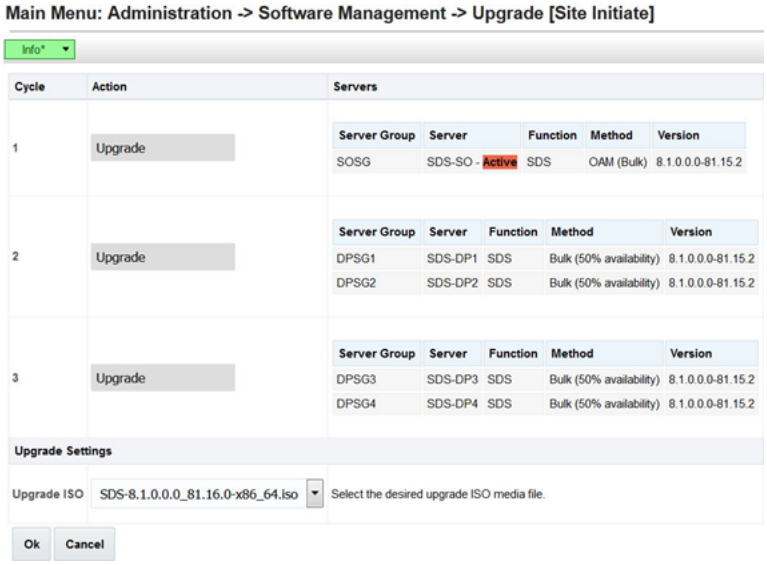
To restart the upgrade, verify the **Entire Site** link is selected and click **Site Upgrade**. The Upgrade Site Initiate screen displays.

Figure 6-12 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 6-12 shows the upgrade that was canceled and only three cycles are needed since the availability requirements can be met by the servers that have already been upgraded. Once an ISO is selected and the **OK** button is clicked, the site upgrade continues normally.

Figure 6-13 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.

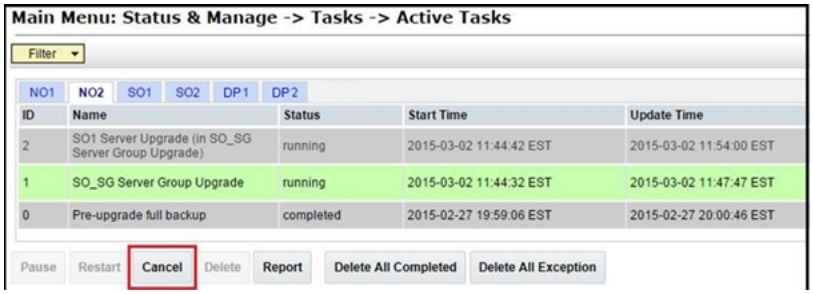
For SDS Automated Server Group (ASG) upgrade refer the steps as specified in Upgrade Server Administration on SDS 9.0.

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 canceled by navigating to **Status & Manage** and clicking **Active Tasks** (Figure 7-1) if necessary. Once the task is canceled, it cannot be restarted. However, a new ASG task can be started using the Upgrade Administration screen.

For example, in Figure 7-1, 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. Canceling 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 7-1). Because the ASG task is canceled, no new server upgrade is initiated by the task.

Figure 7-1 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 canceled and no other servers in that server group are upgraded. Canceling 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.

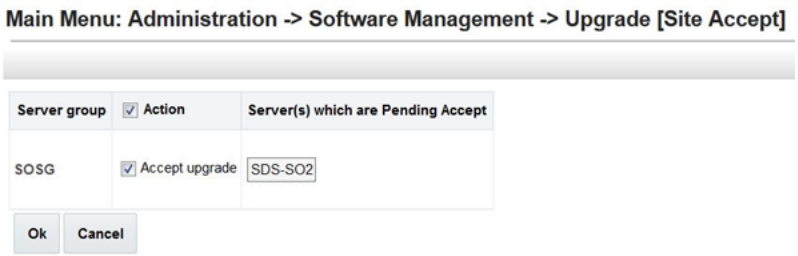
The **Site Accept** button on the upgrade screen provides the capability to nearly simultaneously accept the upgrade of some or all servers for a given site. When the button is selected, a subsequent screen displays the servers that are ready for the Accept action.

Figure 7-2 Site Accept Button

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

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

Figure 7-3 Site Accept Screen



8
Primary or DR SDS NOAM Upgrade Execution

Inform My Oracle Support about your plans to upgrade the system before executing the upgrade.

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

Note:

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.

Note:

If a procedural step fails to run successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact My Oracle Support 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 displayed 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 host names.
- 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, tool bars, and button layouts.

After completing each step and at each point where data is recorded from the screen. Procedures which have run multiple times and each additional iteration that the step has performed is noted.

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 or DR NOAM Pre- upgrade)

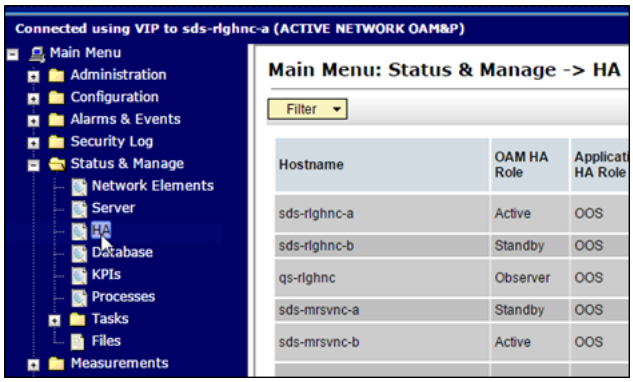
This procedure is part of software upgrade preparation and is used to determine the health and status of the entire SDS network and servers. This may have run multiple times, but must also be run at least once within the period of 24-36 hours before starting a maintenance window.

- Run SDS Health Check procedures as specified in Health Check Procedures
- Upgrade the Primary SDS NOAM, this procedure is used to upgrade the SDS NOAM servers.

> **Note:**
>
> The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 3-7. See section Primary SDS Site or DR SDS Site Upgrade Execution Overview for more details before proceeding.

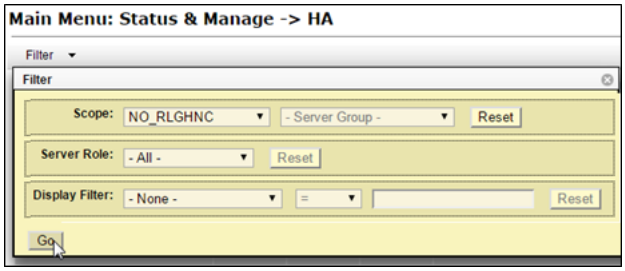
1. Log in to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP GUI, expand **Status & Manage** click **HA**
3. Click **Filter**

Figure 8-1 Filter



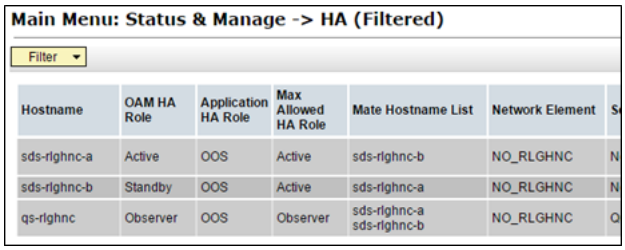
4. Locate the primary SDS NOAM NE, using the information provided in section Logins, Passwords, and Site Information, select the primary SDS NOAM Network Element from the **Scope** field. Click **Go**.

Figure 8-2 Scope



5. Identify servers and record server names, identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 8-3 Identify Server

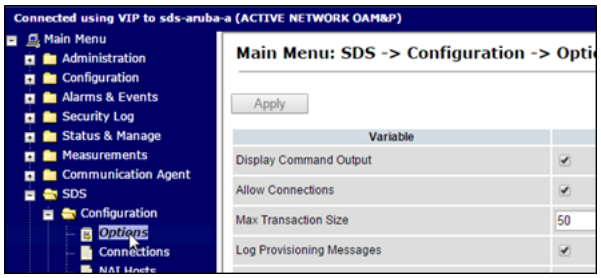


Note the following information:

- Active Primary SDS NOAM.
- Standby Primary SDS NOAM.
- Primary Query Server (if equipped).

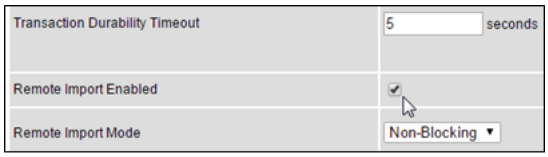
6. Expand **SDS** select **Configuration** click **Options**.

Figure 8-4 Options



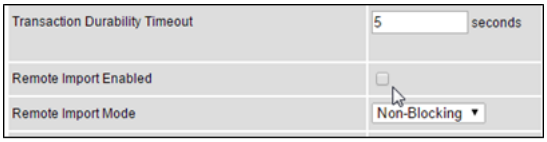
7. Locate the **Remote Import Enabled** check box and record the pre-upgrade state.

Figure 8-5 Remote Import Enabled



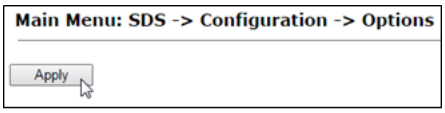
8. Un-check the **Remote Import Enabled** check box if it was checked previously.

Figure 8-6 Uncheck



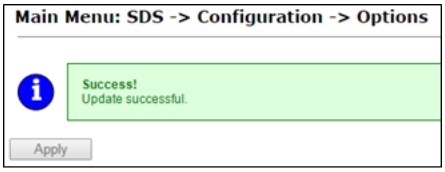
9. Apply the changes and verify the same.

Figure 8-7 Apply



10. Verify the successful response in the banner.

Figure 8-8 Success Banner



11. Upgrade the Standby Primary SDS NOAM server, upgrade the Standby Primary SDS NOAM server (as identified and recorded in step 5 of this procedure) using Upgrade Server Administration on SDS 9.0.
12. Access the active primary SDS NOAM, use the VIP address to log into the active primary SDS NOAM with the `admusr` account.

```
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
```

13. 1. Verify if the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM** and **Query Server**, if equipped.

```
[admusr@sds-rlghnc-a ~]$ sudo irepstat -w
-- Policy 0 ActStb [DbReplication]
```

```
AA To   sds-rlghnc-b      Active   0   0.25 1%R 0.05%cpu 47B/s
AA To   qs-rlghnc         Active   0   0.25 1%R 0.05%cpu 56B/s
AA To   sds-mrsvnc-a      Active   0   0.50 1%R 0.04%cpu 47B/s
AB To   kauai-sds-SO-b    Active   0   0.50 1%R 0.04%cpu 63B/s
AB To   florence-sds-SO-a Active   0   0.51 1%R 0.03%cpu 65B/s
AB To   turks-sds-SO-b    Active   0   0.50 1%R 0.04%cpu 65B/s
irepstat (  8 lines) (h)elp
```

14. 2. If a **DbReplication** status is received as **Audit**, then repeat the command until **Active** status is returned.

> **Note:**
>
> Do not proceed until the status is **Active**. Check Replication is showing as Active for the standby primary SDS NOAM, Query server, active DR SDS NOAM, and standby DR SDS NOAM (if equipped).

15. Repeat the step until the status is **Active** for all the mentioned servers.

> **Note:**
>
> If a **DbReplication** status is received as **Audit** or some other value for these servers, repeat this step until a status of **Active** is returned. Servers are:
>
> - Standby Primary SDS NOAM
> - Query Server
> - Active DR SDS NOAM
> - Standby DR SDS NOAM

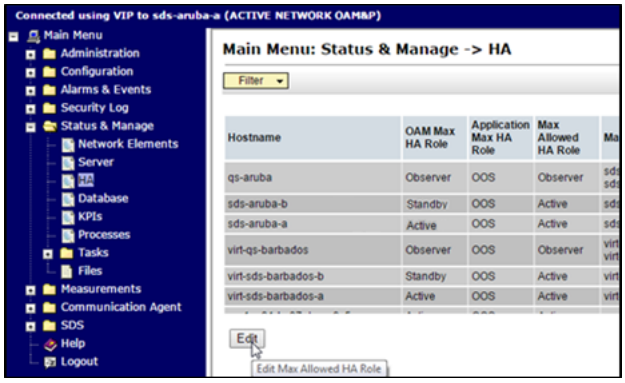
Contact My Oracle Support for any assistance.

16. Exit the CLI prompt for the Active Primary SDS NOAM.

```
[admusr@sds-rlghnc-a filemgmt]$ exit
logout
```

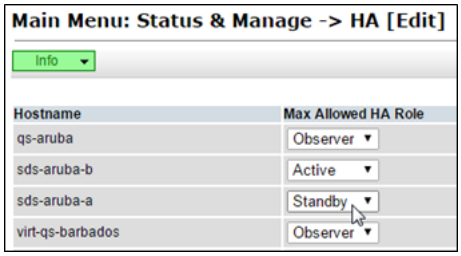
17. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
18. In the Primary SDS NOAM VIP, edit the server. Expand **Status & Manage** click **HA**.
19. Click **Edit**.

Figure 8-9 Edit Server



20. Change Max Allowed HA Role status, select the **Active Primary SDS NOAM** server and change a **Max Allowed HA Role** value from **Active** to **Standby**.

Figure 8-10 Standby



Click **OK**. The users GUI session ends as the active primary SDS server goes through HA fail over and becomes the standby server.

21. 3. If an automatic log out of the GUI does not happen, click **Logout** to log out of the SDS NOAM GUI.

Figure 8-11 Log out

22. In the 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.

    Follow this procedure:

    a. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers).

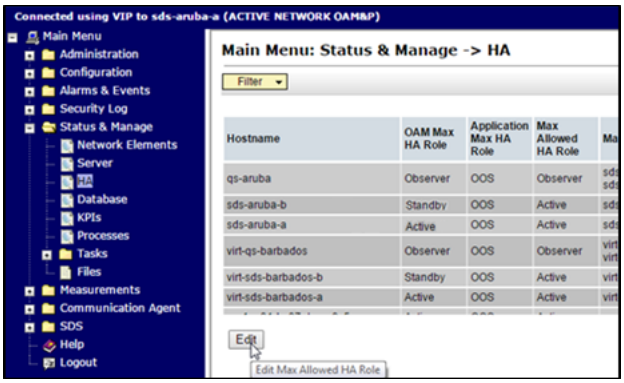
    b. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, so on). Other browsers may label these objects differently.

c. Clear the cached data.

> **Note:**
>
> Do NOT proceed until the browser cache has been cleared.

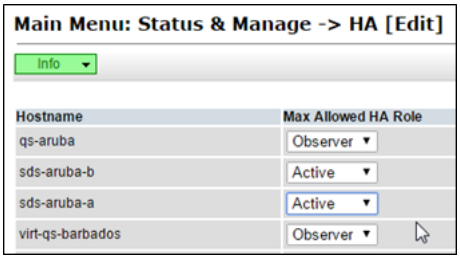
23. Log in to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
24. In the Primary SDS NOAM VIP, edit the server. Expand **Status & Manage** click **HA**.
25. Click **Edit**.

Figure 8-12 Edit Server



26. Change Max Allowed HA Role status, select the **Standby Primary SDS NOAM** server and change a **Max Allowed HA Role** value from **Standby** to **Active** .

Figure 8-13 Active



Click **OK**.

27. In the Primary SDS NOAM VIP, verify the change to Active state. Verify the **Max Allowed HA Role** value has been updated to **Active** for the **Standby Primary SDS NOAM** server.

Figure 8-14 Max Allowed HA Role

Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mat
qs-aruba	Observer	OOS	Observer	sds sds
sds-aruba-b	Active	OOS	Active	sds
sds-aruba-a	Standby	OOS	Active	sds
virt-qs-barbados	Observer	OOS	Observer	virt- virt-

28. If the server in topology shows as an **Out of Service** state, perform a **CmHA** restart, otherwise, proceed to the next step. Refer to Workaround to Resolve Server HA Failover Issue for more information.

> **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.

29. Upgrade the current Standby Primary SDS NOAM server (as identified and recorded in step 5 of this procedure) using Upgrade Server Administration on SDS 9.0.
30. Upgrade the Primary Query server (as identified and recorded in step 5 of this procedure) using Upgrade Server Administration on SDS 9.0.

> **Note:**
>
> If the Query server status is not reported on the **Status and Manage** server screen, refer to Workaround to Fix DNS Issue for more details.

31. Verify status, perform a replication check as explained in step 13.

> **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.

32. Proceed to step 42 for remote import.
33. In the Primary SDS NOAM VIP (CLI), log in using the VIP address, log into the **Active Primary SDS NOAM** with the `admusr` account.

```
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
```

34. Verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM**, **Query Server**, **Active DR SDS NOAM**, and **Standby NOAM servers** (if equipped).

```
[admusr@sds-rlghnc-a ~]$ sudo irepstat -w
-- Policy 0 ActStb [DbReplication]
AA To sds-rlghnc-b      Active  0  0.25 1%R 0.05%cpu 47B/s
AA To qs-rlghnc         Active  0  0.25 1%R 0.05%cpu 56B/s
AA To sds-mrsvnc-a      Active  0  0.50 1%R 0.04%cpu 47B/s
AB To kauai-sds-SO-b    Active  0  0.50 1%R 0.04%cpu 63B/s
AB To florence-sds-SO-a Active  0  0.51 1%R 0.03%cpu 65B/s
AB To turks-sds-SO-b    Active  0  0.50 1%R 0.04%cpu 65B/s
irepstat (  8 lines) (h)elp
```

35. Repeat the step until the status is **Active** for all mentioned servers.

> **Note:**
>
> If a DbReplication status is received as **Audit** or some other value for these servers, repeat this step until a status of **Active** is returned. Servers are:
>
> - Standby Primary SDS NOAM
> - Query Server
> - Active DR SDS NOAM
> - Standby DR SDS NOAM

Contact My Oracle Support for assistance.

36. Exit the CLI for the Active Primary SDS NOAM.

```
[admusr@sds-rlghnc-a filemgmt]$ exit
logout
```

37. Verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM**, **Query Server**, **DR Site Active**, and **Standby NOAM** servers (if equipped).
38. Repeat step 13 to step 16 to verify **irepstat** is showing Active.
39. Ensure the replication is **Active** for the **Standby Primary SDS NOAM, Query Server, Active DR SDS NOAM**, and **Standby DR SDS NOAM** servers (if equipped).
40. If the server in topology shows as an Out of Service state, perform a **CmHA** restart; otherwise, proceed to the next step. Refer Workaround to Resolve Server HA Failover Issue for more information.

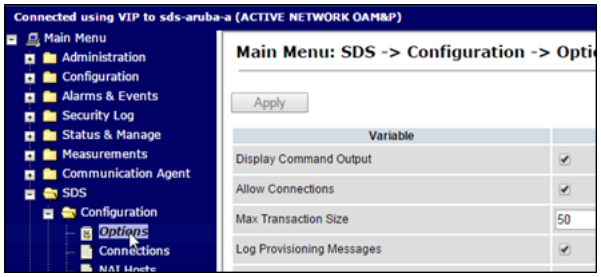
> **Note:**
>
> You will see Out of Service state on the server on which **CmHA** restart is performed. Ignore this state and continue with the upgrade.

41. In the Primary SDS NOAM VIP, verify status. Perform a replication check as explained in step 34.

> **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.

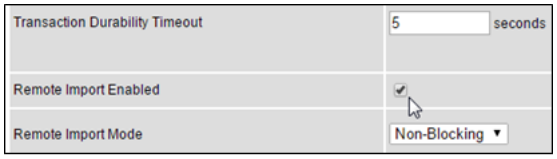
42. In the Primary SDS NOAM VIP, re-enable provisioning Remote Import (if applicable). Re-enable the **Remote Import Enabled** check box if the check box recorded in step 7 of this procedure was Checked. If the **Remote Import Enabled** check box recorded in step 7 of this procedure was not checked, then this procedure is complete.
43. Expand **SDS** select **Configuration** click **Options**

Figure 8-15 Options



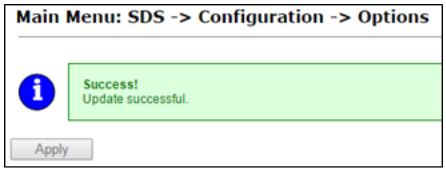
44. Locate the **Remote Import Enabled** check box and check mark it.

Figure 8-16 Remote Import Enabled



45. In the Primary SDS NOAM VIP, apply change and verify. Click **Apply**. Verify the successful response in the banner.

Figure 8-17 Success Banner



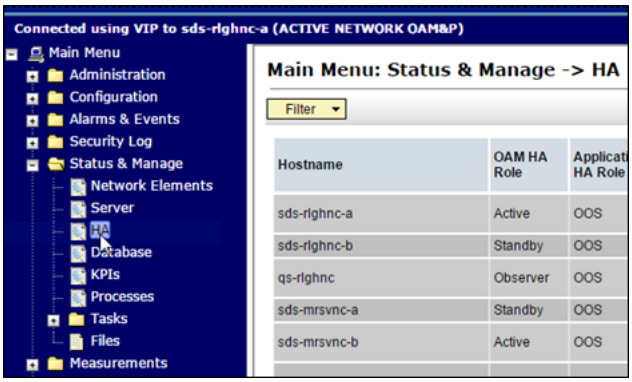
8.2 Upgrade DR SDS NOAM

This procedure upgrades the DR SDS NOAM servers.

> **Note:**
>
> The order of the upgrade for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 3-7. See section Primary SDS Site or DR SDS Site Upgrade Execution Overview for more details before proceeding.

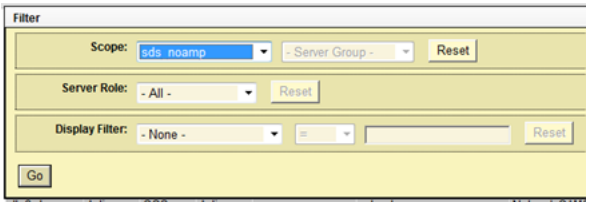
1. Log in to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP GUI, record name of DR SDS NE site. Expand **Status & Manage** click **HA**
3. Click **Filter**

Figure 8-18 Filter



4. In the primary SDS NOAM NE list servers, using the information provided in section Logins, Passwords, and Site Information, select the DR SDS NOAM Network Element from the **Scope** field. Click **Go**.

Figure 8-19 Scope



5. Identify servers and record server names, identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 8-20 Identify 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

Note the following information:

- Active DR SDS NOAM.
- Standby DR SDS NOAM.
- DR SDS Query Server (if equipped)

6. In the Primary SDS NOAM VIP, upgrade the **Standby DR SDS NOAM** server (as identified and recorded in step 5 of this procedure) using Upgrade Server Administration on SDS 9.0.
7. The next two steps of this procedure can be run in parallel using the **Upgrade Server** option.
8. In the Primary SDS NOAM VIP, upgrade the **Active DR SDS NOAM** server (as identified and recorded in step 5of this procedure) using Upgrade Server Administration on SDS 9.0.

> **Note:**
>
> This causes an HA activity fail over to the mate primary SDS NOAM server. This happens a couple minutes after initiating the upgrade.

9. Upgrade the DR SDS Query server (as identified and recorded in step 5 of this procedure) using Upgrade Server Administration on SDS 9.0.

8.3 Perform Health Check (Primary or 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.

Run SDS Health Check procedures as specified in Health Check Procedures.

8.4 SNMP Configuration Update (Post Primary or DR NOAM Upgrade)

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

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

This can be checked by navigating to **Administration** selecting **Remote Servers** and clicking **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 9-1 Site Upgrade Planning — Automated vs. Manual Upgrade

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

9.1 Automated Site Upgrade

Before executing this procedure, contact My Oracle Support.

Before upgrading, users must perform the system Health Check as described in Health Check Procedures. 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.

Note:

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.

Note:

If a procedural step fails to run successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact My Oracle Support 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 host names.
- 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, tool bars, and button layouts.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade logs the information. For procedures, which are run multiple times, the technician has to keep a track of each additional iteration performed.

Retention of captured data is required as a future support reference if this procedure is run 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 have run multiple times, it must run at least once within the period of 24-36 hours before starting a maintenance window.

Run SDS Health Check procedures as specified in Health Check Procedures.

9.1.2 Upgrade SOAM

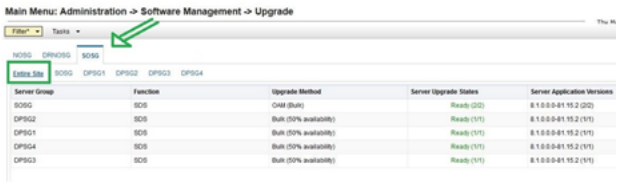
The following procedure details how to upgrade SDS SOAM sites.

> **Note:**
>
> 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.

1. This step verifies the servers and server groups to be upgraded are in the proper state. Review site upgrade plan and site readiness.
   a. Log into the NOAM GUI using the VIP.
   b. Expand **Administration** select **Software Management** click **Upgrade**.
   c. Select the SOAM tab of the site to be upgraded.
   d. 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.

Figure 9-1 Upgrade

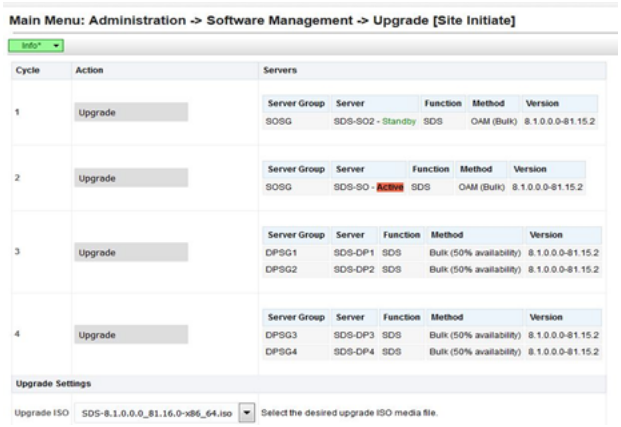


> **Note:**
>
> The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including **Accept or Reject**, **Ready**, **Backup Needed**, **Failed**, or **Not Ready**. Only the servers in the Ready state or Failed state are upgrade eligible.

2. In the Active NOAM VIP, initiate the site upgrade. Verify no Server Groups are selected on the upgrade administration screen. The **Site Upgrade** button is not available if a Server Group is selected. Click **Site Upgrade**.

   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.

Figure 9-2 Upgrade



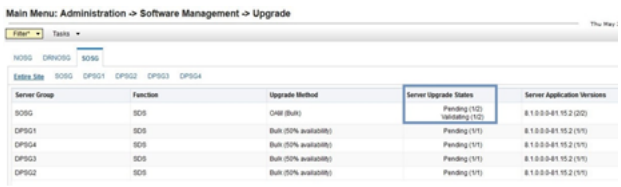
> **Note:**
>
> If you need to rearrange the upgrade cycle, see section Rearrange Automate Site Upgrade Cycles.

3. In the Upgrade Settings section of the form, use the **Upgrade ISO** option to select the target ISO. Click **OK** to start the upgrade sequence. Control returns to the Upgrade Administration screen.
4. In the Active NOAM VIP, view In-Progress Status. In **View the Upgrade Administration** form Monitor the upgrade progress. See step 5 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.

Figure 9-3 Monitor Progress



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.

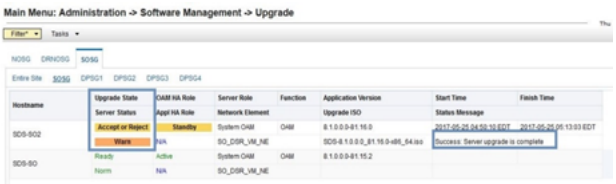
> **Note:**
>
> Not all servers have all alarms:**Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)**
>
> - Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)
> - Alarm ID = 31101 (DB Replication To Slave Failure)
> - Alarm 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 Fail over Inhibited)
> - Alarm ID = 31114 (DB Replication over SOAP has failed)
> - Alarm ID = 31225 (HA Service Start Failure)

Do not accept any upgrades at this time.

Contact My Oracle Support for any assistance. Refer Recover from a Failed Upgrade for failed server recovery procedures.

5. Upon completion of a successful upgrade, every server in the site is in the **Accept** or **Reject** state.

Figure 9-4 Server State



6. In the Server CLI, if the upgrade of a server fails, access the server command line (using SSH or a console), and collect the following files:
   - /var/TKLC/log/upgrade/upgrade.log
   - /var/TKLC/log/upgrade/ugwrap.log
   - /var/TKLC/log/upgrade/earlyChecks.log
   - /var/TKLC/log/platcfg/platcfg.log

   Contact My Oracle Support for assistance. Refer to Upgrade Server Administration on SDS 9.0 for failed server recovery procedures.

7. Update the tuned profile, after successful upgrade has been verified above, access each of the servers on command line (using SSH or console), and update the tuned profile:

   ```
   $ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh
   ```

   Verify whether tuned profile has been successfully set to **comcol_app**:

   ```
   $ sudo tuned-adm active
   ```

   Sample Output:

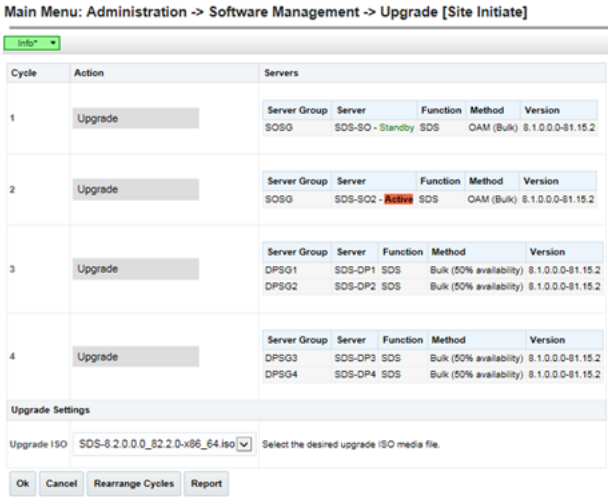
   ```
   [admusr@SOAM1 ~]$ sudo tuned-adm active
   Current active profile: comcol_app
   Service tuned: enabled, running
   Service ktune: enabled, running
   [admusr@SOAM1 ~]$
   ```

9.1.3 Rearrange Automate Site Upgrade Cycles

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

1. In the Active NOAM VIP rearrange the upgrade cycle as needed, click **Rearrange Cycles**.

Figure 9-5 Rearrange Cycles

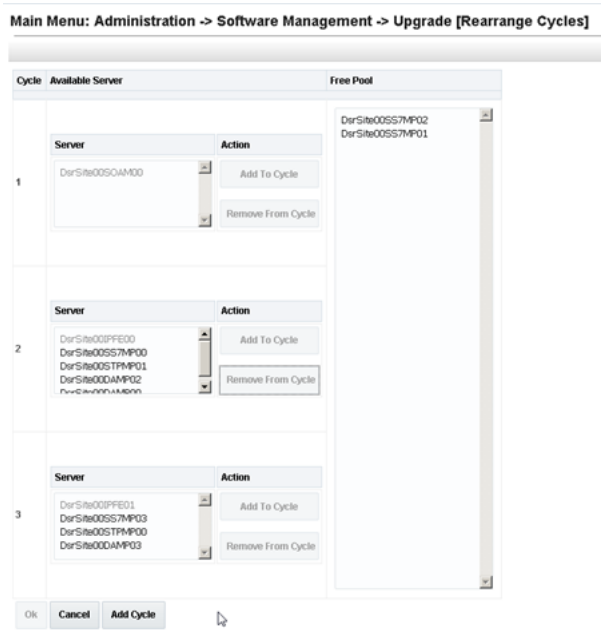


2. Click **Rearrange Cycles** on the Upgrade screen to rearrange servers.

Figure 9-6 Upgrade Rearrange Cycles

3. When a server needs to be removed from cycle and needs to be added in an existing cycle or a new cycle, select the desired server in the list and click **Remove from Cycle**. The server moves to the Free Pool on the right side.

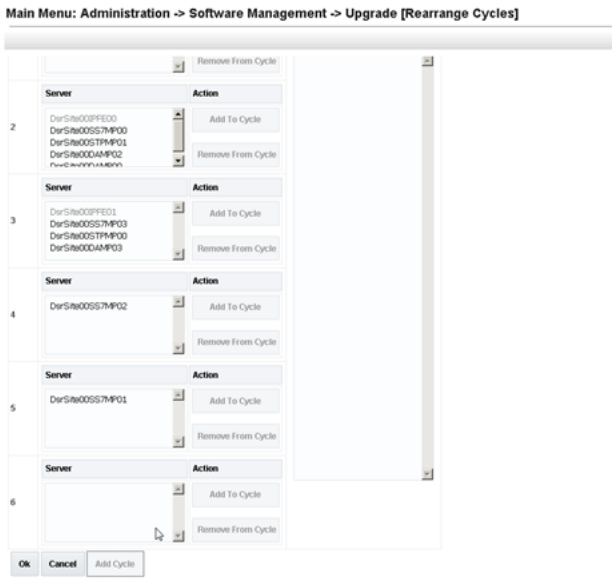
Figure 9-7 Remove from Cycle



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

4. This 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. Click **Add Cycle**.

Figure 9-8 Add Cycle



After adding new cycle, servers available in free pool can be added in new cycle.

5. 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. Run SDS Health Check procedures as specified in Health Check Procedures

9.2 SOAM Upgrade Execution (Manual and Automated Server Group)

Before executing this procedure, contact My Oracle Support.

Before upgrading, users must perform the system Health Check as described in Health Check Procedures. 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.

> **Note:**
>
> 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.

Note:

If a procedural step fails to run successfully or fails to receive the desired output, **STOP** the procedure. It is recommended to contact My Oracle Support 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 host names.
- 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, tool bars, and button layouts.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade logs the information. For procedures, which are run multiple times, the technician has to keep a track of each additional iteration performed.

Retention of captured data is required as a future support reference if this procedure is run 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 run multiple times, but must also be run at least once within the period of 24-36 hours before starting a maintenance window. Run SDS Health Check procedures as specified in Health Check Procedures

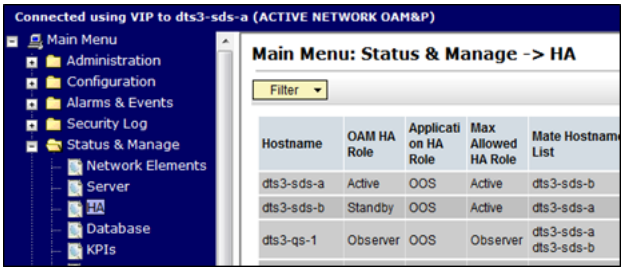
9.2.2 Upgrade SOAM

The following procedure details how to upgrade SDS SOAM sites.

> **Note:**
>
> 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.

1. In the SDS NOAM GUI, log in using the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM)
2. In the Primary SDS NOAM VIP (GUI), record name of the SOAM NE site. Expand **Status & Manage** click **HA**. Click **Filter**.

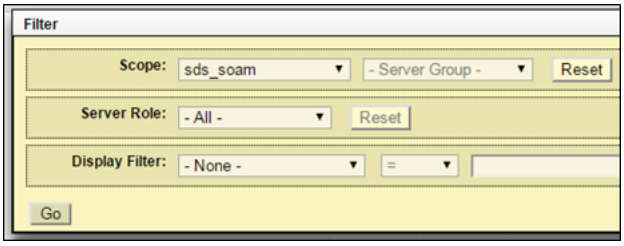
Figure 9-9 Filter



Using the information provided in section Logins, Passwords, and Site Information record the name of the SOAM NE site.

3. In the Primary SDS NOAM VIP, list servers. Using the information provided in section Logins, Passwords, and Site Information select the primary SDS SOAM Network Element from the **Scope** field. Click **Go**.

Figure 9-10 Scope



4. Identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 9-11 Identify Servers

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 the following SOAM NE site servers:

- Active SOAM Server
- Standby SOAM Server
- DP 1 Server
- DP 2 Server
- DP 3 Server
- DP 4 Server
- DP 5 Server
- DP 6 Server
- DP 7 Server
- DP 8 Server
- DP 9 Server
- DP 10 Server

5. Upgrade the Standby SOAM server (as identified and recorded in step 4 of this procedure) using Upgrade Server Administration on SDS 9.0.

> **Note:**
>
> If using the **Auto Upgrade** option, SOAM servers are upgraded serially (standby then active).

6. Upgrade the Standby SOAM server (as identified and recorded in step 4 of this procedure) using Upgrade Server Administration on SDS 9.0.

> **Note:**
>
> Half 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 Upgrade Server Administration on SDS 9.0

7. In the Primary SDS NOAM VIP, upgrade up to half of the installed DP servers in parallel. Upgrade up to half (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 Upgrade Server Administration on SDS 9.0.
8. 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 Upgrade Server Administration on SDS 9.0.

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. Run SDS Health Check procedures as specified in Health Check Procedures

9.3 Post Upgrade Procedures

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

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

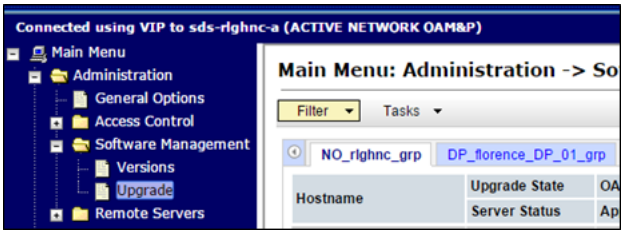
9.3.1 Accept the Upgrade

The upgrade needs either to be accepted or rejected before any subsequent upgrades may be performed in the future. The **Event ID: 32532Server Upgrade Pending Accept/Reject** displays for each server until **Accept** or **Reject** is performed.

> **Note:**
>
> 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 back out to the previous release.

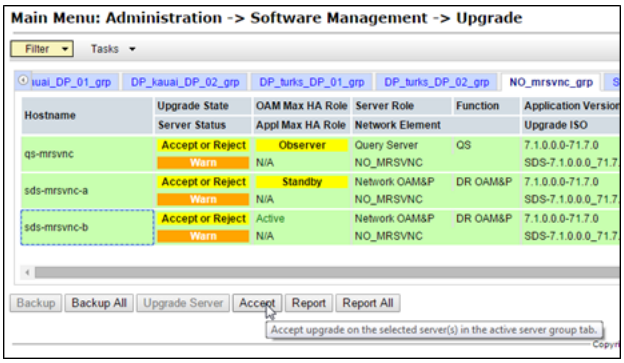
1. Log in to the SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP, accept the upgrade. Expand **Administration** select **Software Management** click **Upgrade**.

Figure 9-12 Upgrade



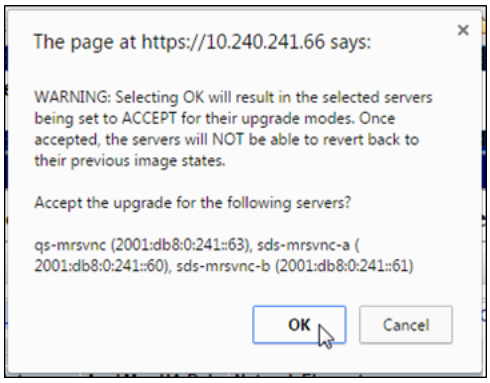
3. Select the Server Group tab containing the server(s) to **Accept** the upgrade.
4. Press and hold the **Ctrl** key to select multiple server(s) in the server group.
5. Click **Accept**.

Figure 9-13 Accept



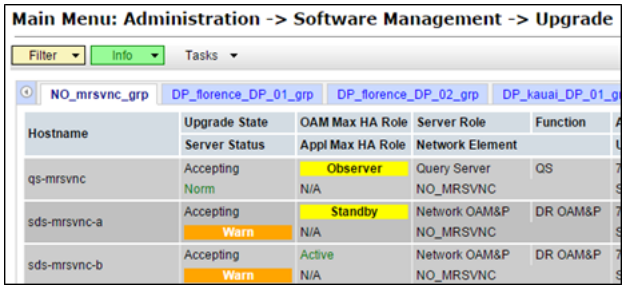
6. In the Primary SDS NOAM VIP, monitor status. Click **OK** to confirm.

Figure 9-14 Monitor Status



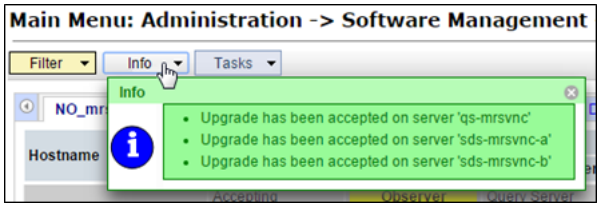
7. The **Upgrade State** changes to **Accepting**.

Figure 9-15 Upgrade State



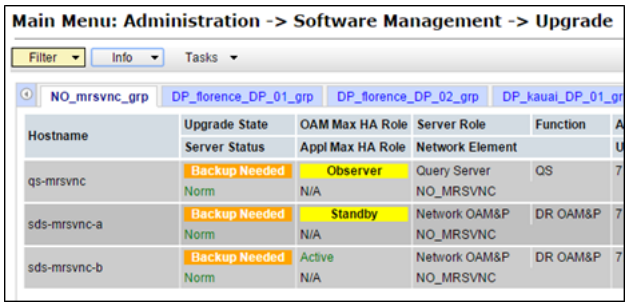
8. The banner displays an **Upgrade has been accepted on** message for each server.

Figure 9-16 Accept Upgrade



9. Primary SDS NOAM VIP, monitor status. The **Upgrade State** changes to **Backup Needed**.

Figure 9-17 Backup Needed

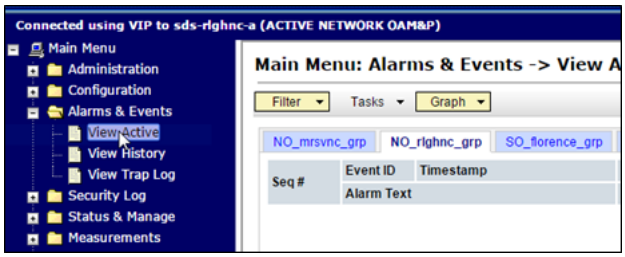


> **Note:**
>
> The **Backup Needed Upgrade State** is expected to remain until the next software upgrade is performed. Do not re-run COMCOL backups except when directed to do so during the upgrade process.

> **Note:**
>
> 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.

10. In the Primary SDS NOAM VIP, repeat steps 2 up to 9 of this procedure for each additional Server Group tab until the upgrade has been accepted on all servers in the SDS topology.
11. In the Primary SDS NOAM VIP, verify upgrade acceptance. Expand **Alarms & Events** click **View Active**.

Figure 9-18 View Active Alarms



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 8.0 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 (Accept the Upgrade).

- The SOAM VM profile update applies only to SDS 8.0 and later.
- The SOAM VM profile update can be applied only after the upgrade to SDS 8.0/8.1/8.2/8.3/8.4/8.5/8.6 has been accepted.
- The SOAM VM profile update does not apply to VE-DSR and cloud deployments.

Add New SOAM Profile on Existing VM is an independent procedure and may be run 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, run **Add New SOAM Profile on Existing VM** or skip this step.

10
Recovery Procedures

Upgrade procedure recovery issues should be directed to the Oracle's customer care. Before executing any of these procedures, refer to My Oracle Support.

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

> **Note:**
>
> Back out procedures cause traffic loss.

> **Note:**
>
> These recovery procedures are provided for the back out of an upgrade only (for example, for the back out from a failed target release to the previously installed release). Back out of an initial installation is not supported.

> **Note:**
>
> 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. Expand **Administration** select **Software Management** click **Upgrade**.
2. Based on the **Application Version** column, identify all the host names that need to be backed out.
3. Expand **Configuration** click **Servers**.
4. Identify the IMI IP addresses of all the host names identified in step 2. These are required to access the server when performing the back out.

The reason to run a back out has a direct impact on any additional back out preparation that must be done. The back out procedure causes traffic loss. All possible reasons cannot be predicted ahead of time.

> **Note:**
>
> Verify the two backup archive files created in using Full Database Back up (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 file names from other database backup files.

The file names 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 back out can only be run once all necessary corrective setup steps have been taken to prepare for the back out. Contact My Oracle Support 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:

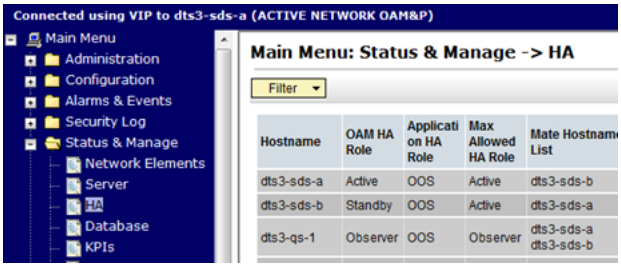
- Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
- Alarm ID = 31109 (Topology config error)
- Alarm ID = 31114 (DB Replication over SOAP has failed)
- Alarm ID = 31106 (DB Merge To Parent Failure)
- Alarm ID = 31134 (DB replication to slave failure)
- Alarm ID = 31102 (DB 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 back out for servers in the SOAM NE.

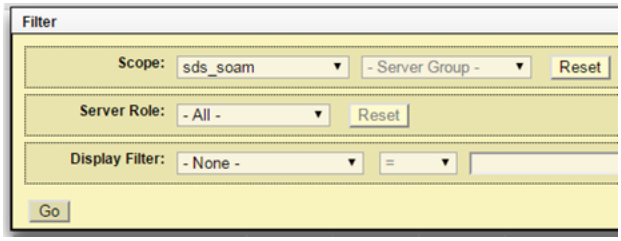
1. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP (GUI), record the name of the SOAM NE site. Expand **Status & Manage** click **HA**. Click **Filter**.

Figure 10-1 Filter



3. In the Primary SDS NOAM VIP, list servers. Using the information provided in Logins, Passwords, and Site Information select the primary SDS SOAM Network Element from the **Scope** field. Click **Go**.

Figure 10-2 Scope



4. Identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 10-3 Identify 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 2 Server
- DP 3 Server
- DP 4 Server
- DP 5 Server
- DP 6 Server
- DP 7 Server
- DP 8 Server

- DP 9 Server
- DP 10 Server

5. In the Primary SDS NOAM VIP, downgrade DP 1 Server (as identified and recorded) in step 4 of this procedure using Back Out a Single Server.
6. Downgrade all remaining DP servers in serial or parallel (as identified and recorded) in step 4 of this procedure using 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. Downgrade the Standby SOAM server (as identified and recorded) in step 4 of this procedure using Back Out a Single Server.

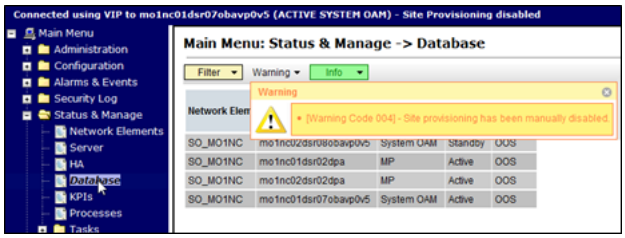
   During the back out, the servers may have the following expected alarms:

   - Alarm ID = 31114 (DB replication over SOAP has failed)
   - Alarm ID = 31282 (HA management fault)

> **Note:**
>
> Do not proceed with the next step until steps 5 through step 7 of this procedure have been successfully completed.

8. Downgrade the Active SOAM server, (as identified and recorded) in step 4 of this procedure using Back Out a Single Server.
9. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
10. This is an optional step, in the SOAM VIP (GUI), enable site provisioning. Use this step, in case Site Provisioning is Disabled. Expand **Status & Manage** click **Database**

Figure 10-4 Database



11. Click **Enable Site Provisioning**.

Figure 10-5 Enable Site Provisioning

12. Click **OK** to confirm.
13. Click **Logout** to log out of the SOAM GUI.

Figure 10-6 Log out

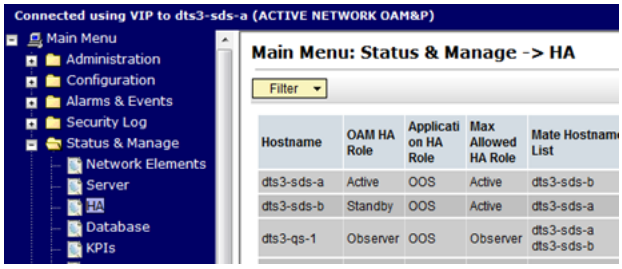
14. In the Primary SDS NOAM VIP, run downgrade for the remaining SOAM NE site(s).Repeat all above steps of this procedure for the remaining SOAM NE site(s) (as identified and recorded in section Logins, Passwords, and Site Information) until all SOAM NE site(s) requiring the downgrade have been backed out.
15. Run Health Check Procedures at this time only if no other server requires the downgrade, else proceed with the next back out procedure.

10.2.2 Back Out the DR SDS NOAM

This procedure is used to back out the DR SDS NOAM.

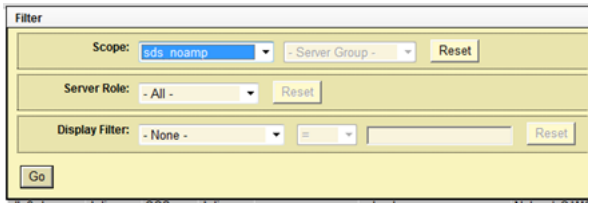
1. Log in to the SDS NOAM GUI. Use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP, record name of DR SDS NE site. Expand **Status & Manage** click **HA**. Click **Filter**.

Figure 10-7 Filter



3. In the Primary SDS NOAM VIP, list servers. Using the information provided in section Logins, Passwords, and Site Information select the DR SDS Network Element from the **Scope** field. Click **Go**.

Figure 10-8 Scope



4. Identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 10-9 Server Information

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

Record the names of primary DR SDS NE site servers:

- Active DR SDS NOAM
- Standby DR SDS NOAM
- DR SDS Query Server (if equipped)

5. Downgrade the Standby DR SDS NOAM server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.

> **Note:**
>
> Do not proceed to the next step until this step of the procedure is successfully completed.

> **Note:**
>
> The next two steps of this procedure may run parallel using the **Upgrade Server** option.

6. Downgrade the DR SDS Query server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.
7. Downgrade the ActiveDR SDS server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.
8. Run Health Check Procedures at this time only if no other servers require the downgrade. Proceed with the next back out procedure.

10.2.3 Back Out the Primary SDS NOAM

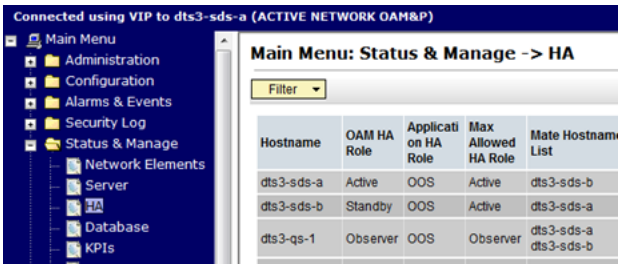
The following procedure details how to perform software back out for servers in the primary SDS NOAM NE.

> **Note:**
>
> The order of the back out for the primary NOAM NE and DR NOAM NE needs to be followed as shown in Table 3-10. See section Recovery Procedures Overview for more details before proceeding.

1. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).

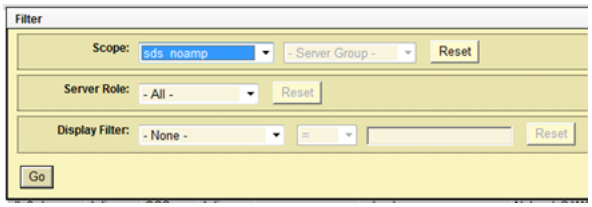
2. In the Primary SDS NOAM VIP, expand **Status & Manage** click **HA**. Click **Filter**.

Figure 10-10 Filter



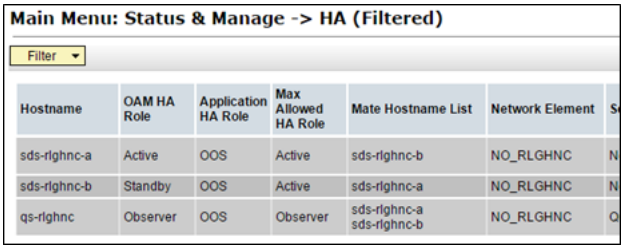
3. In the Primary SDS NOAM VIP, locate the primary SDS NOAM NE. Using the information provided in section Logins, Passwords, and Site Information, select the primary SDS Network Element from the **Scope** field. Click **Go**.

Figure 10-11 Scope



4. Identify each server by Host name, Server Role, and OAM HA Role and record the name of each server.

Figure 10-12 Identify Servers



Record the following information:

- Active Primary SDS NOAM
- Standby Primary SDS NOAM
- Primary SDS Query Server (if equipped)

5. Downgrade Standby Primary SDS NOAM server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.

6. In the 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.

```
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 ~]$
```

7. In the Primary SDS NOAM VIP, verify the **DbReplication** status is **Active** for the **Standby Primary SDS NOAM** and **Query Server**, if equipped.

```
[admusr@sds-rlghnc-a ~]$ sudo irepstat -w
-- Policy 0 ActStb [DbReplication]
AA To  sds-rlghnc-b      Active  0  0.25 1%R 0.05%cpu 47B/s
AA To  qs-rlghnc         Active  0  0.25 1%R 0.05%cpu 56B/s
AA To  sds-mrsvnc-a      Active  0  0.50 1%R 0.04%cpu 47B/s
AB To  kauai-sds-SO-b    Active  0  0.50 1%R 0.04%cpu 63B/s
AB To  florence-sds-SO-a Active  0  0.51 1%R 0.03%cpu 65B/s
AB To  turks-sds-SO-b    Active  0  0.50 1%R 0.04%cpu 65B/s
irepstat (  8 lines) (h)elp
```

8. If a **DbReplication** status is **Audit** is received, then repeat the command until **Active** is returned.

> **Note:**
>
> Do not proceed until the status is **Active**. Check Replication is showing **Active** for Standby Primary SDS NOAM, Query Server, Active DR SDS NOAM and Standby DR SDS NOAM (if equipped).

9. Repeat the step until the status is **Active** for all the mentioned servers.

> **Note:**
>
> If a DbReplication status is received as **Audit** or some other value for these servers, repeat this step until a status of **Active** is returned. Servers are:

- Standby Primary SDS NOAM
- Query Server
- Active DR SDS NOAM
- Standby DR SDS NOAM

Contact My Oracle Support for any assistance.

10. Exit the CLI for the ActivePrimary SDS NOAM.

```
[admusr@sds-rlghnc-a filemgmt]$ exit
logout
```

> **Note:**
>
> The next two steps of this procedure can be run in parallel.

11. Downgrade Primary Query server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.
12. Downgrade Active Primary SDS NOAM server (as identified and recorded in step 4 of this procedure) using Back Out a Single Server.

> **Note:**
>
> This causes an HA activity fail over to the mate primary SDS NOAM server. This occurs within a few minutes of initiating the upgrade.

13. Allow system to auto-clear temporary alarm states. Wait up to ten minutes for Alarms associated with server back out to auto clear.

> **Note:**
>
> If PDB Relay was recorded as Enabled in Back Out a Single Server, 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.

14. Run Health Check procedures (Post back out) as specified in Health Check Procedures, if downgrade procedures have been completed for all required servers.

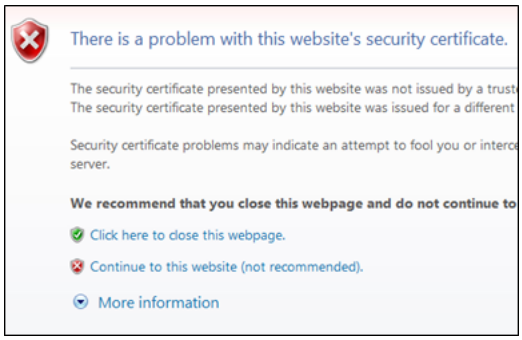
A

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

This procedure describes how to access and log in to the NOAM/SOAM GUI.

1. In the OAM VIP (GUI), log in to the OAM site.
   a. Open an approved web browser (Internet Explorer 8.0, 9.0, or 10.0).
   b. Connect to the XMI virtual IP address (VIP) assigned to the OAM site (primary SDS site or SOAM site.
   c. If a certificate error is received, click **Continue to this website (not recommended)**.

Figure A-1 Website Security



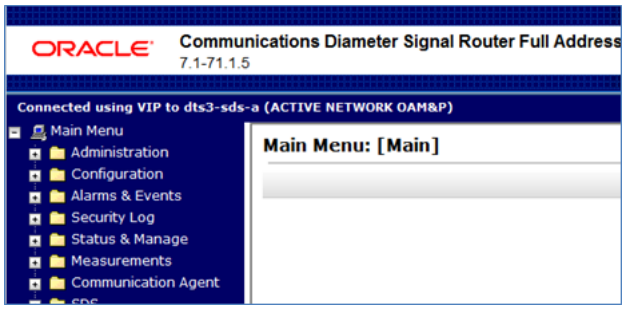
> **Note:**
>
> Not applicable for cloud deployments.

2. In the OAM VIP (GUI), log in using the default user and password.

Figure A-2 Oracle System Log in

3. Verify the connection to the active OAM server and also verify that the browser is using the VIP connected to the active OAM server.

Figure A-3 OAM Server



The source release is 8.x, the Release Banner displays the browser is successfully connected using the Active Network OAM&P. .

Figure A-4 Release Banner

> **Note:**
>
> The message may show the connection to either a **NETWORK OAM&P** or a **SYSTEM OAM** depending on the selected Network Element.

A.1 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.

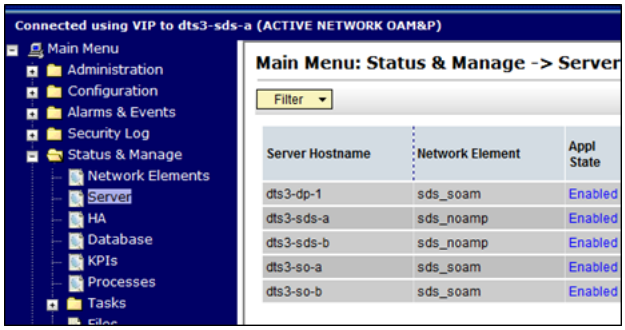
> **Note:**
>
> If syscheck fails on any server during pre-upgrade Checks or in early checks stating that "cpu: FAILURE:: No record in alarm table for FAILURE", see Workaround to Resolve Syscheck Error for CPU Failure.

If the **31201 - Process Not Running** alarm displays, for instance, as cmsoapa, then run Workaround to Fix cmsoapa Restart.

1. In the SDS NOAM GUI, log in use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).

2. In the Primary SDS NOAM VIP, verify status. Expand **Status & Manage** click **Server**.

Figure A-5 Server



3. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).

Figure A-6 Server Status

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.

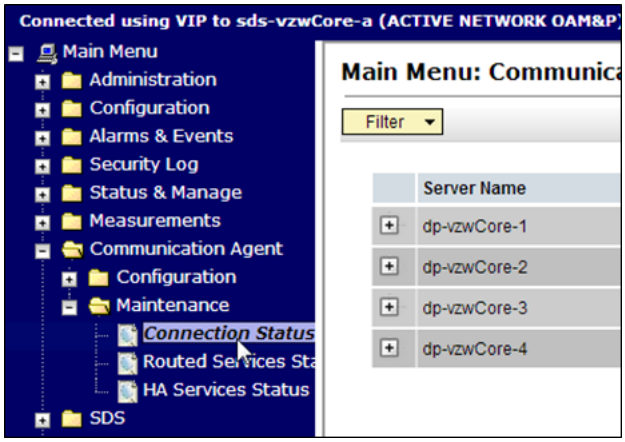
> **Note:**
>
> Post-Upgrade, upgraded servers have an **Alm** status of **Err** due to the **Event ID (s): 32532 Server Upgrade Pending Accept/Reject** expected alarm. This alarm displays until the upgrade is accepted and may be ignored at this time.

> **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 run Workaround to Fix cmsoapa Restart to solve this issue.

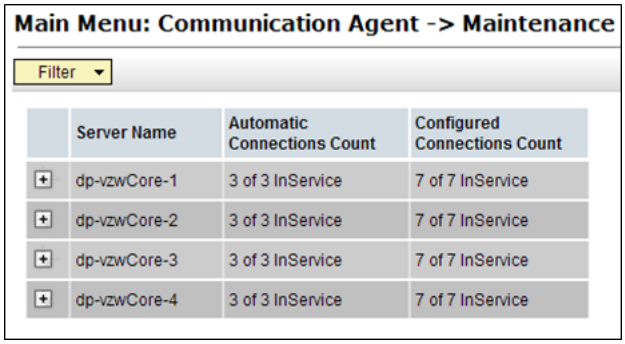
4. In the Primary SDS NOAM VIP, verify connection counts. Expand **Communication Agent** select **Maintenance** click **Connection**.

Figure A-7 Connection



5. Verify all **Connection Counts** show equivalent counts (that is, n of n InService for Automatic or y of y InService for Configured)

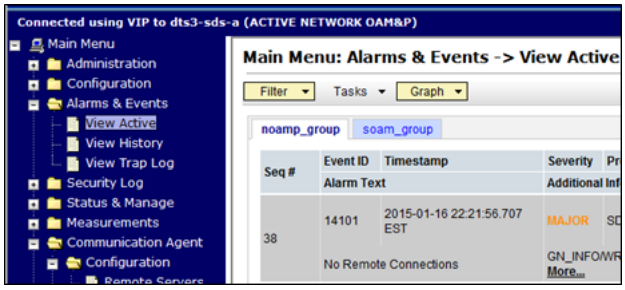
Figure A-8 Maintenance



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

6. In the Primary SDS NOAM VIP, view alarm status. Expand **Alarms & Events** click **View Active**.

Figure A-9 View Active



7. When viewing pre-upgrade status, if any alarms are present, stop and contact My Oracle Support for assistance before attempting to continue.
8. When viewing post-upgrade status, verify the following:

   Active NO server may have the following expected alarms:

   - Alarm ID = 10075 (Application processes have been manually stopped)

   Servers that still have replication disabled have the following expected alarm:

   - Alarm ID = 31113 (Replication Manually Disabled)

   The following alarms may also be seen:

   - Alarm ID = 10010 (Stateful database not yet synchronized with mate database)
   - Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
   - Alarm ID = 31114 (DB Replication over SOAP has failed)
   - Alarm ID = 31225 (HA Service Start Failure)

   Following alarms can be ignored during the upgrade:

   - Alarm ID = 31109 (Topology Config Error)
   - Alarm ID = 31282 (HA Management Fault)
   - Alarm ID = 31283 (Lost Communication with server)
   - Alarm ID = 31106 (DB Merge To Parent Failure)
   - Alarm ID = 31107 (DB Merge From Child Failure)
   - Alarm ID = 10009 (Config and Prov DB not yet synchronized)

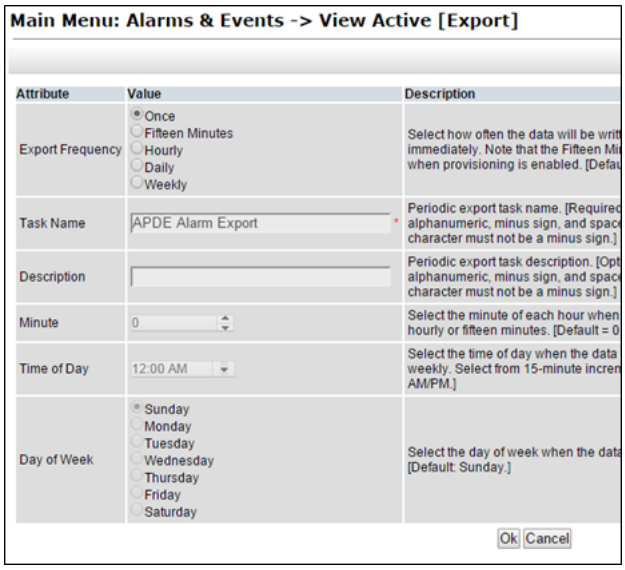
   > **Note:**
   >
   > If Alarm 10009 persists after the upgrade, reboot the server once using the `sudo init 6` command on the effected server.

   These alarms may display until all the NOAM and DR-NOAM servers upgrade has been completed.
9. In the Primary SDS NOAM VIP, create Alarms and Events report. Click **Export**.

Figure A-10 Export

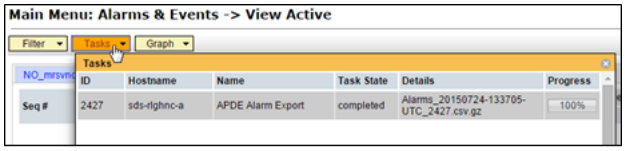
10. Click **OK**.

Figure A-11 OK



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

Figure A-12 Tasks



12. Primary SDS NOAM VIP, record the file names of alarm CSV files. The files have the format `Alarms<yyyymmdd>_<hhmmss>.csv`.

    Record the following files:

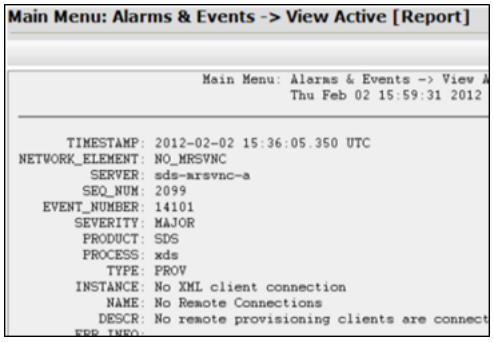
    - Pre-ISO Administration
    - Post-ISO Administration
    - Pre-Primary NOAM Upgrade (MW1)
    - Post-DR NOAM Upgrade (MW1)
    - Pre-SOAM Upgrade (MW2)
    - Post-SOAM Upgrade (MW2)

- Pre-SOAM Upgrade (MW3)
- Post-SOAM Upgrade (MW3)
- Pre-SOAM Upgrade (MW4)
- Post-SOAM Upgrade (MW4)
- Pre-SOAM Upgrade (MW5)
- Post-SOAM Upgrade (MW5)

13. In the Primary SDS NOAM VIP, save the Alarms and Events report. Click **Report**

Figure A-13 Report

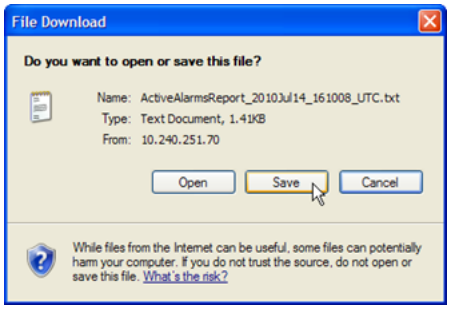
Figure A-14 View Active Alarms



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

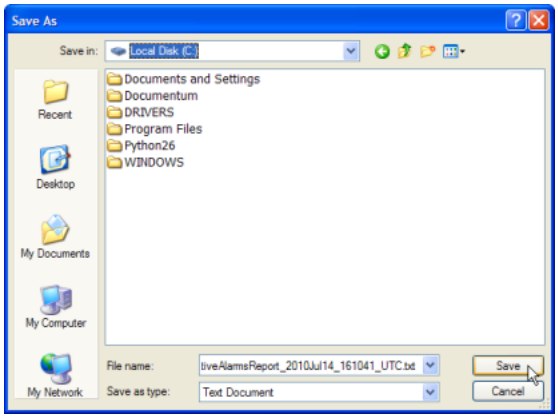
Figure A-15 Save

Figure A-16 Save



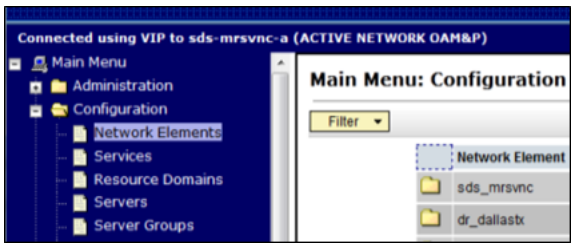
15. Select a directory on a local disk drive to store the active **Alarms and Events** report and click **Save**.

Figure A-17 Save As



16. In the Primary SDS NOAM VIP, create **Network Element** report. Before 8.x, expand **Configuration** click **Network Elements**.

Figure A-18 Network Elements

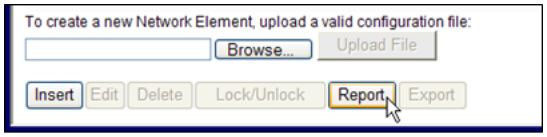


17. Expand **Configuration**, select **Networking** and click **Networks**.

Figure A-19 Networks

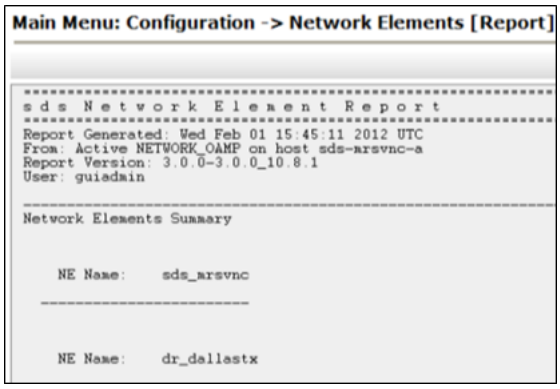
18. Click **Report**.

Figure A-20 Report



19. The **Network Element Report** is generated.

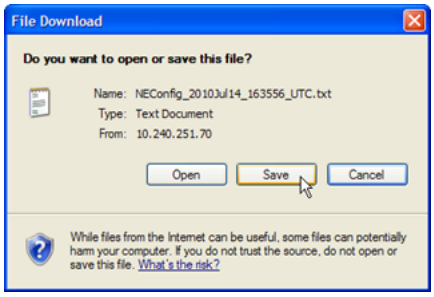
Figure A-21 Network Element Report



20. In the Primary SDS NOAM VIP, save the **Network Element** report. Click **Save** on the **Network Element** report and click **Save** on the File Download screen.

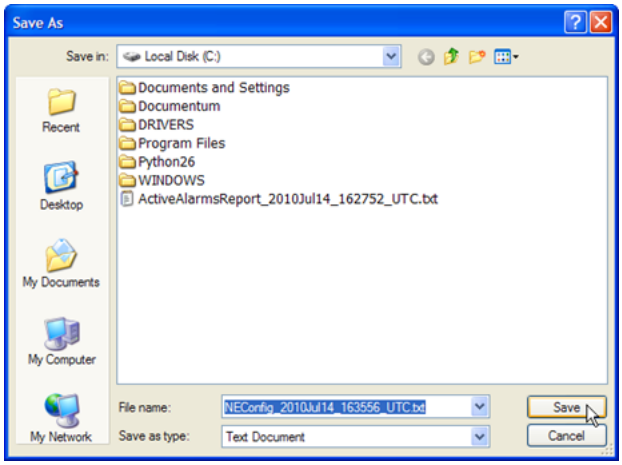
Figure A-22 Save

Figure A-23 Save File



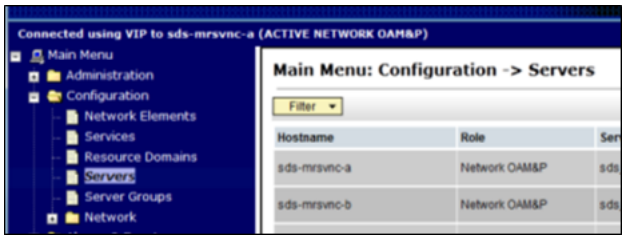
21. Select a directory on a local disk drive to store the **Network Element** report and click **Save**.

Figure A-24 Save As



22. In the Primary SDS NOAM VIP, create the **Servers** report. Expand **Configuration** click **Servers**.

Figure A-25 Servers



23. Click **Report**.

Figure A-26 Report

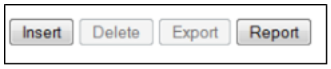
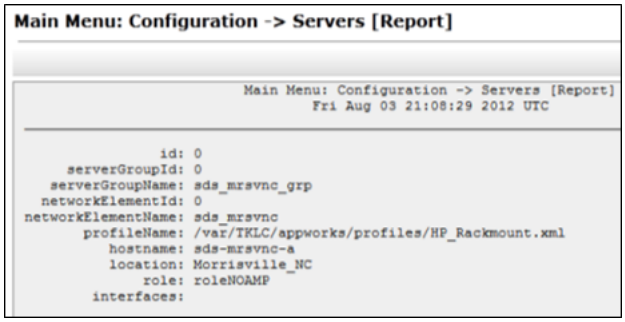


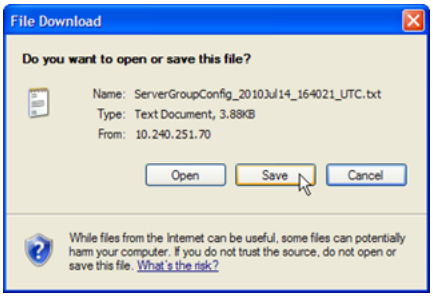
Figure A-27 Server Report



24. In the Primary SDS NOAM VIP, save the Servers report. Click **Save** on the **Servers** report and click **Save** on the File Download screen.

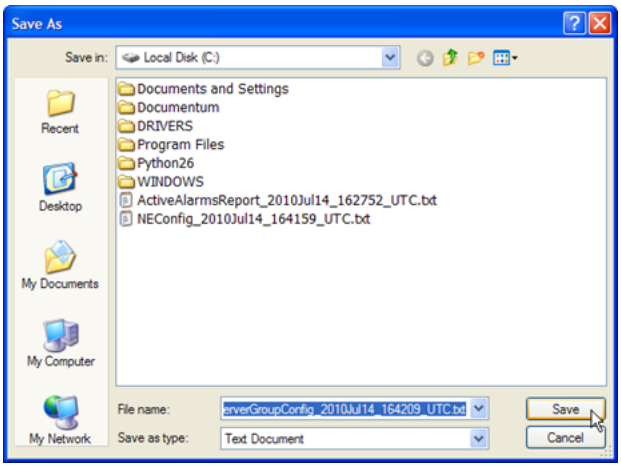
Figure A-28 Save

Figure A-29 Save File



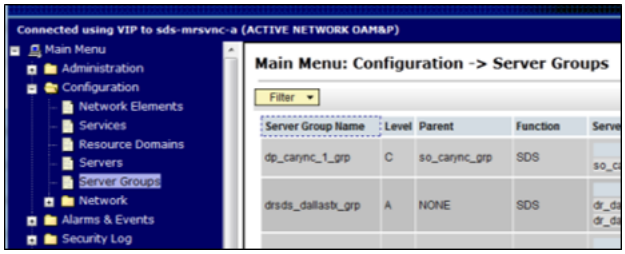
25. Select a directory on a local disk drive to store the **Servers** report and click **Save**.

Figure A-30 Save Server Report



26. In the Primary SDS NOAM VIP, create **Server Groups** the report. Expand **Configuration** click **Server Groups**.

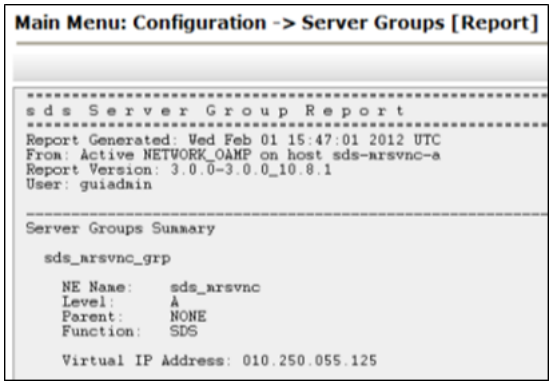
Figure A-31 Server Groups



27. Click **Report**.

Figure A-32 Report

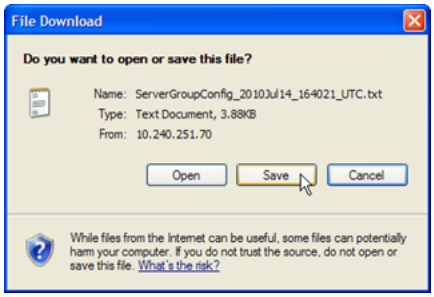
Figure A-33 Sever Groups Report



28. In the Primary SDS NOAM VIP, save the Servers report. Click **Save** on the **Server Groups** report and click **Save** on the File Download screen.

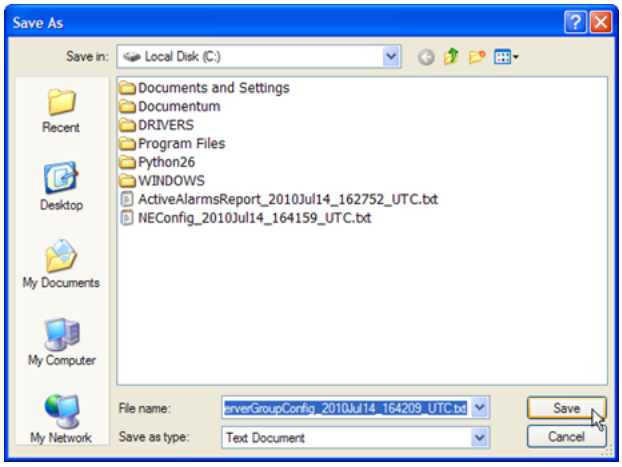
Figure A-34 Save

Figure A-35 Save File



29. Select a directory on a local disk drive to store the **Server Groups** report and click **Save**.

Figure A-36 Save Server Report



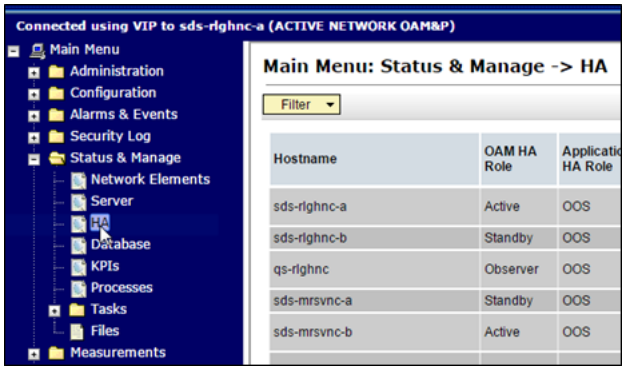
30. Share the saved files with My Oracle Support. If these procedures are run as pre- or post-upgrade health check (HC1/HC2/HC3), sharing the files with My Oracle Support to obtain a proper health check analysis.

    A health check analysis includes verifying the following information collected from Access the OAM GUI Using the VIP (NOAM/SOAM) procedure.

    - Active **Alarms and Events** report.
    - **Network Elements** report.
    - **Server** report.
    - **Server Group** report.

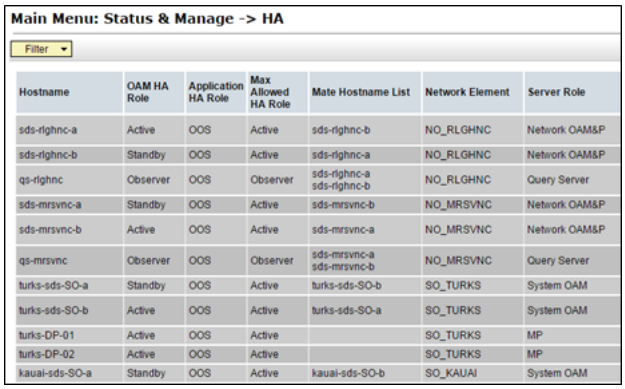
31. Verify OAM HA Role status, expand **Status & Manage** click **HA**

Figure A-37 HA



32. Verify the **OAM HA Role** for all servers shows either **Active** or **Standby**.

Figure A-38 OAM HA Role



> **Note:**
>
> An **OAM HA Role** shown as **Observer** is allowed when the server role is **Query Server**.

33. Verify the **OAM HA Role** for all remaining servers, expand **Main Menu** select **Status & Manage** click **HA**. Scroll through each page until the **OAM HA Role** for has been verified for all servers in the topology.

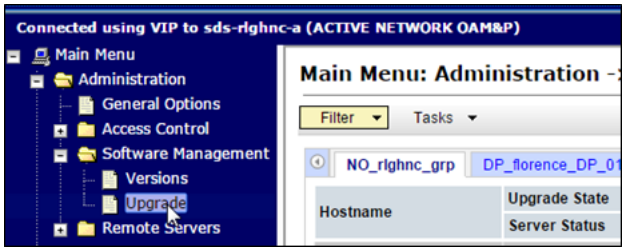
A.2 Upgrade Server Administration on SDS 9.0

> **Note:**
>
> Run this procedure only if **Upgrade State** is **Accept** or **Reject**, unless parallel upgrades are being run.

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

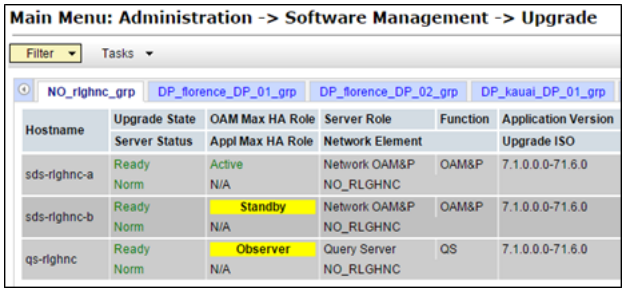
1. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the Primary SDS NOAM VIP, verify status and application version. Expand **Administration** select **Software Management** click **Upgrade**. Select the Server Group tab for the server(s) to be upgraded.

Figure A-39 Upgrade



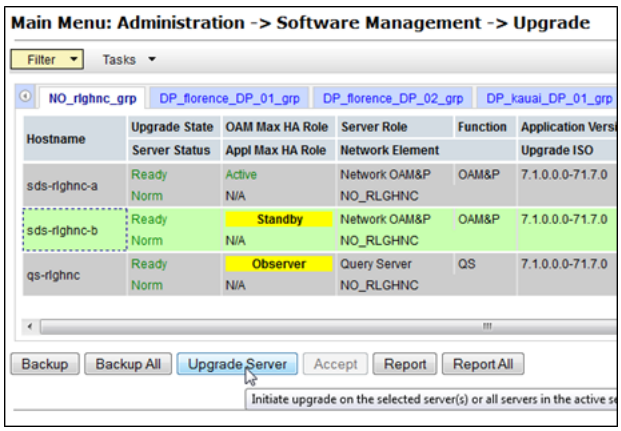
3. Verify the **Upgrade Status** displays as **Ready** for the server(s) to be upgraded. Verify the **Application Version** for the server(s) is the source software release version.

Figure A-40 Application Version



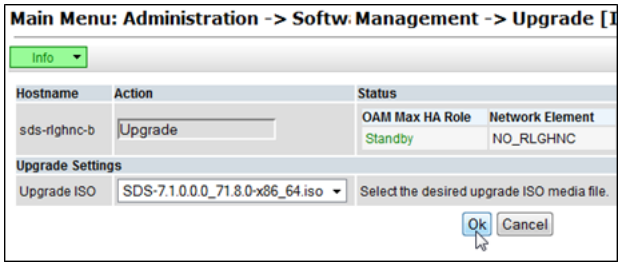
4. If executing Server Group Auto Upgrade, then run step 7 of this procedure. It is allowed for DR NOAM, SOAM, and DP server groups only. If executing Single Server (or multi-selected) upgrade, then continue with the next step of this procedure. This applicable only for primary NOAM and DP server groups.
5. Run this step for single server (or multi-selected) upgrade only. In the Primary SDS NOAM VIP, upgrade server(s). Press and hold the **Ctrl** key to select multiple servers that need to be upgraded. Click **Upgrade Server**.

Figure A-41 Upgrade Server



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

Figure A-42 OK

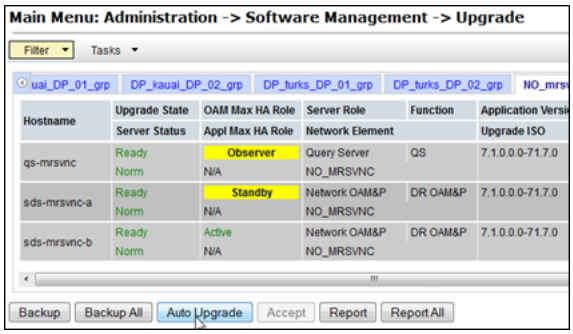


> **Note:**
>
> During the server upgrade, multiple alarms are expected and can be safely ignored. These include but are not limited to Event IDs: 10009, 10073, 10075, 31101, 31102, 31106, 31107, 31109, 31114, 31225, 31282 and 31283. These alarms may display until all the NOAM and DR-NOAM servers upgrade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

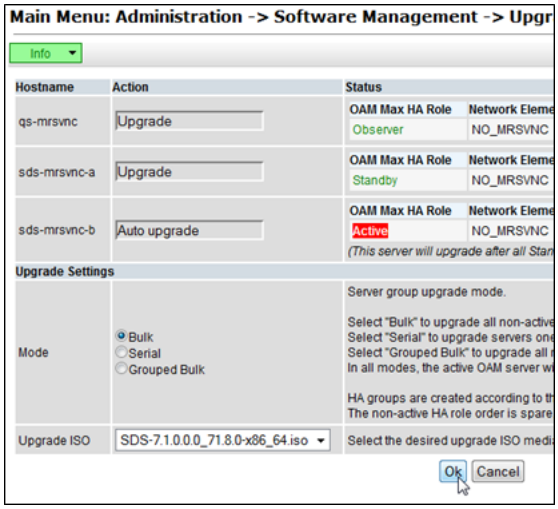
7. Run this step for Server Group **Auto Upgrade** only. Do not use the Auto Upgrade option when upgrading the primary SDS NOAM server group. In the Primary SDS NOAM VIP, upgrade servers. Click **Auto Upgrade**. Do not select any servers with this option.

Figure A-43 Auto Upgrade



8. Select the **Bulk** option. Select the **Upgrade ISO** file to use for the upgrade. Click **OK**.

Figure A-44 Upgrade ISO



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

> **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.

9. If the upgrade procedure is being run for a previously active primary SDS NOAM server (that is 2nd NOAM to be upgraded), then continue with the next step of this procedure, else run step 9 of this procedure.
10. In the 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.
11. Click **Logout** to log out from the SDS NOAM GUI.

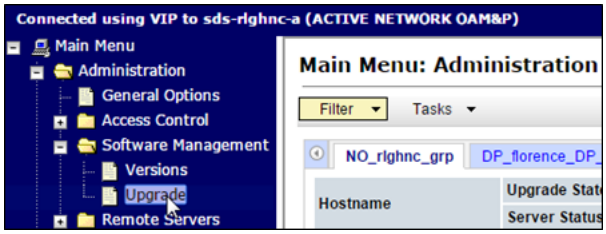
Figure A-45 Log out

12. In the Primary SDS NOAM VIP (GUI), clear the 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:
    a. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers).
    b. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files** and so on). Other browsers may label these objects differently.
    c. Clear the cached data.

> **Note:**
>
> Do not proceed until the browser cache has been cleared.

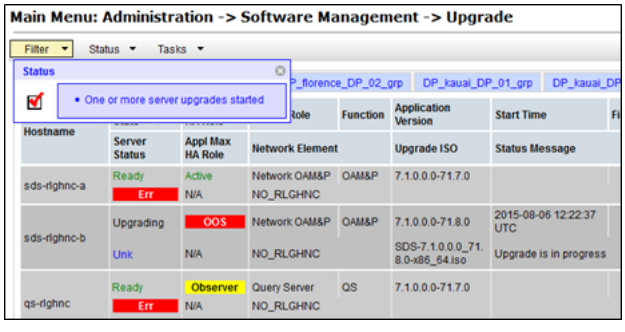
13. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
14. In the Primary SDS NOAM VIP, monitor status expand **Administration** select **Software Management** click **Upgrade**.

Figure A-46 Monitor Status



15. Monitor the **Upgrade State** and the **Status Message** for the servers being upgraded.

Figure A-47 Upgrade State



As the upgrade runs, the following states can be observed:

Table A-1 Status Message

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 Manual Completion of Server Upgrade to restore the server to full operational status and return to this procedure to continue the upgrade.

16. Do not proceed to further steps unless the **Upgrade State** is **Accept** or **Reject** (except in cases where parallel upgrades are being performed).
17. In the primary SDS NOAM VIP, view post upgrade status of the server's. Post-upgrade, the upgraded servers have the **Event ID (s): 32532 (Server Upgrade Pending Accept/ Reject)** expected alarm.
18. In the release Server CLI, update the tuned profile. After a successful upgrade has been verified, access the server on command line (using SSH or console) and update the tuned profile:

    ```
    $ sudo /usr/TKLC/sds/bin/sdsSharedMemTuned.sh
    ```

    Verify whether the tuned profile has been successfully set to **comcol_app**:

    ```
    $ sudo tuned-adm active
    ```

    Sample output:

    ```
    [admusr@SOAM1 ~]$ sudo tuned-adm active
    Current active profile: comcol_app
    Service tuned: enabled, running
    Service ktune: enabled, running
    ```

A.3 Back Out a Single Server

The following procedure performs backout on a single server. Backout can be performed on all upgrades except a major upgrade.

1. In the Primary SDS NOAM VIP, ensure the server to be downgraded is in the **Accept or Reject** state.
2. Expand **Administration** select **Software Management** click **Upgrade**.
3. Select the tab containing the server(s) to be backed out.
4. Verify the Upgrade State is **Accept or Reject**.
5. Set the Max Allowed HA Role to **Standby**.
6. Expand **Status & Manage** click **HA**.
7. Click **Edit**.
8. 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**).
9. Click **OK**.

> **Note:**
>
> If downgrading the active primary SDS NOAM server, then continue with the next step of this procedure; otherwise, skip to step 14 of this procedure.

10. If downgrading the active primary SDS NOAM server, a HA fail over occurs. The user's GUI session ends as the active primary SDS server goes through HA fail over and becomes the **Standby** server.

> **Note:**
>
> If the server being backed out is the active NOAM and an HA fail over 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 L to have the NOAMP HA fail over.

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

Figure A-48 Log out

12. In the Primary SDS NOAM VIP, clear the 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:

a. Simultaneously press and hold the **Ctrl**, **Shift**, and **Delete** keys (most Web browsers).

b. Select the appropriate object types to delete from the cache (for example, **Temporary Internet Files**, **Cache**, or **Cached images and files**, and so on). Other browsers may label these objects differently.

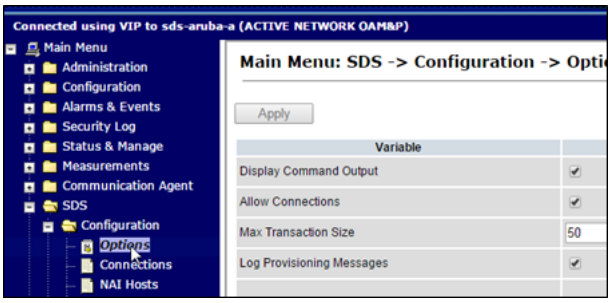
c. Clear the cached data.

> **Note:**
>
> Do NOT proceed until the browser cache has been cleared.

13. Access the primary SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).

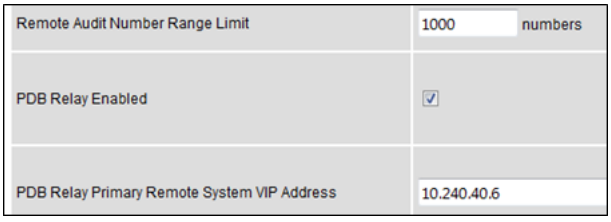
14. In the Primary SDS NOAM VIP, record PDB Relay Enabled state. Expand **SDS** select **Configuration** click **Options**.

Figure A-49 Options



15. Locate the **PDB Relay Enable** check box and record if it is checked or not checked.

Figure A-50 PDB Relay Enable check box



> **Note:**
>
> 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 19 of this procedure.

16. In the 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.

```
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 ~]$
```

17. Set the pdbRelay TimeStamp to "0".

```
[admusr@sds-rlghnc-b ~]$ sudo iset -fvalue=0 ProvOptions where
"var='pdbRelayMsgLogTimeStamp'"
```

18. Exit the CLI for the active primary SDS NOAM.

```
[admusr@sds-rlghnc-b ~]$ exit
```

```
logout
```

19. In the Primary SDS NOAM VIP, stop the software. Expand **Status & Manage** click **Server**.
20. Select the server(s) to be backed out and click **Stop**.
21. Click **OK** to confirm.
22. Verify the Appl State updates to **Disabled**.
23. Verify the server(s) are back out ready. Expand **Administration** select **Software Management** click **Upgrade**. Select the tab for the server group containing the server(s) to be backed out.

> **Note:**
>
> It may take a couple minutes for the grid to update.

24. Verify the Upgrade State displays as **Backout Ready**.

> **Note:**
>
> If this is the active server in an Active-Standby pair, these steps cause an HA fail over. The HA fail over is an expected outcome. Continue with the steps on the new active NOAMP.

25. In the Server CLI, the SSH to the server(s) to be backed out. Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.

```
ssh <NOAM XMI IP address>
```

```
login as: admusr
```

```
password: <enter password>
```

> **Note:**
>
> If direct access to the XMI is not available, then access the target server using a connection through the active NO. SSH to the active NO XMI first. Once logged into the NO, SSH to the target server's XMI address.

26. Run the back out using the reject script.

```
$ sudo /var/TKLC/backout/diUpgrade --reject
        ***Executing.. /var/TKLC/backout/backout_server
        --checkVerifying that backout is possible.Checking for stale RPM
DB locks...Current platform version:
        7.0.2.0.0-86.30.0Continue backout?
        [y/N]: y
```

The server reboots and the user is automatically logged out.

27. Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.

```
ssh <NOAM XMI IP address>
login as: admusr
password: <enter password>
```

28. Verify the Back out, examine the upgrade logs in the `/var/TKLC/log/upgrade` directory and verify no errors are reported.

```
$ grep ERROR /var/TKLC/log/upgrade/upgrade.log
```

> **Note:**
>
> The following errors can be ignored:
>
> - DEBUG: 'iqt' command failed (is IDB running?)
> - 1477080063::ERROR: TKLCsds-7.0.0-7.0.1_70.12.0: Failure running command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'
> - 1477080521::ERROR: prod.dbdown: unknown option (-i)
> - 1517455316::ERROR: Cannot execute command!
> - 1517455316::ERROR: CMD: /usr/sbin/hpacucli controller all show config detail
> - 1517455316::ERROR: ERROR: No such file or directory
> - 1517455316::ERROR: Unable to get the HP disk configuration!
> - 1517455316::ERROR: Command Failed!
> - 1517455316::ERROR: Child process has exited with
> - 1517455316::SYSERROR: No such file or directory
> - 1526453748::ERROR: Cannot reduce filemgmt enough to leave room for dual image upgrade
>
> If the back out was not successful, because other errors were recorded in the logs, then contact My Oracle Support for further instructions. If the back out was successful (no errors or failures), then continue with the remaining steps.

29. Restore the COMCOL Full DB/Run environment, Run the `backout_restore` utility to restore the full database run environment.

```
$ sudo /var/tmp/backout_restore
*** TRUNCATED OUTPUT ***
This process will totally destroy the existing DB on this server.  This
should only be done to recover a server when an upgrade has been backed-
out/rolled-back.
Are you sure you want to proceed? (y|n): y
Answer y to continue the restore.
```

> **Note:**
>
> The COMCOL restore process may take several minutes to complete. If the restore was successful, the following displays:

```
Success: Full restore of COMCOL run env has completed.
```

If an error is encountered and reported by the utility, then work with My Oracle Support for further instructions.

> **Note:**
>
> In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory, resulting in the **/var/tmp/backout_restore: No such file or directory** error message. If this message occurs, copy the file using sudo from **/usr/TKLC/appworks/sbin to /var/tmp** and repeat the command.

30. Reboot the server. Run the command:

    ```
    $ sudo init 6
    ```

    This step can take several minutes and terminates the SSH session.

31. Use the SSH command (on UNIX systems — or putty if running on Windows) to log into the active NOAM.

    ```
    ssh <NOAM XMI IP address>
    login as: admusr
    password: <enter password>
    ```

32. 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:

Figure A-51 Comagent link

```
[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 Awpss7 ->
/usr/TKLC/awpss7/gui/
lrwxrwxrwx  1 root    root    29 Dec 15 02:07 TransportMgr ->
/usr/TKLC/awptransportmgr/gui
lrwxrwxrwx  1 root    root    38 Dec 15 02:07 Exgstack ->
/usr/TKLC/awptransportmgr/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.

33. In the Server CLI, verify if the httpd service has restarted. If this is an NO or SO, verify httpd service is running.

    ```
    sudo systemctl status httpd.service
    ```

    ```
    httpd (pid xxxx) is running...
    ```

    > **Note:**
    >
    > The process IDs are variable so the actual number value can be ignored.

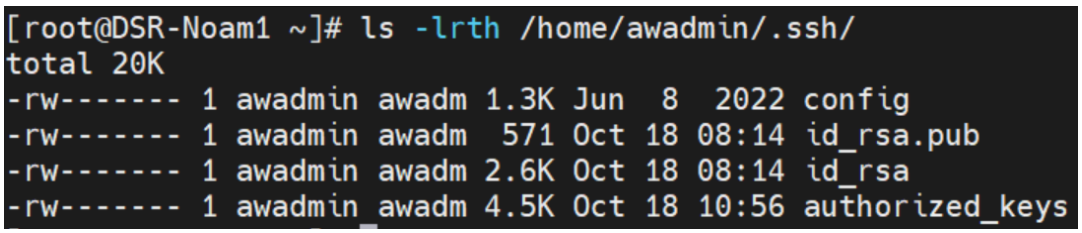
34. If httpd is not running, wait for a few minutes and retry the command. If httpd is still not running after 3 minutes, then services have failed to restart. Contact My Oracle Support for further instructions.

35. Verify if the file id_rsa has required ownership, check the ownership of the file:

    ```
    ls -ltr /home/awadmin/.ssh/
    ```

The file permission should be defined as shown:

Figure A-52 Permission



If the file ownership is not set for `awadmin`, then change the permission:

```
sudo chown awadmin:awadm /home/awadmin/.ssh/id_rsa
```

Verify file ownership is changed to `awadmin awadm`.

36. In the Primary SDS NOAM VIP, verify the server(s) application version and upgrade state. Expand **Administration** select **Software Management** click **Upgrade**. Select the tab containing the server(s) that were backed out. Verify the Application Version value for this server has been backed out to the source release version. Verify the Upgrade State.

> **Note:**
>
> Full audit between active NO and backed out server is conducted and it may take up to 10 minutes before the Upgrade State is changed to **Ready**.

37. In the Primary SDS NOAM VIP, set the Max Allowed HA Role to Active. Due to back out being initiated from the command line instead of through the GUI, modify the backed out server so its Upgrade State changes to **Ready**. Expand **Status & Manage** click **HA**. Click **Edit**.
38. 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**). Click **OK**.Verify the Max Allowed HA Role is set.
39. Restart the software, Expand **Status & Manage** click **Server**. If the server(s) that was backed out displays an Appl State, state of **Enabled**, skip to the next step. If the server(s) that was backed out displays an Appl State, state of **Disabled**, select the server(s) and click **Restart**. Click **OK** to confirm. Verify the Appl State changes to **Enabled**.
40. In the Primary SDS NOAM VIP, verify the Upgrade State. Expand **Administration** select **Software Management** click **Upgrade**. Select the tab of the server group containing the server(s) that was backed out. Verify the Upgrade State is now **Ready**(it may take several seconds for the grid to update).
41. Stop the software (if necessary). Due to backout being initiated from the command line instead of through the GUI, modify the Upgrade State of the backed out server(s) to achieve a state of **Not Ready**. Expand **Status & Manage** click **Server**. If the server(s) that was backed out displays an Appl State state of **Enabled**, then select the server(s) and click **Stop**.
42. In the primary SDS NOAM VIP, verify the server(s) Upgrade State. Expand **Administration** select **Software Management** click **Upgrade**. If the server(s) that was backed out displays an Upgrade State of **Not Ready**, then go back to step 37 of this procedure.

43. Complete the backout action (if necessary), If the server(s) that was backed out displays an Upgrade State of **Ready** or **Success**, then:
    - Select the server(s) that was backed out and click **Complete**.Leave the Action set to its default value of **Complete**.
    - Click **OK** to confirm the action.

    This changes the **Max Allowed HA Role** of the backed out server(s) to **Active**, which causes the server **Upgrade State** to change to **Not Ready**.

    The user may see the following SOAP error display on the GUI banner.

    ```
    SOAP error while clearing upgrade status of hostname=[frame10311b6]
            ip=[172.16.1.28]
    ```

    It is safe to ignore this error message.

A.4 Manually Perform ISO Validation

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.

1. In the 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.

   ```
   sds-rlghnc-a login: admusr
   Password: <admusr_password>
   *** TRUNCATED OUTPUT ***
   RELEASE=6.4
   RUNID=00
   VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/
   comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/sds
   PRODPATH=/opt/comcol/prod
   RUNID=00
   ```

2. Verify the ISO file is located in the `/var/TKLC/upgrade/` directory.

   ```
   [admusr@sds-rlghnc-a ~]$ ls /var/TKLC/upgrade/SDS-9.0.2.0.0_98.15.0-
   x86_64.iso
   ```

3. If the ISO file is not present, copy the ISO file to the `var/TKLC/upgrade/` directory.

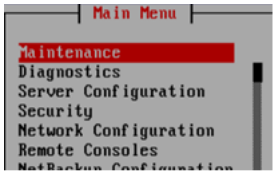
   ```
   [admusr@sds-rlghnc-a ~]$ cp -p /var/TKLC/db/filemgmt/
   SDS-9.0.2.0.0_98.15.0.iso /var/TKLC/upgrade/
   ```

4. Become the `platcfg` user by using the `su` command. For password information, refer to Logins, Passwords, and Site Information.

   ```
   [admusr@sds-rlghnc-a ~]$ su - platcfg
   Password: <platcfg_password>
   ```

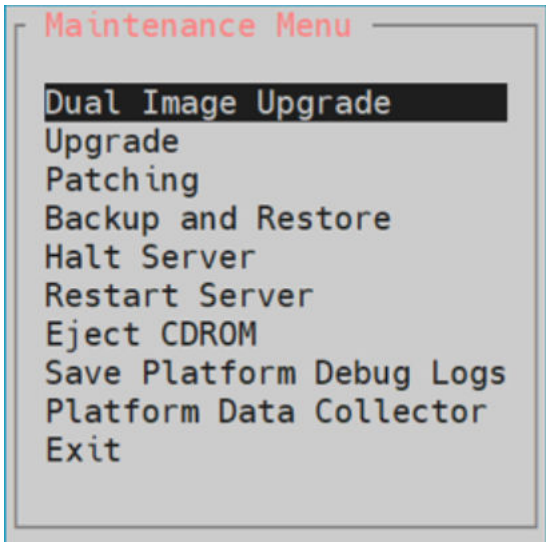
5. In the Primary SDS NOAM VIP, select the ISO file. From the **platcfg** menu, select **Maintenance** and press **Enter**.

Figure A-53 Maintenance



6. Select **Dual Image Upgrade** and press **Enter**.

Figure A-54 Dual Image Upgrade



7. Select **Validate Media** and press **Enter**.

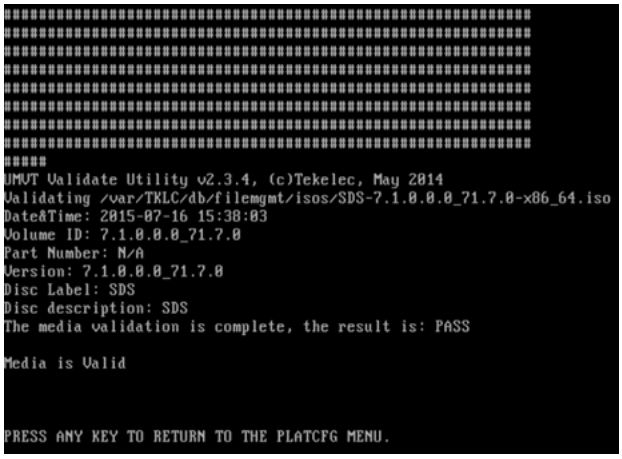
Figure A-55 Validate Media

8. Select **Choose Upgrade Media Menu**, select the target ISO file, and press **Enter**.

Figure A-56 Upgrade Media Menu

9. In the Primary SDS NOAM VIP, verify if the ISO media is **Valid**.

Figure A-57 ISO Media

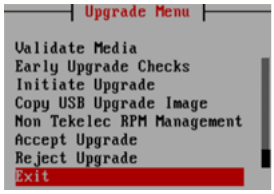


10. Press **Enter** to return to the `platcfg` menu.
11. In the Primary SDS NOAM VIP, exit from menu. Select **Exit** and press **Enter**.

Figure A-58 Exit

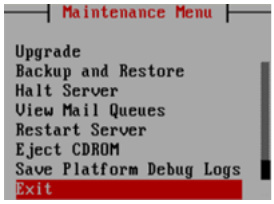
12. Select **Exit** and press **Enter**.

Figure A-59 Upgrade Menu



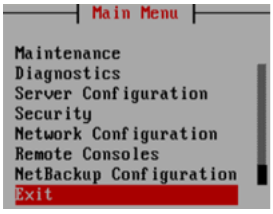
13. Select **Exit** and press **Enter**.

Figure A-60 Maintenance



14. Select **Exit** and press **Enter**.

Figure A-61 Main Menu



15. In the Primary SDS NOAM VIP, exit the CLI for the Active Primary SDS NOAM.

```
[admusr@sds-rlghnc-a ~]$ exit

logout
```

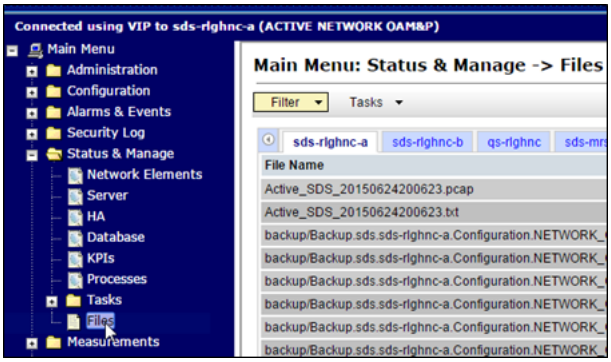
16. Return to the procedure step that directed the execution of this procedure.

A.5 Undeploy an ISO File (Post Upgrade Acceptance)

This procedure should only be run 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** click **Files**.

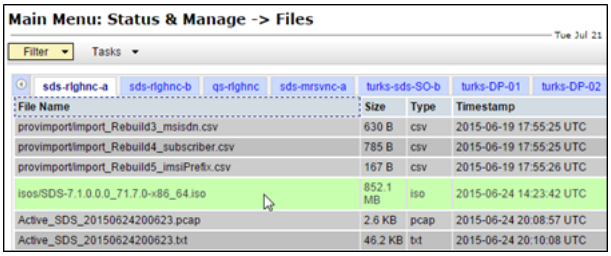
1. Log in to SDS NOAM GUI, use the VIP address to access the primary SDS NOAM GUI as described in Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the primary SDS NOAM VIP, Undeploy the ISO. Expand **Status & Manage** click **Files**.

Figure A-62 Files



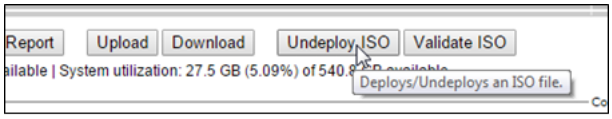
3. Select the ISO file for the target release.

Figure A-63 ISO File



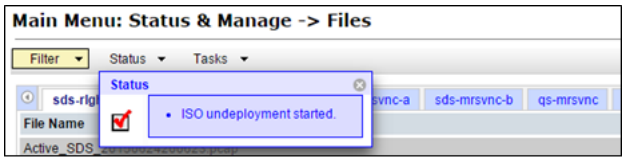
4. Click **Undeploy ISO**.

Figure A-64 Undeploy ISO



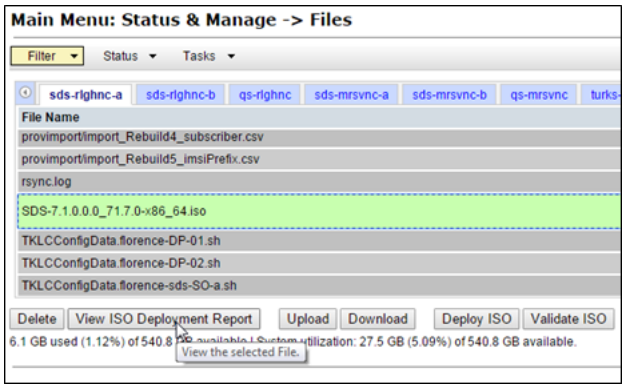
5. Click **OK**.
6. In the Primary SDS VIP, Monitor the ISO un-deployment status. The Status tab in the banner displays the **ISO undeployment started** confirmation message.

Figure A-65 ISO undeployment message



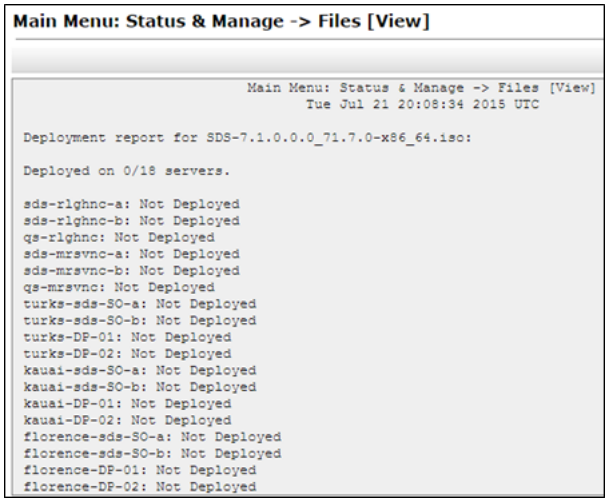
7. Reselect the ISO file for the target release and click **View ISO Deployment Report**.

Figure A-66 ISO Deployment Report



8. 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.

Figure A-67 Report

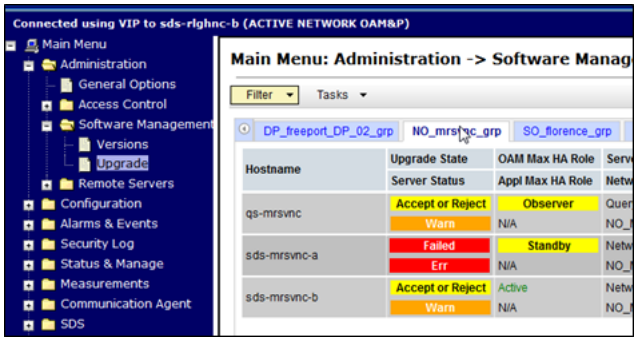


9. Repeat until the ISO displays **Not Deployed** on all servers in the topology.

A.6 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 Access the OAM GUI Using the VIP (NOAM/SOAM).
2. In the primary SDS NOAM VIP, verify upgrade state.
   a. Expand **Administration** navigate to **Software Management** click **Upgrade**.
   b. Verify the host name of the primary active SDS NOAM server from the GUI banner.
   c. Select the Server Group tab for the server(s) being upgraded.
   d. Verify the **Upgrade State** for each server undergoing the software upgrade and identify any servers with a **Failed** state.

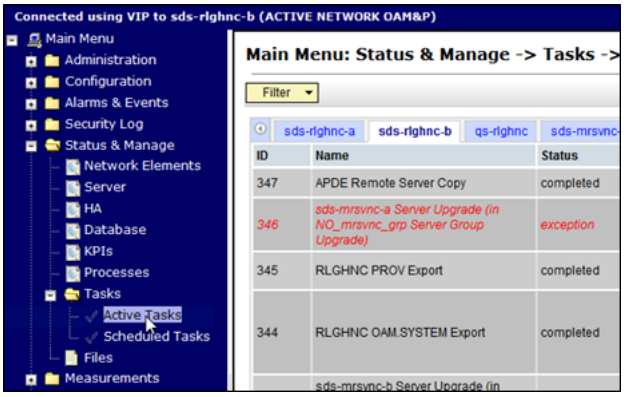
Figure A-68 Server State



> **Note:**
>
> 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 11 of this procedure.

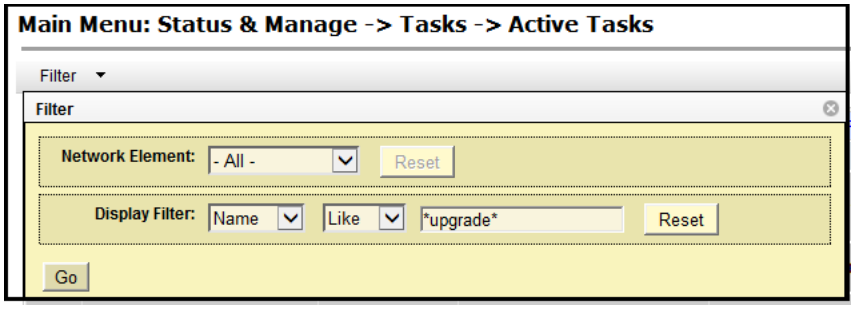
3. In the Primary SDS NOAM VIP, filter the servers that need upgrading. Expand **Status & Manage** navigate to **Tasks** click **Active Tasks**.

Figure A-69 Active Tasks



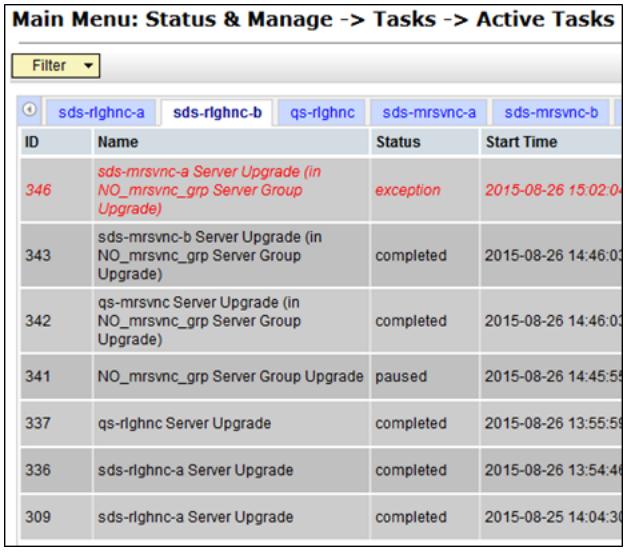
4. From the **Filter** option, enter the following filter values:
   a. Network Element: **All**
   b. Display Filter: **Name Like *upgrade***
5. Click **Go**

Figure A-70 Active Status



6. In the primary SDS NOAM VIP, locate the Server Group Upgrade task. If not already selected, select the tab displaying the host name of the active SDS NOAM server. Locate the task for the **Server Group Upgrade**. It shows a status of **paused**.

Figure A-71 Server Group Upgrade

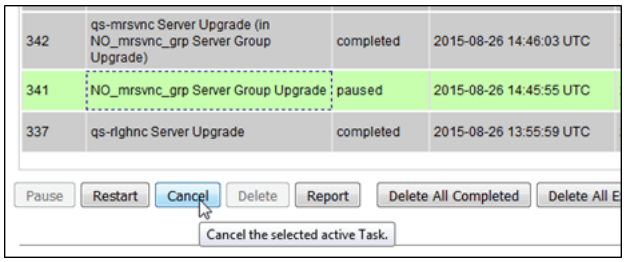


> **Note:**
>
> Consider the case of an upgrade cycle where it is seen that the upgrade of one or more servers in the server group has the status as exception (that is, failed), while the other servers in that server group have upgraded successfully. However, the server group upgrade task still shows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

> **Note:**
>
> Before clicking **Cancel** for the server group upgrade task, ensure the upgrade status of the individual servers in that particular server group have status as completed or exception (that is, failed for some reason). Make sure you are not canceling a task with some servers still in running state.

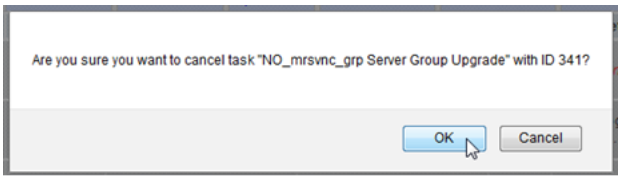
7. In the primary SDS NOAM VIP, cancel the Server group Upgrade task.
   a. Click the Server Group Upgrade task to select it.
   b. Click **Cancel** to cancel the task.

Figure A-72 Cancel Task



8. Click on the confirmation screen to confirm the cancellation.

Figure A-73 Confirm Cancellation

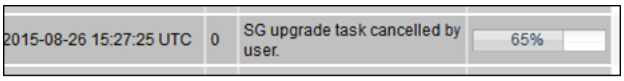


9. In the primary SDS NOAM VIP, verify if the Server Group Upgrade task is canceled. On the **Active Tasks** screen, verify the Status changed from **paused** to **completed**.

Figure A-74 Status

10. Verify the Result Details column now states “SG upgrade task canceled by user.

Figure A-75 SG upgrade task cancelled



11. Access the failed CLI server, Use the XMI address to log into the failed server with the `admusr` account.

```
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
```

12. Inspect the upgrade.log file and identify the reason for the failure in the upgrade.log file.

```
[admusr@sds-mrsvnc-a ~]$ tail /var/TKLC/log/upgrade/upgrade.log
1439256874:: INFO: Removing '/etc/my.cnf' from RCS repository
1439256874:: INFO: Removing '/etc/pam.d/password-auth' from RCS repository
1439256874:: INFO: Removing '/etc/pam.d/system-auth' from RCS repository
1439256874:: INFO: Removing '/etc/sysconfig/network-scripts/ifcfg-eth0'
from RCS repository
```

```
1439256874:: INFO: Removing '/var/lib/prelink/force' from RCS repository
1439256874::Marking task 1439256861.0 as finished.
1439256874::
1440613685::Early Checks failed for the next upgrade
1440613691::Look at earlyChecks.log for more info
1440613691::
```

13. Inspect the earlyChecks.log file, identify the reason for the failure in the earlyChecks.log file.

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

> **Note:**
>
> 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.
>
> Do not proceed to the next step until the alarm condition has been cleared.

14. In the Failed Server (CLI), verify platform alarms are cleared from the failed server. Use the alarmMgr utility to verify all platform alarms have been cleared from the system.

```
[admusr@sds-mrsvnc-b ~]$ alarmMgr –alarmStatus
```

15. Exit the CLI for the failed server.

```
[admusr@sds-mrsvnc-a ~]$ exit


logout
```

16. In the Primary SDS NOAM VIP (GUI), run the server upgrade again. Return to the upgrade procedure being run when the failure occurred. Re-run the upgrade for the failed server using the `Upgrade Server` option.

> **Note:**
>
> Once a server has failed while using the `Automated Server Group Upgrade` option, the `Auto Upgrade` option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the `Upgrade Server` option.

A.7 Add New SOAM Profile on Existing VM

> **Note:**
>
> The procedures in this appendix can be run only after the SDS has been upgraded to release 9.0.2 and the upgrade has been accepted.

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

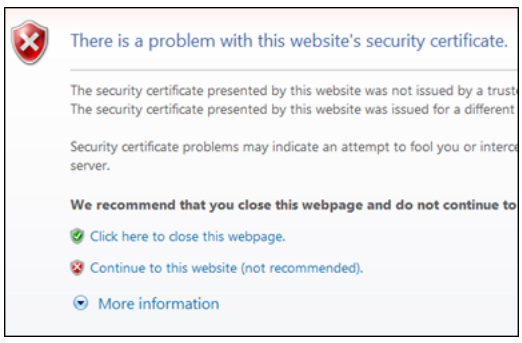
This appendix updates the SOAM VM profile to support 1 billion subscribers. This appendix applies only to systems that have been upgraded to release 9.0.2. The upgrade must be accepted before initiating these procedures. The SOAM VMs are updated with the new profile using the following sequence:

1. Remove the SOAM from the SOAM server group
2. Delete the existing SOAM VM and recreate the SOAM VM with the new profile
3. Add the new SOAM VM to the SOAM server group

A.8 Remove the SDS SOAM VM from the SOAM Server Group

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

Figure A-76 Website Security

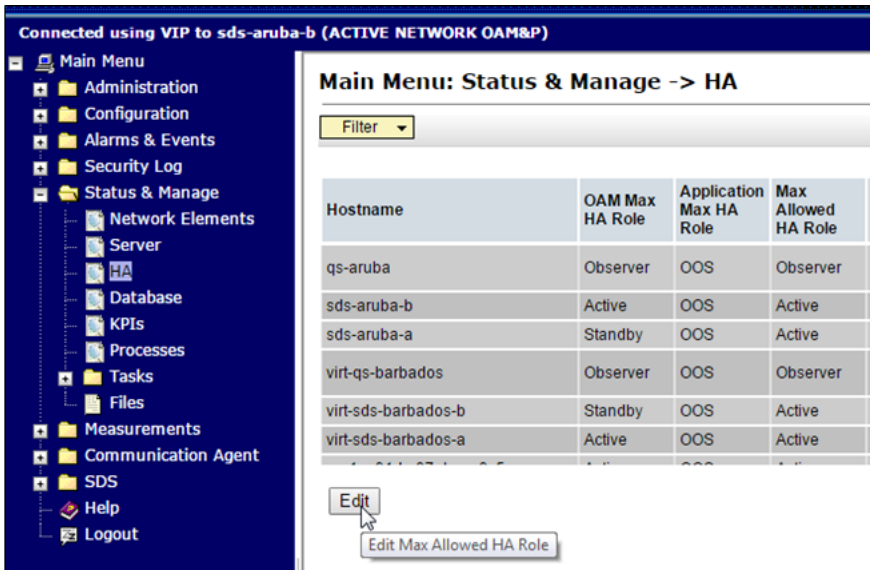


2. Log in to the Primary NOAM VIP using default user name and password.

Figure A-77 NOAM VIP GUI

3. In the Primary SDS NOAM VIP, edit an HA role. Expand **Status & Manage** click **HA**. Click **Edit**.

Figure A-78 Edit



4. In the Primary SDS NOAM VIP, change the SOAM server HA role to **Standby**. Select the active primary SDS SOAM server and change the **Max Allowed HA Role** to **Standby**. Click **OK**.

Figure A-79 Edit HA

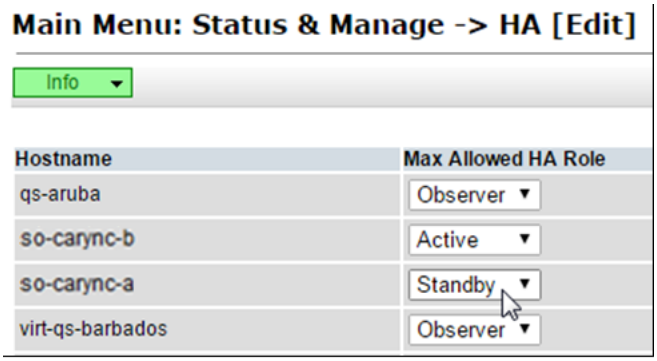
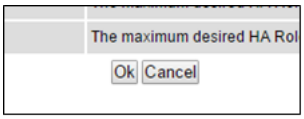
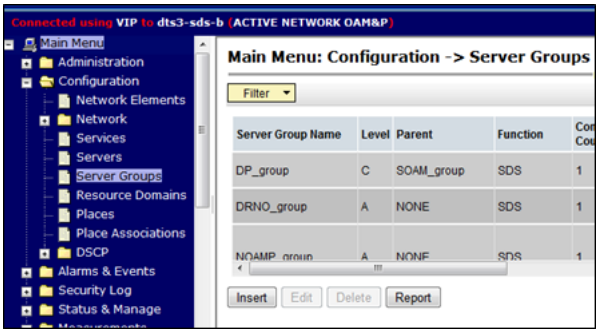


Figure A-80 OK



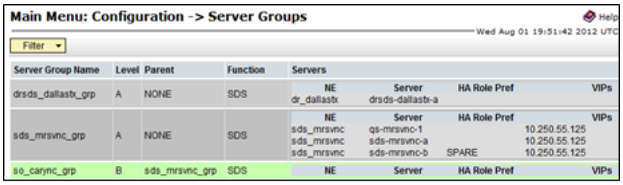
5. In the Primary NOAM VIP, edit the SOAM server. Expand **Configuration** click **Server Groups**.

Figure A-81 Server Groups



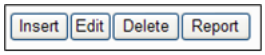
6. Select the server group with the SOAM server to be converted to the aB subscriber.

Figure A-82 Select Server Group



7. Click **Edit**.

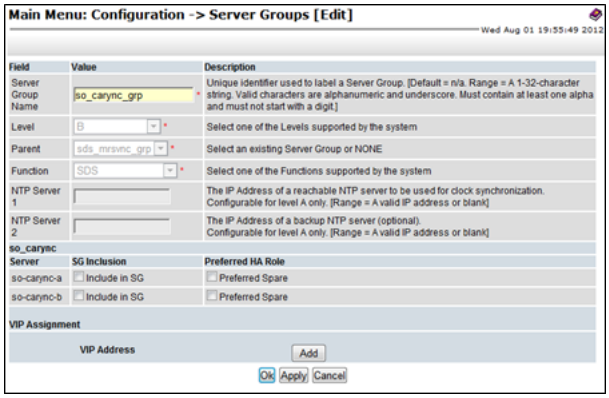
Figure A-83 Edit



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

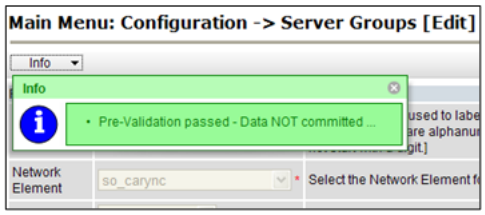
8. In the Primary NOAM VIP prepare server for pre-validation. Remove the **SG Inclusion check mark** from the server group.

Figure A-84 SG Inclusion



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

Figure A-85 Pre-validation passed



10. In the Primary NOAM VIP, Click **Logout** to log out of the SDS GUI.

Figure A-86 Log out

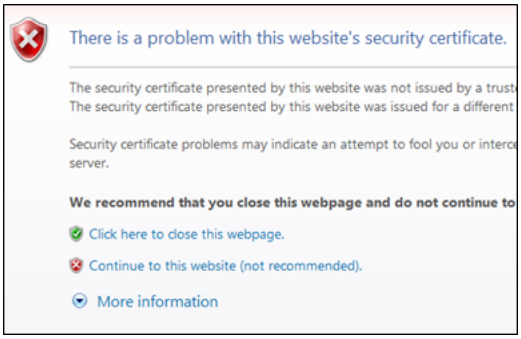
A.9 Recreate the SDS SOAM VM with the 1B Subscriber Profile

For further information, see Common KVM, OpenStack Tasks, OAM Installation for DP-SOAM Sites (All DP-SOAM), and OAM Pairing for DP-SOAM Sites (All DP-SOAM Sites) sections in *Subscriber Data Server Cloud Installation Guide*.

A.10 Place the SDS SOAM VM into the SOAM Server Group

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

Figure A-87 Web Security

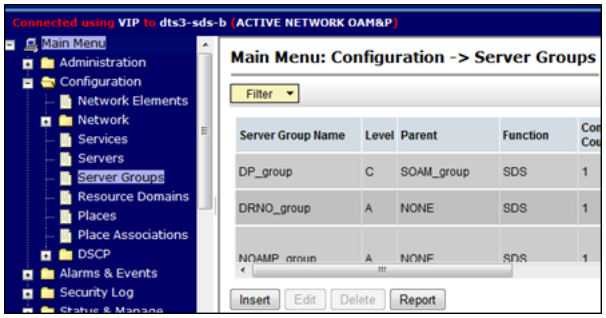


2. In the SDS NOAM VIP, log in using the default user and password.

Figure A-88 NOAM GUI Log in

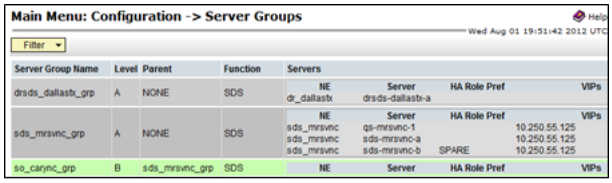
3. In the SDS NOAM VIP, edit the SOAM server. Expand **Configuration** click **Server Groups**.

Figure A-89 Server Groups



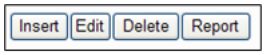
4. Select the SOAM server that was converted to the 1B Subscriber profile.

Figure A-90 Select SOAM Server



5. Click **Edit**.

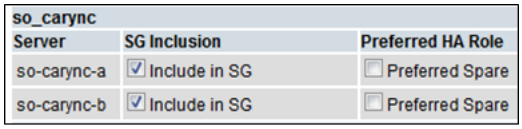
Figure A-91 Edit



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

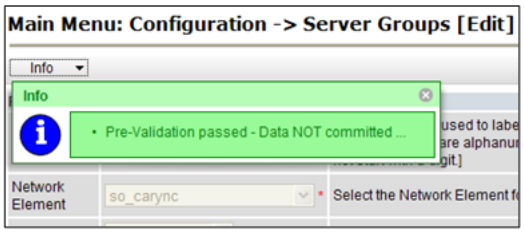
6. In the SDS NOAM VIP, prepare the server for pre-validation. Mark the **SG Inclusion** check box for the server.

Figure A-92 SG Inclusion



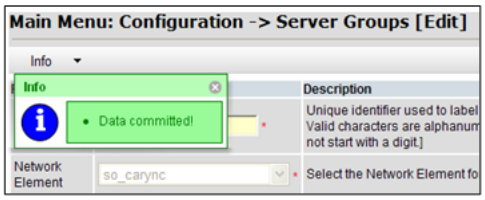
7. When the **Pre-Validation** passed message displays, click **Apply**.

Figure A-93 Pre-Validation passed



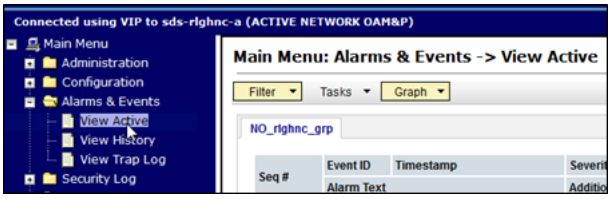
8. The Info banner changes to **Data committed**.

Figure A-94 Data committed



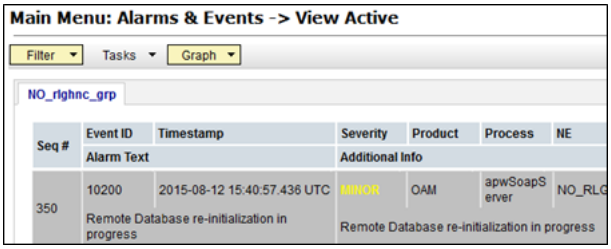
9. In the SDS NOAM VIP, view the alarm status. Expand **Alarms & Events** click **View Active**.

Figure A-95 Alarm Status



10. Verify if **Event ID 10200 Remote Database re-initialization in progress** is present with the SDS SOAM server host name.

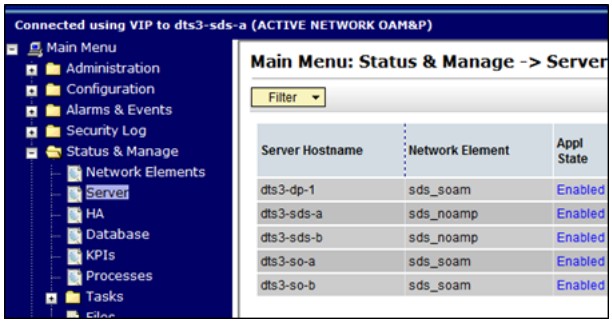
Figure A-96 Event ID



> **Note:**
>
> 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.

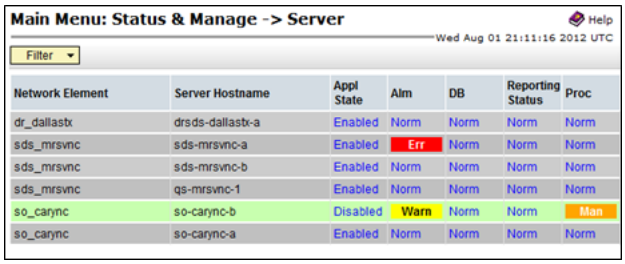
11. In the SDS NOAM VIP, verify status. Expand **Status & Manage** click **Server**.

Figure A-97 Status



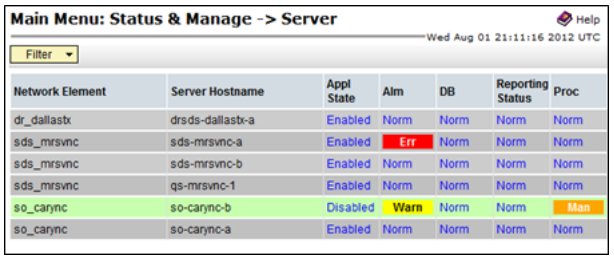
12. Verify Server Status is Normal (Norm) for Database (DB) and Man for Processes (Proc).

Figure A-98 Server Status



13. In the SDS NOAM VIP restart the SOAM server.
14. Select the SOAM server.

Figure A-99 Select Server

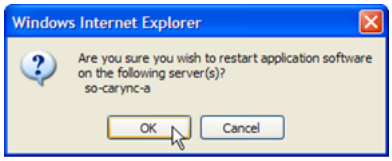


15. Click **Restart**.

Figure A-100 Restart

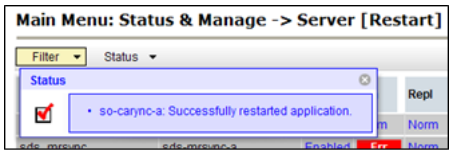
16. Click **OK** to confirm.

Figure A-101 OK



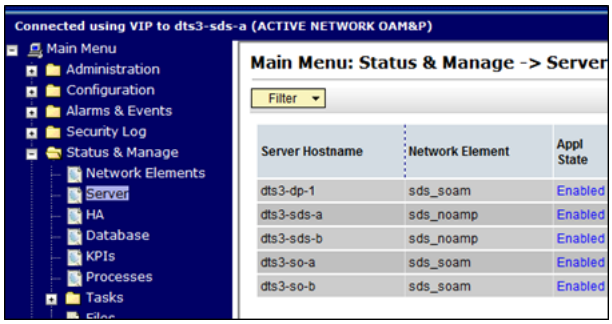
17. A **Successfully restarted application** message displays in the banner.

Figure A-102 Successfully restarted application



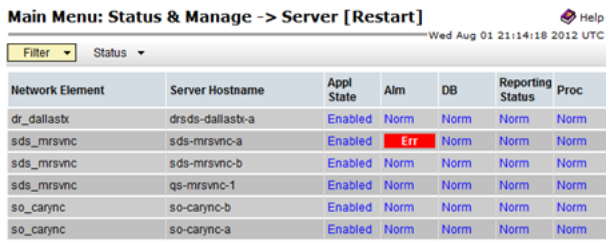
18. In the SDS NOAM VIP, verify status. Expand **Status & Manage** click **Server**

Figure A-103 Server Status



19. Verify Appl State is **Enabled** and Server Status is Normal (**Norm**) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).

Figure A-104 Server State



20. Log out from the SDS NOAM VIP. Click **Logout** to log out of the SDS GUI.

Figure A-105 Log out

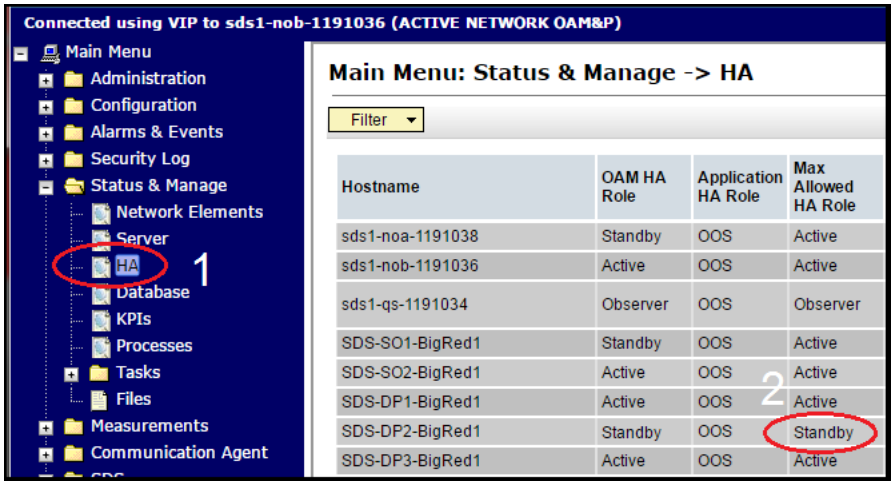
21. Run SDS Health Check procedures as specified in Health Check Procedures.

A.11 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.

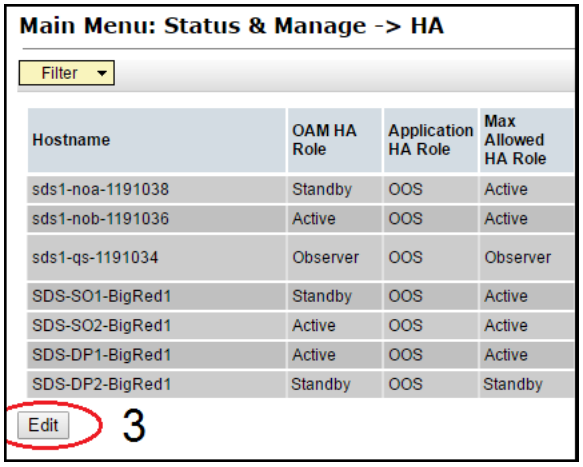
1. In the primary SDS NOAM VIP, edit the Max Allowed HA Role. Expand **Status & Manage** and click **HA**. Locate the server to be completed and verify if the Max Allowed HA Role is in Standby mode.

Figure A-106 HA



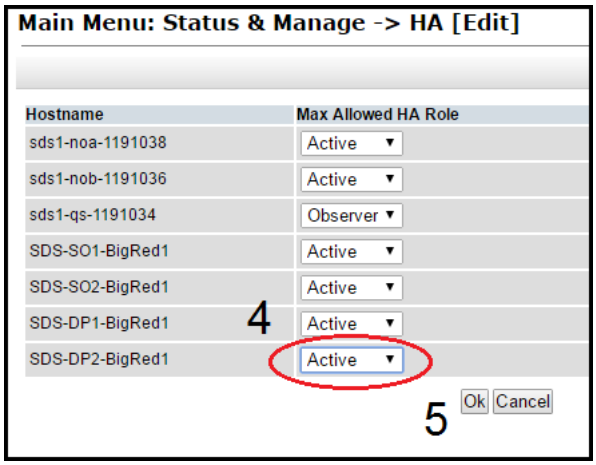
2. Click `Edit`.

Figure A-107 Edit



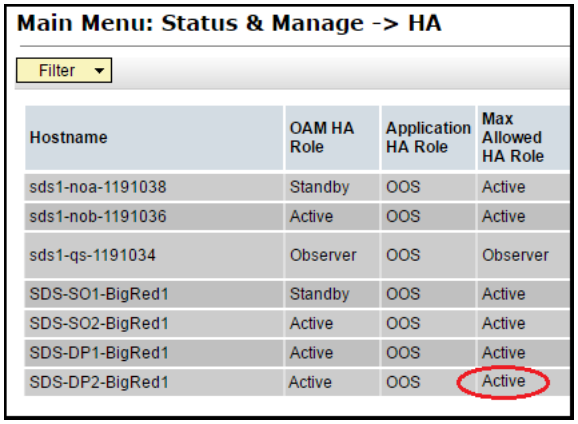
3. Change the Max Allowed HA Role to `Active`.
4. Click `OK`.

Figure A-108 HA Status Active



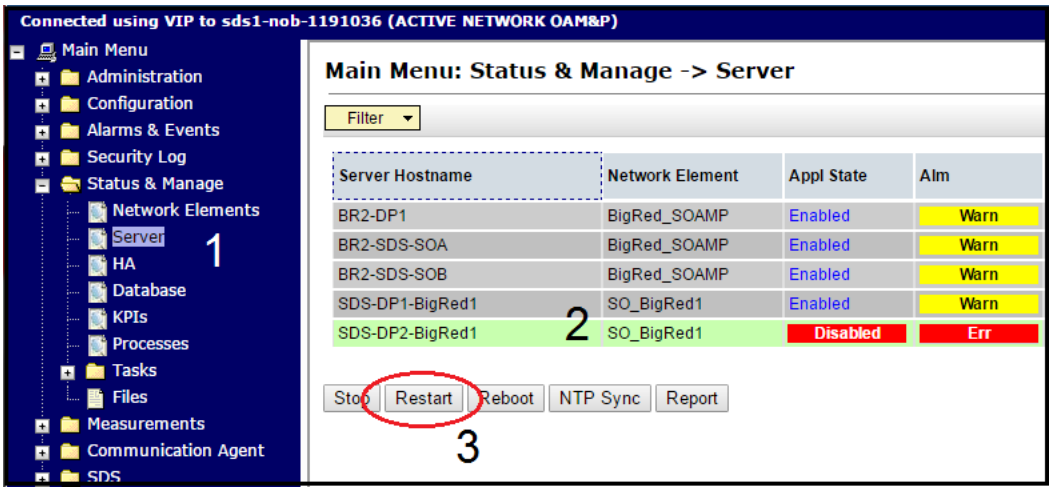
5. In the primary SDS NOAM VIP, verify the Max Allowed HA Role changes to **Active.**

Figure A-109 Max allowed HA Role



6. In the primary SDS NOAM VIP, re-start the server. Expand **Status & Manage** click **Server**. Select the server to be completed and click **Restart**.

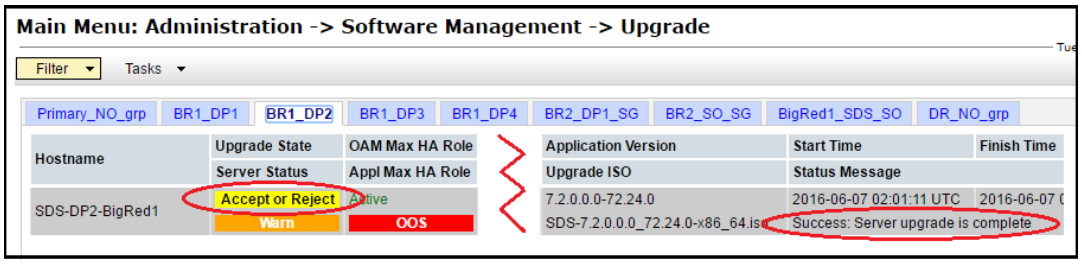
Figure A-110 Restart



After a few minutes, the Appl State changes to **Enabled**.

7. In the primary SDS NOAM VIP, verify server completion. Expand **Administration** navigate to **Software Management** click **Upgrade**. Verify the Upgrade State changes to **Accept or Reject** and the status message changes to **Success: Server manually completed**.

Figure A-111 Accept or Reject



A.12 Workaround to Resolve Server HA Failover Issue

This procedure resolves the HA failover issue by restarting the cmha process on the server.

1. Log into the server CLI, use the SSH command (on UNIX systems – or putty if running on Windows) to log into the NOAM server which is experiencing the HA failover issue.

   ```
   ssh admusr@<server address>
   ```

   ```
   password: <enter password>
   ```

   Answer **yes** if you are asked to confirm the identity of the server.

2. Resolve HA failover issue(s), run the command:

   ```
   sudo pm.kill cmha
   ```

3. Repeat procedure on each affected server, if required. Return to procedure/step in upgrade process which pointed to refer this procedure.

A.13 Workaround for SNMP Configuration

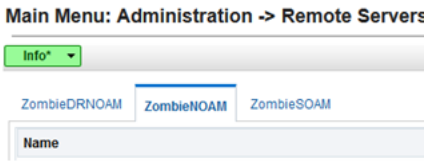
This procedure configures or updates the SNMP with **SNMPv2c and SNMPv3** as the enabled versions for SNMP traps configuration, as PMAC does not support SNMPv3.

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.

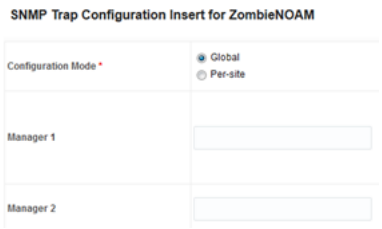
1. Login to the NOAM VIP GUI using the VIP. Expand **Administration** navigate to **Remote Servers** click **SNMP Trapping**. Select the Server Group tab for SNMP trap configuration:

Figure A-112 Remote Servers



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

Figure A-113 Manager IPs



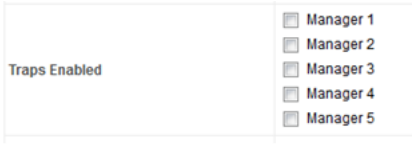
4. Set the Enabled Versions as SNMPv2c and SNMPv3.

Figure A-114 Enabled Versions

> **Note:**
>
> In case, enabled versions of already configured SNMP is V3Only, then update the enabled versions as above.

5. Mark the Traps Enabled checkboxes for the Manager servers being configured.

Figure A-115 Traps Enabled

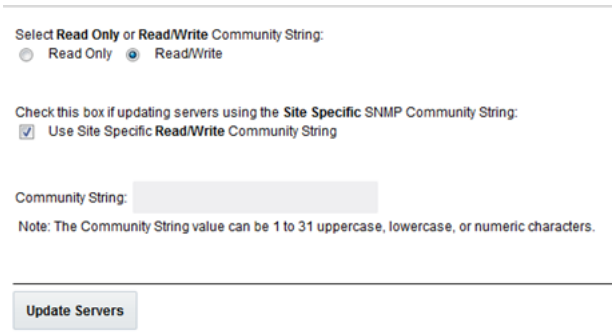


6. Type the SNMP Community Name.

Figure A-116 SNMP Community Name

7. Leave all other fields at their default values, click **OK**.
8. Log in to PMAC GUI. If needed, open a web browser and enter the command `http://<pmac_management_ip>`. Log in as the `pmacadmin` user.
9. In the PMAC GUI, update the TVOE host SNMP community string. Expand the folder **Administration** navigate to **Credentials** click **SNMP Community String Update**. Select the "Use Site Specific Read/Write Community String" option.

Figure A-117 Read/Write Option



10. Click Update Servers.

Figure A-118 Update Server

11. Click OK.
12. Return to the procedure step that directed the execution of this procedure.

A.14 Workaround to Resolve Syscheck Error for CPU Failure

This procedure resolves the syscheck errors for CPU failure.

1. Log into server using CLI on which syscheck is failing, use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.

   ```
   ssh admusr@<SERVER_XMI>
   password: <enter password>
   ```

   Answer **yes** if you are asked to confirm the identity of the server.
2. In the server CLI, run the workaround:
   a. Edit the cpu config file.

      ```
      $ sudo vim /usr/TKLC/plat/lib/Syscheck/modules/system/cpu/config
      ```

   b. Comment out the text that reads: "EXPECTED_CPUS=" by putting # in the beginning of the line. For example: `# EXPECTED_CPUS=2`
   c. Save the cpu config file.
   d. Reconfig the syscheck, run the following commands:

      ```
      sudo syscheck --unconfig
              sudo syscheck --reconfig
          sudo syscheck
      ```

      CPU related errors do not display.

A.15 Workaround to Fix cmsoapa Restart

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

1. Log in to the NOAM VIP GUI. 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>`
2. Log into the NOAM GUI as the `guiadmin` user.

Figure A-119 NOAM VIP GUI Log in

3. In the NOAM VIP GUI, identify the servers with the 31201 alarm for the cmsoapa process not running.
   a. Navigate to current alarm details and identify the server on which 31201 - Process Not Running alarm is getting raised for Instance as cmsoapa.
   b. Expand **Alarms & Events** click **View Active**.
   c. Look for "31201" alarm instances and make a list of servers with the cmsoapa alarm instance.
4. Login into Server using CLI on which cmsoapa is restarting. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.

   ```
   ssh admusr@<SERVER_XMI>
   password: <enter password>
   ```

   Answer **yes** if you are asked to confirm the identity of the server.
5. In the server CLI, run the workaround.
   a. Enter the command `$ sudo prod.dbdown`.
   b. After few minutes, when processes are down. Run `prod.start`. Enter the command `$ sudo prod.start`.
   c. Repeat the steps on all server(s) where the alarm is, that is, where the cmsoapa process is restarting.

A.16 Workaround to Fix DNS Issue

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

1. Verify the QS server transitions to a “A” State, log in to QS Server with the `admusr` account. Run the command:

   ```
   [admusr@SG2-SDS-QS ~]$ sudo prod.state
                                  ...prod.state RUNID=00)...
                                  ...getting current state...
          Current state:  A  (product under procmgr)
   ```

a. If current state is "A", stop and continue completing the upgrade.

b. If not, then continue to the next step.

2. Verify the permissions of the `/etc/resolv.conf` file is `644`. Execute:

```
[admusr@SG2-SDS-QS ~]$ ll
        /etc/resolv.conf
    -rw-r--r-- 1 root root 73 Feb 21 19:47 /etc/resolv.conf
```

3. Verify the `/etc/resolv.conf` file contains the upgraded standby server. Check the file content:

```
[admusr@SG2-SDS-QS ~]$ sudo cat
        /etc/resolv.conf<Primary Server
        A><Primary Server
        B><Secondary Server
        B>
```

If not, checkout and edit the file as shown using the steps below.

4. Using the rcstool checkout the `/etc/resolv.conf` file.

```
[admusr@SG2-SDS-QS ~]$ sudo
        rcstool co /etc/resolv.conf
    RCS_VERSION=x.x
```

5. Edit the `/etc/resolv.conf` file.

```
[admusr@SG2-SDS-QS ~]$ sudo vi /etc/resolv.conf
```

6. Double Check that the `/etc/resolv.conf` file updates are as desired from edit above.

```
[admusr@SG2-SDS-QS ~]$ sudo cat /etc/resolv.conf
         <Primary Server A>
         <Primary Server B>
         <Secondary Server B>
```

7. Using the rcstool check in the `/etc/resolv.conf` file.

```
[admusr@SG2-SDS-QS ~]$ sudo rcstool ci /etc/resolv.conf
```

8. Clear DNS cache using the `nscd` command.

```
[admusr@SG2-SDS-QS ~]$ sudo nscd -i hosts
```

9. Verify the QS server transitions to a “A” State.

```
[admusr@SG2-SDS-QS ~]$ sudo prod.state
                           ...prod.state (RUNID=00)...
                           ...getting current state...
    Current state:  A (product under procmgr)
```

A.17 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.

A.18 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.”
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

A.19 Restoring Custom MySQL User

Perform the following procedure to restore custom MySQL users:

1. Log in to the query server as **admin user**.

2. Run the following commands on the query server to create a new directory:

   ```
   cd /var/TKLC/db/filemgmt
   ```

   ```
   mkdir user_backup_restore
   ```

3. Download and copy the script to the following path `/var/TKLC/db/filemgmt/user_backup_restore`.

   Script file - Script

4. Run the following command to provide permission to the script:

   ```
   chmod 777 restore_mysqluser.py
   ```

5. Run the script using the following command:

   ```
   cd /var/TKLC/db/filemgmt/user_backup_restore
   ```

   ```
   ./restore_mysqluser.py
   ```

   An output file (DUMP_COMMANDS_<YYYY_MM_DD_HR_MIN_SEC>.sql) is generated in the following path `/var/TKLC/db/filemgmt/user_backup_restore`.

6. Run the following command on MySQL database to retrieve custom users configured:

   ```
   select user from mysql.user;
   ```

7. Perform the SDS upgrade.

8. After the upgrade is completed, run the following restore command:

   ```
   cd /var/TKLC/db/filemgmt/user_backup_restore
   ```

   ```
   sudo Imysql -uroot -pImysql23root mysql <
   DUMP_COMMANDS_<YYYY_MM_DD_HR_MIN_SEC>.sql
   ```

   For example:

   ```
   sudo Imysql -uroot -pImysql23root mysql <
   DUMP_COMMANDS_2023_10_30_07_17_19.sql
   ```

9. Run the following command on MySQL database, to ensure custom users are restored:

   ```
   select user from mysql.user;
   ```

10. Compare the output of step 6 and 9 to ensure the script has successfully restored the MySQL custom users.

11. To remove the following files:

    - old user file (user_<YYYY_MM_DD_HR_MIN_SEC>.txt)
    - log file (log_create_sql_<YYYY_MM_DD_HR_MIN_SEC>.txt)
    - .sql generated files (DUMP_COMMANDS_<YYYY_MM_DD_HR_MIN_SEC>

- .sql, (USER_COMMANDS_<YYYY_MM_DD_HR_MIN_SEC>.sql)

Run the following command:

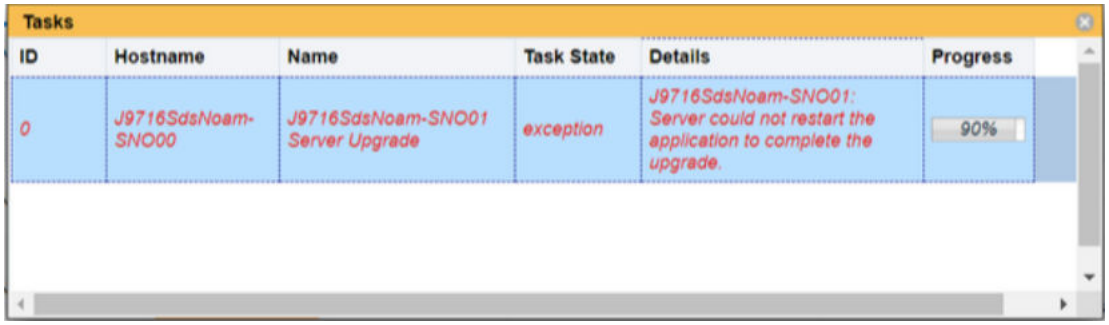
```
./restore_mysqluser.py --clean
```

A.20 Workaround to Resolve Failed Upgrade

Error: Upgrade failed from 9.x to 9.0.2 with error: "Server could not restart the application to complete the upgrade".

Following are the steps to resolve a failed upgrade:

Figure A-120 Failed upgrade



1. Set **Max HA Role** to **Active** for the failed server on **HA** screen.
2. Restart the server on the server screen.

A.21 Workaround To Resolve Alarms while upgrading from build 8.5 to 9.0.2.0.0_99.13.0

Following are the alarms received while upgrading from the build 8.5 to 9.0.2.0.0_99.13.0:

- 14152 MAJOR Failed to transfer file from remote host, see trace log for details.
- 31214 MINOR Scheduled Process Fault.

Resolution

To resolve the alarm, run the following command

```
sudo irem RecentAlarmEv.0 where "eventNumber=14152"
```

.

B

Dual Hop Upgrade from SDS-8.6.x to SDS-9.0.2 Using Ansible

This section provides information and the procedure for Dual Hop Upgrade from release 8.6.x VM to SDS 9.0.2 VM or above release.

Note:

Points to be considered during Dual Hop upgrade:

- Use only `admusr` as username for all the commands.
- Do not perform ISO deployment for Dual Hop Upgrade.
- During "Fatal Error", the server cannot be restored, a new server build is required. The server must be rebuilt using the same DSR release of its mate server.
- During typical failure, the system can be restored using the following command: `/var/TKLC/backout/diUpgrade --clearError`
- In case of upgrade failure due to an early check, restart the server prior to retrying the upgrade.
- This procedure is applicable for VSTP installation as well.
- SDS must be upgraded before DSR.
- For the User Data Repository upgrade, refer to User Data Repository upgrade document.
- Backout is not supported for OL6 to OL8 Upgrade (DSR-8.6 to DSR-9.0).
- `majorUpgrade.sh` will run the dual hop upgrade command and copy the ISO file to the required path. In order to perform the upgrade, it will also install Ansible RPM.

Prerequisites

- SDS 9.0.2.0.0 requires more disk space and RAM capacity. Hence, create flavor to resize the instance and refer to *DSR Cloud Benchmarking Guide* for flavor details.
- Ensure the instance which must be upgraded does not contain any alarms. To check the alarm status before triggering the upgrade, run the following command:

  ```
  alarmMgr --alarmStatus
  ```

- Space utilization should be less than 70% for all partitions and no hard disk alarm should be present. Run the following command to check:

  ```
  df -kh
  ```

- Download the `dualHopUpgrade.tar.gz` file from Oracle Software Delivery Cloud (OSDC) site. Extract the file to retreive the following files, which are required to perform this upgrade:
  - `pre_upgrade_check.sh`
  - `extend_partition.sh`
  - `post_partition.sh`
  - `diuMajHosts`
  - `vault.yml`
  - `majorUpgrade.sh`

> **Note:**
>
> Backout is not supported for OL6 to OL8 upgrade (DSR 8.6 to 9.0).

The following table provides the time required by each task while performing Dual Hop Upgrade (DIU) from SDS 8.6.X VM to SDS 9.0.x VM.

Table B-1 Time Required for Dual Hop Upgrade

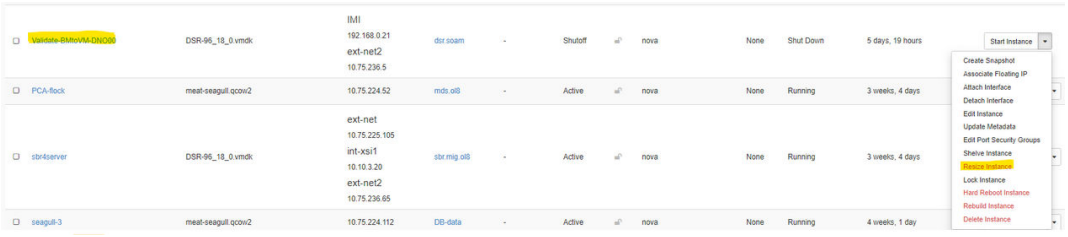
Procedure	Time Required (hr:min)	Reference
Step 1	0:10 - 0:20 for each VM	Resizing all the Instances in the Setup
Step 2	0:10 - 0:20 for each VM	Extending the Partition
Step 3	0:20 - 0:30	Setting up the Active NOAM as Controller
Step 4	0:40 - 0:60	Upgrading Standby NOAM
Step 5	0:05 - 0:10	Configuring Upgraded Standby NOAM
Step 6	0:05 - 0:10	Setting up Active NOAM as Controller
Step 7	0:40 - 0:60 for each Group	Upgrading Other Servers

B.1 Resizing all the Instances in the Setup

> **Note:**
>
> For procedure to resizing instances if the setup used is in KVM environment, see Resizing Instances if Setup is in KVM Environment.

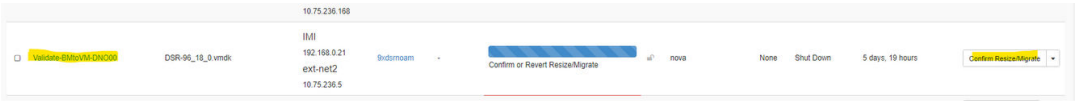
1. Login to OpenStack GUI.
2. Shutdown the instance.
3. Select **Resize Instance** option and configure the required flavour.

Figure B-1 Resizing Instance



4. Select the instance and click **Confirm Resize**.

Figure B-2 Confirm Resize



5. Start the instance.

B.1.1 Resizing Instances if Setup is in KVM Environment

> **Note:**
>
> Perform this procedure on the Host where VM is deployed.

1. Shutdown VM by running the following command:

```
virsh shutdown <VM Name>
```

   Wait for the VM to shut down.

2. Run the following commands:

```
virsh dumpxml <VM Name> | grep 'disk type' -A 5
```

Output:

```
[root@ol-server ~]# virsh dumpxml Dsrtestsetup-Noam1 | grep 'disk type' -A
5
<disk type='file' device='disk'>
<driver name='qemu' type='qcow2'/>
<source file='/mnt/data/ova/Dsrtestsetup-Noam1.qcow2'/>
<target dev='vda' bus='virtio'/>
<address type='pci' domain='0x0000' bus='0x05' slot='0x00' function='0x0'/>
</disk>
```

```
qemu-img info {{ path with image name }}.qcow2
```

Output:

```
[root@ol-server ~]# qemu-img info /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
image: /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
file format: qcow2
virtual size: 120 GiB (128849018880 bytes)
disk size: 7.56 GiB
cluster_size: 65536
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
```

```
qemu-img resize {{ path with image name }}.qcow2 +<additional required
size>G
```

Output:

```
[root@ol-server ~]# qemu-img resize /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
+40G
Image resized.
```

3. Verify VM sixe, by running the following command:

```
qemu-img info {{ path with image name }}.qcow2  (To verify VM size)
```

Output:

```
[root@ol-server ~]# qemu-img info /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
image: /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
file format: qcow2virtual size: 160 GiB (171798691840 bytes)
disk size: 7.56 GiB
cluster_size: 65536
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
    extended l2: false
```

4. Start VM by running the following command:

```
virsh start <VM Name>
```

B.2 Extending the Partition

1. Provide `chmod 777` permission to all the scripts.
2. Download the scripts from the tar file and place it in `/home/admusr` directory.

3. Run the following command:

   ```
   sudo ./extend_partition.sh
   ```

4. Restart the server.

   ```
   sudo init 6
   ```

5. Run the following commands:

   ```
   sudo ./post_partition.sh.
   ```

   ```
   sudo ./pre_upgrade_check.sh
   ```

   > **Note:**
   >
   > This is a manual step and must be run on all the servers.

6. Switchover the roles from Standby to Active and Active to Standby.

   > **Note:**
   >
   > - Resize new standby, by performing Resizing all the Instances in the Setup and Extending the Partition procedures.
   > - For NOAM, SOAM, and IPFE, perform Resizing all the Instances in the Setup and Extending the Partition procedures on both Standby and Active.
   > - For DAMP, perform Resizing all the Instances in the Setup and Extending the Partition procedures except Switchover step.

B.3 Setting up the Active NOAM as Controller

1. Place the TPD OL7 DIU ISO and SDS DIU ISO on `/var/TKLC/db/filemgmt` of Active NOAM.
2. Create diuMajHosts file in `/home/admusr` of Active NOAM.

Note:

Description of diuMajHosts file:

- image_name_tpd: TPD OL7 DIU ISO name should be given
- image_name_dsr: SDS DIU ISO name should be given

For the SDS Dual hop upgrade, use the groups as mentioned below:

- Divide the servers into the groups with the xmi IP of the servers that need to be upgraded, as shown in the example below.
- group1 → We have included the IP of Stanby Noam in group1, as this would be the first server we want to upgrade.
- group2 → In this group Active Noam IP is included. (Stanby noam after switchover) and Query Server
- group3 → This group will contain the IP of Standby Soam.
- group4 → This group will contain the IP of Active Soam.
- group5 and group6→ These groups will contain 50% of C-level servers respectively.

There can be n number of groups in the below file.

Host name (host1, host2....) must be different for different groups.

For example:

```
[all:vars]
image_name_tpd=TPD OL7 DIU ISO
image_name_sds=SDS DIU ISO

[group1]
host1 ansible_host=<XMI IP of StandBy NOAM>  ansible_user=admusr
ansible_port=22

[group2]
host2 ansible_host=<XMI IP of Active NOAM>  ansible_user=admusr
ansible_port=22
host3 ansible_host=<XMI IP of Query Server>  ansible_user=admusr
ansible_port=22

[group3]
host4 ansible_host=<XMI IP of Standby SOAM> ansible_user=admusr
ansible_port=22

[group4]
host5 ansible_host=<XMI IP of Active SOAM> ansible_user=admusr
ansible_port=22

[group5]
host6 ansible_host=10.75.237.93  ansible_user=admusr ansible_port=22  -----
> DMP00
.
.
```

```
.
[group6]
host8 ansible_host=10.75.237.141ansible_user=admusr ansible_port=22  -----
> DMP01
.
.
.
```

3. Create the `vault.yml` file in `/home/admusr` of Active NOAM.

   ```
   ansible_ssh_pass: secret_password(password for admusr)
   ```

4. Place the `majorUpgrade.sh` script in `/var/TKLC/db/filemgmt` of Active NOAM.
5. Run the following command:

   ```
   chmod 777 /var/TKLC/db/filemgmt/majorUpgrade.sh
   ```

B.4 Upgrading Standby NOAM

- Run the following commands on the Active NOAM Shell.

  ```
  cd /var/TKLC/db/filemgmt


  ./majorUpgrade.sh upgrade group1
  ```

B.5 Verifying Upgrade

Perform the following steps to verify whether the upgrade is successful on a particular host.

1. To print the logs whether the upgrade is successful, run the `majorUpgrade.sh` script.

   > **Note:**
   >
   > Before starting with the next step run `majorUpgrade.sh` script on every group.

2. Run the following command on the instance which was upgraded:

   ```
   sudo verifyUpgrade
   ```

   If the upgrade is successful , the above command would not return any output.

B.6 Configuring Upgraded Standby NOAM

1. Login to Active NOAM.
2. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
3. Click **Edit** and update the **Max Allowed HA Role** value of Active NOAM to `Standby`, then click **Ok**.

4. Login to Standby NOAM from GUI, which is now the Active NOAM.
5. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
6. Click **Edit** and update the **Max Allowed HA Role** value of Standby NOAM to `Active`, then click **Ok**.

B.7 Setting up Active NOAM as Controller

1. Copy `majorUpgrade.sh` file from Standby NOAM to Active NOAM in `/var/TKLC/db/filemgmt` path, by performing the following steps:
   a. SSH to Standby NOAM console.
   b. Navigate to `/var/TKLC/db/filemgmt` path.
   c. Run the following command to copy the `majorUpgrade.sh` script to file management path of Active NOAM:

      ```
      scp majorUpgrade.sh admusr@<Active Noam IP>:/var/TKLC/db/filemgmt
      ```

2. Copy `diuMajHosts` and `vault.yml` files from Standby NOAM to Active NOAM in `/home/admusr` path, by performing the following steps:
   a. SSH to Standby NOAM console.
   b. Navigate to `/home/admusr/` path.
   c. Run the following command to copy the `diuMajHosts` and `vault.yml` files to `/home/admusr` path of Active NOAM:

      ```
      scp diuMajHosts admusr@<Active Noam IP>:/home/admusr
      ```

      ```
      scp vault.yml admusr@<Active Noam IP>:/home/admusr
      ```

B.8 Upgrading Other Servers

- Run the following commands to upgrade remaining servers:

  ```
  cd /var/TKLC/db/filemgmt
  ```

  ```
  ./majorUpgrade.sh upgrade group2
  ```

  ```
  ./majorUpgrade.sh upgrade group3
  ```

> **Note:**
> Run this command for all remaining groups.