Oracle® Communications

Diameter Signaling Router

DSR Cloud Software Upgrade Guide

Release 8.0

E75969-02

May 2017

ORACLE

Oracle® Communications Diameter Signaling Router, DSR Cloud Software Upgrade Guide, Release 8.0

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

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

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

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

Table of Contents

List of Figures

List of Tables

List of Procedures

1. Introduction

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform the following upgrades:

- Major upgrade from DSR 7.0.x, 7.1.x, 7.2, and 7.3 to 8.0
- Incremental upgrade from an earlier DSR 8.0 build to a later 8.0 build

The upgrade of cloud deployments is covered by this document. The audience for this document includes Oracle customers as well as following internal groups: Software Development, Quality Assurance, Information Development, and Consulting Services including NPx. This document provides step-by-step instructions to execute any incremental or major cloud software upgrade.

The execution of this procedure assumes that the target DSR 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.

1.1.1 What is Not Covered by this Document

The following items are beyond the scope of this document. Refer to the specified reference for additional information.

- Distribution of DSR 7.x/8.0 software loads. It is recommended you contact MOS for the software loads as described in Appendix M.
- Initial installation of DSR software. Refer to [1] DSR 8.0 Cloud Installation Guide, E76331, Oracle.
- SDS installation. Refer to [2] SDS Cloud Installation document, E76333, Oracle.

1.2 References

[1] DSR 8.0 Cloud Installation Guide, E76331, Oracle
[2] SDS Cloud Installation document, E76333, Oracle
[3] Maintenance Window Analysis Tool CGBU_010314, Oracle
[4] DSR 6.0 to 7.0 Migration – IPFE Aspects, CGBU_770, Oracle
[5] Fast Deployment and Configuration Tool Technical Reference, CGBU_ENG_24_2353, Oracle
[6] Cloud DSR 8.0 Disaster Recovery Guide, E76332, Oracle
[7] Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) in DSR 7.1 by Enabling SCTP AUTH Extensions By Default, OSD 2019141.1

1.3 Acronyms

Table 1. Acronyms

Acronym	Definition
ASG	Automated Server Group upgrade
ASU	Automated Site Upgrade
CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
cSBR	Charging Session Binding Repository
DA	Diameter Agent

Acronym	Definition
DA MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
DSR DR NOAM	Disaster Recovery DSR NOAM
FABR	Full Address Based Resolution
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
HA	High Availability
IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent
SBR	Session Binding Repository
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

1.4 Terminology

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

Table 2. Terminology

Term	Definition
1+1	Setup with one active and one standby server.
Backout	The process of converting a single DSR 8.0 server to a prior version. This could be performed due to failure in single server upgrade or the upgrade cannot be accepted for some other reason. Backout is a user-initiated process.
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.
Geographic Site	A **Geographic Site** is defined as the physical location of a SOAM and its co-located children as well as its non-preferred spare SOAM(s). In this document, a geographic site is designated as **GSite**.
Health Check	Procedure used to determine the health and status of the DSR's internal network. This includes status displayed from the DSR GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
Incremental Upgrade	An upgrade within a given DSR release, e.g., 8.0.x to 8.0.y.
Major Upgrade	An upgrade from one DSR release to another DSR release, e.g., DSR 7.0.1 to DSR 7.x or 8.0.
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (active/standby) policy to N+ 0 (multiple active) policies.
N+0	Setup with N active DA-MP(s), but no standby DA-MP.
NOAM	Network OAM for DSR.
Primary NOAM Network Element	The network element containing the active and standby NOAM servers in a DSR.
Release	Release is any particular distribution of software that is different from any other distribution.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.
Signaling Network Element	Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. Each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element.
Single Server Upgrade	The process of converting a DSR 8.0 server from its current release to a newer release.
Site	Physical location where one or more network elements reside. The site is defined by the SOAM.
SOAM	System OAM for DSR.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.

Term	Definition
Source Release	Software release to upgrade from
Target Release	Software release to upgrade to
Topological Site	A **Topological Site** is defined as a SOAM server group and all C-level server groups that are children of the SOAM. All servers within a server group belong to the server group's site, regardless of the physical location of the server. Thus, for upgrade, a topological site does not correlate to a network element or a place. In this document, a topological site is designated as **TSite**.
UI	User interface. Platcfg UI refers specifically to the Platform Configuration Utility User Interface, which is a text-based user interface.
Upgrade	The process of converting an application from its current release on a system to a newer release.
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 upgrading a server. The state is defined by the following attributes: • Server is forced standby • Server is application disabled (signaling servers do not process any traffic)

1.5 How to Use this Document

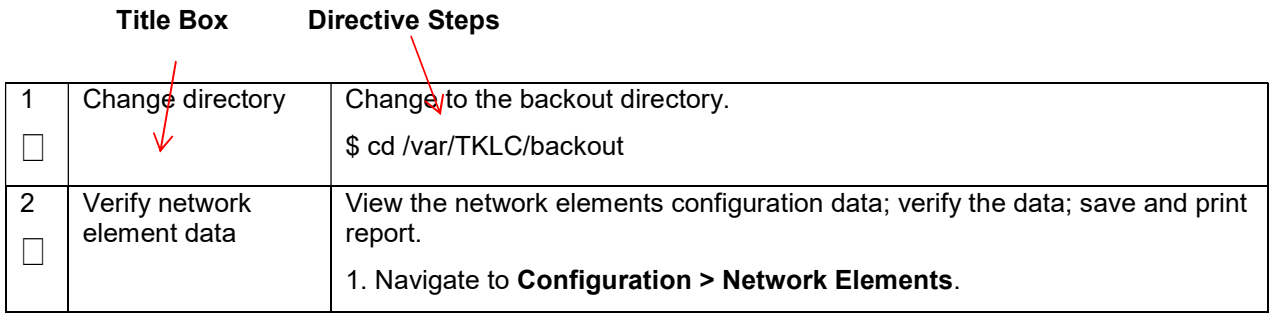
When executing the procedures in this document, there are a few key points that help to ensure the user understands procedure convention. These points are:

- Before beginning a procedure, completely read the instructional text (it displays immediately after the section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before execution of a STEP within a procedure, completely read the left and right columns including any STEP-specific WARNINGS or NOTES.
- If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP. It is recommended you contact My Oracle Customer Support for assistance, as described in Appendix M, before attempting to continue.

1.5.1 Executing Procedures

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

- Each step has a checkbox the user should check-off to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as Step X.Y. The example in Figure 1 shows Step 1 and Step 2.1 to Step 2.6.
- The title box describes the operations to be performed during that step.
- GUI menu items, action links, and buttons to be clicked on are in **bold** Arial font.
- GUI fields and values to take note of during a step are in **bold** Arial font.
- Each command that the user enters, as well as any response output, is formatted in `10-point bold Courier` font.



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

Figure 1. Example Procedure Steps Used in This Document

1.6 Recommendations

This section provides some recommendations to consider when preparing to execute the procedures in this document.

1.6.1 Frequency of Health Checks

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

1.6.2 Large Installation Support

For large systems containing multiple signaling network elements, it is impossible to upgrade multi-site systems in a single maintenance window.

1.6.3 Logging of Upgrade Activities

It is a best practice to use a terminal session with logging enabled to capture user command activities and output during the upgrade procedures. These can be used for analysis in the event of issues encountered during the activity. These logs should be saved off line at the completion of the activity.

1.7 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 you contact My Oracle Customer Support as directed in Appendix M before starting the upgrade.

1.7.1 PCA/PDRA Application – PCRF Pooling Migration Precheck

If the PCA application or the PDRA application has been activated in the source release, PCRF pooling **MUST** be enabled, and the PCRF Pooling Migration **MUST** be completed before the start of a major upgrade to DSR 8.0.

!! WARNING!! **THE UPGRADE TO RELEASE 8.0 FAILS IF PCRF POOLING MIGRATION IS NOT COMPLETED WHEN THE PCA/PDRA APPLICATION IS ENABLED.**

The PCRF Pooling Migration Tool is provided to determine the status of the PCRF Pooling Migration. The tool has options to determine if the migration is complete, to indicate if upgrade is allowed or not allowed, and to estimate the time required to complete the Pooling migration.

The upgrade to DSR 8.0 CANNOT be scheduled until the PCRF Pooling Migration Tool is run to determine the status of the migration. Pooling migration can take days or weeks to complete, depending on the PCA/PDRA configuration and when PCRF Pooling was enabled.

When the tool determines that pooling migration is completed, a flag is set internally, which allows the upgrade to proceed.

Refer to Appendix C: PCRF Pooling Migration Check for instructions on how to execute the PCRF Pooling Migration check.

The PCRF pooling migration check is not required in the following scenarios:

- The PCA/PDRA application has not been activated.
- When upgrading from release 7.1.x, 7.2, or 7.3 (in this case, pooling migration has already completed).
- DSR 8.0 incremental upgrade.

1.7.2 PCA/PDRA Application – PCRF Pooling Enablement

For PCA/PDRA customers on release 5.1, 6.0, or 7.0, PCRF pooling must be enabled before upgrading to DSR 8.0. In addition, a workaround is required to correlate binding-dependent session creation messages on IMSI or MSISDN without an APN. There are two possible workarounds, described in the following sections. It is recommended you contact My Oracle Customer Support per Appendix M on which option is best for the customer.

1.7.2.1 Option A – Using Mediation Rules

This section provides an outline of the steps required to implement the mediation workaround. Note that this is not a step-by-step procedure for creating and using the mediation rules, but rather an overview of the process.

- Verify all APNs are mapped to the **default** PCRF pool.

  This ensures only one binding exists for a given subscriber even after enabling PCRF pooling.
- Configure ingress mediation rule to add a called-station-ID AVP (code=30, RFC 4005) to binding dependent session creation Diameter messages (e.g., Rx AAR).
  - The AVP value must match one of the APNs that created the binding(s) for the subscriber.
  - Using this APN value, existing PDRA/SBR logic finds a bound PCRF and routes the Diameter message to it.
  - Since ALL APNs are bound to the same PCRF, it is not important what APN was used to find the binding as long as a binding is found.
- Configure egress mediation rule to remove the called-station-ID AVP if it was added by mediation at ingress.
- Enable PCRF pooling and wait for the migration to complete

  All PCRF pooling configuration requirements for binding capable interfaces must still be met.
- Upgrade to DSR 8.0.

1.7.2.2 Option B – Patch

This section provides an outline of the steps required to implement the patch workaround. Note that this is not a step-by-step procedure for creating and using the patch.

- Build patches on a customer-to-customer basis.
  - The patch does the following:
    - Relax the mandate to have APNs in the binding dependent session creation request
    - Find the first final binding for the subscriber and return the PCRF identifier
    - Route the binding dependent session creation request to the bound PCRF.
  - Verify all APNs are mapped to the **default** PCRF pool.
    - This ensures only one binding exists for a given subscriber even after enabling PCRF pooling.
    - Enable PCRF pooling and wait for the migration to complete.

      All PCRF pooling configuration requirements for binding capable interfaces must still be met.
- Upgrade to DSR 8.0.

1.7.3 Netbackup 7.7 Support

Netbackup 7.7 requires additional disk space that is not available before DSR Release 8.0. Thus, the DSR must be upgraded to Release 8.0 before upgrading to Netbackup 7.7.

!! WARNING!! **UPGRADE THE DSR TO RELEASE 8.0 BEFORE UPGRADING TO NETBACKUP 7.7.**

1.7.4 Network IDIH Compatibility

Upgrading an IDIH site to release 8.0 makes it incompatible for viewing network trace data contained in remote IDIH sites that are running a prior release. The incompatibility is removed once all network IDIH systems have been upgraded to release 8.0.

To view network traces for a network of IDIH systems where there is a mix of systems running release 8.0 and systems running a prior release, Procedure 67 in Appendix I must be executed to prepare the systems running IDIH release 8.0 to support IDIH systems running the prior release. After executing Procedure 67, network traces should be viewed only from an IDIH system running the prior IDIH release. Viewing a network trace from an IDIH 8.0 results in a visualization that is incomplete because the IDIH 8.0 system fails to retrieve Trace Transaction Records (TTRs) from IDIH systems running the prior IDIH release.

When all IDIH systems have been upgraded to release 8.0, Procedure 68 should be executed on each IDIH system where Procedure 67 was previously executed to ensure that no errors occur when viewing network traces.

1.7.5 Review Release Notes

Before starting the upgrade, it is recommended to review the release notes for the target release to understand the functional differences and possible traffic impacts of the upgrade.

2. General Description

This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release

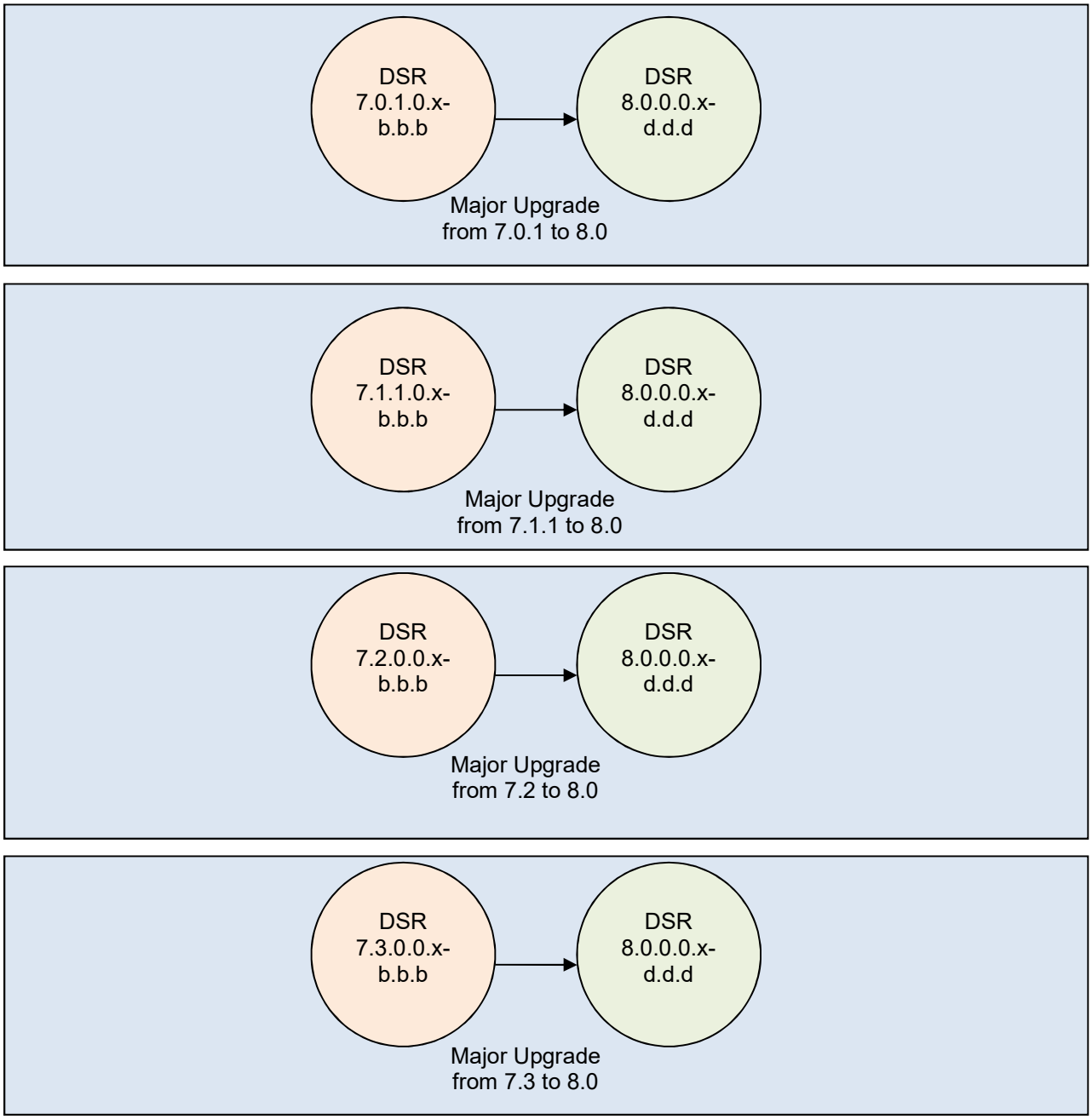
7.x to target release 8.0. An incremental upgrade advances the DSR from an earlier DSR 8.0 source release to a more recent 8.0 target release.

Note that for any incremental upgrade, the source and target releases must have the same value of **x**. For example, advancing a DSR from 8.0.0.0.0-80.1.0 to 8.0.0.0.0-80.2.0 is an incremental upgrade. But advancing a DSR running a 7.2 release to an 8.0 target release constitutes a major upgrade.

2.1 Supported Upgrade Paths to 8.0

The supported paths to upgrade to a DSR 8.0 target release are shown in Figure 2.

Note: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.



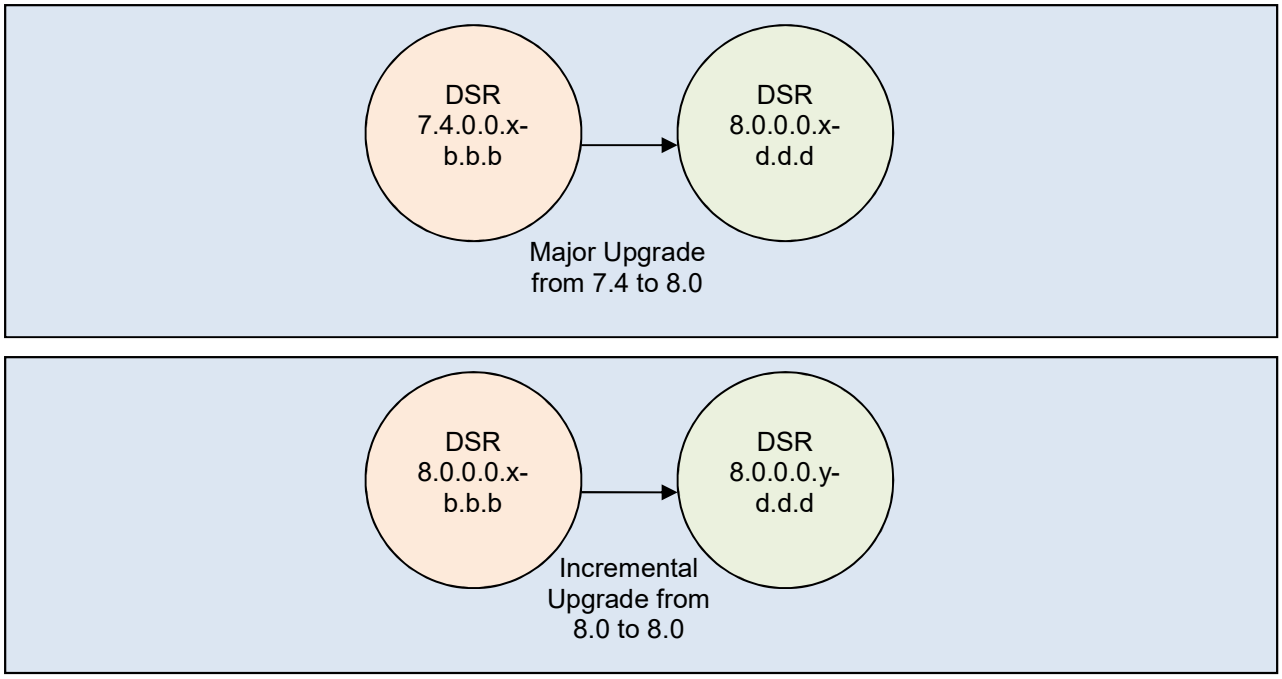


Figure 2. DSR 8.0 Supported Upgrade Paths

2.2 Geo-Diverse Site (Active/Standby/Spare PCA configuration)

With a Geo-Diverse site, the upgrade of the SOAM active/standby servers must also include an upgrade of the spare SOAM at the geo-redundant site, in the same maintenance window.

2.3 Traffic Management during Upgrade

The upgrade of the NOAM and SOAM servers is not expected to affect traffic processing at the DA-MPs and other traffic-handling servers.

For the upgrade of the DA-MPs and IPFEs, traffic connections are disabled only for the servers being upgraded. The remaining servers continue to service traffic.

!! WARNING!! SCTP Datagram Transport Layer Security Change

Oracle introduced SCTP Datagram Transport Layer Security (DTLS) in DSR 7.1 by enabling SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced in [7] Cloud DSR 8.0 Disaster Recovery Guide, E76332, Oracle. It is highly recommended that customers upgrading to Release 8.0 should prepare clients before the DSR is upgraded. This ensures the DSR-to-Client SCTP connection establishes with DTLS with SCTP AUTH extensions enabled.

If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices WILL NOT restore after the DSR is upgraded to DSR 8.0. In the event the SCTP connections do not re-establish after the upgrade, follow the Disable/Enable DTLS procedure in [1] DSR 8.0 Cloud Installation Guide, E76331, Oracle.

2.4 Automated Site Upgrade

With DSR 8.0, 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 all C-level 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 DSR servers. However, Automated Site Upgrade cannot be used to upgrade IDIH servers at a site.

An important definition with regard to a site upgrade is the **site**. For the purposes of DSR site upgrade, a **site** is defined as a SOAM server group plus all subtending servers of that server group, **regardless of physical location**. To demonstrate this definition, Figure 3 shows three physical locations, labeled **TSite 1**, **TSite 2**, and **TSite3**. Each site contains a SOAM server group and an MP server group. Each SOAM server group has a spare SOAM that, although physically located at another site, is a member of the site that **owns** the server group. With site upgrade, SOA-Sp is upgraded with the Site 1 SOA server group, and SOB-sp is upgraded with the Site 2 SOB server group. The MP server groups are upgraded in the same maintenance window as their respective site SOAMs. These sites conform to the **Topological Site** definition of Table 2. Terminology.

With this feature, a site upgrade can be initiated on SO-A SG and all of its children (in this example, MP1 SG) using a minimum of GUI selections. The upgrade performs the following actions:

- Upgrade SOA-1, SOA-2, and SOA-sp.
- Upgrade the servers in MP1 SG based on an availability setting and HA roles.
- Immediately begins the upgrade of any other server groups, which are also children of SO-A SG (not shown). These upgrades begin in parallel with step 2.

Server groups that span sites (e.g., SOAMs and SBRs) are upgraded with the server group to which the server belongs. This results in upgrading spare servers that physically reside at another site, but belong to a server group in the SOAM that is targeted for site upgrade.

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

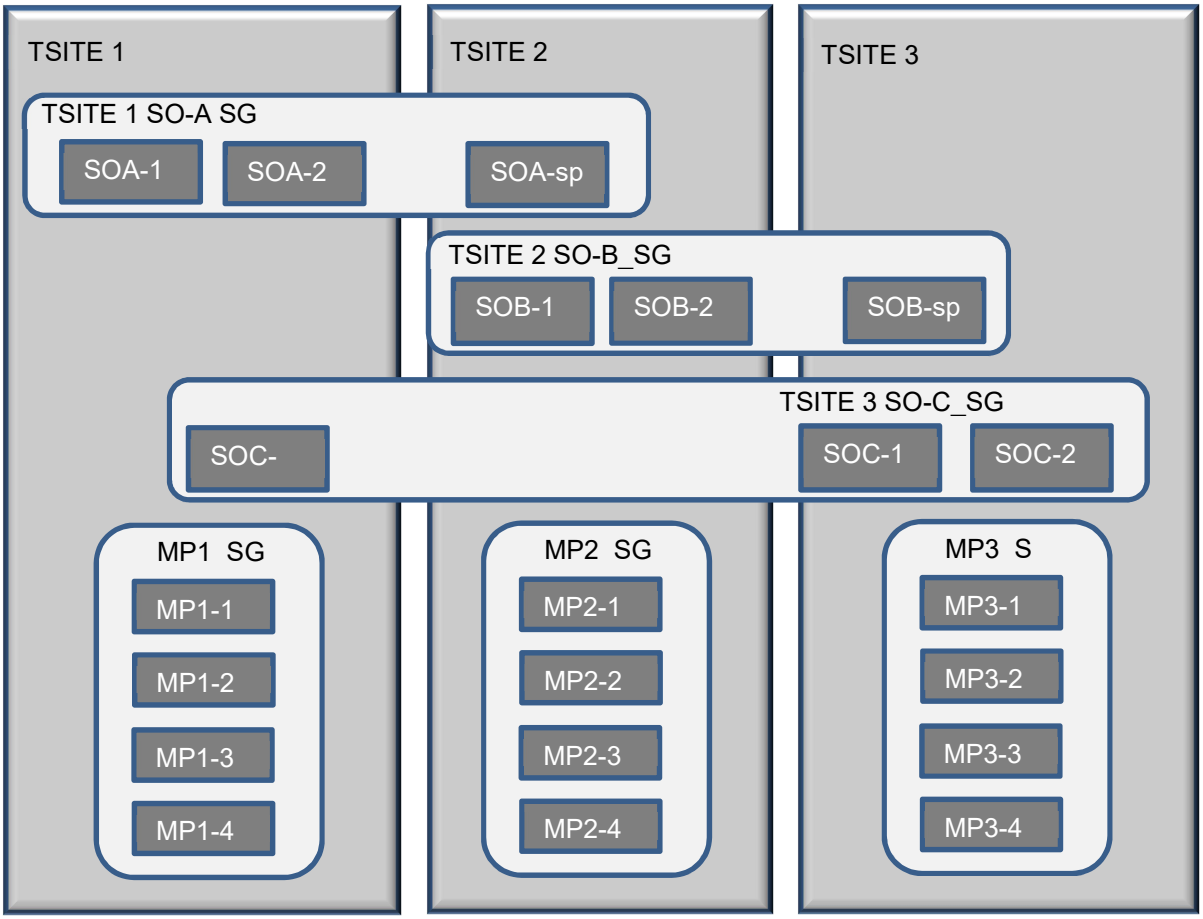


Figure 3. Upgrade Perspective of DSR Site Topology

2.4.1 Site Upgrade Execution

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

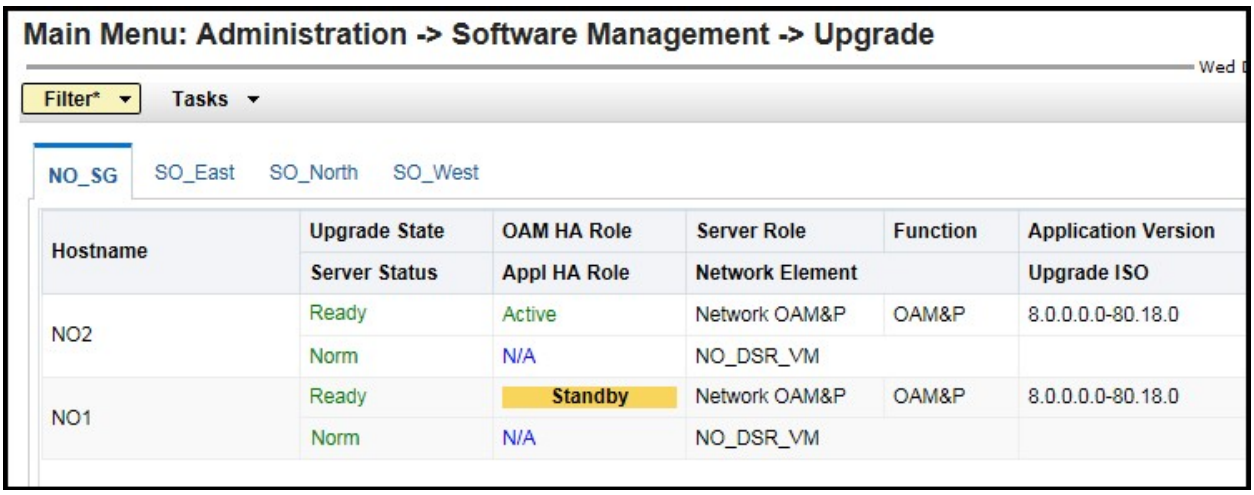


Figure 4. Site Upgrade – NOAM View.

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

- The Upgrade Method column shows how the server group will be upgraded. The upgrade method is derived from the server group function and the bulk availability option (see Section 2.4.3 for additional details on bulk availability).
- The Server Upgrade States column groups the servers by state, indicating the number of servers in the server group that are in each state.
- The Server Application Versions column indicates the current application version, indicating the number of servers in the server group that are at each version.

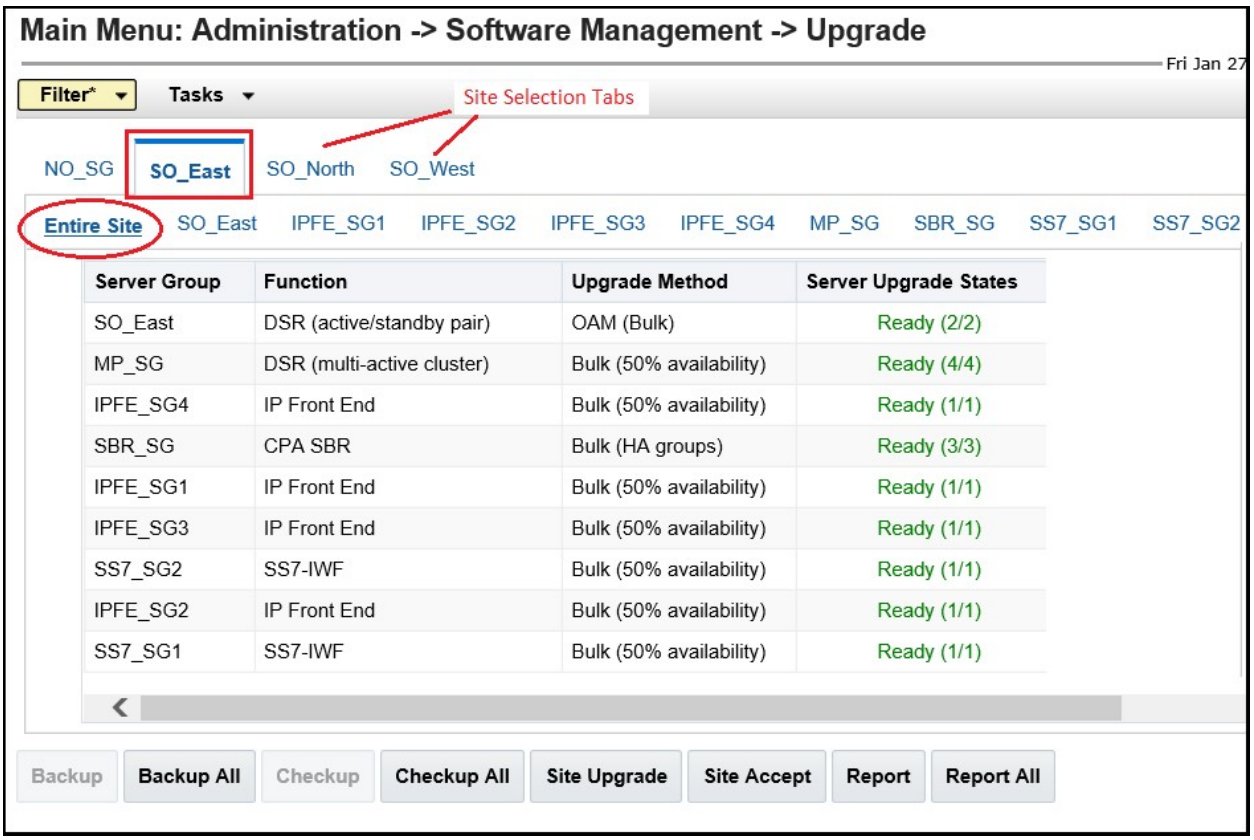


Figure 5. Site Upgrade – Entire Site View.

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

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

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

Click **Site Upgrade** from the **Entire Site** view to display the Upgrade [Site Initiate] screen (Figure 6). The Site Initiate screen presents the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 6, Cycle 1 is 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 2.4.3.

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

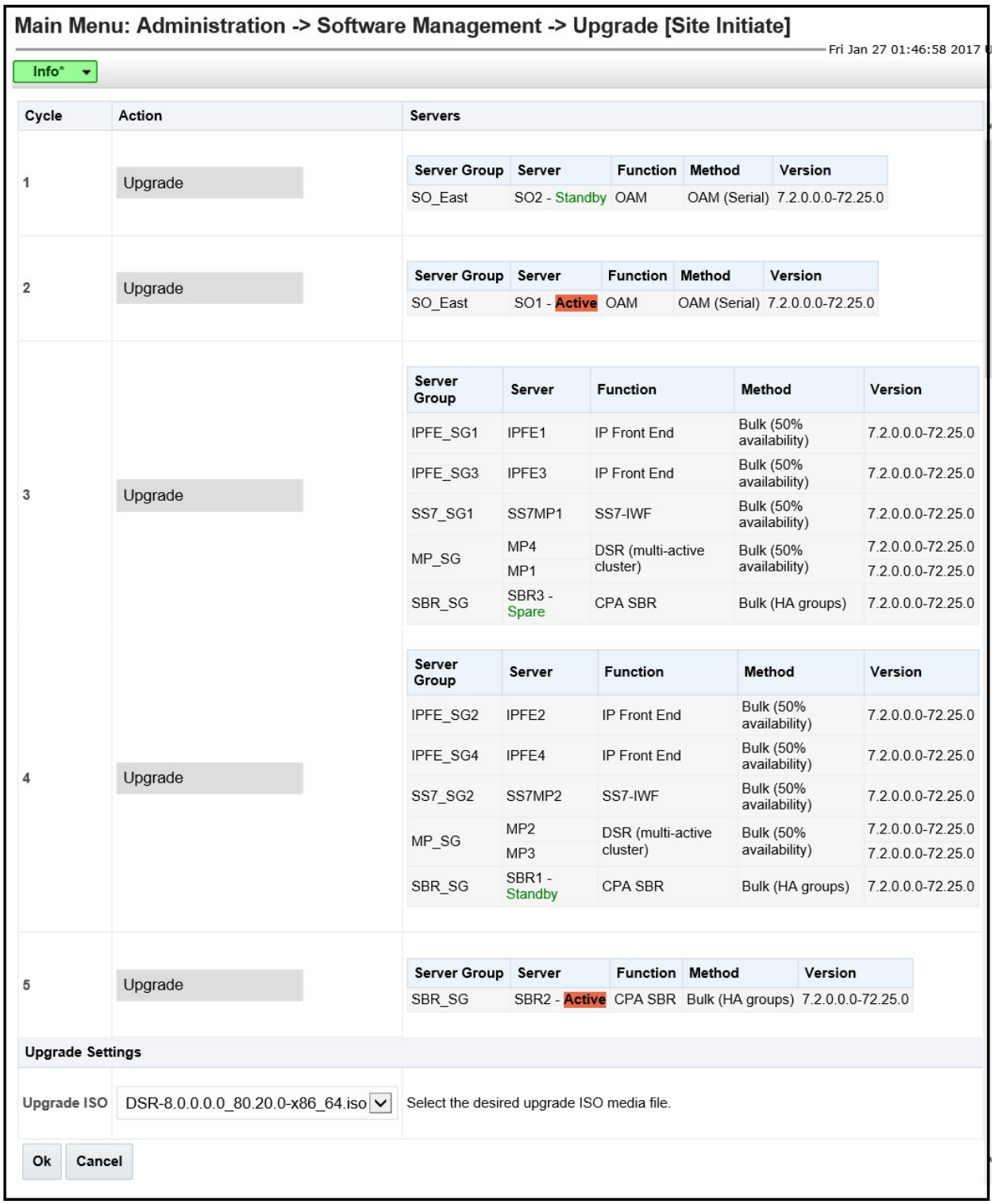


Figure 6. Site Upgrade – [Site Initiate] Screen.

Cycles 3 through 5 upgrade all of the C-level servers for the site. These cycles are **not** atomic.

In Figure 6, Cycle 3 consists of IPFE1, IPFE3, MP1, MP4, and SBR3. Because some servers can take longer to upgrade than others, there may be some overlap in Cycle 3 and Cycle 4. For example, if IPFEs 1 and 3 complete the upgrade before SBR3 is finished (all are in Cycle 3), the upgrade allows IPFEs 2

and 4 to begin, even though they are part of Cycle 4. This is to maximize maintenance window efficiency. The primary factor for upgrading the C-level servers is the upgrade method for the server group function (i.e., bulk by HA, serial, etc.).

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. Table 3 describes the server selection considerations for each server group function.

Note: The minimum availability option is a central component of the server selections for site upgrade. The effect of this option on server availability is described in detail in Section 2.4.2.

Table 3. Server Selection vs. Server Group Function

SG Function	Selection Considerations
DSR (multi-active cluster) (e.g., DA-MP)	The selection of servers is based primarily on the minimum server availability option. Servers are divided equally (to the extent possible) among the number of cycles required to enforce minimum availability. For DA-MPs, an additional consideration is given to the MP Leader. The MP with the leader designation is the last DA-MP to be upgraded to minimize leader changes[1].
DSR (active/standby pair) (e.g., DA-MP)	The DA-MP active/standby pair configuration is not supported for Automated Site Upgrade.
DSR (active/standby pair) (e.g., SOAM)	The SOAM upgrade method is dependent on the Site SOAM Upgrade option on the General Options page. See Section 2.4.3.
SBR	SBRs are always upgraded serially, thus the primary consideration for selection is the HA designation. The upgrade order is spare – spare – standby – active.
IP Front End	IPFEs require special treatment during upgrade. One consideration for selection is the minimum server availability, but the primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2. If minimum availability permits, IPFE A1 can be upgraded with IPFE B1, and IPFE A2 can be upgraded with B2.
SS7-IWF	SS7-MPs are treated as a multi-active cluster of servers, similar to DA-MPs, even though each server is in a separate server group. The selection of SS7-MPs is based primarily on the minimum server availability option. Servers are divided equally (to the extent possible) among the number of cycles required to enforce minimum availability.

[1] In the event of a leader change while upgrades are in progress, the MP leader may not be the last MP to be upgraded.

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

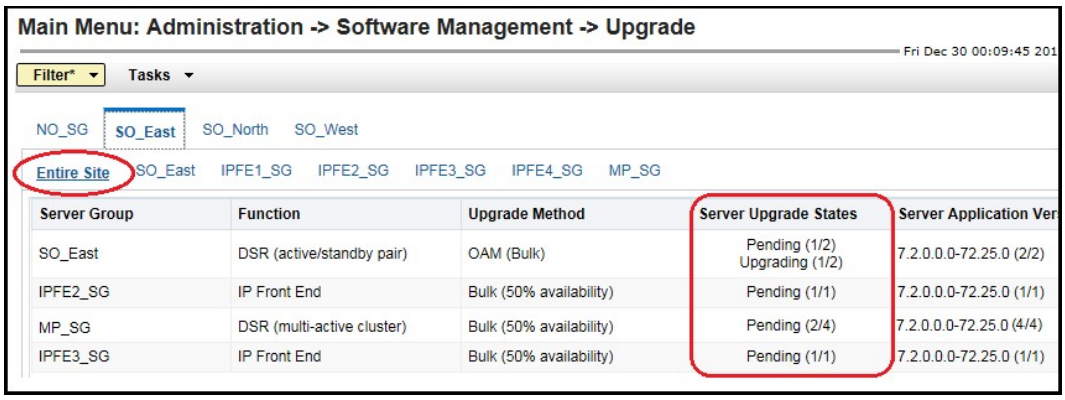


Figure 7. Site Upgrade Monitoring

Select a server group link on the upgrade administration screen to populate the table rows with the upgrade details of the individual servers within that server group (Figure 8).

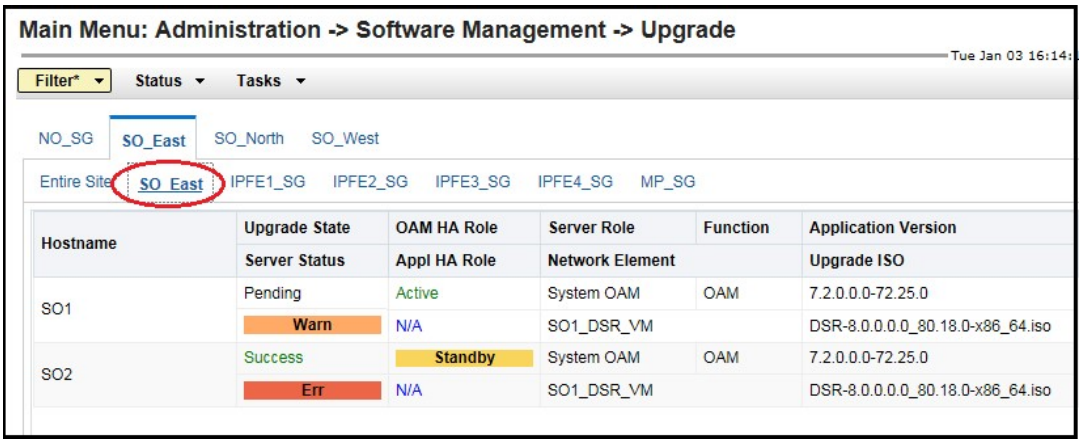


Figure 8. Server Group Upgrade Monitoring

Upon completion of a successful upgrade, every server in the site is in the **Accept** or **Reject** state. See Section 2.4.4 for a description of cancelling and restarting the Automated Site Upgrade.

2.4.2 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 servers 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 2.4.3.

The application of minimum server availability differs for the various server group functions. For some function types, it is a straight calculation of a percentage. However, for others, minimum availability does not apply due to overriding operational considerations. Table 4 describes the application of availability for the various server group functions.

Table 4. Site Upgrade Availability vs. Server Group Function

Server Group Function	Server Availability
DSR (multi-active cluster)	In a multi-active cluster, the availability percentage applies to all of the servers in the server group. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.
SBR	Availability percentage does not apply to SBR server groups. SBRs are upgraded in a very specific order: spare – spare – standby – active.
IP Front End	Availability percentage applies to all IPFEs provisioned in the site. For this function type, the IPFE server groups are treated as a multi-active cluster of servers. To avoid a traffic outage, IPFE-A1 and IPFE-A2 are not upgraded together, and IPFE-B1 and IPFE-B2 are not upgraded together. IPFE-A1 and IPFE-B1 (as well as IPFE-B1 and IPFE-B2) may be upgraded together, if permitted by the availability percentage.
SS7-IWF	Availability percentage applies to all SS7-MPs provisioned in the site. For this function, the SS7-IWF server groups are treated as a multi-active cluster of servers. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.

When calculating the number of servers required to satisfy the minimum server availability, all servers in the server group (or server group cluster) are considered. Servers that are OOS or otherwise unable to perform their intended function, are included, as are servers that have already been upgraded. For example, consider a DA-MP server group with 10 servers; four have already been upgraded, one is OOS, and five are ready for upgrade. With a 50% minimum availability, only four of the servers that are ready for upgrade, can be upgraded in parallel. The four servers that have already been upgraded count toward the five that are needed to satisfy minimum availability. The OOS server cannot be used to satisfy minimum availability, so one of the upgrade-ready servers must remain in-service for minimum availability, thus leaving four servers to be upgraded together. Upgrading the last server would require an additional upgrade cycle.

2.4.3 Site Upgrade Options

To minimize user interactions, the automated site upgrade makes use of a pair of pre-set options to control certain aspects of the sequence. These options control how many servers remain in service while others are upgrading and are located on the **Administration > General Options** screen (Figure 9). The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

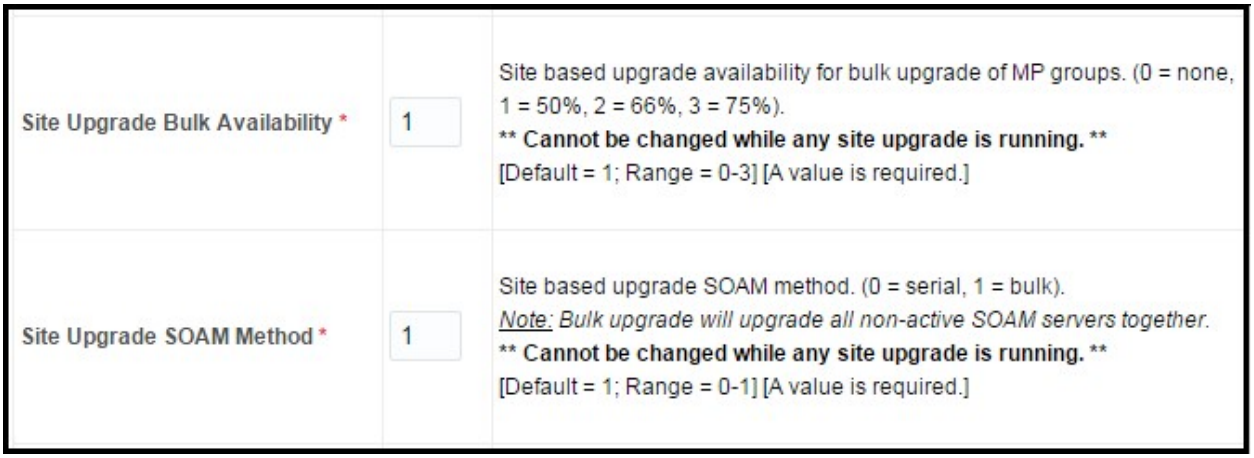


Figure 9. Automated Site Upgrade General Options

The first 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. This upgrade method requires at most two upgrade cycles to upgrade all of the SOAMs, regardless of how many are present. If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

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 (i.e., spare – spare – standby – active). If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

Regardless of the SOAM upgrade method, the active SOAM is always upgraded after the standby and spare SOAMs.

The second 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 that 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 DA-MPs to be upgraded at once. This setting is not recommended for live production systems.

The application of minimum server availability varies for the different types of C-level servers. For example, for a multi-active DA-MP server group, the minium availability applies to all of the DA-MPs within the server group. But, for other server types, such as SS7-MP, there is only one server per server group. For this server type, the SS7-MP server groups are treated as a multi-active cluster of servers. The availability percentage applies across all of the SS7-MP server groups. This same setup applies to IPFEs as well. Table 4 defines how the Site Upgrade Bulk Availability setting on the General Options page affects the various server group function types.

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.
```

2.4.4 Cancelling and Restarting Automated Site Upgrade

When an Automated 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 via the Active Task screen (**Status & Manage > Tasks > Active Tasks**).

The main site upgrade controller task is identified by the naming convention **<site_name> Site Upgrade**. In Figure 10, the main task is task ID 22. This task is controlling the server group upgrade task (task ID 23), which in turn is controlling the server upgrade task (task ID 24).

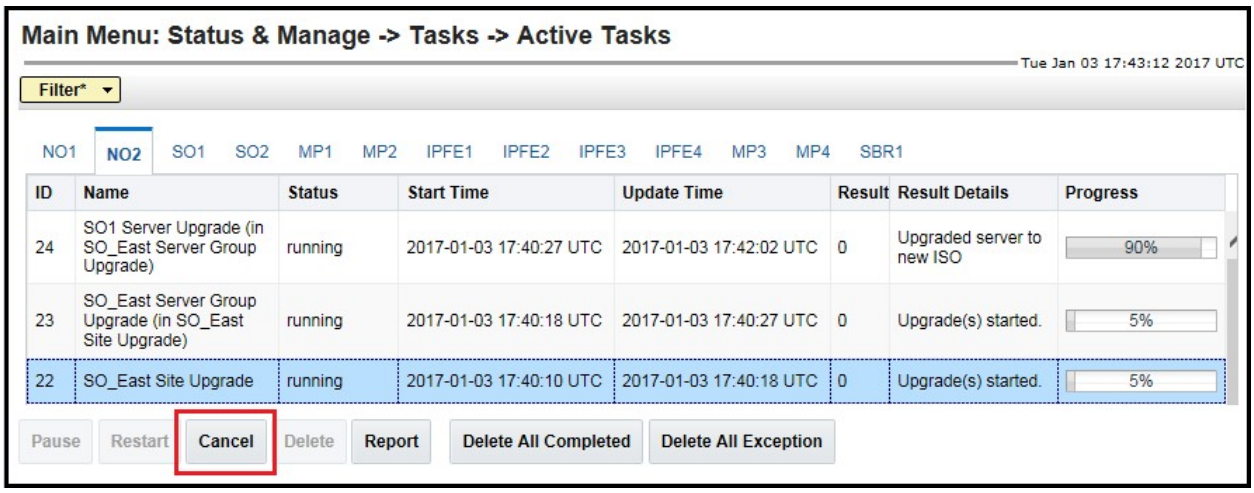


Figure 10. Site Upgrade Active Tasks

To cancel the site upgrade, select the site upgrade task and click **Cancel**. A screen requests confirmation of the cancel operation. The status changes from **running** to **completed**. The **Results Details** column updates to display **Site upgrade task cancelled by user**. All server group upgrade tasks that 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 11 shows the Active Task screen after a site upgrade has been cancelled.

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

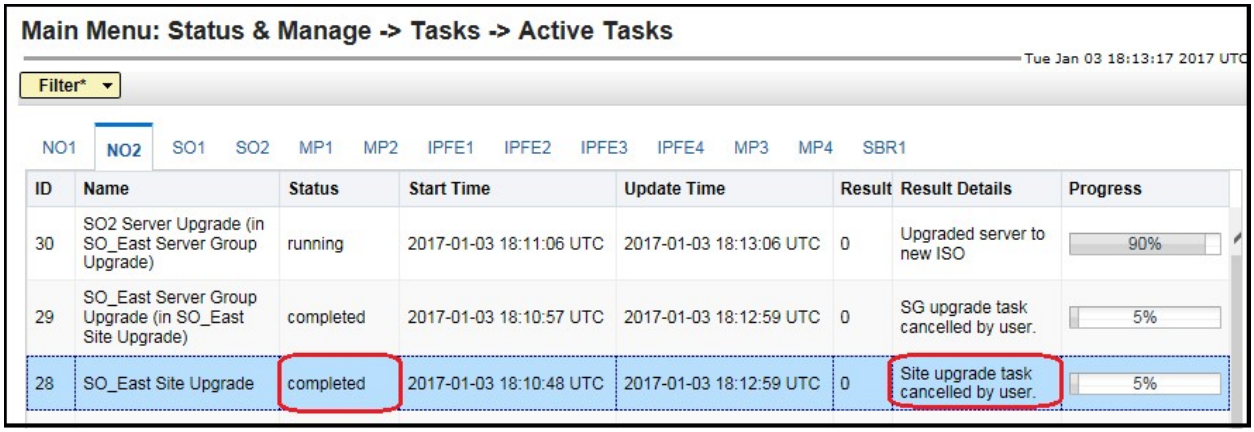


Figure 11. Cancelled Site Upgrade Tasks

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

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

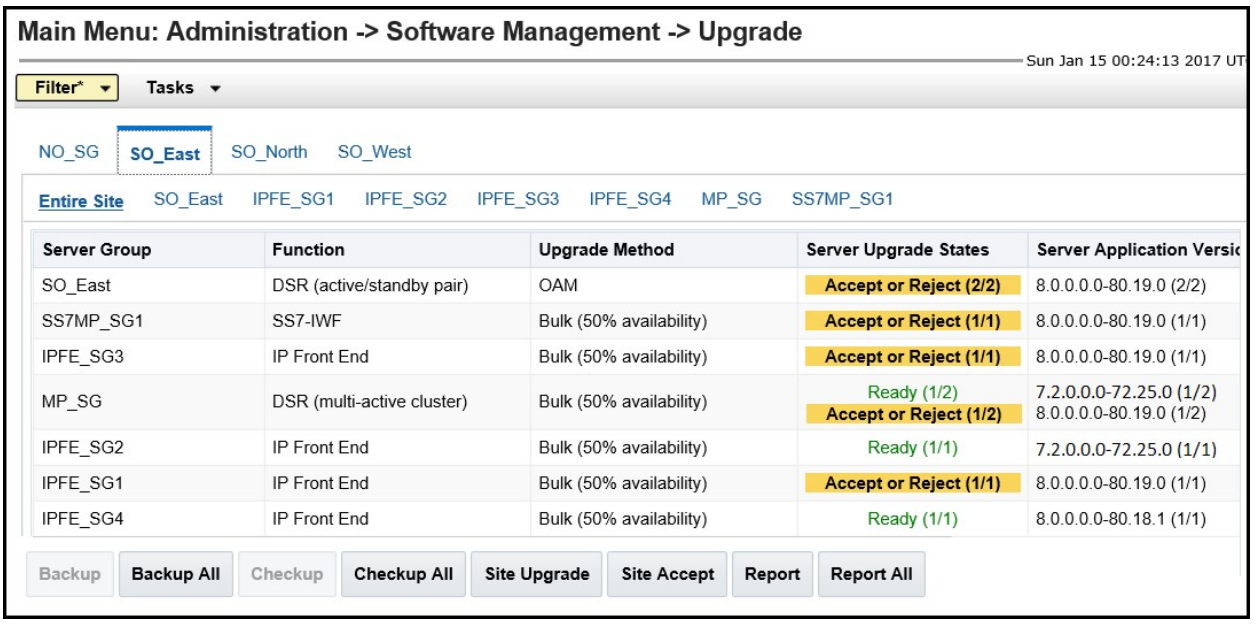


Figure 12. Partially Upgraded Site

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. For the upgrade that was cancelled in Figure 11, only a single cycle is needed since the availability requirements can be met by the servers that have already been upgraded. Select an ISO and click **OK** to continue the site upgrade.

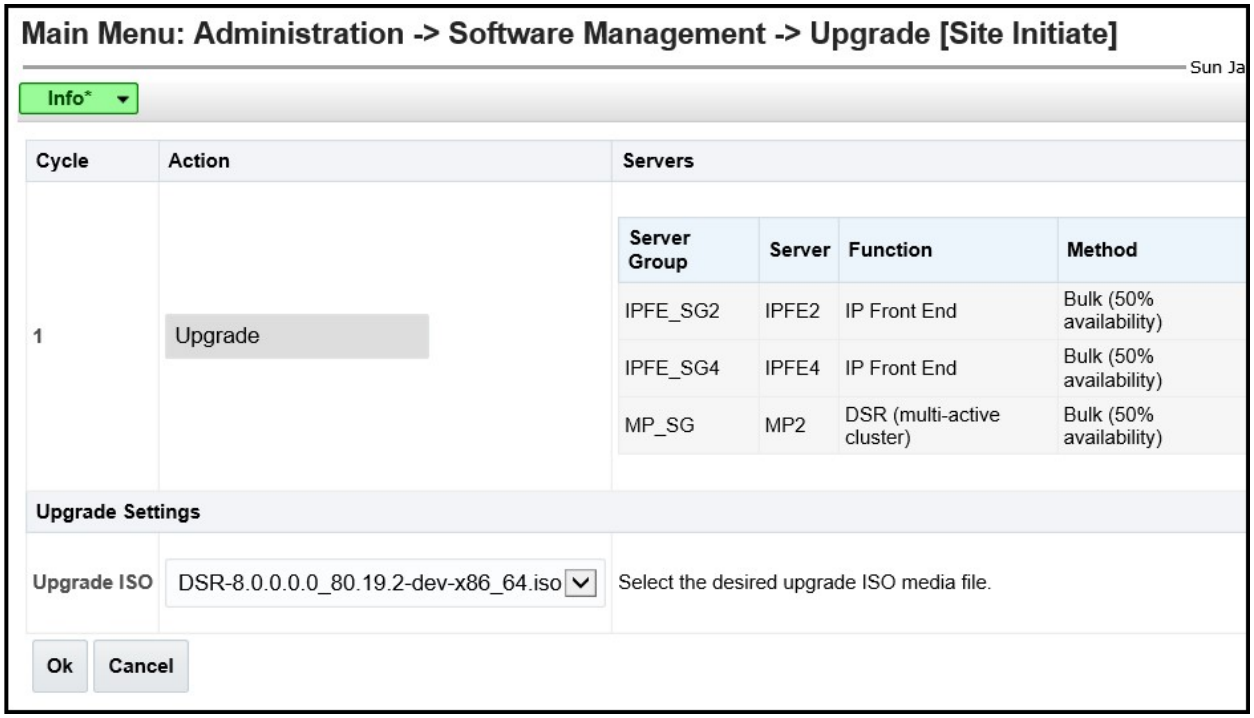


Figure 13. Restarting Site Upgrade

2.5 Automated Server Group Upgrade

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

The purpose of ASG is to simplify and automate segments of the DSR upgrade. The DSR 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 affect 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, as well as the appropriate parameters that should be selected for each server group type.

ASG is the default upgrade method for most server group types associated with the DSR. However, the manual upgrade method is used in some instances. 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.

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

2.5.1 Cancelling and Restarting Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be manually cancelled from the **Status & Manage > Active Tasks** screen (Figure 14) if necessary. Once the task is cancelled, it cannot be restarted. However, a new ASG task can be restarted via the Upgrade Administration screen.

For example, in Figure 14, task ID #1 (SO_SG Server Group Upgrade) is an ASG task, while task ID #2 is the corresponding individual server upgrade task. When the ASG task is selected (highlighted in green), the **Cancel** button is enabled. Cancelling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tas ks that were started by the ASG task (i.e., task ID #2 in Figure 14). Because the ASG task is cancelled, no new server upgrades are initiated by the task.

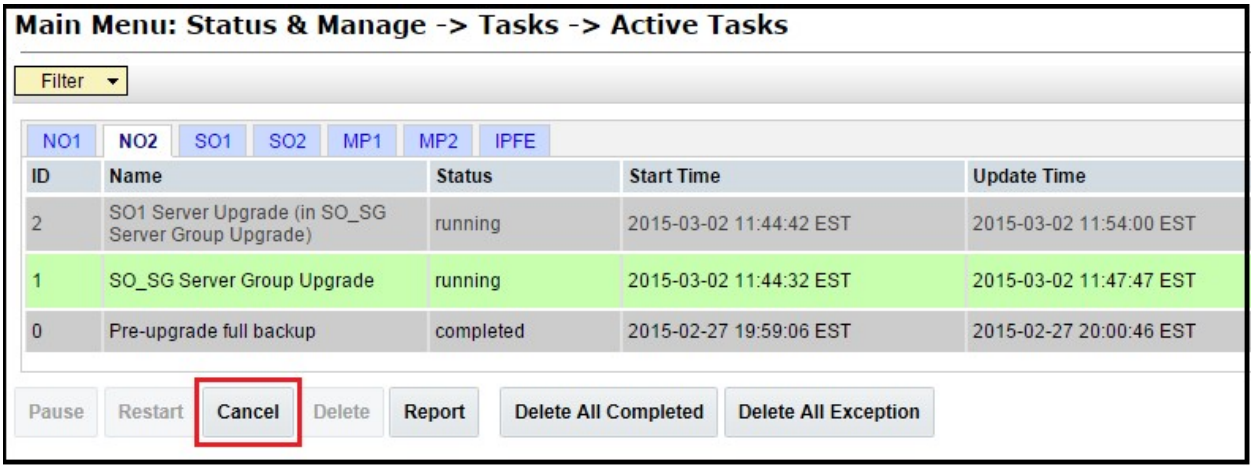


Figure 14. Active Tasks Screen

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

2.5.2 Site Accept

Before DSR 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.

Click **Site Accept** on the upgrade GUI (Figure 15) to nearly simultaneously Accept the upgrade of some or all servers for a given site. A subsequent screen (Figure 16) displays the servers that are ready for the Accept action.

Figure 15. Site Accept Button

A checkbox on the Upgrade [Site Accept] screen allows for the selective application of the Accept action. However, normal procedure calls for the Accept to be applied to all of the servers at a site only after the upgrade to the new release is stable and the back out option is no longer needed. After verifying the information presented is accurately, click **OK** to confirm the server upgrade.

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**.

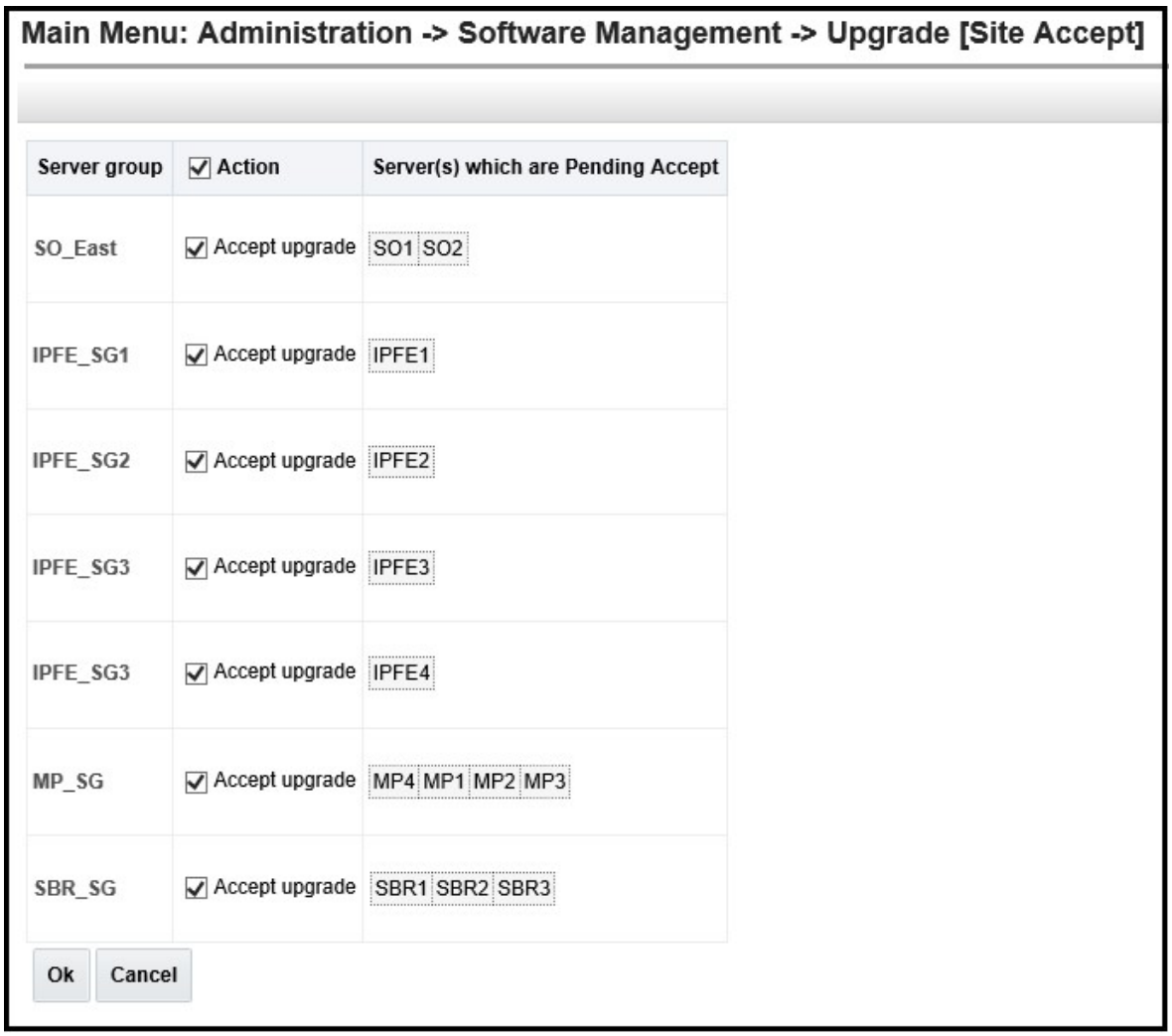


Figure 16. Site Accept Screen

3. Upgrade Planning and Pre-Upgrade Procedures

This section contains all information necessary to prepare for and execute an upgrade. The materials required to perform an upgrade are described, as are pre-upgrade procedures that should be run to ensure the system is fully ready for upgrade. Then, the actual procedures for each supported upgrade path are given.

There are overview tables throughout this section that help plan the upgrade and estimate how long it takes to perform various actions. The stated time durations for each step or group of steps are estimates only. Do not use the overview tables to execute any actions on the system. Only the procedures should be used when performing upgrade actions, beginning with Procedure 1. Required Materials Check.

3.1 Required Materials and Information

The following materials and information are needed to execute an upgrade:

- Target-release application ISO image file or target-release application media.
- The capability to log into the DSR 7.x Network OAM servers with Administrator privileges.

Note: All logins into the DSR NOAM servers are made via the External Management VIP unless otherwise stated.

- User logins, passwords, IP addresses, and other administration information. See [Table 5].
- VPN access to the customer's network is required if that is the only method to log into the OAM servers.

3.1.1 Application ISO Image File/Media

Obtain a copy of the target release ISO image file or media. This file is necessary to perform the upgrade.

The DSR ISO image file name is in the following format (version changes from release to release):

DSR-8.0.0.0.0_80.xx.0-x86_64.iso

Note: Before the execution of this upgrade procedure it is assumed the DSR ISO image file has already been delivered to the customer's premises. The ISO image file must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image file. If the user performing the upgrade is at a remote location, it is assumed the ISO file is already available before starting the upgrade procedure.

The ISO is deployed as part of the pre-upgrade activities in Section 3.4.

3.1.2 Logins, Passwords and Server IP Addresses

Table 5 identifies the information that is called out in the upgrade procedures, such as server IP addresses and login credentials. For convenience, space is provided in Table 5 for recording the values, or the information can be obtained by other means. This step ensures the necessary administration information is available before an upgrade.

Consider the sensitivity 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 prevent the actual recording of this information in hard-copy form.

Table 5: Logins, Passwords, and Server IP Addresses

Item	Description	Recorded Values
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username[1]	
	GUI Admin Password	
	DSR admusr Password[2]	
	DSR Root Password[2]	
VPN Access Details	Customer VPN information (if needed)	
NOAM	XMI VIP address[3]	
	NOAM 1 XMI IP Address	
	NOAM 2 XMI IP Address	
SOAM	XMI VIP address	

[1] The user must have administrator privileges. This means the user belongs to the **admin** group in Group Administration.

[2] This is the password for the server login. This is not the same login as the GUI Administrator. The admusr password is required if recovery procedures are needed. If the admusr password is not the same on all other servers, then all those servers' admusr passwords must also be recorded; use additional space at the bottom of this table.

[3] All logins into the NOAM servers are made via the External Management VIP unless otherwise stated.

Item	Description	Recorded Values
	SOAM 1 XMI IP Address (Site 1)	
	SOAM 2 XMI IP Address (Site 1)	
	PCA (DSR) Spare System OAM&P server – Site 1 Spare in Site 2, XMI IP Address	
	SOAM 1 XMI IP Address (Site 2)	
	SOAM 2 XMI IP Address (Site 2)	
	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 1)	
	Binding SBR SR2 Server Group Servers (Site 1)	
	Binding SBR SR3 Server Group Servers (Site 1)	
	Binding SBR SR4 Server Group Servers (Site 1)	
PCA MP Server Group	PCA MP Server Group Servers (Site 1)	
	PCA MP Server Group Servers (Site 1)	
IPFE Server Groups(For PDRA)	PCA IPFE A1 Server Group Server (Site 1)	
	PCA IPFE A 2 Server Group Server (Site 1)	
	PCA IPFE B 1 Server Group Server (Site 1)	
	PCA IPFE B 2 Server Group Server (Site 1)	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 2)	
	Binding SBR SR2 Server Group Servers (Site 2)	
	Binding SBR SR3 Server Group Servers (Site 2)	
	Binding SBR SR4 Server Group Servers (Site 2)	
PCA MP Server Group	PCA MP Server Group Servers (Site 2)	
IPFE Server Groups (For PCA)	PCA IPFE A1 Server Group Server (Site 2)	
	PCA IPFE A 2 Server Group Server (Site 2)	
	PCA IPFE B 1 Server Group Server (Site 2)	
	PCA IPFE B 2 Server Group Server (Site 2)	
SS7-IWF Server Groups	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
Software	Target Release Number	
	ISO Image (.iso) file name	
Misc.[4]	Miscellaneous additional data	

[4] As instructed by Oracle CGBU Customer Service.

3.2 Plan Upgrade Maintenance Windows

This section provides a high-level checklist to aid in tracking individual server upgrades. The servers are grouped by maintenance window, and it is expected that all servers in a group can be successfully upgraded in a single maintenance window. Use this high-level checklist together with the detailed procedures that appear later in this document.

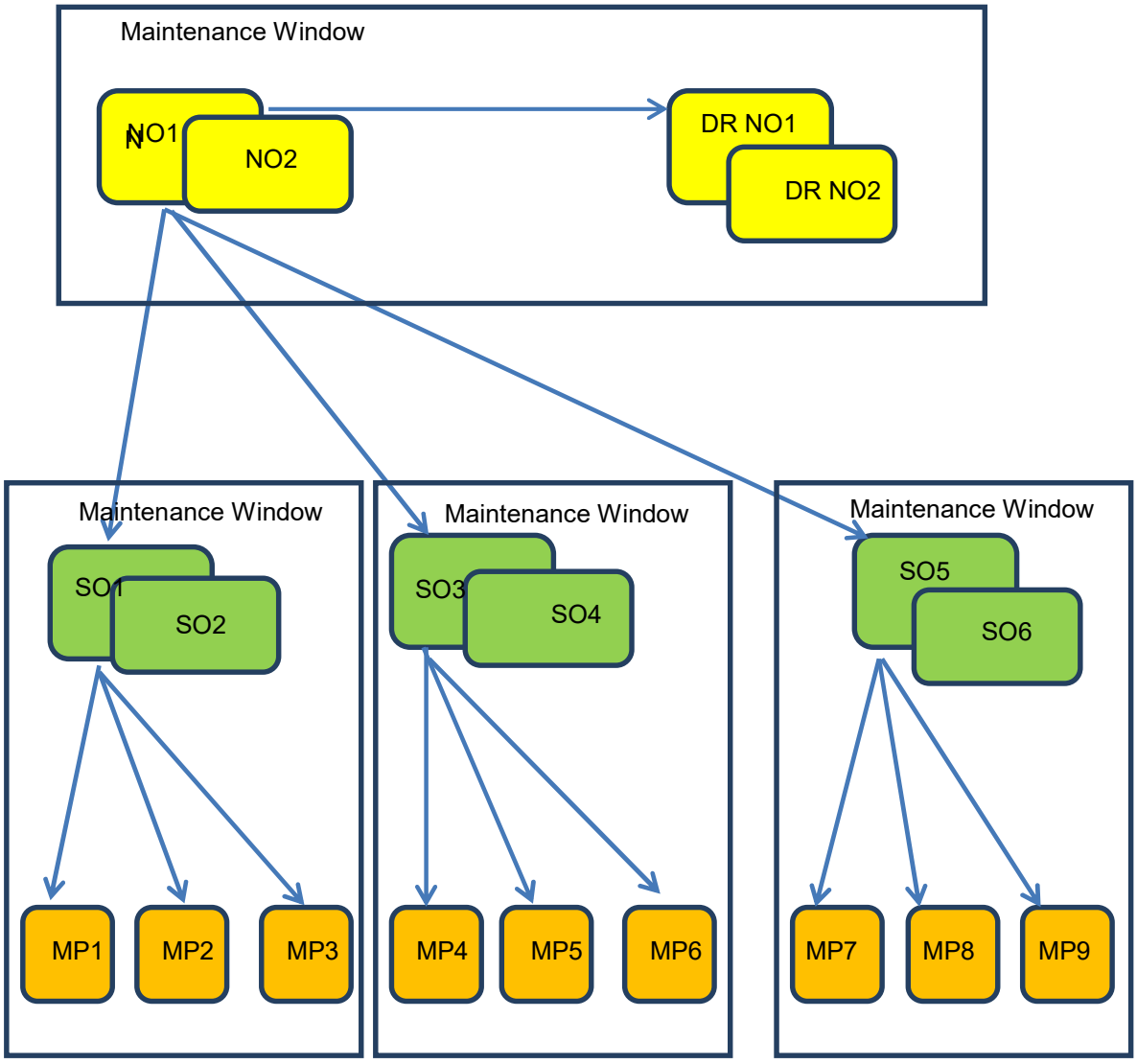


Figure 17. Upgrade Maintenance Windows for 3-Tier Upgrade

!! WARNING!! **MATED SOAM SITES MUST BE UPGRADED IN SEPARATE MAINTENANCE WINDOWS**

3.2.1 Calculating Maintenance Windows Required

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see reference [3] SDS Cloud Installation document, E76333, Oracle).

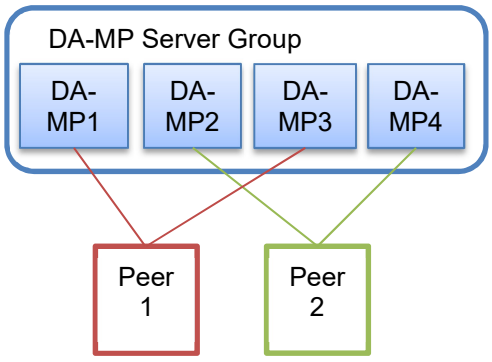
This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. The spreadsheet also specifies, in detail, which servers need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in reference [3] SDS Cloud Installation document, E76333, Oracle. Please see the instructions tab of the spreadsheet for more information and details.

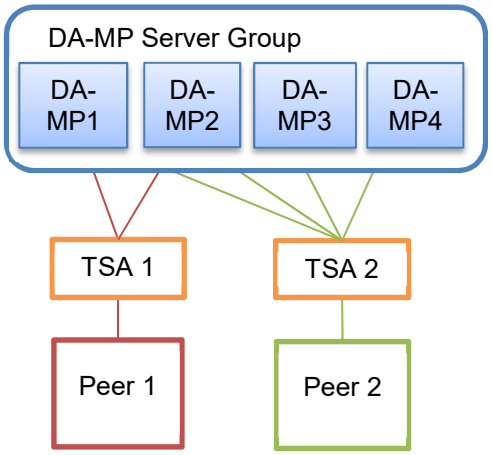
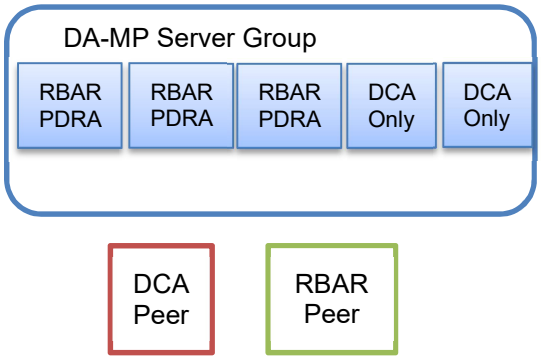
3.3 Site Upgrade Methodology Selection

There are three primary methods for upgrading a DSR site: Automated Site Upgrade, Automated Server Group Upgrade, and manual upgrade. The Automated Site Upgrade is the easiest and most efficient site upgrade method; however, it is not suitable for all customers or all configurations. The Automated Server Group upgrade incorporates many of the conveniences of Automated Site Upgrade, but allows for more customer control of the upgrade process. Again, Automated Server Group upgrade is not for all customers or all configurations. The manual upgrade method gives maximum control to the customer and can be used for all configurations. A combination of upgrade methods can be used to upgrade a given site to maximize efficiency with customer peace-of-mind.

Table 6 is a worksheet for determining which upgrade method meets the needs of the customer while ensuring compatibility with the DSR configuration. Upon completion of the worksheet, a recommended upgrade method is identified.

Table 6. Traffic Analysis Checklist

	Criteria	Yes	No	Notes
1.	Do any of the site's DA-MPs have fixed diameter connections to any peer node, similar to the depiction below? 	☐	☐	Automated Site Upgrade and Automated Server Group upgrade do not consider fixed peer connections when selecting servers to upgrade. It is possible that all DA-MPs servicing a given peer (such as DA-MPs 1 and 3) is upgraded simultaneously, thereby isolating the peer. Automated Site Upgrade and Automated Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. If no, continue with step 2.

	Criteria	Yes	No	Notes
2	If peer nodes are configured via IPFE TSAs, are there any TSAs that are not distributed across all DA-MPs, similar to the depiction below? 	☐	☐	Automated Site Upgrade and Automated Server Group upgrade do not consider non-uniformly distributed TSAs when selecting servers to upgrade. It is possible that all DA-MPs servicing a given TSA (such as DA-MPs 1 and 2) is upgraded simultaneously, thereby isolating the peer. Automated Site Upgrade and Automated Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. If no, continue with step 3.
3	Do any of the site's DA-MPs have specialized distribution of DSR features, similar to the depiction below? 	☐	☐	Automated Site Upgrade and Automated Server Group upgrade do not consider non-uniform distribution of features when selecting servers to upgrade. It is possible that all DA-MPs hosting a given feature (such as DCA) is upgraded simultaneously, thereby eliminating service functionality. Automated Site Upgrade and Automated Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. If no, continue with step 4.
4	Is the DA-MP server group in the active/standby pair (1+1) configuration?	☐	☐	The DA-MP active/standby pair is not supported for Automated Site Upgrade. The site is a candidate for Automated Server Group upgrade. If yes, proceed to step 7. If no, continue with step 5.

	Criteria	Yes	No	Notes
5	Automated Site Upgrade is a candidate for this system. Automated Site Upgrade supports 50% minimum server availability by default. A general option allows availability percentage settings of 66% or 75%. Is 50%, 66%, or 75% server availability during upgrade acceptable to the customer?	☐	☐	In general, a higher minimum availability setting increases the time required to upgrade a site. On the other hand, a lower minimum availability may reduce operational redundancy during the upgrade. If none of the minimum availability options are acceptable, Automated Site Upgrade should not be used to upgrade the site. If yes, continue with step 6. If no, proceed to step 7.
6	Is the customer comfortable with minimum user intervention (i.e., user input) during the upgrade?	☐	☐	Once initiated, Automated Site Upgrade requires no additional user input to complete the upgrade. User control is limited to cancelling the site upgrade task. If yes, Automated Site Upgrade is the recommended upgrade method. If no, proceed to step 7.
7	Automated Server Group Upgrade is a candidate for this system. Is the customer comfortable with the level of control afforded by the Automated Server Group upgrade?	☐	☐	Automated Server Group upgrade allows the user to start the upgrade of each server group, while the individual servers within the server group upgrade automatically. If yes, Automated Server Group upgrade is the recommended upgrade method. If no, proceed to step 8.
8	A manual upgrade affords the maximum level of control over upgrade sequencing. 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, SBRs can be upgraded with Automated Server Group upgrade, while the DA-MPs may be upgraded manually to control the order of upgrade for traffic continuity.	☐	☐	A Manual upgrade is the recommended upgrade method.

3.3.1 DA-MP Upgrade Planning

If a manual upgrade is recommended by the Table 6 worksheet, additional planning is required to ensure a successful upgrade of the DA-MP server group. A manual upgrade is typically required/recommended when the DA-MPs are configured in a way such that an upgrade could result in a traffic outage. Pre-planning the upgrade of the DA-MPs is key to avoiding an outage.

Table 7 is an aid to laying out the sequence of the DA-MP upgrades, taking into consideration configuration and traffic continuity. **This worksheet must be completed by the customer and provided to Oracle if Oracle personnel are performing the upgrade**. It is highly recommended that the worksheet be completed for customer-driven upgrades as well.

Customer: perform an analysis of the Diameter application and connection configurations to assess any potential traffic loss due to the DA-MP upgrade. Complete the worksheet, specifying the order in which the DA-MPs are upgraded, and which MPs, if any, can be upgraded in parallel.

The worksheet is divided into four upgrade **cycles**. Each cycle represents an upgrade period during which one or more servers are upgraded. Distributing the DA-MPs servers over two or more cycles, takes advantage of parallism, thereby reducing the time required to upgrade the entire server group.

To achieve 50% server availability, half of hostnames would be listed in Cycle 1 while the other half would be listed in Cycle 2, requiring two upgrade cycles. Similarly, 75% availability can be achieved by spreading the hostname over all four cycles.

In all cases, regardless of the number of cycles used to upgrade the DA-MP server group, the DA-MP Leader should be the last server upgraded. Upgrading the DA-MP Leader last minimizes the number of leader changes during the upgrade. The DA-MP Leader is designated on the active SOAM at **Main Menu > Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader** = Yes.

Note: If desired, the DA-MPs can be upgrade serially, in which case, all hostnames would be listed in cycle 1. List the DA-MPs in the order in which they are upgraded.

Table 7. DA-MP Upgrade Planning Sheet

	Hostnames			
Upgrade Cycle 1 or Serial Upgrade				
	Hostnames			
Upgrade Cycle 2				
	Hostnames			
Upgrade Cycle 3				
	Hostnames			
Upgrade Cycle 4				
DA-MP Leader:				

3.3.2 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded.

Maintenance Window 1 (NOAM Sites) Date: _____ ***Note***: The NE Name may be viewed from the DSR NOAM GUI under **Main Menu -> Configuration -> Network Elements**.	• Record the Site **NE Name** of the DSR NOAM to be upgraded during Maintenance Window 1 in the space provided below: • Check off the associated checkbox as upgrade is completed for each server. ☐ DR Standby NOAM: _____ ☐ DR Active NOAM: _____ ☐ Primary Standby NOAM: _____ ☐ Primary Active NOAM: _____

3.3.3 Maintenance Window 2 and Beyond (SOAM Site Upgrades)

During Maintenance Window 2, all servers associated with the first SOAM aite are upgraded. All servers associated with the second SOAM site are upgraded during Maintenance Window 3.

For DSRs configured with multiple mated-pair sites, or DSRs having multiple, distinct sites (e.g., geo-redundant PCA installations), use the following form for the subsequent SOAM Site upgrades.

	**It is strongly recommended that mated pair SOAM sites are NOT upgraded in the same Maintenance Window.**

Maintenance Window (SOAM Sites) Date: _____ ***Note***: For 1+1 configuration, only 2 DA-MP(s) are present, one is active while the other is standby.	Record the Site NE Name of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided. Check off the associated checkbox as upgrade is completed for each server. SOAM Site: _____ ☐ Spare SOAM1: _____ (If equipped) ☐ Spare SOAM2: _____ (If equipped) ☐ Standby SOAM: _____ ☐ Active SOAM: _____

	☐ DA-MP1: _____ ☐ DA-MP2: _____ ☐ DA-MP3: _____ ☐ DA-MP4: _____ ☐ DA-MP5: _____ ☐ DA-MP6: _____ ☐ DA-MP7: _____ ☐ DA-MP8: _____ ☐ DA-MP9: _____ ☐ DA-MP10: _____ ☐ DA-MP11: _____ ☐ DA-MP12: _____ ☐ DA-MP13: _____ ☐ DA-MP14: _____ ☐ DA-MP15: _____ ☐ DA-MP16: _____
	☐ IPFE1: _____ ☐ IPFE2: _____ ☐ IPFE3: _____ ☐ IPFE4: _____
	☐ SS7-MP1: _____ ☐ SS7-MP2: _____ ☐ SS7-MP3: _____ ☐ SS7-MP4: _____ ☐ SS7-MP5: _____ ☐ SS7-MP6: _____ ☐ SS7-MP7: _____ ☐ SS7-MP8: _____

	Binding Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 2 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Binding Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ **(If equipped)**
	Session Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 2

	☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped) Session Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 **(Mate)**: _____ ☐ Spare SBR2 **(Mate)**: _____ (If equipped)

3.4 Prerequisite Procedures

The pre-upgrade procedures shown in the following table are executed outside a maintenance window, if desired. These steps have no effect on the live system and can save upon maintenance window time, if executed before the start of the maintenance window.

Table 8: Prerequisite Procedures Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 1	0:10-0:30	0:10-0:30	Required Materials Check	None
Procedure 2	0:20-0:30	0:30-1:00	Verification of Configuration Data	None

Procedure	Elapsed Time (hr:min) This Step	Elapsed Time (hr:min) Cum.	Procedure Title	Impact
Procedure 3 or Procedure 4 or Procedure 5 Procedure 6	0:45-2:00 0:45-1:00 0:15-0:20 0:15-0:20	1:15-3:00 1:15-2:00 0:45-1:20 0:45-1:20	Data Collection for Source Release 7.0.1 Data Collection for Source Release 7.1.x Data Collection for Source Release 7.2, 7.3, 7.4 Data Collection for Source Release 8.0 and later	None None None None
Procedure 7	0:15-3:00[1]	1:00-6:00	DSR ISO Administration	None
Procedure 8	0:05	1:05-6:05	ISO Link Correction	
Procedure 9 or Procedure 10	0:10-2:00	1:15-8:05	Full Backup of DB Rbun Environment for Release 7.0.1 or Full Backup of DB Run Environment for Release 7.1.x and later	None None
Procedure 11	0:03-2:30	1:18-10:35	Network Interface Workaround	None

[1] ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed, and may require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed before, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

3.4.1 Required Materials Check

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

Procedure 1. Required Materials Check

S T E P #	This procedure verifies that all required materials are present. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Verify all required materials are present	Materials are listed in Section 3.1 Required Materials. Verify required materials are present.
2. ☐	Verify all administration data needed during upgrade	Double-check all information in Section 3.2 Plan Upgrade Maintenance Windows is filled-in and accurate.
3. ☐	Contact My Oracle Customer Support	It is recommended you contact My Oracle Customer Support and inform them of plans to upgrade this system. See Appendix M for these instructions. Note that obtaining a new online support account can take up to 48 hours.

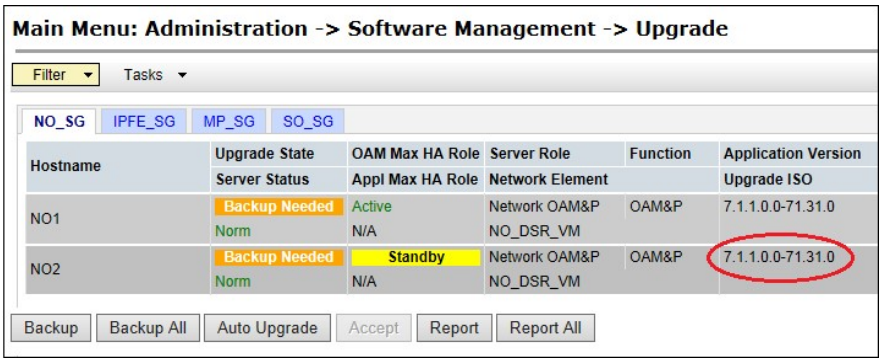
3.4.2 Data Collection – Verification of Global and Site Configuration Data

The procedures in this section are part of Software Upgrade Preparation and are used to collect data required for network analysis, Disaster Recovery, and upgrade verification. Data is collected from both the active NOAM and various other servers at each site.

3.4.2.1 Verification of Configuration Data

This procedure checks the configuration data of the system and servers to ensure a successful upgrade.

Procedure 2: Verification of Configuration Data

S T E P #		
	This procedure checks the configuration data and server status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**	• Navigate to **Administration -> Software Management -> Upgrade**. • Verify the Upgrade path to the target release is supported as documented in Section 2.1 Supported Upgrade Paths. • Select the NOAM server group and verify the **Application Version**. 
2. ☐	**Server CLI**: Check if the setup has customer supplied Apache certificate installed and protected with a passphrase	• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM. `ssh admusr@<NOAM_VIP>` Answer **yes** if you are asked to confirm the identity of the server. • cd to **/etc/httpd/conf.d** and open the file named **ssl.conf**. • Locate the line beginning with the phrase **SSLCertificateFile**. • The path that follows **SSLCertificateFile** is the location of the Apache certificate. If the path is **/usr/TKLC/appworks/etc/ssl/server.crt**, then the certificate is supplied by Oracle and no further action is required. Continue with the next procedure. • If the path is anything other than **/usr/TKLC/appworks/etc/ssl/server.crt**, then a customer-supplied Apache certificate is likely installed. Rename the certificate, but note the original certificate pathname for use in Section 4.4.

The following data collection procedures collect similar data; however, the collection method varies depending on the source release. Only one of the following procedures is to be executed for the pre-upgrade data collection. Refer to Table 9 for guidance on which procedure to use.

Table 9. Release Specific Data Collection Procedures.

If the Source Release is:	Use This Pre-Upgrade Data Collection Procedure:
7.0.x	Procedure 3: Data Collection for Source Release 7.0.1
7.1.x	Procedure 4: Data Collection for Source Release 7.1.x
7.2, 7.3, or 7.4	Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4
8.0 and later	Procedure 6: Data Collection for Source Release 8.0 and later

3.4.2.2 Data Collection for Source Release 7.0.1

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.0.1.

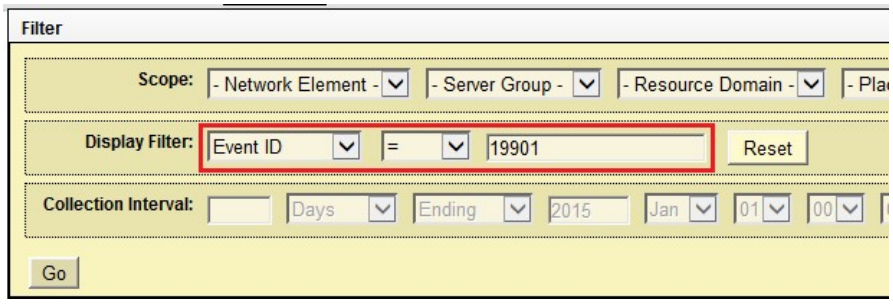
Procedure 3: Data Collection for Source Release 7.0.1

S T E P #		
		This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.

1. ☐	**Active SOAM CLI**: Database consistency check	Check the transport connections tables.
		• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active SOAM.
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Enter the following commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		`iqt -zhp ConnectionAdmin | wc -l`
		`iqt -zhp TransportConnection | wc -l`
		Sample output:
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		• If the entry counts match, proceed to step 2.
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, DO NOT PROCEED WITH THE UPGRADE. It is recommended you consult with My Oracle Customer Support **before continuing**.

Procedure 3: Data Collection for Source Release 7.0.1

2. ☐	**Server CLI**: Verify uptime for each server in the topology	Starting with the active NOAM, execute the following procedure.
		• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server using the server XMI IP Address.
		`ssh admusr@<target_server_XMI_IP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Execute the **uptime** command:
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		`02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		• Record the hostname of any server with an **uptime** value > 200 days.
		• Inform the customer that a **Cold Reboot** is required for all servers with an **uptime** value > 200 days before beginning any upgrade activity.
		Note: This is required response due to Red Hat Bug 765720. It is recommended you contact My Oracle Customer Support if instruction is needed on how to gracefully perform a **Cold Reboot**.
		• Repeat steps 1 through 4 for each server in the topology.

3. ☐	Repeat checks	Repeat steps 1 and 2 for each SOAM site in the topology.
4. ☐	**Active NOAM VIP**: Alarm check	Check for the presence of alarm 19901 – CFG-DB Validation Error. From the active NOAM GUI: • Navigate to **Alarms & Events -> View Active**. • Click **Filter** to open the filter selection box. • Enter the following values and click **Go**.  • If the filter returns no results, the database is consistent; proceed to the next step. Otherwise, do not continue with the upgrade until the alarm is cleared. It is recommended you consult with My Oracle Customer Support for guidance if the alarm does not clear within 60 minutes.

Procedure 3: Data Collection for Source Release 7.0.1

5. ☐	**Active NOAM VIP**: Verify IPFE server groups	Verify the IPFE server groups are properly configured. • Log into the NOAM GUI using the VIP. • Navigate to **Configuration -> Server Groups**. • Examine each IPFE server group. Verify each IPFE server group is configured with one, and only one, IPFE server. • If any IPFE server group contains more than one IPFE server, refer to the server group configuration procedure of [1] DSR 8.0 Cloud Installation Guide, E76331, Oracle to correct the configuration.
6. ☐	**Active NOAM VIP**: Verify and collect network element configuration data	• Navigate to **Configuration -> Network Elements**. • Click **Report** at the bottom of the table to generate a report for all entries. • Verify the configuration data is correct for the network. • Save the report and/or print the report. Keep these copies for future reference.
7. ☐	**Active NOAM VIP**: Verify and collect services configuration data	• Navigate to **Configuration -> Server Groups**. • Click **Report** at the bottom of the table to generate a report for all entries. • Verify the configuration data is correct for the network. • Save the report and/or print the report. Keep these copies for future reference.
8. ☐	**Active NOAM VIP**: Verify and collect services configuration data	• Navigate to **Configuration -> Servers**. • Click **Report** at the bottom of the table to generate a report for all entries. • Verify the configuration data is correct for the network. • Save the report and/or print the report. Keep these copies for future reference.
9. ☐	**Active NOAM VIP**: Verify and collect services configuration data	• Navigate to **Configuration -> Services**. • Click **Report** at the bottom of the table to generate a report for all entries. • Verify the configuration data is correct for the network. • Save the report and/or print the report. Keep these copies for future reference.

Procedure 3: Data Collection for Source Release 7.0.1

10. ☐	**Active NOAM VIP**: Verify and collect signaling network configuration data for DSR	• Navigate to **Configuration -> Network**. • Click **Report** at the bottom of the table to generate a report for all entries. • Verify the configuration data is correct for the network. • Save the report and/or print the report. Keep these copies for future reference. • Navigate to **Configuration -> Network -> Devices**. • Click **Report All** at the bottom of the table to generate a report for all entries. • Save the report and/or print the report. Keep these copies for future reference. • Navigate to **Configuration -> Network -> Routes**. • Click **Report All** at the bottom of the table to generate a report for all entries. Save the report and/or print the report. Keep these copies for future reference.
11. ☐	**Active NOAM VIP**: verify server status is normal – NOAM	• Navigate to **Status & Manage -> Server**. • Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB), and Processes (Proc). • Do not proceed with the upgrade if any server status displayed is not **Norm**. • Do not proceed if there are any Major or Critical alarms.
12. ☐	**Active NOAM VIP**: Log all current alarms at NOAM	• Navigate to **Alarms & Events -> View Active**. • Click **Report** to generate an Alarms report. • Save the report and/or print the report. Keep these copies for future reference. ***Note***: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the **stuck** alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
13. ☐	**Active NOAM VIP**: View communication agent status for all connections	• Navigate to **Communication Agent -> Maintenance -> Connection Status**. • Verify the connection status of each connection is InService.

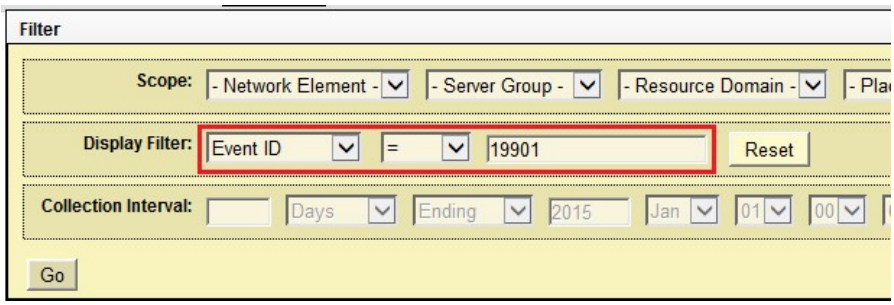
Procedure 3: Data Collection for Source Release 7.0.1

14. ☐	**Active NOAM VIP**: View SBR status (if equipped)	View SBR status if PDRA/PCA is enabled. **If the active NOAM is on release 7.0.1, 7.1.x:** • Navigate to **Policy and Charging -> Maintenance -> SBR Status**. • Select the Binding tab. • Expand each server group. • Verify Congestion Level is **Normal** for all servers. • Repeat sub-steps 3 and 4 for the PDRA Mated Triplet tab. **If the active NOAM is on release 7.2 and later:** • Navigate to **SBR -> Maintenance -> SBR Status**. • Select the Binding tab. • Expand each server group. • Verify Congestion Level is **Normal** for all servers. • Repeat sub-steps 3 and 4 for the PCA Mated Triplet tab.
15. ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA, which is out-of-service during the upgrade sequence. • Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 14. • It is recommended to plan for any MP upgrades by consulting My Oracle Customer Support to assess the impact of out-of-service MP servers. • Determine the exact sequence in which MP servers are upgraded for each site.

3.4.2.3 Data Collection for Source Release 7.1.x

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.1.x.

Procedure 4: Data Collection for Source Release 7.1.x

S T E P #		
	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Verify IPFE server groups	Verify the IPFE server groups are properly configured. From the active NOAM GUI: • Log into the NOAM GUI using the VIP. • Navigate to **Configuration -> Server Groups**. • Examine each IPFE server group. Verify each IPFE server group is configured with one, and only one, IPFE server. If any IPFE server group contains more than one IPFE server, **DO NOT PROCEED WITH THE UPGRADE**. It is recommended you consult with My Oracle Customer Support before continuing.
2. ☐	**Active NOAM VIP**: Alarm check	Check for the presence of alarm 19901 – CFG-DB Validation Error. From the active NOAM GUI: • Navigate to **Alarms & Events -> View Active**. • Click **Filter** to open the filter selection box. • Enter the following values and click **Go**.  • If the filter returns no results, the database is consistent; proceed to the next step. • Otherwise, do not proceed with the upgrade until the alarm is cleared. It is recommended you consult with My Oracle Customer Support for guidance if the alarm does not clear within 60 minutes.

Procedure 4: Data Collection for Source Release 7.1.x

3. ☐	**Active NOAM CLI**: Verify NOAM pre-upgrade status	Execute the following commands on the active DSR NOAM and active DR NOAM servers.
		• Use an SSH client to connect to the active NOAM:
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheck`
		This command creates three files in /var/TKLC/db/filemgmt/UpgradeHealthCheck/ with the filename format:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<NOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		• If the **Server <hostname> needs operator attention before upgrade** message is output, inspect the Server Status Report to determine the reason for the message. If the following message displays in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended you contact My Oracle Customer Support for guidance.
		• Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

Procedure 4: Data Collection for Source Release 7.1.x

4. ☐	**Server CLI**: Verify uptime for each server in the topology	Starting with the active NOAM, execute the following procedure.
		• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server using the server XMI IP Address.
		`ssh admusr@<target_server_XMI_IP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Execute the **uptime** command:
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		`02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		• Record the hostname of any server with an **uptime** value > 200 days.
		• Inform the customer that a **Cold Reboot** is required for all servers with an **uptime** value > 200 days before beginning any upgrade activity.
		Note: This is required response due to Red Hat Bug 765720. It is recommended you contact My Oracle Customer Support if instruction is needed on how to gracefully perform a **Cold Reboot**.
		• Repeat steps for each server in the topology.

5. ☐	**Active SOAM CLI**: Database consistency check	Check the transport connections tables.
		• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM
		`ssh admusr@<NOAM_VIP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Enter the following commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		`iqt -zhp ConnectionAdmin | wc -l`
		`iqt -zhp TransportConnection | wc -l`
		`Sample output:`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		• If the entry counts match, proceed to step 6.
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, DO NOT PROCEED WITH THE UPGRADE. It is recommended you consult with MOS before continuing.

Procedure 4: Data Collection for Source Release 7.1.x

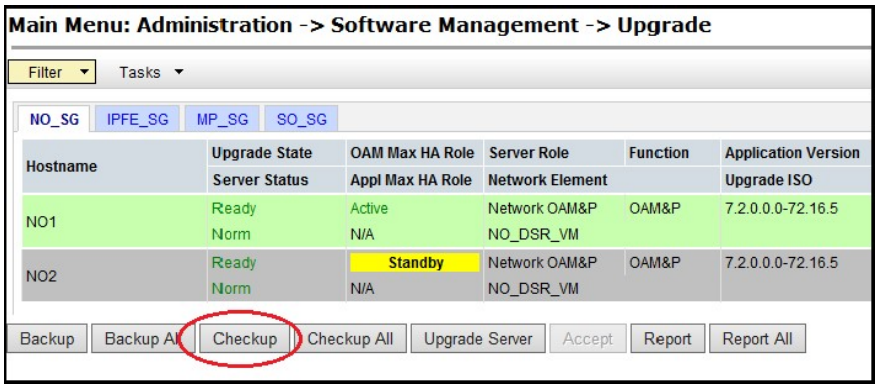
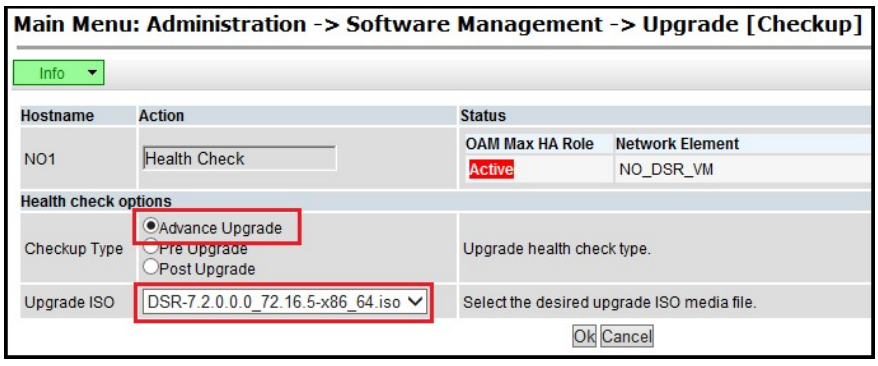
6. ☐	**Active SOAM CLI**: Log SOAM alarm status	• Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		This command creates two files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. If the following message displays in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		• Verify all Peer MPs are available.
		• Note the number of Total Connections Established _____
		• Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

7. ☐	**Active SOAM CLI**: Verify PCA status (if equipped)	• Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. • Verify Operational Status is **Available** for all applications.
8. ☐	Repeat for each network element	**Repeat** steps 5 – 7 for each SOAM site in the topology.
9. ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA, which is out-of-service during the upgrade sequence. • Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 8 of this procedure. • It is recommended to plan for MP upgrades by consulting My Oracle Customer Support to assess the impact of out-of-service MP servers. • Determine the exact sequence in which MP servers are upgraded for each site.

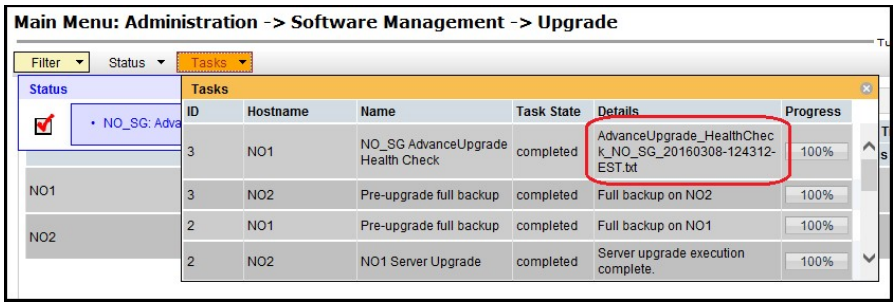
3.4.2.4 Data Collection for Source Release 7.2, 7.3, 7.4

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.2, 7.3, or 7.4.

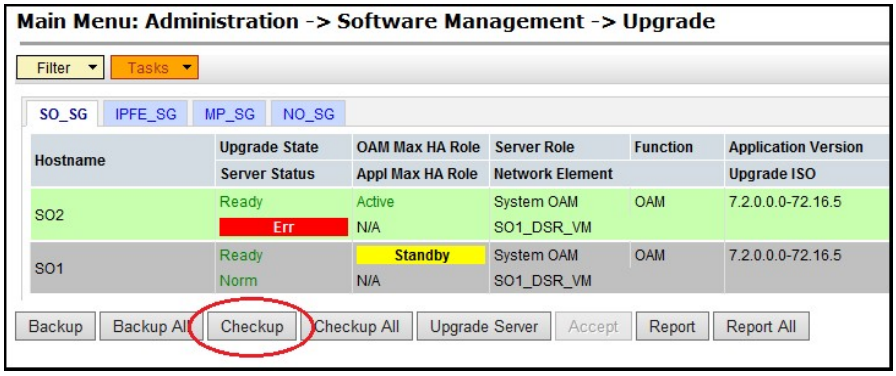
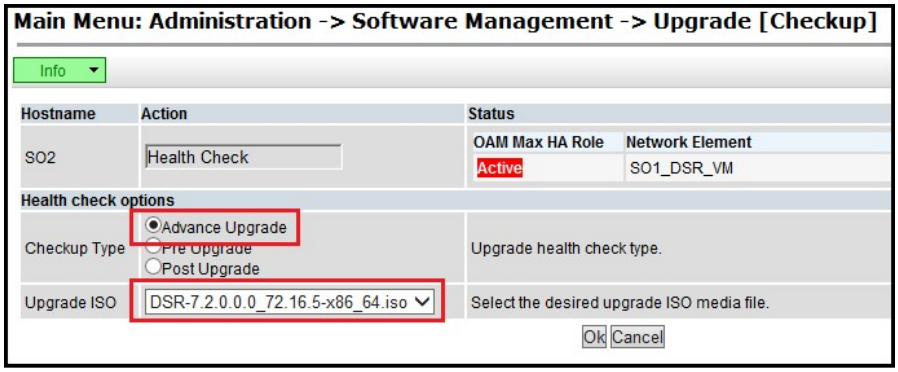
Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4

S T E P #		
	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Initate NOAM health check	This procedure runs the automated health checks on the active NOAM. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the active NOAM.  • Click **Checkup**. • In the Healtch Check options section, click **Advance Upgrade**. • If the ISO Administration procedure has already been performed for the target ISO, use the **Upgrade ISO** list to select the target release ISO. Otherwise, do not select an ISO. • Click **OK**. Control returns to the Upgrade screen. 

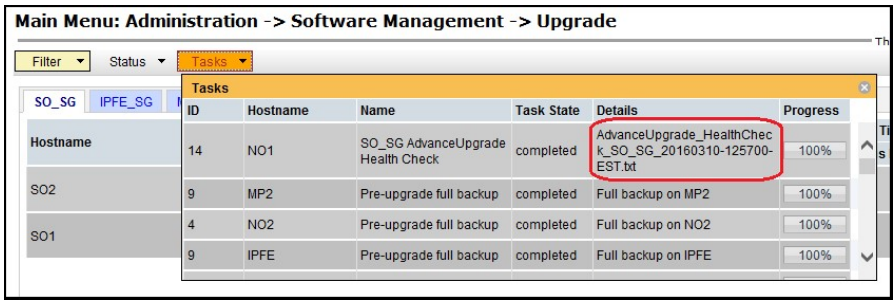
Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4

2. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <NOServerGroup> AdvanceUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. • Click the hyperlink in the Details column to download the Health Check report. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze any Health Check failure	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. • Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M.

Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4

4. ☐	Active NOAM VIP: Initate SOAM health check	This procedure runs the automated health checks on the active SOAM. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM server group tab. • Select the active SOAM.  • Click **Checkup**. • In the Healtch Check options section, click **Advance Upgrade**. • For a major upgrade, use the **Upgrade ISO** list to select the target release ISO. Do not select an ISO for an incremental upgrade. • Click **OK**. Control returns to the Upgrade screen. 

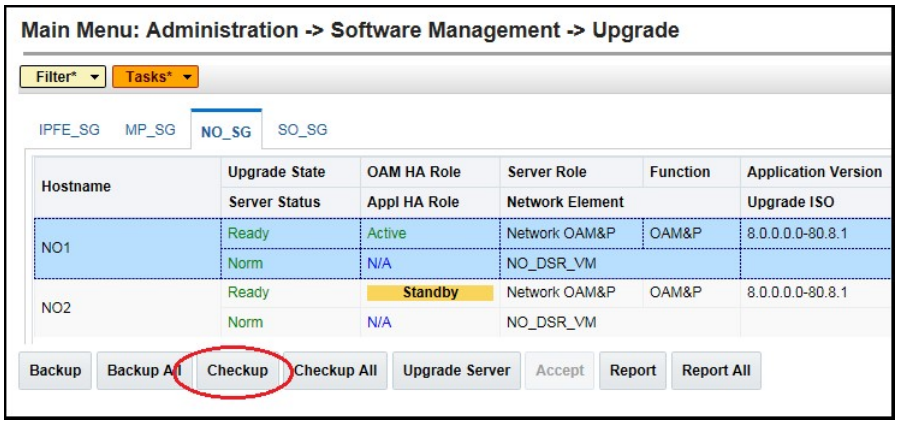
Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4

5. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <SOServerGroup> AdvanceUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. • Click the hyperlink in the Details column to download the Health Check report. Open the report and review the results. 
6. ☐	**Active NOAM VIP**: Analyze health check failure	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the active SOAM tab. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M. If the health check log contains the **Unable to execute Health Check on <Active SOAM hostname>** message, perform health checks in accordance with Procedure 4.
7. ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP / IPFE / SBR / PCA, which is out-of-service during the upgrade sequence. • Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 6 of this procedure. The Health Check reports from steps 3 and 6 can be found in **Status & Manage -> Files** on the active SOAM. • It is recommended to plan for MP upgrades by consulting My Oracle Customer Support to assess the impact of out-of-service MP servers • Determine the manner in which the MP servers are upgraded: Manually or Automated Server Group Upgrade. If the MPs are upgraded manually, determine the exact sequence in which MP servers are upgraded for each site.

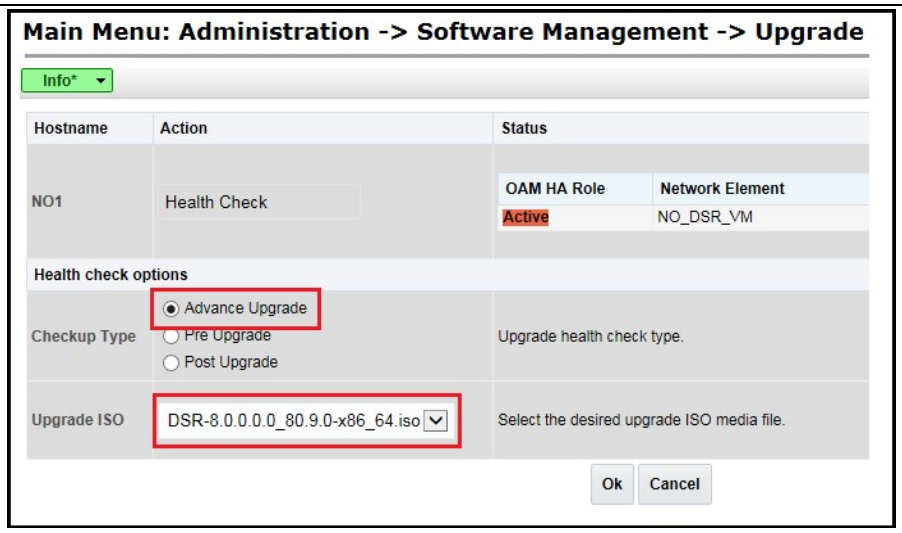
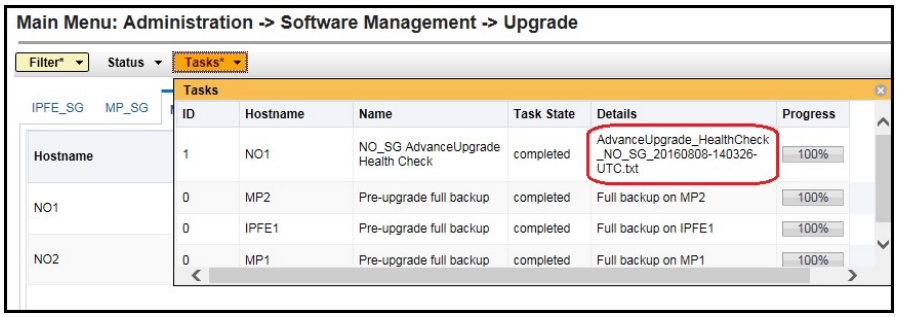
3.4.2.5 Data Collection for Source Release 8.0 and later

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 8.0 and later.

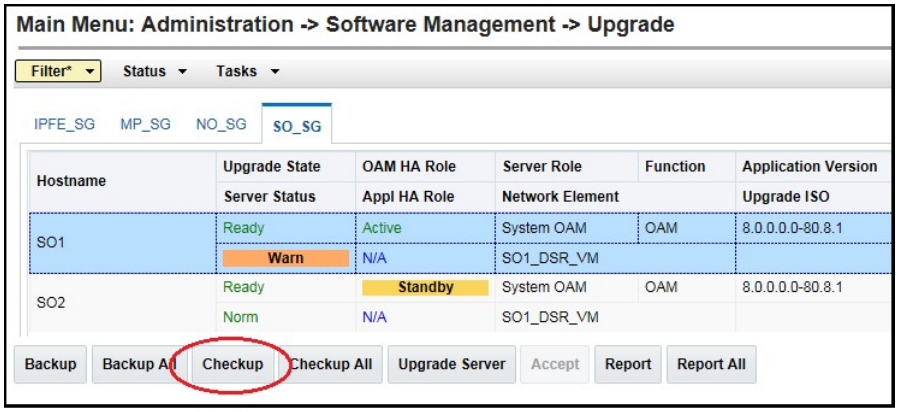
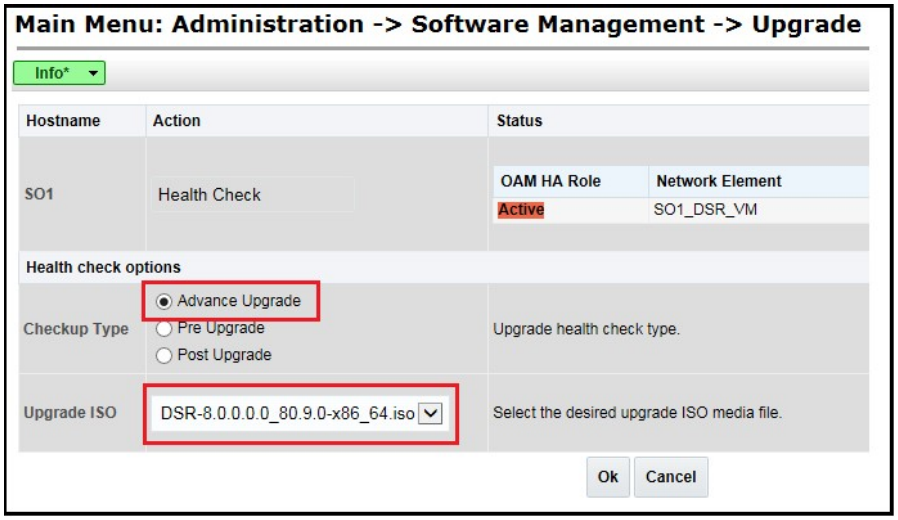
Procedure 6: Data Collection for Source Release 8.0 and later

S T E P #		
	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**	This procedure runs the automated health checks on the active NOAM. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the active NOAM.  • Click **Checkup**. • In the Health Check Options section, click **Advance Upgrade**. • If the ISO Administration procedure has already been performed for the target ISO, use the **Upgrade ISO** list to select the target release ISO. Otherwise, do not select an ISO. • Click **OK**. Control returns to the Upgrade screen.

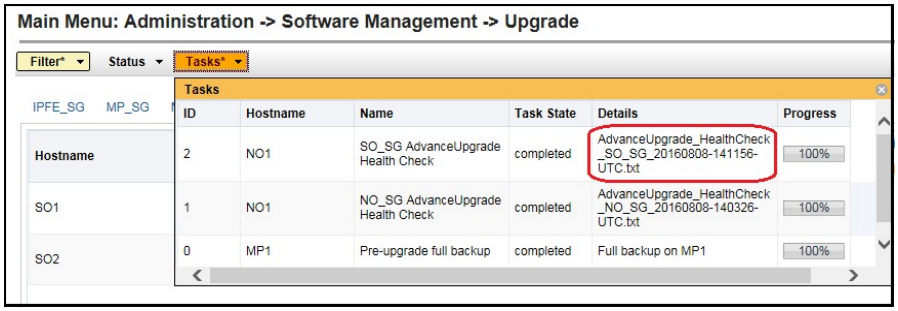
Procedure 6: Data Collection for Source Release 8.0 and later

		
2. ☐	**Active NOAM VIP**	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <NOServerGroup> AdvanceUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. • Click the hyperlink in the Details column to download the Health Check report. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze any health check failure	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. • Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix I.

Procedure 6: Data Collection for Source Release 8.0 and later

4. ☐	**Active NOAM VIP**	This procedure runs the automated health checks on the active SOAM. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM server group tab. • Select the active SOAM.  • Click **Checkup**. • In the Health Check Options section, click **Advance Upgrade**. • For a major upgrade, use the **Upgrade ISO** list to select the target release ISO. Do not select an ISO for an incremental upgrade. • Click **OK**. Control returns to the Upgrade screen. 

Procedure 6: Data Collection for Source Release 8.0 and later

<table>
<tr>
<td>5.
☐</td>
<td>Active NOAM VIP</td>
<td>Monitor for the completion of the Health Check.
• Click the Tasks list to display the currently executing tasks. The Health Check task name displays as <SOServerGroup> AdvanceUpgrade Health Check.
• Monitor the Health Check task until the Task State is completed.
• Click the hyperlink in the Details column to download the Health Check report. Open the report and review the results.


</td>
</tr>
<tr>
<td>6.
☐</td>
<td>Active NOAM VIP: Analyze Health Check failure</td>
<td>Analyze the Health Check report for failures. If the Health Check report status is anything other than Pass, then analyze the Health Check logs to determine if the upgrade can proceed.
• Navigate to Status & Manage -> Files.
• Select the active SOAM tab.
• Select the UpgradeHealthCheck.log file and click View.
• Locate the log entries for the most recent health check.
Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M.
If the health check log contains the Unable to execute Health Check on <Active SOAM hostname> message, perform health checks in accordance with the following table:
<table>
<tr><th></th><th colspan="3">Release</th></tr>
<tr><th></th><th>7.0.x</th><th>7.1.x</th><th>7.2, 7.3, 7.4</th></tr>
<tr><td>Procedure to Run</td><td>Procedure 3</td><td>Procedure 4</td><td>Procedure 5</td></tr>
</table>
</td>
</tr>
<tr>
<td>7.
☐</td>
<td>Analyze and plan MP upgrade sequence</td>
<td>From the collected data, analyze system topology and plan for any DA-MP / IPFE / SBR / PCA, which is out-of-service during the upgrade sequence.
• Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 6 of this procedure. The Health Check reports from steps 3 and 6 can be found in Status & Manage > Files on the active NOAM.
• It is recommended to plan for MP upgrades by consulting My Oracle Customer Support to assess the impact of out-of-service MP servers
• Determine the manner in which the MP servers are upgraded: Manually or Automated Server Group Upgrade. If the MPs are upgraded manually, determine the exact sequence in which MP servers are upgraded for each site.</td>
</tr>
</table>

3.4.3 DSR ISO Administration

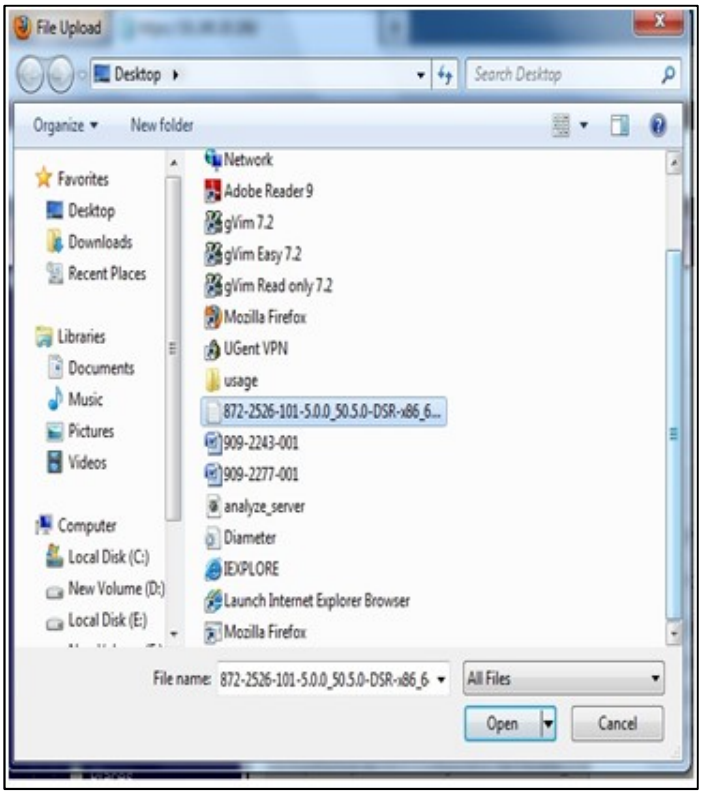
This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

Note: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed and require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed before, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 7: DSR ISO Administration

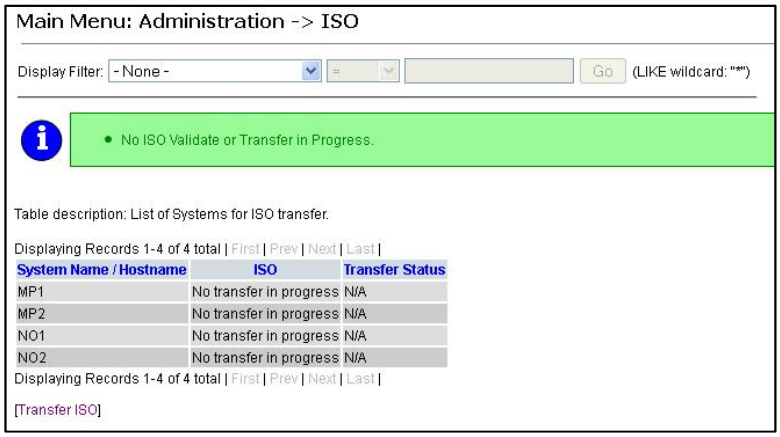
S T E P #	This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Transfer via NOAM GUI	Use the NOAM GUI Upload function for ISO file transfer over the network. Upload the target release ISO image file to the File Management Area of the active NOAM server: • Log into the active NOAM GUI. • Navigate to **Status & Manage -> Files**. • Click the active NOAM server in the network. All files stored in the file management storage area of this server display on the screen. • Ensure that this is actually the active NOAM server in the network by comparing the hostname in the screen title vs. the hostname in the session banner in the GUI. Verify they are the same and the status is ACTIVE in the session banner. • Click **Upload**. The Browse screen opens: ***Note***: Actual screens may vary from those shown below, depending on the browser and browser version used. 

Procedure 7: DSR ISO Administration

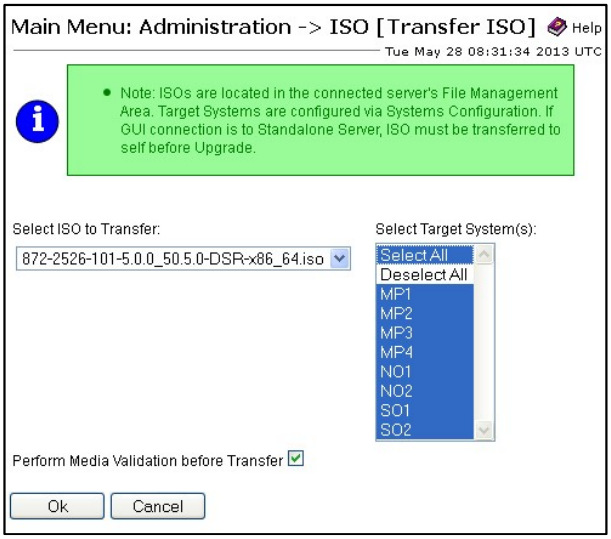
2. ☐	**Active NOAM VIP**	• Click **Browse** to select the file to upload. The Choose File screen displays to select files to upload.  • Select the target release ISO image file and click **Open**. The selected file and its path display on the screen.  • Click **Upload**. The ISO file begins uploading to the file management storage area. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This usually takes between 2 to 10 minutes, but more if the network upload speed is slow.

Procedure 7: DSR ISO Administration

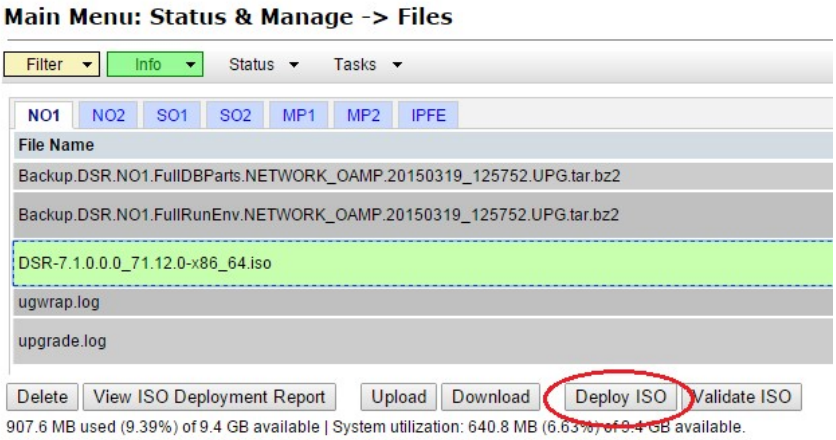
3. ☐	**Active NOAM VIP**: Copy ISO to the standby NOAM. For an active NOAM on release 7.0.1	If the active NOAM is on release 7.0.1, perform this step; otherwise, proceed to step 6.
		• Copy the ISO file to the standby NOAM.
		• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM:
		`ssh admusr@<NOAM_VIP>`
		`login as: admusr`
		`password: <enter password>`
		• Copy the ISO file to the standby NOAM.
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename> admusr@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`

4. ☐	**Active NOAM VIP**: Using NOAM GUI, transfer ISO to all servers to be upgraded. For active NOAM on release 7.0.1	If the active NOAM is on release 7.0.1: Transfer the target release ISO image file from the active NOAM to all other DSR servers. • Navigate to **Administration ->Software Management -> ISO Deployment**. • Click Transfer ISO. 

Procedure 7: DSR ISO Administration

5. ☐	**Active NOAM VIP**: ISO transfer continued. For active NOAM on release 7.0.1	If the active NOAM is on release 7.0.1: • Under the **Select ISO to Transfer** list, select the target release ISO. Under the **Select Target System(s)** list, click **Select All**. • Select the Perform Media Validation before Transfer checkbox.  • Click **OK**. • Control returns to the ISO screen. Monitor the progress until all file transfers have completed. Click **Refresh** to update the status of the transfer. If a file transfer fails, it must be retried. ***Note***: In the unlikely event that an ISO file transfer fails, repeat the transfer selecting only the specific system to which the transfer failed. If file transfers fail repeatedly, it is recommended you contact My Oracle Customer Support for assistance.

Procedure 7: DSR ISO Administration

6. ☐	**Active NOAM VIP**: Using NOAM GUI, deploy ISO to all servers to be upgraded. For active NOAM on release 7.1.1 or later	Deploy ISO to all servers. • Navigate to **Status & Manage -> Files**. • Click the active NOAM server tab. • All files stored in the file management storage area of this server display on the screen. • Select the target release ISO, and click **View ISO Deployment Report**. • In the resulting report, determine if the ISO has been deployed to all servers in the system. • If the ISO has been deployed to all servers, this procedure is complete. Proceed to the next procedure per Table 8. • If the ISO has not been deployed, select the target release DSR ISO in the file list, and click **Validate ISO**. Click **OK** on the resulting confirmation screen. • Verify the ISO status is valid. If the ISO is not valid, repeat this procedure beginning with step 1. If the ISO fails validation more than once, it is recommended you contact My Oracle Customer Support. • If the ISO is valid, select the ISO, and click **Deploy ISO**. Click **OK** on the resulting screen. 

Procedure 7: DSR ISO Administration

7. ☐	**Active NOAM VIP**: Monitor ISO deployment. For active NOAM on release 7.1.1 or later	The deployment progress can be monitored by viewing the **Tasks** list on the **Status & Manage -> Files** screen. Select the target release ISO, and click **View ISO Deployment Report**. Verify the ISO has been deployed to all servers in the system. **Main Menu: Status & Manage -> Files [View]** Main Menu: Status & Manage -> Files [View] Fri Mar 20 11:35:43 2015 EDT Deployment report for DSR-7.1.0.0.0_71.11.0-x86_64.iso: Deployed on 7/7 servers. NO1: Deployed NO2: Deployed SO1: Deployed SO2: Deployed MP1: Deployed MP2: Deployed IPFE: Deployed

3.4.4 ISO Link Correction

This procedure is required when upgrading from Release 7.1, 7.2, 7.3, or 7.4 to DSR 8.0 and later. In DSR 7.x, the ISO image management was changed to put a symlink in the /var/TKLC/upgrade directory to the actual file in the /var/TKLC/db/filemgmt directory. However, to support the Storage Reclamation feature used in DSR 8.0, the symlinks to the ISO image in the /var/TKLC/db/filemgmt/isos directory must be removed and replaced with direct copies of the ISO image in the /var/TKLC/upgrade directory. This must be executed after the application ISO has been deployed but before the software upgrade in Section 4. This may be done in a maintenance window before the actual upgrade maintenance window.

This procedure is not required if the source release is 7.0 or 8.x.

Procedure 8: ISO Link Correction

S T E P #	This procedure performs the ISO symlink correction. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Verify this procedure should be run	Verify this procedure should be run: • Is the topology of servers to be upgraded currently running DSR release 7.1, 7.2, 7.3, or 7.4? • Has the new DSR 8.0 ISO been deployed? If **Yes** to the above questions, then proceed. If **No**, this procedure is complete.

Procedure 8: ISO Link Correction

2. ☐	**Active NOAM GUI**: Undeploy all unneeded ISO images	Use the **Undeploy ISO** selection on the **Main Menu -> Status & Manage -> Files** GUI screen to **remove all unneeded old** ISO images from the /var/TKLC/upgrade directory. Keep deployed the one ISO image file being used for upgrade. This saves space in the **/var/TKLC/upgrade** directory. • Navigate to **Status & Manage -> Files**. • Select the ISOs to be undeployed and click **Undeploy ISO**. • Click **OK** to confirm the ISO undeployment. **This launches the ISO un-deployment to the entire topology.** This function removes the symlink in /var/TKLC/upgrade to the ISO in the isos directory. The **Tasks** list at the top of the Files page displays the status of the undeployment for each server. Select the ISO and click **View ISO Deployment Report** to display the report.
3. ☐	**Active NOAM CLI**: Log into the active NOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM: `ssh admusr@<NOAM_VIP>`
4. ☐	**Active NOAM CLI**: Mount the ISO image	Mount the DSR 8.0 ISO image. The following example uses a DSR ISO image name as an example. Use the appropriate application ISO image name. `$ sudo mount -o loop /var/TKLC/db/filemgmt/isos/DSR-8.0.0.0.0_80.x.y-x86_64.iso /mnt/upgrade`
5. ☐	**Active NOAM CLI**: Copy the script	Copy the script from the mounted ISO to /var/tmp in order to use it. `$ cp /mnt/upgrade/upgrade/bin/changeLinksToFiles.php /var/tmp`
6. ☐	**Active NOAM CLI**: Unmount the ISO image	Unmount the DSR 8.0 ISO image. `$ sudo umount /mnt/upgrade`

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

Procedure 8: ISO Link Correction

8. ☐	**Active NOAM CLI**: Execute the script	Execute the script to change the symlink into a copy of the ISO image file.
		`$ /var/tmp/changeLinksToFiles.php`
		The script uses SSH to contact all the servers in the topology and convert any link to an ISO images in /var/TKLC/upgrade into a copy of the ISO image file.
		Output similar to the following displays for each server in the entire topology.
		`$ /var/tmp/changeLinksToFiles.php`
		`server: NO1`
		`hostname alias based on service: no1-internalimi`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`found link /var/TKLC/upgrade/DSR-8.0.0.0.0_80.16.0-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`Remove command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/DSR-8.0.0.0.0_80.16.0-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi,192.168.1.11' (RSA) to the list of known hosts.`
		`Copy command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/DSR-8.0.0.0.0_80.16.0-x86_64.iso`
		The following expected messages can be ignored:
		`FIPS integrity verification test failed.`
		`Warning: Permanently added '<host>-internalimi,<ip address>' (RSA) to the list of known hosts.`
		If any unexpected failure messages occur, it is recommended you contact My Oracle Customer Support for guidance.

3.4.5 Full Backup of DB Run Environment at Each Server

The procedures in this section are part of software upgrade preparation and are used to conduct a full backup of the run environment on each server, to be used in the event of a backout of the new software release. The backup procedure to be executed is dependent on the software release that is running on the active NOAM.

Note: Do not perform this procedure until the ISO Deployment is completed to all servers in the topology. Failure to complete the ISO may disrupt ISO deployment/undeployment in the event of a partial backout (e.g., backout of one site).

!! WARNING!! **If backout is needed, any configuration changes made after the DB is backed up at each server is lost.**

3.4.5.1 Full Backup of DB Run Environment for Release 7.0.1

This procedure backs up the DB run environment when the active NOAM is on release 7.0.1.

Procedure 9: Full Backup of DB Rbun Environment for Release 7.0.1

S T E P #		
	This procedure (executed from the active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM CLI**: Log into the active NOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM: `ssh admusr@<NOAM_VIP>`
2. ☐	**Active NOAM CLI**: Start a screen session	Enter the following commands: `$ screen` The screen tool creates a no-hang-up shell session, so that the command continues to execute if the user session is lost.

3. ☐	**Active NOAM CLI**: Execute full backup for all servers (managed from this NOAM)	Execute the backupAllHosts utility on the active NOAM. This utility remotely accesses each server managed by the NOAM, and runs the backup command for that server.
		`$ /usr/TKLC/dpi/bin/backupAllHosts`
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.
		Do not proceed until the backup on each server is completed.
		Output similar to the following indicates successful completion:
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`
		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		`Errors also report back to the command line.`
		Note: There is no progress indication for this command; only the final report when it completes.

4. ☐	**Active NOAM CLI**: Exit the screen session.	`# exit`
		`[screen is terminating]`
		Note: **screen -ls** shows active screen sessions on a server, and **screen -dr** re-enters a disconnected screen session.

Procedure 9: Full Backup of DB Rbun Environment for Release 7.0.1

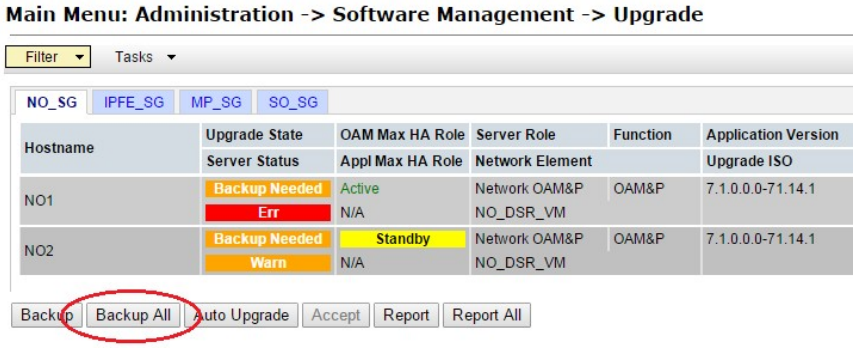
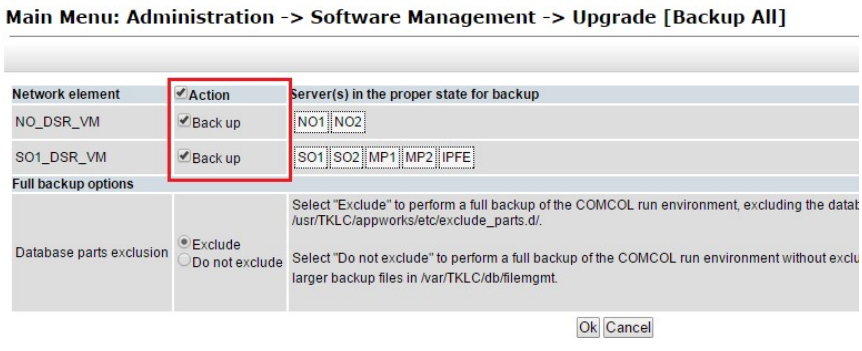
5. ☐	ALTERNATIVE METHOD
	Server CLI: If needed, the alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script (Optional)
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following indicates successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

6. ☐	**Active NOAM VIP**: Verify backup files are present on each server.	• Log into the active NOAM.
		• Navigate to **Status & Manage > Files**.
		• Select each server tab, in turn.
		• For each server, verify the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

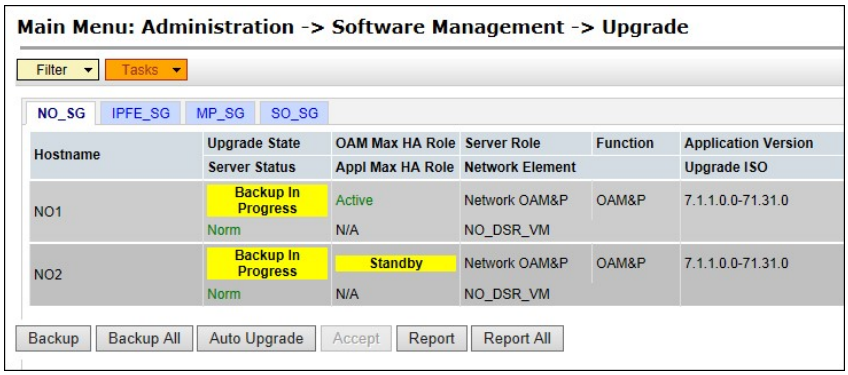
3.4.5.2 Full Backup of DB Run Environment for Release 7.1.x and Later

This procedure backs up the DB run environment when the active NOAM is on release 7.1.x and later.

Procedure 10: Full Backup of DB Run Environment for Release 7.1.x and later

S T E P #		
	This procedure (executed from the active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Start backup of all servers	• Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Click Backup All. 
2. ☐	**Active NOAM VIP**: Select network elements to backup	The Upgrade [Backup All] screen displays the various network elements, and identifies which servers are ready for backup. • In the Action column, select the **Back up** checkbox for each network element. • Ensure the **Exclude** option is selected. • Click **OK**. This initiates a full backup on each eligible server. 

Procedure 10: Full Backup of DB Run Environment for Release 7.1.x and later

3. ☐	**Active NOAM VIP**: Monitor backup progress	Select each server group tab and verify each server transitions from **Backup in Progress** to **Ready**. 

4. ☐	ALTERNATIVE METHOD
	Server CLI: If needed, the Alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script (Optional)
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the GUI method above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following indicates successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

5. ☐	**Active NOAM VIP**: Verify backup files are present on each server	• Log into the active NOAM.
		• Navigate to **Status & Manage -> Files**.
		• Select each server tab, in turn
		• For each server, verify the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

3.4.6 Network Interface Workaround

In some Cloud environments, the network interface names are not persistent across a server boot or upgrade. Interface renaming can result in the loss of IP access to the server. To prevent this from occurring, this procedure creates a network persistence rules file on each server. This procedure is required before upgrading to DSR Release 8.0.

!! WARNING!! **tHIS PROCEDURE MUST BE COMPLETED BEFORE UPGRADING TO DSR RELEASE 8.0**

Procedure 11: Network Interface Workaround

S T E P #	This procedure creates a network persistence rules file. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	Server CLI
	Create network rules file
		Execute the following commands on the server.
		• Use an SSH client to connect to the active NOAM:
		`ssh admusr@<server_ip>`
		`password: <enter password>`
		• Enter the following command to create the rules file:
		`$ sudo udevadm trigger --subsystem-match=net`
		• Verify the rules **70-persistent-net.rules** file is created:
		`$ ls /etc/udev/rules.d`
		`/etc/udev/rules.d/70-persistent-net.rules`

2. ☐	Repeat for all servers	Repeat step 1 for each server in the Cloud deployment.

3.4.7 IDIH Pre-Upgrade

If IDIH is a component of a network element, it may be upgraded either before or after the DSR. The order of upgrade does not impact the functionality of either component. However, it should be noted that certain compatibility limitations may exist while the two components are not on the same release.

The IDIH upgrade procedures are provided in Appendix I and may be performed at any time after Section 3.4.7.1 has been completed.

Table 10: IDIH Upgrade Preparation Overview.

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 12	0:15-0:30	0:15-0:30	IDIH Upgrade Preparation	None

3.4.7.1 IDIH Upgrade Preparation

This procedure prepares the Mediation and Application guests for upgrade.

Procedure 12: IDIH Upgrade Preparation

S T E P #	This procedure prepares the Mediation and Application guests for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Place the Mediation and Application OVAs in the Cloud repository.	Follow the hypervisor's instructions to add the Mediation and Application OVAs to the cloud repository.

3.5 Software Upgrade Execution Overview

It is recommended you contact My Oracle Customer Support as described in Appendix M before executing this upgrade to ensure that the proper media are available for use.

Before upgrade, users must have performed the data collection and system health check instructions in Section 3.4. This check ensures that 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 upgrade can proceed with alarms.

****** WARNING *******

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

If alarms are present on the server, it is recommended you contact My Oracle Customer Support to diagnose those alarms and determine whether they need to be addressed, or if it is safe to proceed with the upgrade.

Please read the following notes on upgrade procedures:

- All procedure completion times shown in this document are estimates. Times may vary due to differences in database size, user experience, and user preparation.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
  - Session banner information such as time and date.
  - System-specific configuration information such as hardware locations, IP addresses and hostnames.
  - ANY information marked with **XXXX** or **YYYY**. Where appropriate, instructions are provided to determine what output should be expected in place of **XXXX** or **YYYY**.
  - Aesthetic differences unrelated to functionality such as browser attributes: window size, colors, toolbars, and button layouts.
- After completing each step, and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A check box is provided. For procedures which are

executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).

- Captured data is required for future support reference if an **Error! Reference source not found.** representative is not present during the upgrade.
- Answer these questions, and record:

  What is the DSR Application version to be upgraded? _____

  What is the DSR Application new version to be applied? _____

  Is this a Major or Incremental Upgrade? _____

  Are there IPFE servers to upgrade? _____

  Is SDS also deployed (co-located) at the DSR site? _____

  Note: SDS does not need to be upgraded at the same time.

  Is IDIH also deployed (co-located) at the DSR site? _____

3.5.1 Accept the Upgrade

After the upgrade of **ALL** Servers in the topology has been completed, and following an appropriate soak time, the Post-Upgrade procedures in **Section 5.7** are performed in a separate maintenance window to finalize the upgrade. Procedure 49 **accepts** the upgrade and performs a final health check of the system to monitor alarms and server status. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4. NOAM Upgrade Execution

NOAM UPGRADE

The NOAM upgrade section is common to all topologies. This section must be completed before executing the site upgrade procedures.

Procedures for the NOAM upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning is disabled before upgrading the NOAM servers. Provisioning activities at the NOAM and SOAM servers have certain limitations during the period when the NOAMs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in Table 11 specifies the time to upgrade the DSR application. All times are estimates.

Table 11: NOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 13 or	0:30-0:45	0:30-0:45	NOAM Health Check for Source Release 7.0.1, 7.1.x	None
Procedure 14 or	0:20-0:30	0:20-0:30	NOAM Health Check for Source Release 7.2, 7.3, 7.4	None
Procedure 14	0:20-0:30	0:20-0:30	Data Collection for Source Release 8.0 and later	None

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 16	0:05-0:10	0:25-0:55	NOAM Pre-Upgrade Backup	None
Procedure 17	0:01-0:05	0:26-1:00	Disable Global Provisioning	Global Provisioning Disabled
Procedure 18	0:40-1:20	1:06-2:20	NOAM Upgrade	No Traffic Impact
Procedure 19	0:01-0:05	1:07-2:25	PCA (formerly PDRA) Topology Hiding Configuration	No Traffic Impact
Procedure 20	0:05-0:15	1:12-2:40	Verify NOAM Post Upgrade Status	None
Procedure 21	0:05-0:10	1:17-2:50	Allow Provisioning (Post NOAM Upgrade)	Global Provisioning Enabled

4.1 NOAM Pre-Upgrade Checks and Backup

The procedures in this section perform health checks and backups to prepare the NOAM NE for upgrade. These procedures must be executed on the active NOAM.

Note: These procedures may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 18.

INCREASE MAX NUMBER OF OPEN FILES

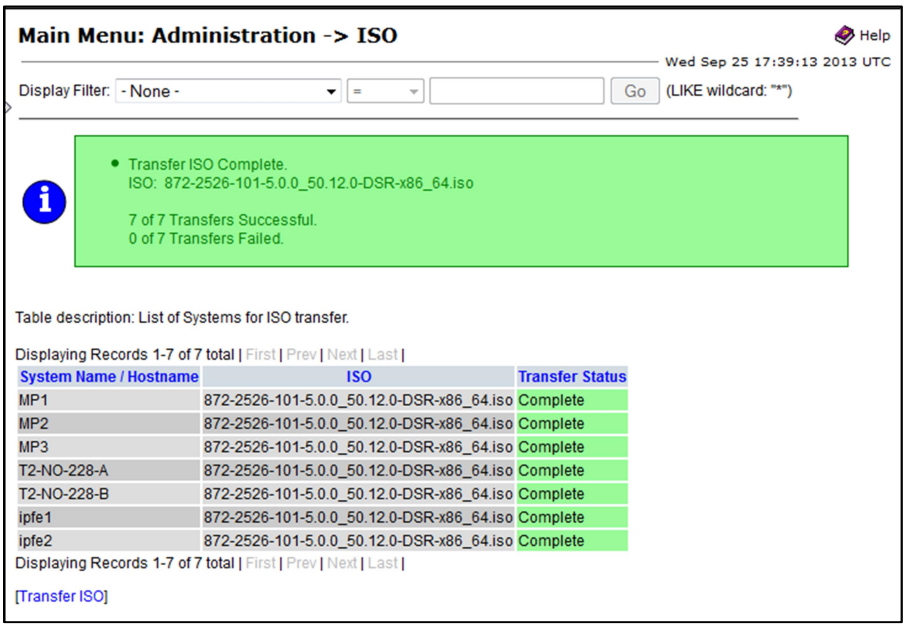
As the number of servers in the topology grows, so does the need for additional files to handle merging data to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files.

See Appendix B to increase the INCREASE MAX NUMBER OF OPEN FILES.

4.1.1 NOAM Health Check for Source Release 7.0.1, 7.1.x

This procedure determines the health and status of the network and servers when the NOAM is on source release 7.0.1 or 7.1.x. This procedure must be executed on the active NOAM.

Procedure 13: NOAM Health Check for Source Release 7.0.1, 7.1.x

S T E P #		
	This procedure performs a health check of the system before upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Verify ISO for upgrade has been deployed. For active NOAM on release 7.0.1 only	This step is for an active NOAM on release 7.0.1. If the active NOAM is on release 7.1.x, proceed to step 2. Verify the DSR ISO file has been transferred to all servers. • Navigate to **Administration -> Software Management -> ISO Deployment**. • Verify the Transfer Status is **Complete** for each server in the topology. • If any server shows **Not Complete**, perform Section 3.4.3 DSR ISO Administration Example:  Proceed to step 3 to complete this procedure.

Procedure 13: NOAM Health Check for Source Release 7.0.1, 7.1.x

2. ☐	**Active NOAM VIP**: Verify ISO for upgrade has been deployed. For active NOAM on release 7.1.x only	Verify the DSR ISO file has been transferred to all servers.
		• Navigate to **Status & Manage -> Files**.
		• Select the target release DSR ISO and click **View ISO Deployment Report**.
		• Review the report to ensure the ISO is deployed to all servers in the topology
		Sample report:
		`Deployment report for DSR-7.1.1.0.0_71.27.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

Procedure 13: NOAM Health Check for Source Release 7.0.1, 7.1.x

3. ☐	**Active NOAM CLI**: Verify NOAM pre-upgrade status	Execute the following commands on the active DSR NOAM and active DR NOAM servers.
		• Use an SSH client to connect to the active NOAM:
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheck`
		This command creates two files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If any alarms are present in the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<NOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		• If the **Server <hostname> needs operator attention before upgrade** message displays, inspect the Server Status Report to determine the reason for the message. If the following message displays in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended you contact My Oracle Customer Support for guidance.
		• Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

4. ☐	**Active NOAM VIP**: Export and archive the Diameter configuration data	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the list. • Verify the data export is complete using the tasks button at the top of the screen. • Navigate to **Main Menu -> Status & Manage -> Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Procedure 13: NOAM Health Check for Source Release 7.0.1, 7.1.x

5. ☐	**Active SOAM CLI**: Pre-upgrade health checks	Execute SOAM pre-upgrade alarm status health checks.
		• Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck alarmStatusOnSoam`
		If any alarms are present in the system, this command creates a file in **/var/TKLC/db/filemgmt/ UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		• Keep this report for future reference. This report is compared to alarm and status reports after the upgrade is complete.

6. ☐	**Active SOAM CLI**: Pre-upgrade health checks	Execute SOAM pre-upgrade DA-MP status health checks. • Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. • Verify all Peer MPs are available • Note the number of Total Connections Established _____
7. ☐	Active SOAM CLI: Verify PCA status (if equipped)	Execute SOAM pre-upgrade PCA status health checks, if equipped. • Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. • Verify Operational Status is 'Available' for all applications
8. ☐	Repeat for each network element	**Repeat** steps 5 – 7 for each SOAM site in the topology.

Procedure 13: NOAM Health Check for Source Release 7.0.1, 7.1.x

9. ☐	Active NOAM VIP: Verify backups are created for all servers	Verify a recent COMCOL Environment backup has been performed.
		• Navigate to **Status & Manage -> Files**.
		• Select each server tab, in turn.
		• Verify the following two files have been created and have a current timestamp:
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		• Repeat this procedure for each site.
		See Section 3.4.4 to perform (or repeat) a full backup, if needed.

4.1.2 NOAM Health Check for Source Release 7.2, 7.3, 7.4

This procedure determines the health and status of the network and servers when the NOAM is on release 7.2, 7.3, or 7.4. This procedure must be executed on the active NOAM.

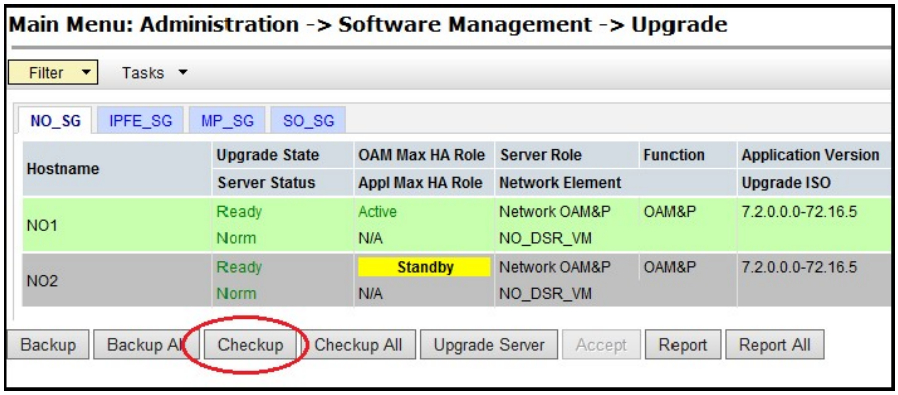
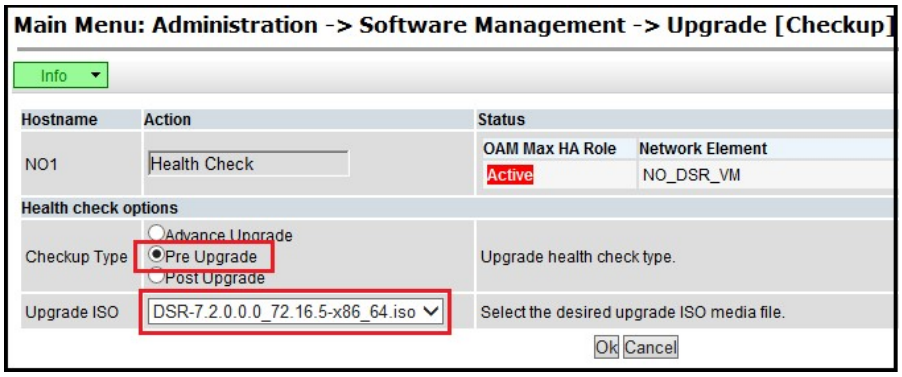
Note: This procedure may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 18.

Procedure 14: NOAM Health Check for Source Release 7.2, 7.3, 7.4

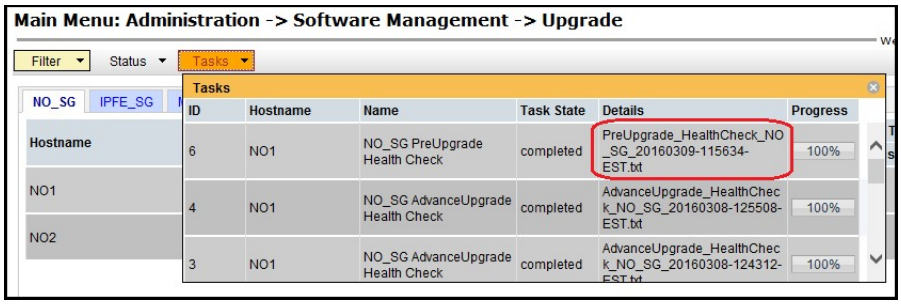
S T E P #	This procedure performs a health check on the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM VIP**: Verify upgrade ISO has been deployed	Verify the DSR ISO file has been transferred to all servers.
		• Navigate to **Status & Manage -> Files**.
		• Select the target release DSR ISO and click **View ISO Deployment Report**.
		• Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.0.0.0.0_80.27.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

Procedure 14: NOAM Health Check for Source Release 7.2, 7.3, 7.4

2. ☐	**Active NOAM VIP**: Export and archive the Diameter configuration data	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the **Export Application** list. • Click **OK**. • Verify the data export is complete using the tasks button at the top of the screen. • Navigate to **Main Menu -> Status & Manage -> Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.
3. ☐	**Active NOAM VIP**: Initiate NOAM health checks	This procedure runs the automated pre-upgrade health checks. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the active NOAM.  • Click **Checkup**. • Under Health Check options, select the **Pre Upgrade** option. • Use the **Upgrade ISO** list to select the target release ISO. • Click **OK**. Control returns to the Upgrade screen. 

Procedure 14: NOAM Health Check for Source Release 7.2, 7.3, 7.4

4. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <NOServerGroup> PreUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. • Click the hyperlink to download the Health Check report. Open the report and review the results. 
5. ☐	**Active NOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M. If the health check log contains the **Unable to execute Health Check on <active NOAM hostname>** message, perform health checks in accordance with Procedure 13.

4.1.3 NOAM Health Check for Source Release 8.0 and later

This procedure determines the health and status of the network and servers when the NOAM is on source release 8.0 or later. This procedure must be executed on the active NOAM.

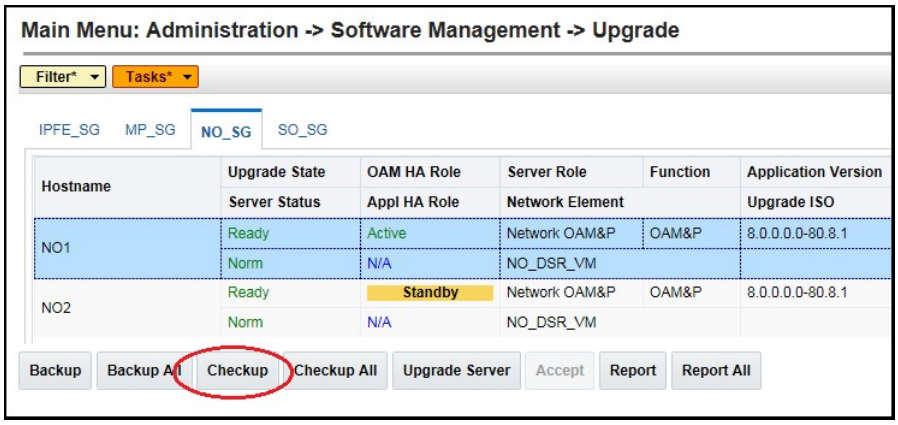
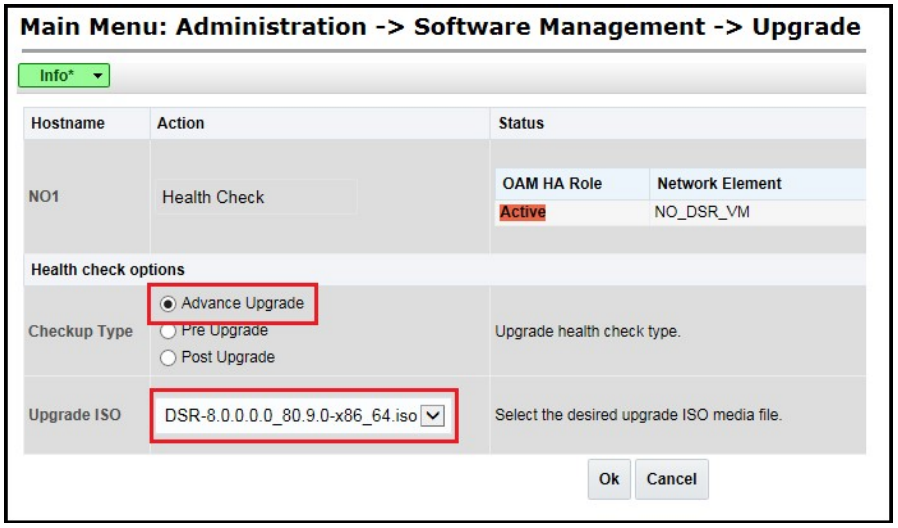
Procedure 15: NOAM Health Check for Source Release 8.0

S T E P #	This procedure performs a health check of the system before upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

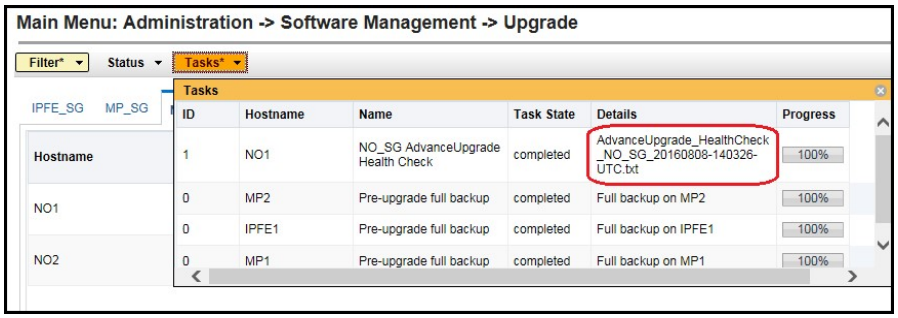
1. ☐	**Active NOAM VIP**: Verify upgrade ISO has been deployed	Verify the DSR ISO file has been transferred to all servers.
		• Navigate to **Status & Manage -> Files**.
		• Select the target release DSR ISO and click **View ISO Deployment Report**.
		• Review the report to ensure the ISO is deployed to all servers in the topology
		Sample report:
		`Deployment report for DSR-8.0.0.0.0_80.27.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

2. ☐	**Active NOAM VIP**: Export and archive the Diameter configuration data	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the **Export Application** list. • Click **OK**. • Verify the data export is complete using the tasks button at the top of the screen. • Navigate to **Main Menu -> Status & Manage -> Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Procedure 15: NOAM Health Check for Source Release 8.0

3. ☐	**Active NOAM VIP**: Initiate NOAM health checks	This procedure runs the automated pre-upgrade health checks. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the active NOAM.  • Click **Checkup**. • Under Healtch Check options, select the **Pre Upgrade** option. • Use the **Upgrade ISO** list to select the target release ISO. • Click **OK**. Control returns to the Upgrade screen. 

Procedure 15: NOAM Health Check for Source Release 8.0

4. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <NOServerGroup> PreUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. • Click the hyperlink to download the Health Check report. Open the report and review the results. 
5. ☐	**Active NOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. From the active NOAM GUI: • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M. If the health check log contains the **Unable to execute Health Check on <active NOAM hostname>** message, perform health checks in accordance with Procedure 13 or Procedure 14.

4.1.4 NOAM Pre-Upgrade Backup

This procedure backs up of the NOAM servers just before the upgrade.

Procedure 16: NOAM Pre-Upgrade Backup

S T E P #	This procedure takes a backup of the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Backup all global configuration databases for NOAM. **IMPORTANT**: Required for disaster recovery	Backup NOAM database. • Navigate to **Status & Manage -> Database** to return to the Database Status screen. • Click to highlight the active NOAM server; click **Backup**. ***Note***: Backup is only enabled when the active server is selected. • Select the **Configuration** checkbox. • Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. • Enter **Comments** (optional). • Click **OK**. ***Note***: On the **Status & Manage -> Database** screen, the active NOAM server displays **Active** in the OAM Max HA Role column.
2. ☐	**Active NOAM VIP**: Save database backups for NOAM. **IMPORTANT**: Required for disaster recovery	Download database files from the NOAM. • Navigate to **Status & Manage -> Files**. • Select the active NOAM server tab. • Select the configuration database backup file and click **Download**. • On the confirmation screen, click **Save**. • On the Choose File screen, select a destination folder on the local workstation to store the backup file. Click **Save**. • On the Download Complete screen, click **Close**.

4.2 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures that no changes are made to the database while the NOAMs are upgraded. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 17: Disable Global Provisioning

S T E P #		
	This procedure disables provisioning for the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Disable global provisioning and configuration	Disable global provisioning and configuration updates on the entire network: • Log into the active NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Disable Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Enable Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`

4.3 NOAM Upgrade

This procedure upgrades the NOAM and DR NOAM servers.

Procedure 18: NOAM Upgrade

S T E P #	This procedure upgrades the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	Upgrade primary DSR standby NOAM	• Upgrade the primary DSR standby NOAM server using upgrade single server procedure:
		If the active NOAM is on DSR 8.0, execute Appendix D -- Upgrade Single Server – DSR 8.x.
		Otherwise, execute Appendix E – Upgrade Single Server – Pre DSR 8.0
		• After successfully completing the procedure in Appendix D or Appendix E, continue with this step.
		• The active NOAM server may have some or all of the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`Alarm ID = 31106 (DB Merge to Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31225 (HA Service Start Failure)`
		`Alarm ID = 31226 (HA Availability Status Degraded)`
		`Alarm ID = 31233 (HA Path Down)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
		If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action.
		If the active NOAM is on release 7.1.1 or later, proceed to step 3.

Procedure 18: NOAM Upgrade

2. ☐	**Active NOAM VIP**: Prepare the active NOAM for upgrade. For NOAM on release 7.0.1 only	**This step is for an active NOAM on release 7.0.1 only.** Prepare the active NOAM for upgrade. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the NOAM server group. • Select the active NOAM. • On the upgrade form, click **Prepare** to make the active NOAM **Upgrade Ready**. • On the Upgrade [Prepare] form, select **Prepare** in the **Action** list. Click **OK**. This starts the Prepare action on the active NOAM and forces an HA failover. ***** Critical *** Do NOT omit this step** • Log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. ***** Critical *** Do NOT omit this step** Clear the Prepared state for the now-standby NOAM. This is required due to the transition from release 7.0.1 to release 8.0. • Navigate to **Status & Manage -> HA**. • Click **Edit**. • For the NOAM to be upgraded (now the standby), set the Max Allowed HA Role to **Active**, and click **OK**. • Navigate to **Status & Manage -> Server**. • Select the standby NOAM and click **Restart**. • Click **OK** and verify the Appl State changes to **Enabled**.
3. ☐	Upgrade second DSR NOAM	Upgrade the second DSR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, continue with the next step.
4. ☐	Upgrade standby DR NOAM	Upgrade the standby DR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x After successfully completing the procedure in Appendix D, continue with the next step.
5. ☐	Upgrade active DR NOAM	Upgrade the active DR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x After successfully completing the procedure in Appendix D, continue with the next procedure per Table 11.

4.3.1 PCA (Formerly PDRA) Topology Hiding Configuration

In DSR 7.0, the Policy and Charging Topology Hiding configuration moved from being site-specific at the SOAM, to being network-wide specific at the NOAM. Because each site could be independently configured, manual intervention is required to determine the appropriate setting for the network-wide configuration. The network-wide settings apply to ALL sites once the site is upgraded.

This procedure is applicable only to systems with the Policy and Charging feature enabled.

This procedure is applicable only to major upgrades from 7.0.1 to DSR 8.0.

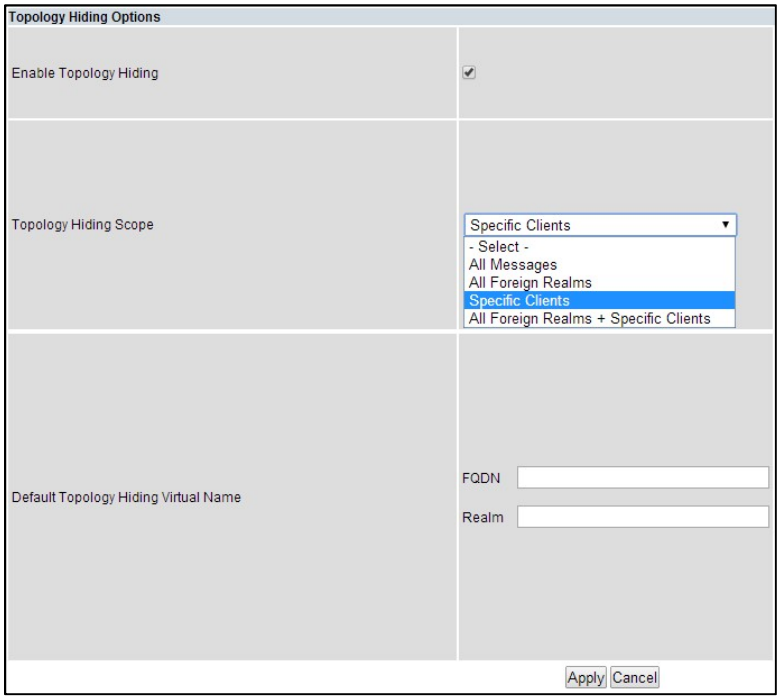
Note: The network-wide Topology Hiding settings at the NOAM apply to each site as it is upgraded. Please note that this may result in a behavior change if the pre-upgrade site settings differ from the network-wide settings.

Note: This procedure can be skipped if Topology Hiding is not in use for this system.

Procedure 19: PCA (formerly PDRA) Topology Hiding Configuration

S T E P #	This procedure sets the network-wide Topology Hiding configuration. This procedure applies only to systems with the Policy and Charging feature enabled. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Enable Global Provisioning	Before the Topology Hiding configuration can be modified, Global Provisioning must be enabled temporarily. • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Provisioning**. • Verify the button text changes to **Disable Provisioning**.

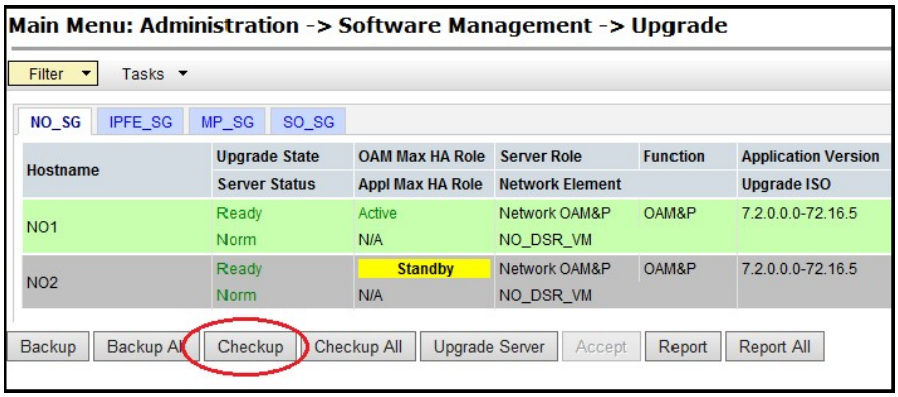
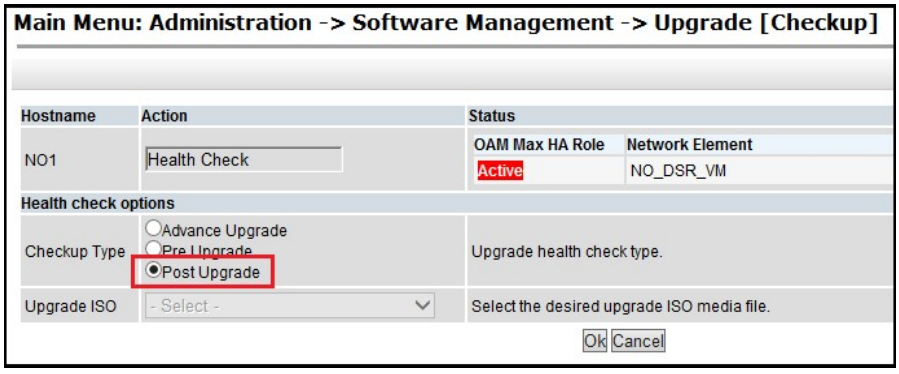
Procedure 19: PCA (formerly PDRA) Topology Hiding Configuration

2. ☐	**Active NOAM VIP**: Configure topology hiding settings	Configure the topology hiding settings. • Navigate to **Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options**. • In the Topology Hiding Options section, select the **Enable Topology Hiding** checkmark. • Select the appropriate Topology Hiding Scope setting. • Enter a Default Topology Hiding Virtual Name – FQDN and Realm. These default values are used if specific values have not been set at a site. • Click **Apply**. 
3. ☐	**Active NOAM VIP**: Disable global provisioning and configuration	Disable global provisioning. • Navigate to **Status & Manage -> Database**. • Click **Disable Provisioning**. • Click **OK** confirm the operation. • Verify the button text changes to **Enable Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`

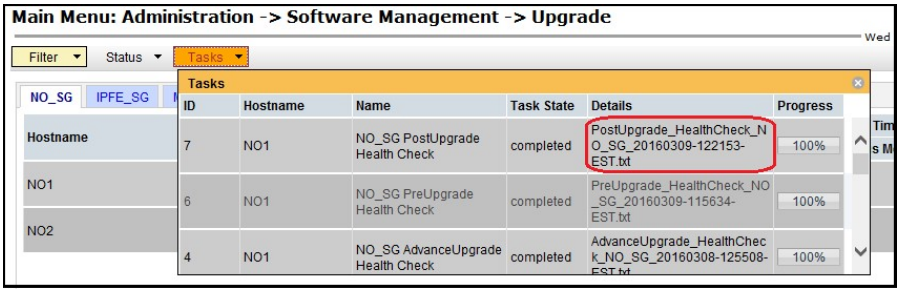
4.4 Verify NOAM Post Upgrade Status

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

Procedure 20: Verify NOAM Post Upgrade Status

S T E P #		
	This procedure verifies post upgrade status for NOAM upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Post-upgrade health checks	This procedure runs the automated post-upgrade health checks. From the active NOAM GUI: • Navigate to **Administration -> Software Management -> Upgrade**. • Select the active NOAM.  • Click **Checkup**. • Under Healtch Check options, select the **Post Upgrade** option. • Click **OK**. Control returns to the Upgrade screen. 

Procedure 20: Verify NOAM Post Upgrade Status

2. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. From the active NOAM GUI: • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <NOServerGroup> PostUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. • Click the hyperlink to download the Health Check report. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. From the active NOAM GUI: • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M.

4.5 Allow Provisioning (Post NOAM Upgrade)

The following procedure enables global provisioning after the NOAM upgrade.

CAUTION **ANY NETWORK-WIDE PROVISIONING CHANGES MADE AT THE NOAM SITE BEFORE THE UPGRADE IS ACCEPTED IS LOST IF THE UPGRADE IS BACKED OUT.**

Procedure 21: Allow Provisioning (Post NOAM Upgrade)

S T E P #		
	This procedure enables provisioning for the NOAM and DR NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Enable global provisioning and configuration	Enable global provisioning and configuration updates on the entire network: • Log into the active NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Provisioning**. • Click **OK** confirm the operation. • Verify the button text changes to **Disable Provisioning**.
Note: After enabling provisioning at the NOAM, it is possible the SOAM GUI(s) will display a banner indicating that global provisioning is disabled. This message can be ignored – global provisioning is enabled. This is a display issue only and is corrected when the SOAMs are upgraded.		
2. ☐	**Active NOAM VIP**: Add new network element (if required)	Perform this step only if the addition of a new network element is required at this time If a new network element is to be added, this procedure can be started now. Addition of the new network element requires a separate maintenance window. The servers in the new network element must be installed with the same DSR release as that of the upgraded NOAM(s). Follow the DSR 8.0 Installation Procedures in reference [1] DSR 8.0 Cloud Installation Guide, E76331, Oracle to install the software on the new servers and add the new network element under the existing NOAM(s). Skip the sections of the installation procedure related to installing and configuring the NOAM(s). This adds a new DSR SOAM site under the existing NOAM(s).

5. Site Upgrade Execution

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

To maximize the maintenance window usage, the procedures in this section make full use of the parallel upgrade capabilities of the DSR, while ensuring traffic continuity and redundancy to the fullest extent possible.

The Automated Site Upgrade procedures are in Section 5.2:Automated Site Upgrade. Use the procedures in this section if Automated Site Upgrade was recommended in Section 3.3:Site Upgrade Methodology Selection.

The manual site upgrade procedures are in Section 5.3:Automated Server Group/Manual Upgrade Overview. Use the procedures in this section if Automated Server Group Upgrade or manual upgrade was recommended in Section 3.3:Site Upgrade Methodology Selection.

5.1 Site Pre-Upgrade Activities

SOAM UPGRADE: Pre-Upgrade Activities

Use this section to execute pre-upgrade planning, pre-upgrade backups, pre-upgrade health checks, and to disable site provisioning.

This section contains the procedures for site upgrade planning, pre-upgrade backups, health checks, and disabling site provisioning.

Table 12 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 12 as a guide for determining the order in which the procedures are to be executed.

Table 12. Site Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 22	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 23 or Procedure 24	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:35	Site Pre-Upgrade Health Check for Release 8.0 and Later Site Pre-Upgrade Health Check for Release 7.x/8.0	None None
Procedure 25	0:03	0:18-0:38	Site Upgrade Options Check	None
Procedure 26	0:01-0:05	0:19-0:48	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 27	0:05-0:10	0:24-0:58	Site Upgrade Pre-Checks	None
Procedure 28	2:40-4:00	3:04-4:58	Automated Site Upgrade	Traffic is not serviced by servers that are actively upgrading.
Procedure 35	0:02	3:06-5:00	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 36	0:10-0:15	3:26-5:15	Site Post-Upgrade Health Check	None

5.1.1 Site Pre-Upgrade Backups

This procedure is non-intrusive and performs a backup of all servers associated with the SOAM Site(s) being upgraded. It is recommended that this procedure be executed no earlier than 36 hours before the start of the upgrade.

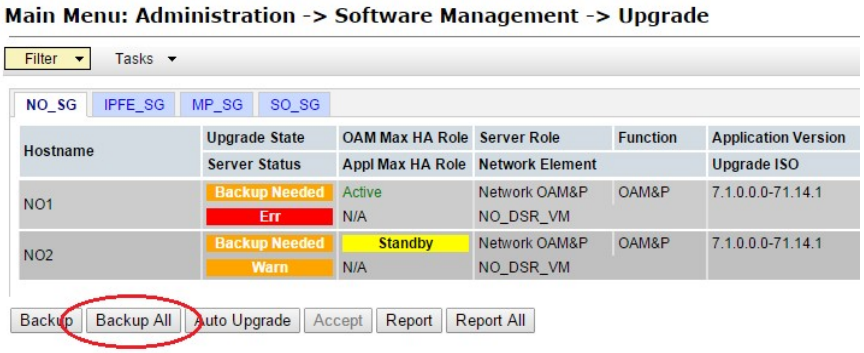
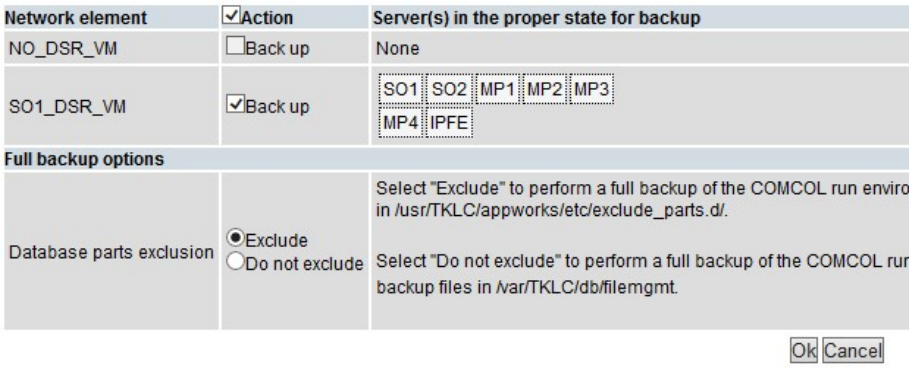
Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 22 is an alternate procedure that can be used to backup a site using the command line. Procedure 22 should only be used by direction of My Oracle Customer Support.

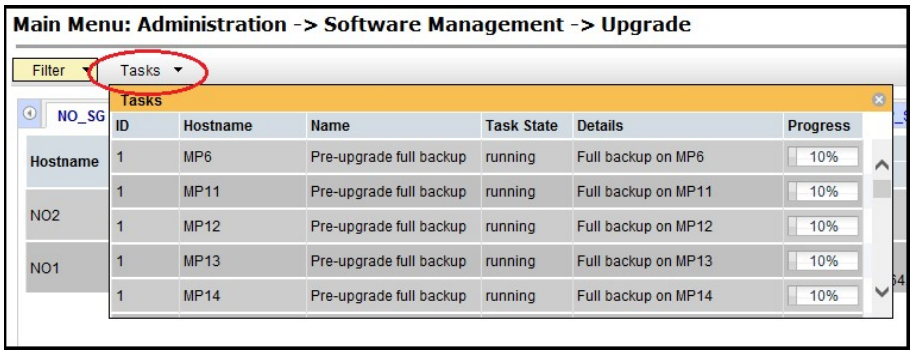
Procedure 22: Site Pre-Upgrade Backups

S T E P #		
	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Backup Site configuration data. **IMPORTANT**: Required for Disaster Recovery	Back up the SOAM database. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> Database** to return to the Database Status screen. • Click to highlight the active SOAM server, and click **Backup**. ***Note***: The Backup button is only enabled when the active server is selected. • Select the **Configuration** checkbox. • Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. • Enter **Comments** (optional). • Click **OK**. ***Note***: The active SOAM can be determined by going to the Status & Manage > HA screen and note which server is currently assigned the VIP in the Active VIPs field. The server having VIP assigned is the active.
2. ☐	**Active SOAM VIP**: Save database backup. IMPORTANT: Required for Disaster Recovery	Download and save backup files. • Navigate to **Status & Manage -> Files**. • Select the active SOAM server tab. • Select the configuration database backup file and click **Download**. • On the confirmation screen, click **Save**. • On the Choose File screen, select a destination folder on the local workstation to store the backup file. Click **Save**. • On the Download Complete screen, click **Close**.

Procedure 22: Site Pre-Upgrade Backups

3. ☐	**Active NOAM VIP**	Back up run environment for site being upgraded. • Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Click **Backup All**. 
4. ☐	**Active NOAM VIP**	The Upgrade [Backup All] screen displays various network elements, and identifies which servers are ready for backup. • In the Action column, select the **Back up** checkbox for the network element to be upgraded. • Verify the NOAM server group checkbox is NOT checked. ***Note***: Backing up the NOAM servers at this point overwrites the pre-upgrade backup files that are needed for backing out the target release. Do NOT backup the NOAM servers. • In the Full backup options section, verify the **Exclude** option is selected. • Click **OK**. This initiates a full backup on each eligible server. 

Procedure 22: Site Pre-Upgrade Backups

5. ☐	**Active NOAM VIP**: Monitor for backup completion	Monitor the backup tasks. From the active NOAM GUI: • From the Upgrade screen, select the **Tasks** list. • Monitor the progress of the backups until the network element(s) selected in step 4 are complete. 

6. ☐	**Active NOAM VIP**: Verify backup files are present on each server	• Log into the active NOAM or SOAM GUI.
		• Navigate to **Status & Manage -> Files**.
		• Select each server tab, in turn
		• For each Server, verify the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		• Repeat sub-steps 1 through 4 for each site being upgraded.

5.1.2 Site Pre-Upgrade Health Checks

This section provides procedures to verify the health of the SOAM site before upgrade. Procedure 23 is the primary procedure to be executed when the active NOAM is on Release 8.0 and later. Alternate release-specific procedures are also provided, to be used as directed.

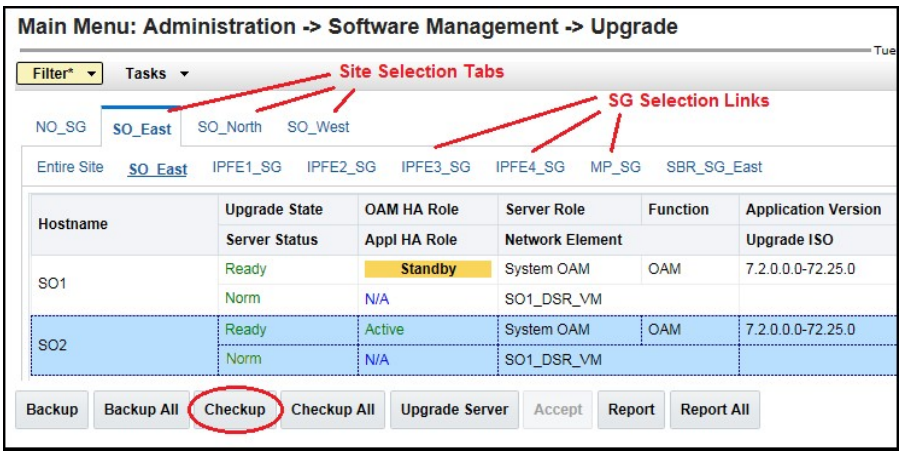
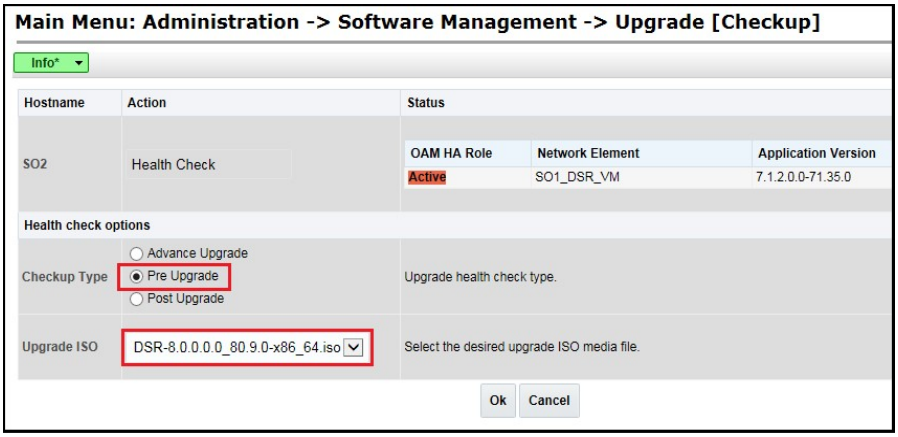
5.1.2.1 Site Pre-Upgrade Health Check for Release 8.0 and Later

This procedure is used when the NOAMs are on Release 8.0 and later. The procedure is non-intrusive and performs a health check of the site before upgrading.

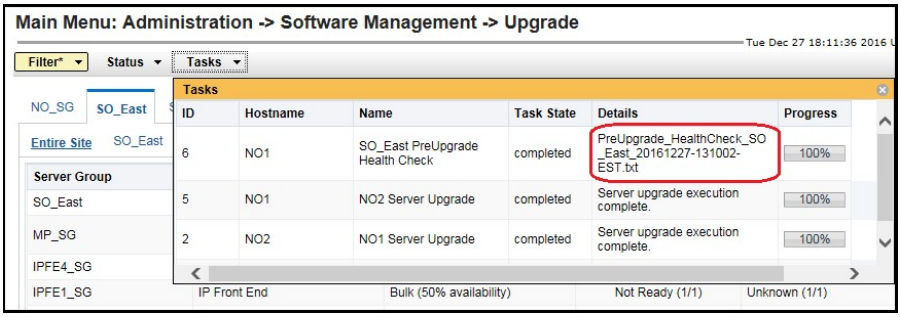
Procedure 23: Site Pre-Upgrade Health Check for Release 8.0 and Later

S T E P #	This procedure performs a health check before upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1.	**Active NOAM VIP**: Run site health	Select the SOAM on which health checks will be run.

Procedure 23: Site Pre-Upgrade Health Check for Release 8.0 and Later

☐	checks (part 1)	• Navigate to **Administration -> Software Management -> Upgrade**. • Select the tab of the site to be upgraded. • Select the SOAM server group link. • Select the active SOAM. • Click **Checkup**. 
2. ☐	**Active NOAM VIP**: Run site health checks (part 2)	Initiate the health checks. • Click **Checkup**. • In the Healtch Check options section, select the **Pre Upgrade** option. • Use the **Upgrade ISO** list to select the target release ISO. • Click **OK** to initiate the health check. Control returns to the Upgrade Administration screen. 

Procedure 23: Site Pre-Upgrade Health Check for Release 8.0 and Later

3. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the Health Check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <SOServerGroup> PreUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. • Click the hyperlink to download the Health Check report. Open the report and review the results. 
4. ☐	**Active SOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. The Health Check log is located in the File Management area of the active SOAM. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M. If the health check log contains the **Unable to execute Health Check on <active SOAM hostname>** message, perform health checks in accordance with Procedure 24 Site Pre-Upgrade Health Check for Release 7.x/8.0
5. ☐	**Active SOAM VIP**: Capture Diameter Configuration on active SOAM GUI	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the **Export Application** list. • Click **OK**. • Verify the data export is complete using the tasks button at the top of the screen. • Click **File Management** to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.
6. ☐	Capture Data for each SOAM Site	Repeat steps 1 through 5 for each configured SOAM site to be upgraded.

5.1.2.2 SOAM Pre-Upgrade Health Check for Release 7.x/8.0

This procedure is an alternate health check that is used when upgrading to Release 8.0 and the active SOAM is on Release 7.x. The procedure is non-intrusive and performs a health check of the site before upgrading. Do not perform this procedure unless directed in Procedure 23, step 4.

Procedure 24: Site Pre-Upgrade Health Check for Release 7.x/8.0

S T E P #	This procedure performs a health check before upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active SOAM CLI**: Verify SOAM pre-upgrade status	Run health checks on active SOAM.
		• Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		This command creates three files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If any alarms are present in the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		• If the **Server <hostname> needs operator attention before upgrade** message displays, inspect the Server Status Report to determine the reason for the message. If the following message displays in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended you contact My Oracle Customer Support for guidance.
		• Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

Procedure 24: Site Pre-Upgrade Health Check for Release 7.x/8.0

2. ☐	**Active SOAM CLI**: Capture Diameter maintenance status	• Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command displays a series of messages providing Diameter Maintenance status. Capture this output and save for later use. ***Note***: The output is also captured in **/var/TKLC/db/filemgmt/UpgradeHealthCheck.log**. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
3. ☐	**Active SOAM CLI**: View DA-MP Status	• Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. • Verify all Peer MPs are available. • Note the number of Total Connections Established _____
4. ☐	**Active SOAM VIP**: Capture Diameter configuration on active SOAM GUI	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the **Export Application** list. • Click **OK**. • Verify the data export is complete using the tasks button at the top of the screen. • Click **File Management** to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Procedure 24: Site Pre-Upgrade Health Check for Release 7.x/8.0

5. ☐	**Active SOAM VIP**	DSR 8.0 introduces **Alarm 22077 – Excessive Request Reroute Threshold Exceeded**. This alarm indicates the request reroutes due to Answer response and/or Answer timeout has exceeded the configured threshold on a DA-MP server. During the upgrade, this threshold is set to 100%, effectively disabling the alarm. Before upgrading a site, measurement stats are collected from the DA-MPs to serve as a baseline for post-upgrade comparisons.
		• Navigate to **Main Menu -> Measurements -> Report**.
		• Click **Go to Export**.
		• On the Report [Export] screen, make the following selections:
		  • **Report Scope**: <Site SOAM NE>
		  • **Report Groups**: Diameter Rerouting
		  • **Time Interval**: Fifteen Minute
		  • **Time Range**: 1 Day
		  • **Export Frequency**: Once
		  • **Task Name**: Leave as is
		• Click **OK** to initiate the export.
		• When the export task is complete, navigate to **Status & Manage -> Files**.
		• Locate the measurements file generated by the export task and download the file to the local workstation. Save this file for later use in the Post Upgrade Procedures section of this document.

6. ☐	Capture data for each SOAM site	Repeat steps 1 through 5 for each configured SOAM site to be upgraded.

5.1.3 Site Upgrade Options Check

Automated Site Upgrade provides user-configurable options that control certain upgrade behaviors. These options are found on the active NOAM's Administration > General Options screen and are described in detail in Section 2.4.3. Before initiating a site upgrade, review these options to verify the current settings are correct, or to modify the settings to meet customer requirements/preferences.

This procedure is applicable only to Automated Site Upgrade. The options have no effect on manual upgrades or Automated Server Group upgrades.

Procedure 25: Site Upgrade Options Check

S T E P #	This procedure reviews the site upgrade options and make changes as necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: View options	• View **Automated Site Upgrade** options. • Log into the active NOAM GUI. • Navigate to **Administration -> General Options**. • Scroll down to the **Site Upgrade Bulk Availability** option. Review the existing value of this option and determine if changes are needed. If the option is changed, click the **OK** to save the change. • Scroll down to the **Site Upgrade SOAM Method** option. Review the existing value of this option and determine if changes are needed. If the option is changed, click the **OK** to save the change.

5.1.4 Disable Site Provisioning

This procedure disables Site Provisioning in preparation for upgrading the site.

!! WARNING!! **THIS PROCEDURE MAY ONLY BE PERFORMED IN THE MAINTENANCE WINDOW IMMEDIATELY BEFORE THE START OF THE SOAM SITE UPGRADE.**

Procedure 26: Disable Site Provisioning

S T E P #	This procedure disables provisioning for the SOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Disable site provisioning	Disable site provisioning at the SOAM. • Log into the SOAM GUI of the site to be upgraded. • Navigate to **Status & Manage -> Database**. • Click **Disable Site Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Enable Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`
2. ☐	Repeat for each SOAM site	Repeat step 1 for each configured SOAM Site to be upgraded.

5.2 Automated Site Upgrade

!! WARNING!!

THE FOLLOWING PROCEDURES MUST BE COMPLETED BEFORE THE STARTING THE AUTOMATED SITE UPGRADE: Procedure 22; [Procedure 23 or Procedure 24]; Procedure 25; Procedure 26; and Procedure 27

5.2.1 Site Upgrade Pre-Checks

This procedure verifies the system is prepared for automated site upgrade.

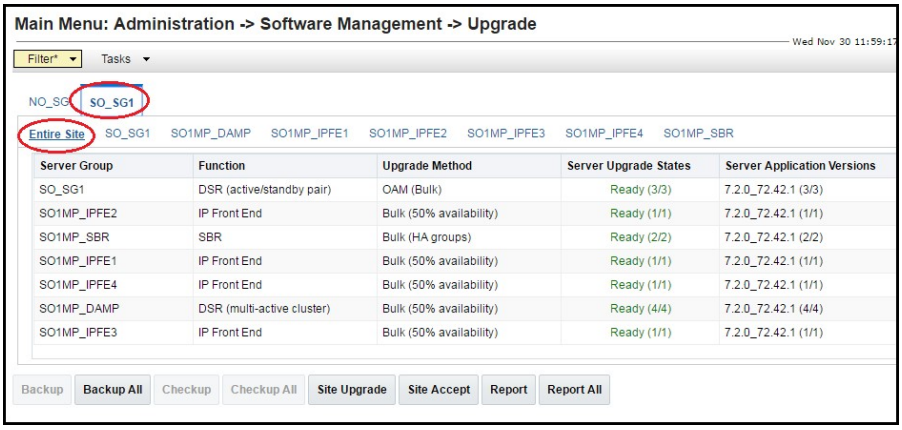
Procedure 27: Site Upgrade Pre-Checks

S T E P #	This procedure verifies traffic status, and verifies that site provisioning is disabled, in preparation for upgrading the site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Verify traffic status	View KPIs to verify traffic status. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> KPIs**. • Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	**Active SOAM VIP**: Verify site provisioning is disabled	Verify Site Provisioning was properly disabled in Procedure 26. • In the GUI status bar, where it says **Connected using** …, check for the **Site Provisioning disabled** message. If the message is present, continue with the next procedure per Table 12, otherwise execute Procedure 17: Disable Global Provisioning.

5.2.2 Initiate Automated Site Upgrade

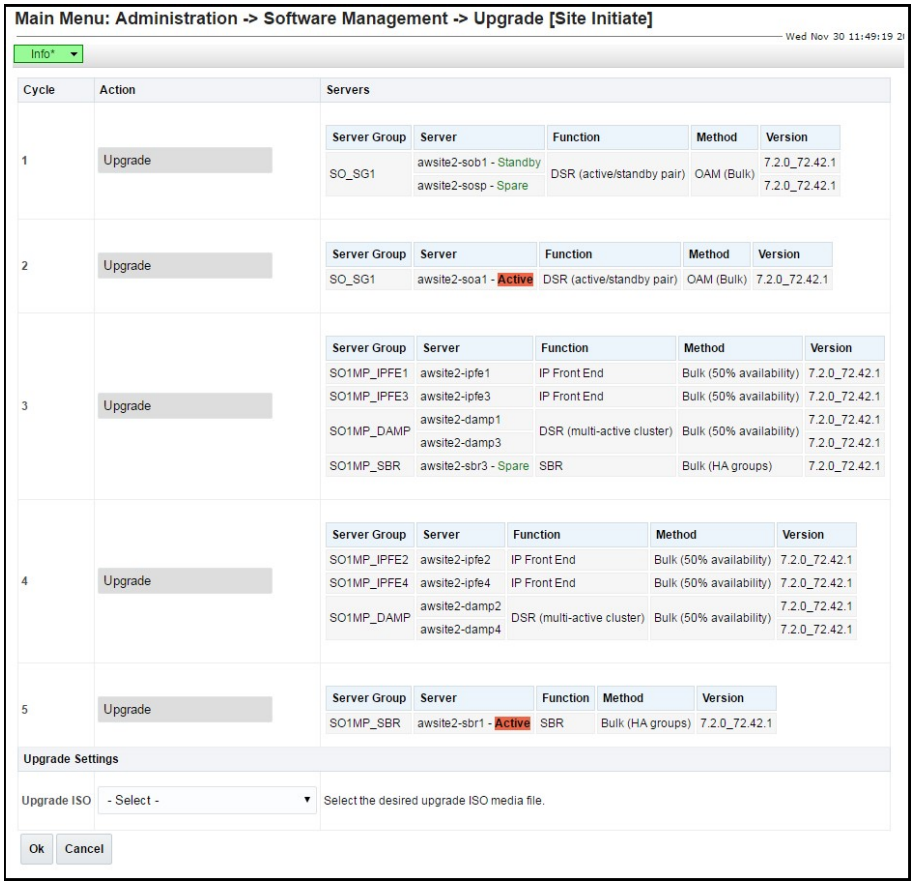
This procedure initiates the Automated Site Upgrade sequence.

Procedure 28: Automated Site Upgrade

S T E P #		
	This procedure upgrades an entire site using the Automated Site Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Review site upgrade plan and site readiness	Review the site upgrade plan created in Section 3.2. This step verifies the servers and server groups to be upgraded are in the proper state. • Log into the NOAM GUI using the VIP • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site to be upgraded. • Verify the **Entire Site** link is selected. The Entire Site screen provides a summary of the server states and upgrade readiness. More detailed server status is available by selecting a specific server group link.  ***Note***: The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including **Accept or Reject**, **Ready**, **Backup Needed**, **Failed**, or **Not Ready**. Only the servers in the **Ready** state or **Failed** state are upgrade eligible.

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versions
SO_SG1	DSR (active/standby pair)	OAM (Bulk)	Ready (3/3)	7.2.0_72.42.1 (3/3)
SO1MP_IPFE2	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_SBR	SBR	Bulk (HA groups)	Ready (2/2)	7.2.0_72.42.1 (2/2)
SO1MP_IPFE1	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_IPFE4	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_DAMP	DSR (multi-active cluster)	Bulk (50% availability)	Ready (4/4)	7.2.0_72.42.1 (4/4)
SO1MP_IPFE3	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)

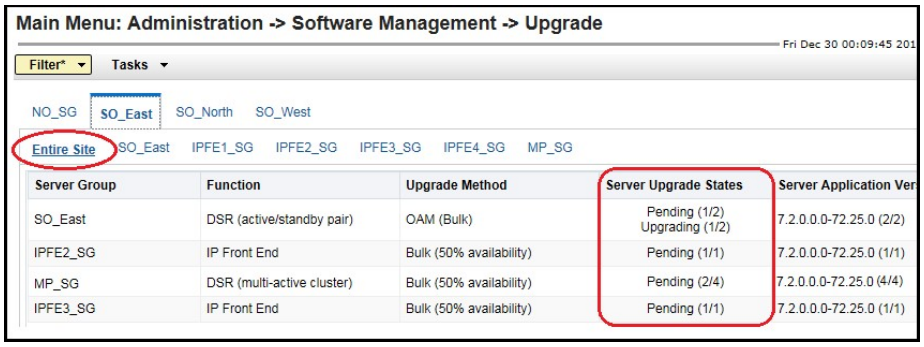
Procedure 28: Automated Site Upgrade

2. ☐	**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 are upgraded. Due to the dynamic nature of upgrade, some servers (typically only C-level) may be upgraded in a different cycle than displayed here.  • In the Upgrade Settings section of the form, select the target ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade sequence. Control returns to the Upgrade Administration screen.
3. ☐	**Active NOAM VIP**	View the Upgrade Administration form to monitor upgrade progress. See step 4 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 displays as **FAILED**.

Procedure 28: Automated Site Upgrade

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 upgrading, and the number of servers pending upgrade. Use this view 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.

During the upgrade, the servers may have a combination of the following expected alarms.

Note: Not all servers have all alarms:

```
Alarm ID = 10008 (Provisioning Manually Disabled)

Alarm ID = 10073 (Server Group Max Allowed HA Role
Warning)

Alarm ID = 10075 (The server is no longer providing
services because application processes have been
manually stopped)

Alarm ID = 31101 (DB Replication To Slave Failure)

Alarm ID = 31106 (DB Merge To Parent Failure)

Alarm ID = 31107 (DB Merge From Child Failure)

Alarm ID = 31228 (HA Highly available server failed to
receive mate heartbeats) or (Lost Communication with
Mate Server)

Alarm ID = 31233 (HA Secondary Path Down)

Alarm ID = 31283 (Highly available server failed to
receive mate heartbeats)

Alarm ID = 32515 (Server HA Failover Inhibited)
```

Note: Do Not Accept any upgrades at this time.

If any upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 28: Automated Site Upgrade

4. ☐	**Server CLI**: If the upgrade of a server fails	If the upgrade of a server fails, access the server command line, via ssh or a console, and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix IM of this document and provide these files.Refer to Appendix K for failed server recovery procedures.

5. ☐	Post upgrade verification	Proceed to Section 5.7 – Site Post-Upgrade Procedures for post upgrade verification procedures.

5.3 Automated Server Group/Manual Upgrade Overview

This section contains alternative site upgrade procedures that can be used when Automated Site Upgrade does not meet the needs or concerns of the customer. These procedures use a combination of Automated Server Group upgrade and manual server upgrades to upgrade a specific site.

Table 13 details the site upgrade plan for a non-PCA/PDRA site, which divides the upgrade into four cycles. A cycle is defined as the complete upgrade of one or more servers, from initiate upgrade to success or failure. The first two cycles consist of upgrading the SOAMs – the first cycle upgrades the standby SOAM, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, SS7-MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, SS7-MPs, and IPFEs to complete the site upgrade.

Table 13. Non-PCA/PDRA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4
Standby SOAM	Active SOAM		
		½ DA-MPs	½ DA-MPs
		½ SS7-MPs	½ SS7-MPs
		½ IPFEs	½ IPFEs

Table 14 details the site upgrade plan for a PCA/PDRA system with two-site redundancy. This upgrade plan is divided into five cycles. The first two cycles consist of upgrading the SOAMs – the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, SS7-MPs, and IPFEs are upgraded in parallel with all of the spare SBRs. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, SS7-MPs, and IPFEs in parallel with all of the standby SBRs.

The fifth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 14. Two-Site Redundancy PCA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5
Standby SOAM, Spare SOAM	Active SOAM			
		½ DA-MPs	½ DA-MPs	
		½ SS7-MPs	½ SS7-MPs	
		½ IPFEs	½ IPFEs	
		Spare SBR(s)	Standby SBR(s)	Active SBR(s)

Table 15 details the site upgrade plan for a PCA/PDRA system with three-site redundancy. This upgrade plan is divided into six cycles. The first two cycles consist of upgrading the SOAMs – the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. Again, this is to ensure that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, SS7-MPs, and IPFEs are upgraded in parallel with one spare SBR. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, SS7-MPs, and IPFEs in parallel with the second spare SBR

The fifth cycle upgrades the standby SBR(s), and the sixth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 15. Three-Site Redundancy PCA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5	Cycle 6
Standby SOAM, Spare SOAM	Active SOAM				
		½ DA-MPs	½ DA-MPs		
		½ SS7-MPs	½ SS7-MPs		
		½ IPFEs	½ IPFEs		
		Spare SBR(s)	Spare SBR(s)	Standby SBR(s)	Active SBR(s)

5.3.1 Site Upgrade Planning

The upgrade of the site servers consists of a mixture of automated upgrades using the Automated Server Group upgrade feature, along with **manual** upgrades that are a little less automated.

Table 16 should be used to plan the upgrade of each site. For the server groups that is upgraded using ASG, the only planning necessary is to record the server group name. ASG automatically selects the individual servers to be upgraded. The SS7-MP and IPFE server groups must be upgraded manually since there is only one server per server group. Planning is necessary for these server groups to ensure traffic continuity. Record the hostname of the servers to be upgraded in each iteration.

Table 16. Site Upgrade Planning Sheet

Iterations	Record Hostname	Notes
Iteration 1		
Standby SOAM Hostname Spare SOAM Hostname		If a spare SOAM exists, the spare and standby SOAMs are upgraded manually. Otherwise, the SOAMs are upgraded with ASG.
Iteration 2		
Active SOAM		The active SOAM is upgraded in iteration 2, either manually or by ASG.
Iteration 3		
DA-MP Group 1		ASG automatically selects DA-MPs for upgrade
SS7-MP 1 Hostname		Manual upgrade
SS7-MP 3 Hostname		Manual upgrade
SS7-MP 5 Hostname		Manual upgrade
SS7-MP 7 Hostname		Manual upgrade
IPFE 1 Hostname		Manual upgrade
IPFE 3 Hostname		Manual upgrade
Spare SBR(s)		ASG automatically selects the Spare SBR(s) for upgrade
Iteration 4		
DA-MP Group 2		ASG automatically selects DA-MPs for upgrade
SS7-MP 2 Hostname		Manual upgrade
SS7-MP 4 Hostname		Manual upgrade
SS7-MP 6 Hostname		Manual upgrade
SS7-MP 8 Hostname		Manual upgrade
IPFE 2 Hostname		Manual upgrade
IPFE 4 Hostname		Manual upgrade
Standby SBR(s)		ASG automatically selects the Standby SBR(s) for upgrade
Iteration 5		
Active SBR(s)		ASG automatically selects the active SBR(s) for upgrade

Table 17 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 17 as a guide for determining the order in which the procedures are to be executed.

Table 17. Site Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 22	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 23 or Procedure 24	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:25	Site Pre-Upgrade Health Check for Release 8.0 and Later Site Pre-Upgrade Health Check for Release 7.x/8.0	None None
Procedure 26	0:01-0:05	0:16-0:35	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 27	0:01-0:05	0:17-0:40	Site Upgrade Pre-Checks	No Traffic Impact
Iteration 1	0:40-1:00	0:57-1:40	Standby SOAM, Spare SOAM (if equipped)	Refer to Section 5.3.2 for details
Iteration 2	0:40-1:00	1:37-2:40	Active SOAM	Refer to Section 5.3.2 for details
Iteration 3	0:40-1:00	2:17-3:40	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Spare SBR(s)	Refer to Section 5.4 for details
Iteration 4	0:40-1:00	2:57-4:40	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s)	Refer to Section 5.5 for details
Iteration 5	0:00-1:00	2:57-5:40	Active SBR(s)	Refer to Section 5.6 for details
Procedure 35	0:02	2:59-5:42	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 36	0:10-0:15	3:09-5:57	Site Post-Upgrade Health Check	None

5.3.2 SOAM Upgrade Overview

This section contains the steps required to perform a major or incremental upgrade of the SOAMs for a DSR site.

During the site upgrade (SOAMs plus all C-level servers), site provisioning is disabled. Provisioning is re-enabled at the completion of the site upgrade.

For each site in the DSR, the SOAM(s) and associated MPs and IPFEs should be upgraded within a single maintenance window.

Table 18 shows the estimated execution times for the SOAM upgrade. Procedure 31 is the recommended procedure for upgrading the SOAMs when there is **no spare SOAM**. ASG automatically upgrades the standby SOAM, followed by the active SOAM.

If the site does have a spare SOAM, Procedure 31: Manual SOAM Upgrade (Active/Standby/Spare) is the recommended procedure. The manual procedure upgrades the standby and spare SOAMs in parallel, followed by the active SOAM.

Table 18: SOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Iteration 1 & 2 Procedure 30 or Procedure 31	1:20-2:40	1:20-2:40	Automated SOAM Upgrade (Active/Standby) Manual SOAM Upgrade (Active/Standby/Spare)	No traffic impact

5.3.3 Upgrade SOAMs

!! WARNING!!

THE FOLLOWING PROCEDURES MUST BE COMPLETED BEFORE THE START OF SOAM UPGRADE:

Procedure 22; [Procedure 23 or Procedure 24]; Procedure 26

This section provides the procedures to upgrade the SOAMs. The SOAMs can be upgraded manually under user control, or automatically using the Automated Server Group Upgrade option. The recommended method for SOAM upgrade depends on the existence of a spare SOAM. If the site includes a spare SOAM, then the SOAMs are upgraded manually so that the spare and standby can be upgraded concurrently. This reduces the time required to upgrade the SOAMs.

Regardless of which SOAM upgrade option is used, Procedure 29 is required to ensure site provisioning is disabled.

If the site does ***not*** include a spare SOAM, use the automated SOAM upgrade in Procedure 30.

If the site does include a spare SOAM, use the manual SOAM upgrade in Procedure 31.

Procedure 29: SOAM Upgrade Pre-Checks

S T E P #	This procedure verifies traffic status, and verifies that site provisioning is disabled, in preparation for upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Verify traffic status	View KPIs to verify traffic status. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> KPIs**. • Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	**Active SOAM VIP**: Verify site provisioning is disabled	Verify Site Provisioning was properly disabled in Procedure 26. • In the GUI status bar, where it says **Connected using** …, check for the **Site Provisioning disabled** message. If the message is present, continue with the next procedure per Table 17, otherwise execute Procedure 26: Disable Site Provisioning.

5.3.3.1 Automated SOAM Upgrade (Active/Standby)

Procedure 30 is the recommended method for upgrading the SOAMs **if the site does not include a spare SOAM**. If the site has a spare SOAM, upgrade using Procedure 31. Upon completion of this procedure, proceed to Section 5.4:Upgrade Iteration 3 Overview.

Procedure 30: Automated SOAM Upgrade (Active/Standby)

S T E P #		
	This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Upgrade SOAM server group	Upgrade the SOAM server group using the Upgrade Multiple Servers procedure with the following options: • Use the Automated Server Group Upgrade option. • Select the Serial upgrade mode. • Execute Appendix F Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix F, return to this point and proceed to Section 5.4:Upgrade Iteration 3 Overview.

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored by way of Disaster Recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

5.3.3.2 Manual SOAM Upgrade (Active/Standby/Spare)

Procedure 31 upgrades the SOAM server group if the site includes a spare SOAM. If the SOAM server group was upgraded using Procedure 30, do not execute this procedure; proceed to Section 5.4:Upgrade Iteration 3 Overview.

Procedure 31: Manual SOAM Upgrade (Active/Standby/Spare)

S T E P #		
	This procedure upgrades the SOAM(s) in a DSR. This procedure upgrades the SOAMs manually. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Upgrade standby and spare SOAMs	Upgrade the standby and spare SOAM servers in parallel using the Upgrade Multiple Servers procedure: • Execute Appendix F Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix F, return to this point and continue with the next step.

Procedure 31: Manual SOAM Upgrade (Active/Standby/Spare)

2. ☐	Upgrade active SOAM	Upgrade the active SOAM server using Upgrade Single Server procedure : • Execute Appendix D Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, return to this point and proceed to Section 5.4:Upgrade Iteration 3 Overview.

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored by way of Disaster Recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

5.4 Upgrade Iteration 3 Overview

Upgrade iteration 3 begins the upgrade of the site C-level servers. As shown in Table 16, iteration 3 consists of upgrading the DA-MPs, SS7-MPs, IPFEs, and spare SBR(s), if equipped. The C-level components are upgraded in parallel to maximize maintenance window usage.

Table 19 shows the estimated time required to upgrade the C-level servers for iteration 3.

Table 19: Iteration 3 Upgrade Execution Overview

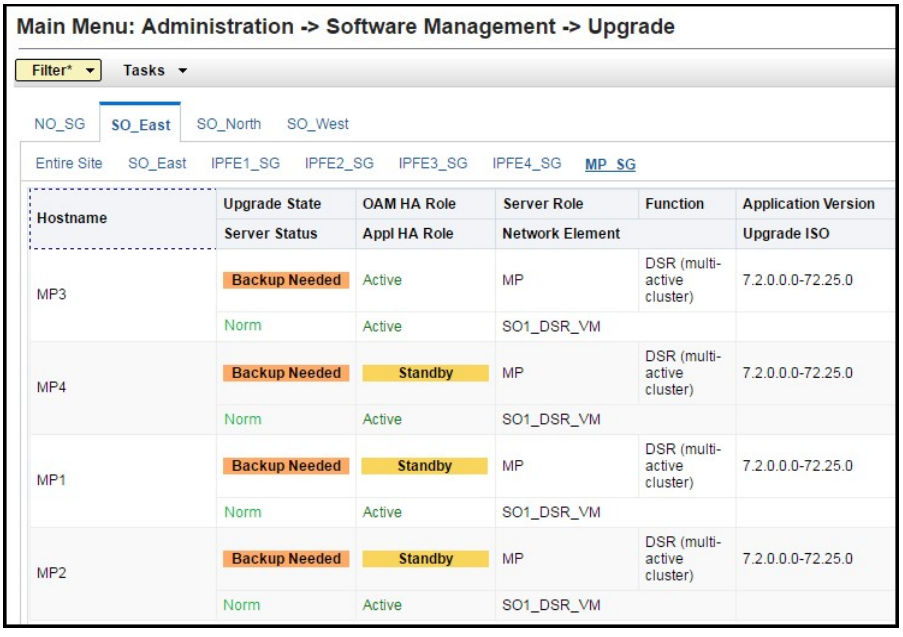
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 32	0:40-1:00	0:40-1:00	Upgrade Iteration 3	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, spare SBR(s) are offline

ASG DOES NOT ALLOW THE OPERATOR TO SPECIFY THE UPGRADE ORDER OF THE DA-MP SERVERS. IF A MANUAL UPGRADE WAS RECOMMENDED IN SECTION 5.3.2, DO NOT USE ASG TO UPGRADE THE DA-MPS IN THIS ITERATION. ALTERNATE UPGRADE PROCEDURES ARE PROVIDED IN Appendix G.3.

5.4.1 Upgrade Iteration 3

Procedure 32 provides the steps to upgrade ½ of the DA-MPs, ½ of the SS7-MPs, ½ of the IPFEs, and the spare SBR(s). Refer to Table 16 for the hostnames of the servers to be upgraded in this iteration.

Procedure 32: Upgrade Iteration 3

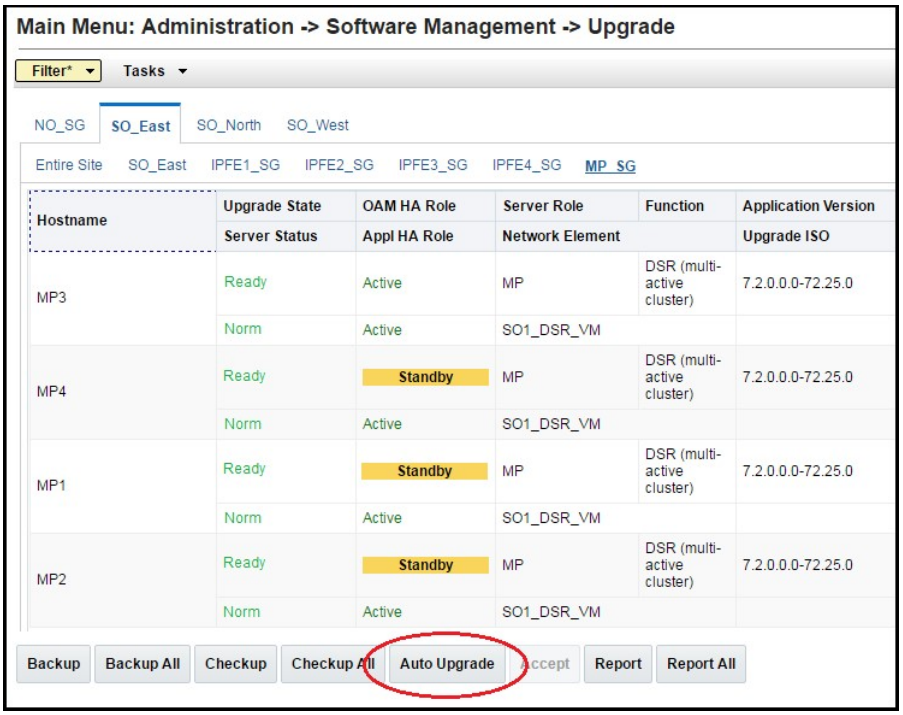
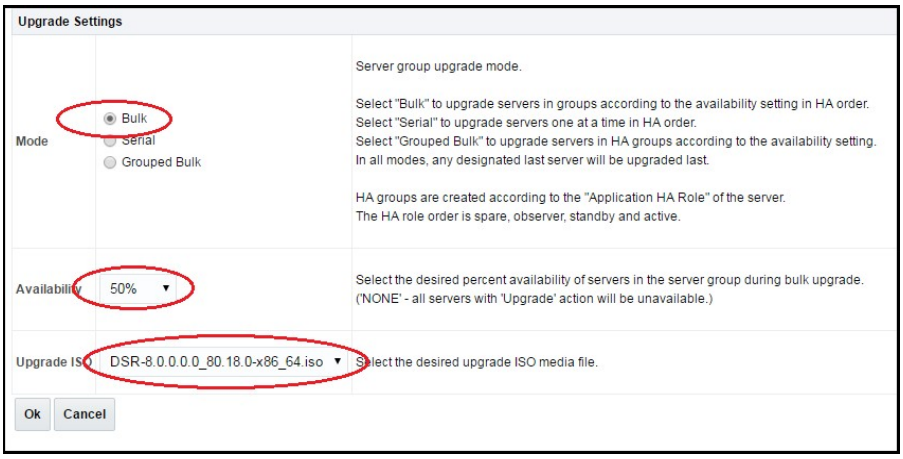
S T E P #	This procedure upgrades a portion of the C-level servers for iteration 3. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: View pre-upgrade status of DA-MPs	Select the DA-MP server group. • Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the **DA-MP Server Group** link. • For the DA-MP servers to be upgraded in iteration 3, verify the **Application Version** is the expected software release version.
2. ☐	**Active NOAM VIP**: View pre-upgrade status of DA-MPs	View the pre-upgrade status of the DA-MP servers. • If the servers are in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

Procedure 32: Upgrade Iteration 3

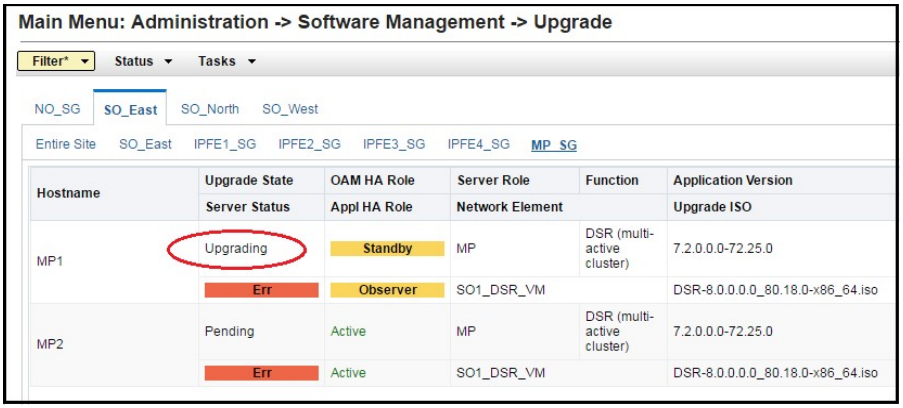
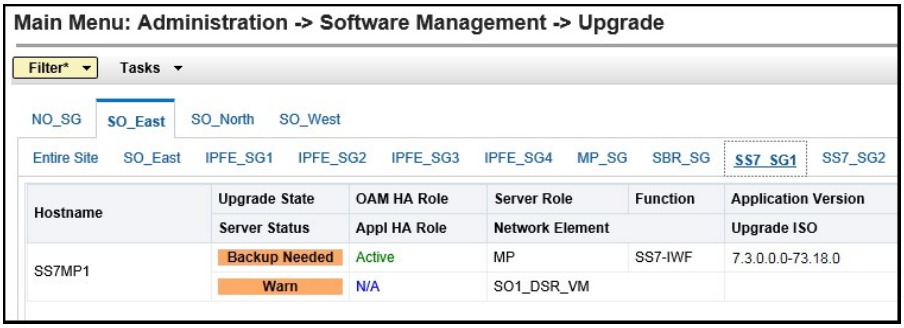
3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		
		The Upgrade Administration screen displays. Navigate to the DA-MP server group of the site being upgraded.
		
		Main Menu: Administration -> Software Management -> Upgrade
		Filter* Tasks
		NO_SG SO_East SO_North SO_West
		Entire Site SO_East IPFE1_SG IPFE2_SG IPFE3_SG IPFE4_SG MP_SG
		
		Servers may have a combination of the following expected alarms.
		
		Note: Not all servers have all alarms:
		
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		
		`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 = 32515 (Server HA Failover Inhibited)`
		
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		
		`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)`

Hostname	Upgrade State / Server Status	OAM HA Role / Appl HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO
MP3	Ready	Active	MP	DSR (multi-active cluster)	7.2.0.0.0-72.25.0
	Norm	Active	SO1_DSR_VM		
MP4	Ready	Standby	MP	DSR (multi-active cluster)	7.2.0.0.0-72.25.0
	Norm	Active	SO1_DSR_VM		
MP1	Ready	Standby	MP	DSR (multi-active cluster)	7.2.0.0.0-72.25.0
	Norm	Active	SO1_DSR_VM		
MP2	Ready	Standby	MP	DSR (multi-active cluster)	7.2.0.0.0-72.25.0
	Norm	Active	SO1_DSR_VM		

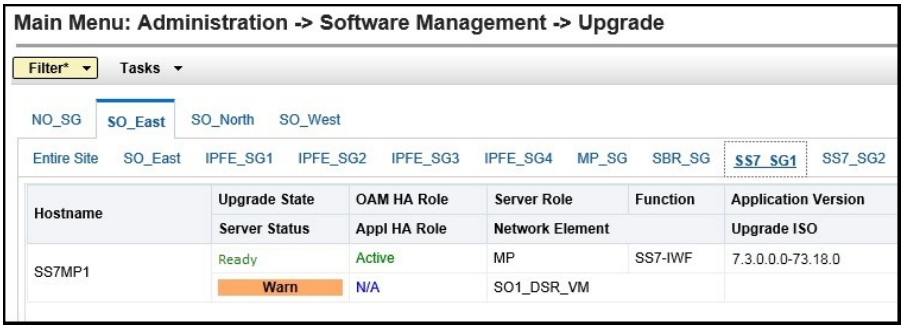
Procedure 32: Upgrade Iteration 3

4. ☐	**Active NOAM VIP**: Initiate DA-MP upgrade (part 1)	Select the Automated Server Group Upgrade option. • To use the Automated Server Group upgrade option, verify no servers in the server group are selected. • Click **Auto Upgrade**. 
5. ☐	**Active NOAM VIP**: Initiate DA-MP upgrade (part 2)	Start the Automated Server Group Upgrade of the DA-MPs. • The Upgrade Settings section of the Initiate screen controls the behavior of the server group upgrade. Select **Bulk** Mode. • Select **50%** for the Availability setting. • Select the appropriate ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 

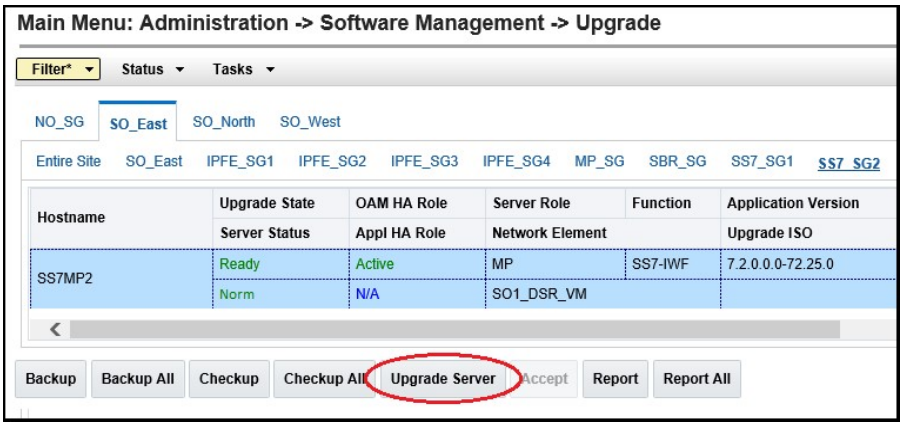
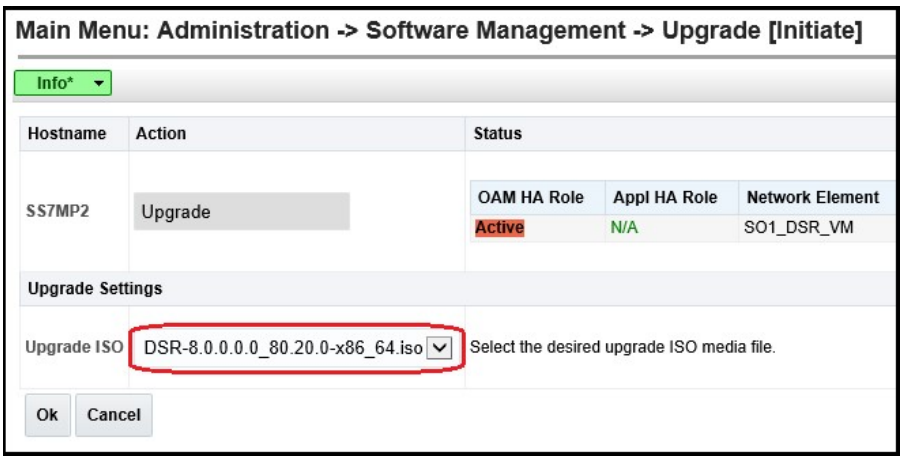
Procedure 32: Upgrade Iteration 3

6. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the DA-MP servers. Upgrade status displays under the **Status Message** column.  Main Menu: Administration -> Software Management -> Upgrade Filter* Status Tasks NO_SG SO_East SO_North SO_West Entire Site SO_East IPFE1_SG IPFE2_SG IPFE3_SG IPFE4_SG MP_SG Hostname / Upgrade State / OAM HA Role / Server Role / Function / Application Version Server Status / Appl HA Role / Network Element / Upgrade ISO MP1 — Upgrading — Standby — MP — DSR (multi-active cluster) — 7.2.0.0.0-72.25.0 Err — Observer — SO1_DSR_VM — DSR-8.0.0.0.0_80.18.0-x86_64.iso MP2 — Pending — Active — MP — DSR (multi-active cluster) — 7.2.0.0.0-72.25.0 Err — Active — SO1_DSR_VM — DSR-8.0.0.0.0_80.18.0-x86_64.iso While the DA-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
7. ☐	Identify the SS7-MP server group(s) to upgrade	From the data captured in Table 16, identify the SS7-MP server group(s) to upgrade in iteration 3.
8. ☐	**Active NOAM VIP**: View pre-upgrade status of SS7-MPs	View the pre-upgrade status of the SS7-MP servers. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the link for each SS7-MP server group to be upgraded. • For the SS7-MP servers to be upgraded in iteration 3, verify the **Application Version** is the expected software release version. • If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_East SO_North SO_West Entire Site SO_East IPFE_SG1 IPFE_SG2 IPFE_SG3 IPFE_SG4 MP_SG SBR_SG SS7_SG1 SS7_SG2 Hostname / Upgrade State / OAM HA Role / Server Role / Function / Application Version Server Status / Appl HA Role / Network Element / Upgrade ISO SS7MP1 — Backup Needed — Active — MP — SS7-IWF — 7.3.0.0.0-73.18.0 Warn — N/A — SO1_DSR_VM

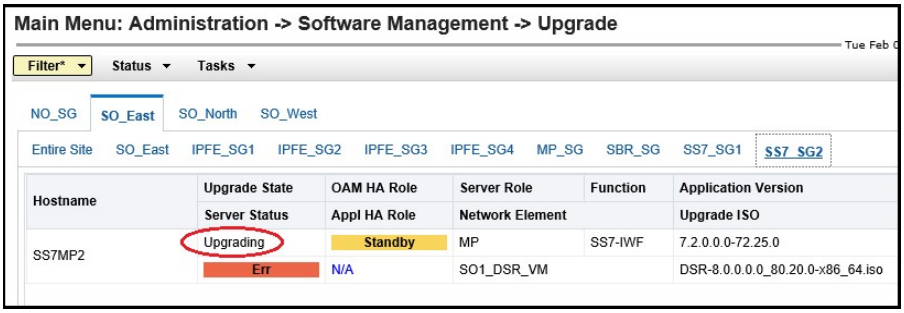
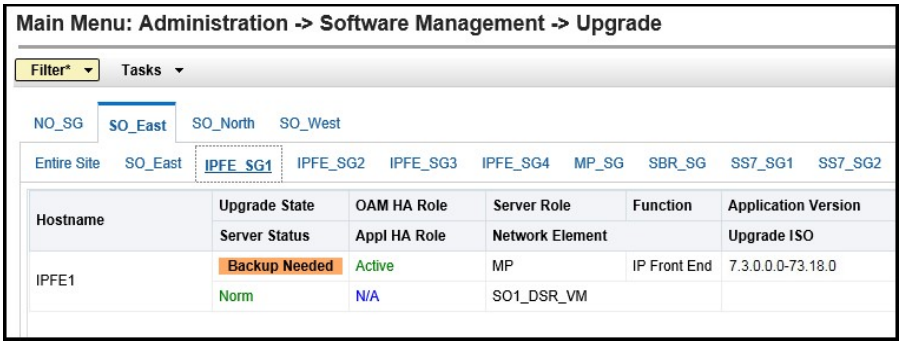
Procedure 32: Upgrade Iteration 3

9. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		The Upgrade Administration screen displays. Navigate to the SS7-MP server group being upgraded.
		 
		
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`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 = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`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)`

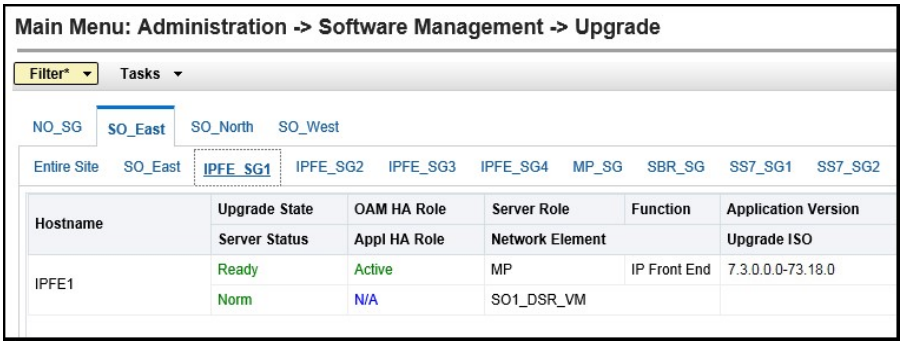
Procedure 32: Upgrade Iteration 3

10. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 1)	Select the Upgrade Server upgrade method. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**. 
11. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 2)	Select target ISO. • On the Upgrade [Initiate] screen, select the target ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 

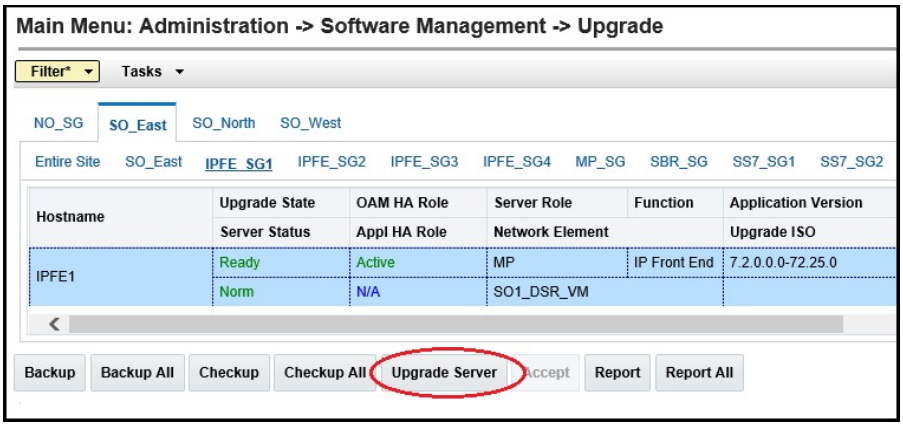
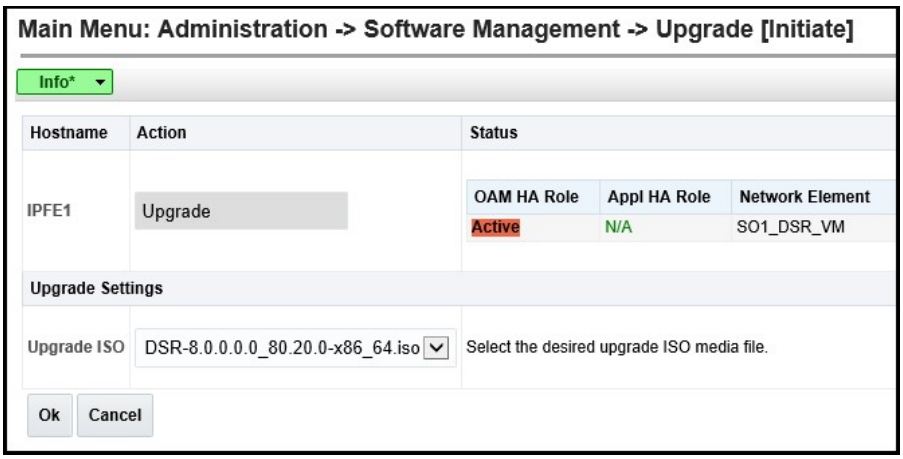
Procedure 32: Upgrade Iteration 3

12. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the SS7-MP server. Upgrade status displays under the **Status Message** column. 
13. ☐	Repeat for each SS7-MP	**Repeat** steps 6 through 12 for the next SS7-MP to be upgraded per Table 16.
14. ☐	Continue upgrade iteration 3	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
15. ☐	Identify the IPFE server group(s) to upgrade	From the data captured in Table 16, identify the IPFE server group(s) to upgrade in iteration 3.
16. ☐	**Active NOAM VIP**: View pre-upgrade status of IPFEs	View the pre-upgrade status of the IPFE servers to be upgraded. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the link for each IPFE server group to be upgraded. • For the IPFE servers to be upgraded in iteration 3, verify the **Application Version** is the expected software release version. • If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

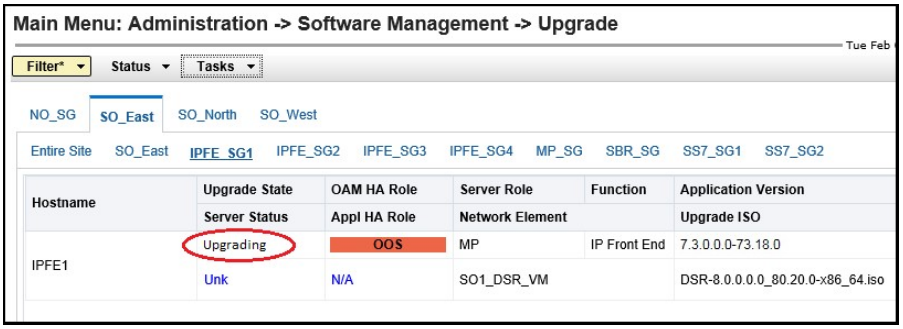
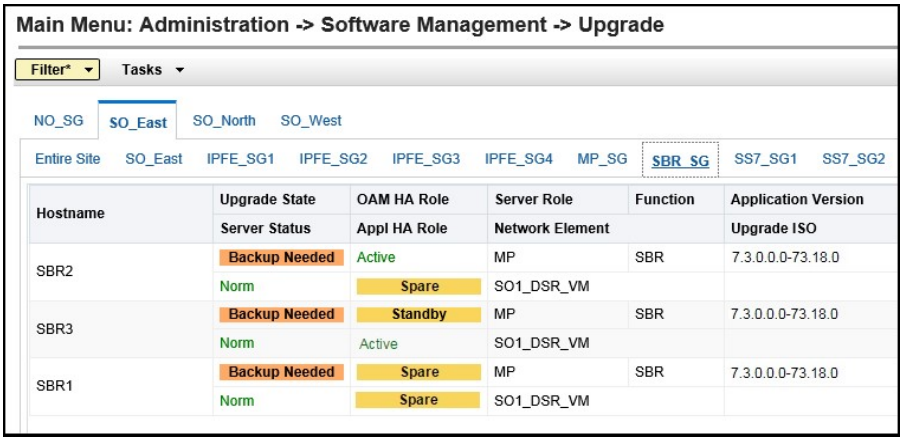
Procedure 32: Upgrade Iteration 3

17. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		The Upgrade Administration screen displays. Navigate to the IPFE server group being upgraded.
		 
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`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 = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`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)`

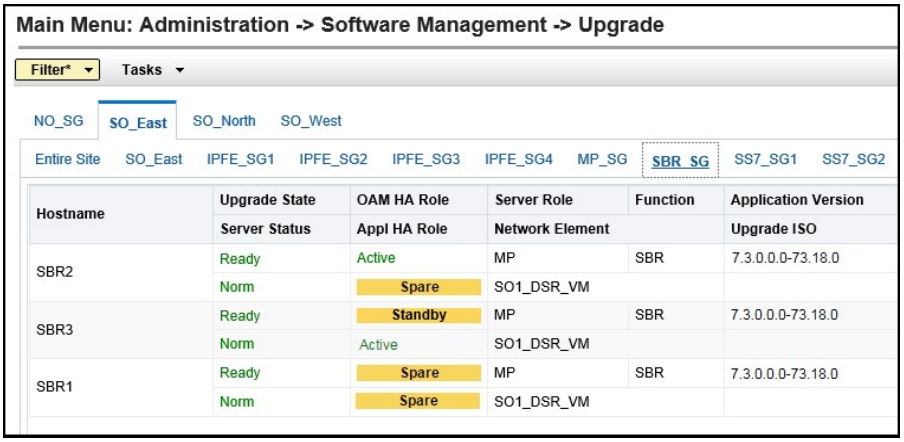
Procedure 32: Upgrade Iteration 3

18. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 1)	Select the Upgrade Server upgrade method. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**. 
19. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 2)	Select target ISO. • On the Upgrade [Initiate] screen, select the target ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 

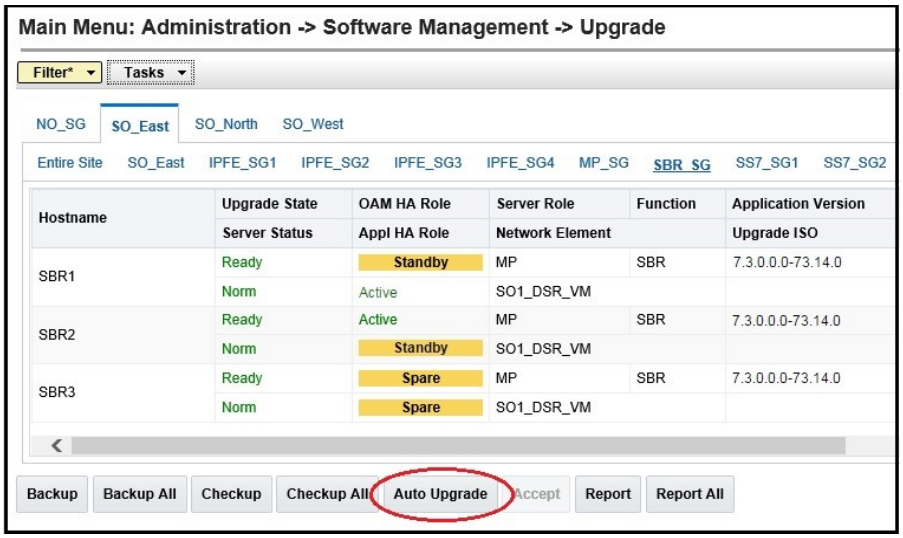
Procedure 32: Upgrade Iteration 3

20. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the IPFE server. Upgrade status displays under the **Status Message** column. 
21. ☐	Repeat for each IPFE	**Repeat** steps 15 through 20 for the next IPFE to be upgraded in this iteration per Table 16.
22. ☐	Identify the SBR server group(s) to upgrade	From the data captured in Table 16, identify the SBR server group(s) to upgrade in iteration 3.
23. ☐	**Active NOAM VIP**: View pre-upgrade status of SBRs	View the pre-upgrade status of the SBR servers to be upgraded. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the link of the SBR server group to be upgraded. • For the SBR servers to be upgraded in iteration 3, verify the **Application Version** is the expected software release version. • If the server is in **Backup Needed** state, select the server and click **Backup**. T he Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (spare, standby or active). This depends on the server being upgraded. 

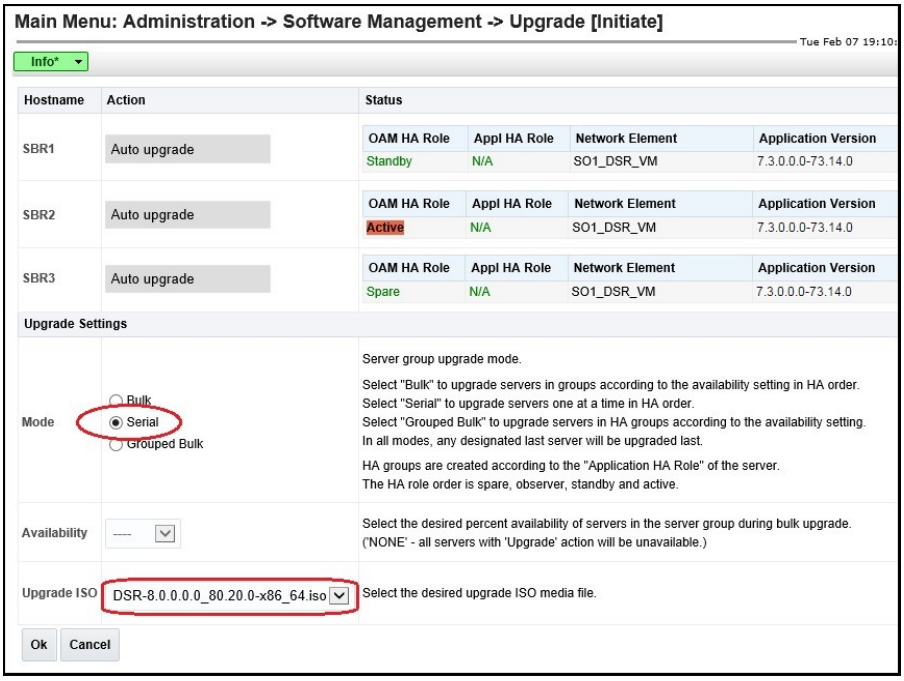
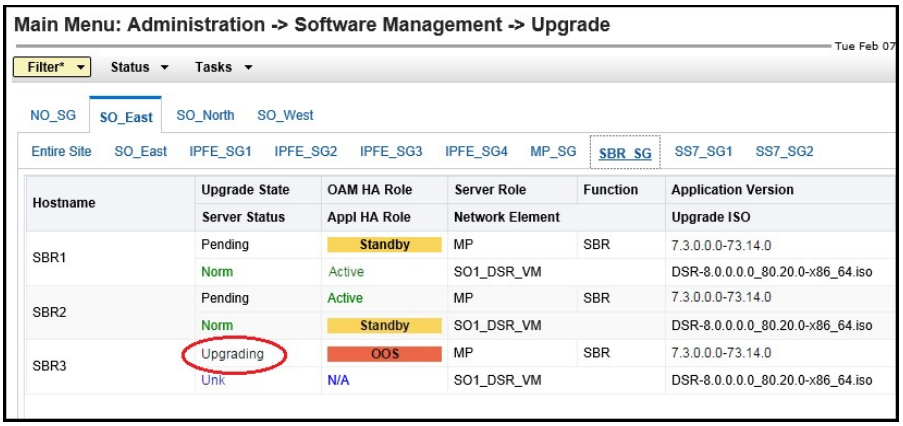
Procedure 32: Upgrade Iteration 3

24. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		
		The Upgrade Administration screen displays. Navigate to the SBR server group being upgraded.
		
		 
		
		Servers may have a combination of the following expected alarms.
		
		Note: Not all servers have all alarms:
		
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		
		`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 = 32515 (Server HA Failover Inhibited)`
		
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		
		`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)`

Procedure 32: Upgrade Iteration 3

25. ☐	**Active NOAM VIP**: Initiate SBR upgrade (part 1)	Select the Auto Upgrade upgrade method. • To use the Automated Server Group upgrade option, select the SBR server group to be upgraded. • Verify no servers in the server group are selected. • Click **Auto Upgrade**. 

Procedure 32: Upgrade Iteration 3

26. ☐	**Active NOAM VIP**: Initiate SBR upgrade (part 2)	Set upgrade options and start the Automated Server Group Upgrade. • The Upgrade Settings section of the Initiate screen controls the behavior of the automated upgrade. Select **Serial** Mode. • Select the appropriate ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 
27. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the SBR server group. Upgrade status displays under the **Status Message** column (not shown). 
28. ☐	Repeat for each SBR server group	**Repeat** steps 22 through 27 for the next SBR server group to be upgraded per Table 16.

Procedure 32: Upgrade Iteration 3

29. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress.
		See step 30 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 displays as **FAILED**.
		The execution time may be shorter or longer depending on the point in the upgrade where there was a problem.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		• Select the SOAM tab of the site being upgraded.
		• Sequence through the server group links for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status displays under the Status Message column.
		During the upgrade, the servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31101 (DB Replication To Slave Failure)`
		`Alarm ID = 31106 (DB Merge To Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		`Alarm ID = 31233 (HA Secondary Path Down)`
		`Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)`
		`Alarm ID = 32515 (Server HA Failover Inhibited)`
		However, database (DB) replication failure alarms may be raised during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix L to resolve this issue.
		• Half of the DA-MP and SBR server groups are upgraded in iteration 3. ASG automatically sequences to iteration 4 to upgrade the remaining servers. Monitor these servers for failures.
		• For the SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The Status Message column displays **Success** after approximately 20 to 50 minutes. Do not proceed to iteration 4 until

Procedure 32: Upgrade Iteration 3

		the SS7-MP and IPFE servers have completed the upgrade. ***Note***: Do Not Accept any upgrades at this time. If any upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

30. ☐	**Server CLI**: If the upgrade of a server fails	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

5.5 Upgrade Iteration 4 Overview

Upgrade iteration 4 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 4 consists of upgrading the second half of the DA-MPs, SS7-MPs, and IPFEs, as well as the standby SBR(s), if equipped.

Table 20 shows the estimated time required to upgrade the C-level servers for iteration 4.

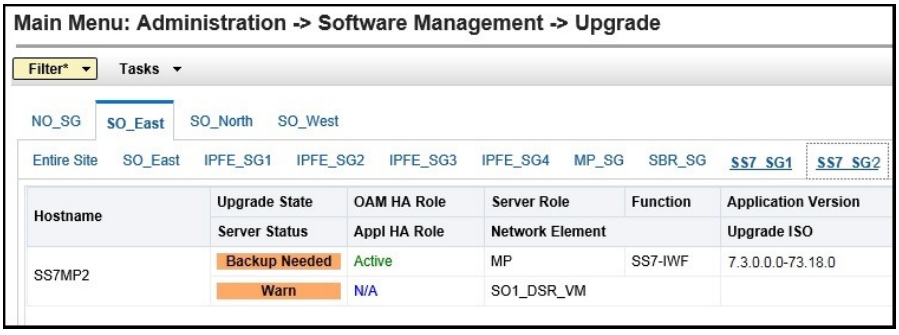
Table 20: Iteration 4 Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 33	0:40-1:00	0:40-1:00	Upgrade Iteration 4	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, standby SBR(s) are offline

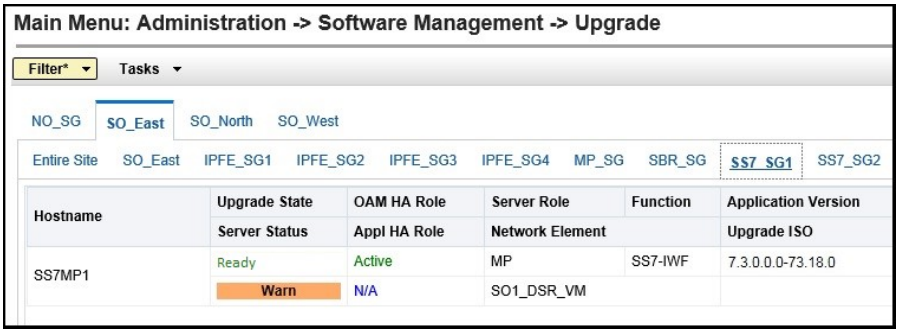
5.5.1 Upgrade Iteration 4

Procedure 33 provides the steps to upgrade ½ of the SS7-MPs, and ½ of the IPFEs. The DA-MPs and SBRs are automatically upgraded by ASG. Refer to Table 16 for the hostnames of the servers to be upgraded in this iteration.

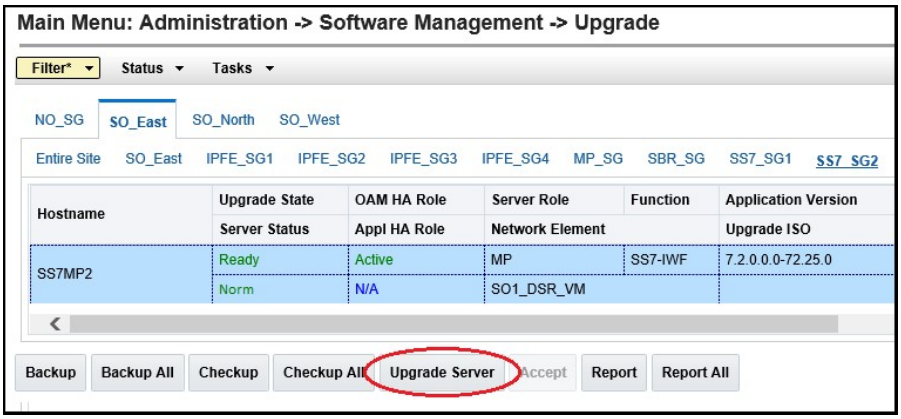
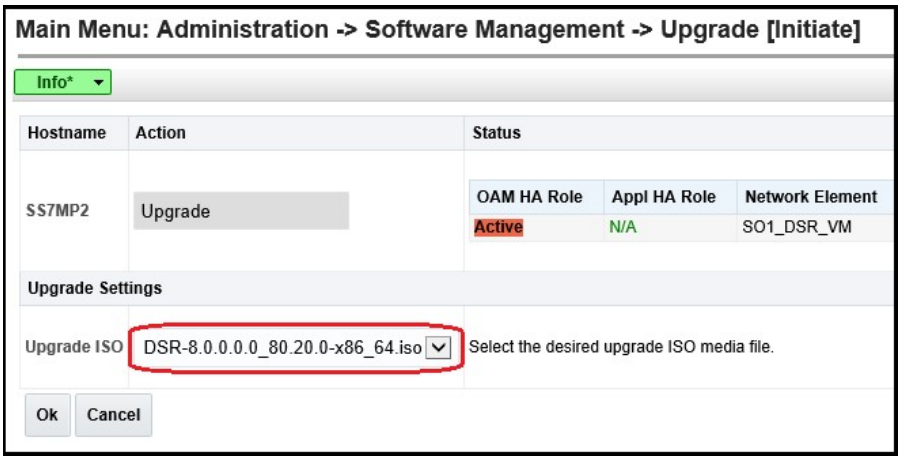
Procedure 33: Upgrade Iteration 4

S T E P #		
	This procedure upgrades a portion of the C-level servers for iteration 4. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Identify the SS7-MP server group(s) to upgrade	From the data captured in Table 16, identify the SS7-MP server group(s) to upgrade in iteration 4.
2. ☐	**Active NOAM VIP**: View pre-upgrade status of SS7-MPs	View the pre-upgrade status of the SS7-MP servers. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the link for each SS7-MP server group to be upgraded. • For the SS7-MP servers to be upgraded in iteration 4, verify the **Application Version** is the expected software release version. • If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

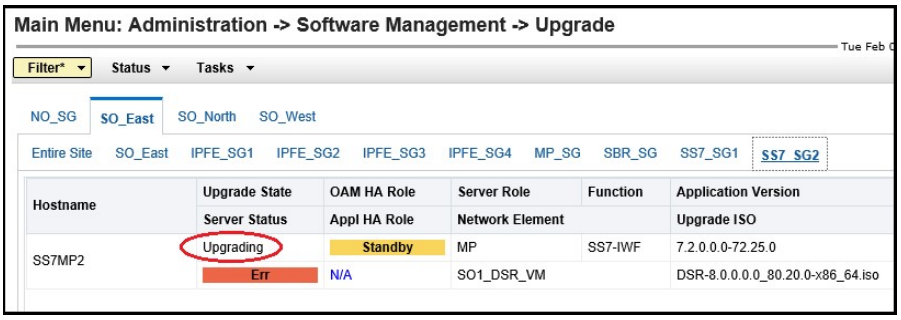
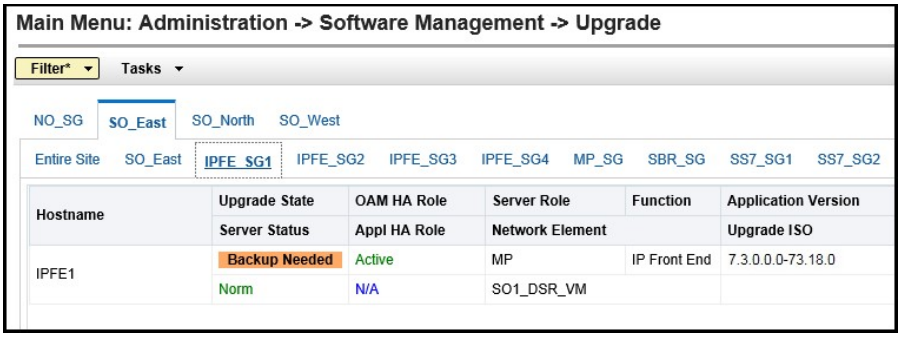
Procedure 33: Upgrade Iteration 4

3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		The Upgrade Administration screen displays. Navigate to the SS7-MP server group being upgraded.
		 
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`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 = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`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)`

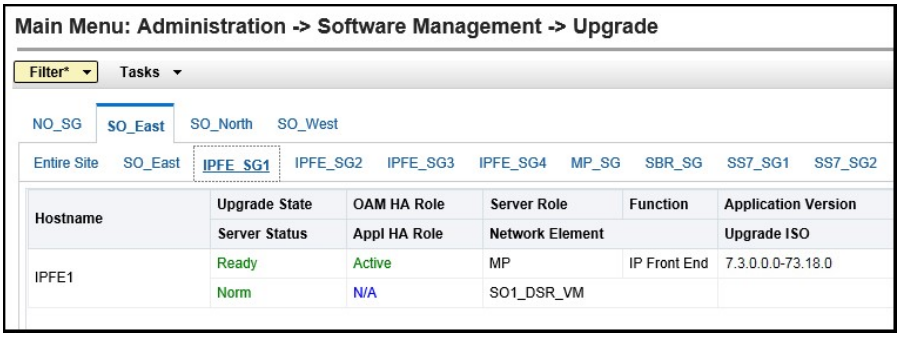
Procedure 33: Upgrade Iteration 4

4. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 1)	Select the Upgrade Server upgrade method. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**. 
5. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 2)	Select target ISO. • On the Upgrade [Initiate] screen, select the target ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 

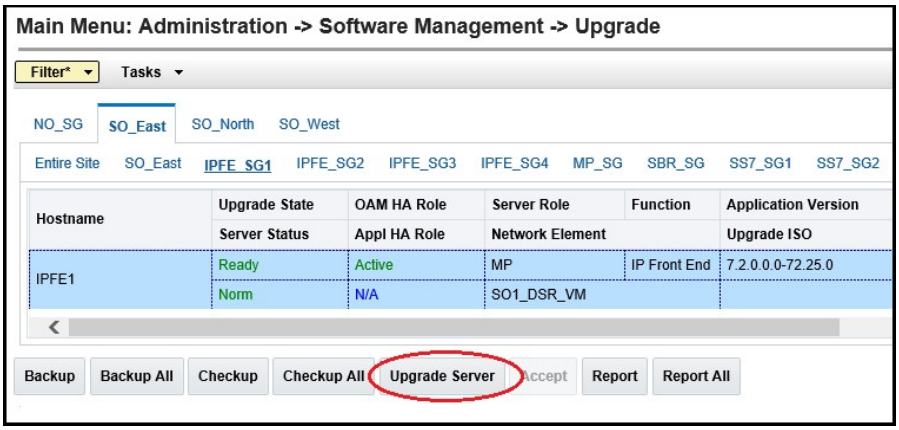
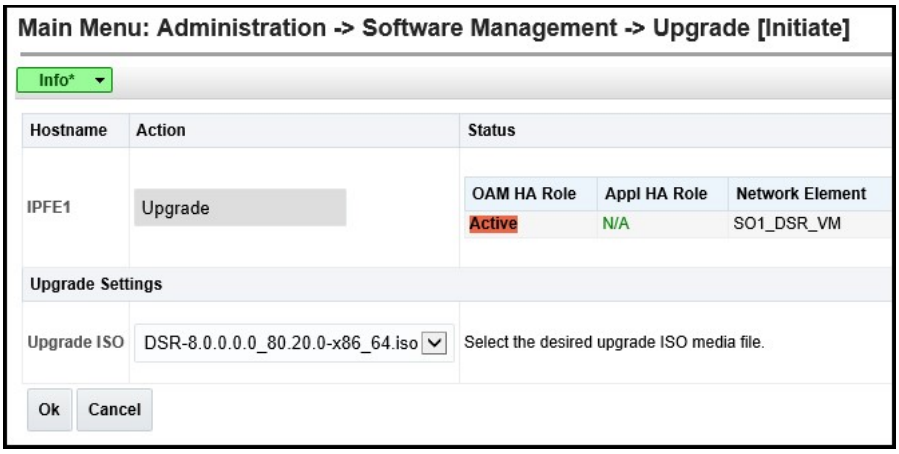
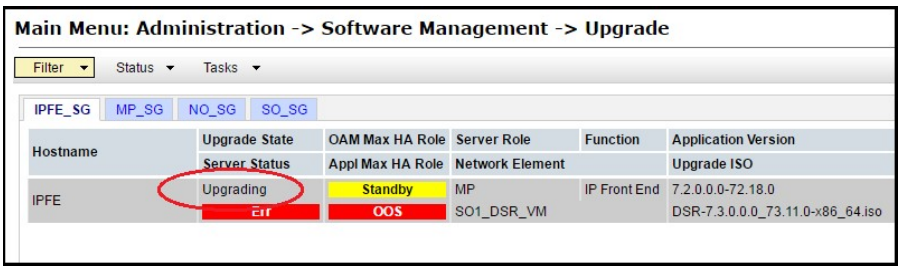
Procedure 33: Upgrade Iteration 4

6. ☐	**Active NOAM VIP**: View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the SS7-MP server. Upgrade status displays under the **Status Message** column. 
7. ☐	Repeat for each SS7-MP	**Repeat** steps 1 through 6 for the next SS7-MP to be upgraded in this iteration per Table 16.
8. ☐	Continue upgrade iteration 4	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
9. ☐	Identify the IPFE server group(s) to upgrade	From the data captured in Table 16, identify the IPFE server group(s) to upgrade in iteration 4.
10. ☐	**Active NOAM VIP**: View pre-upgrade status of IPFEs	View the pre-upgrade status of the IPFE servers. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the link of each IPFE server group to be upgraded. • For the IPFE servers to be upgraded in iteration 4, verify the **Application Version** is the expected software release version. • If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

Procedure 33: Upgrade Iteration 4

11. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	Verify the Upgrade Status is **Ready** for the server to be upgraded. This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur.
		The Upgrade Administration screen displays. Navigate to the IPFE server group being upgraded.
		 
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`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 = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`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)`

Procedure 33: Upgrade Iteration 4

12. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 1)	Select the Upgrade Server upgrade method. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**. 
13. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 2)	Select target ISO. • On the Upgrade [Initiate] screen, select the target ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 
14. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress. • Observe the **Upgrade State** of the IPFE server. Upgrade status displays under the **Status Message** column. 

Procedure 33: Upgrade Iteration 4

15. ☐	Repeat for each IPFE	**Repeat** steps 9 through 14 for the next IPFE to be upgraded per Table 16.

16. ☐	**Active NOAM VIP**: View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress.
		See step 17 below 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 displays as **FAILED**.
		The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		• Select the SOAM tab of the site being upgraded.
		• Sequence through the server group tabs for the server groups being upgraded. Observe the Upgrade State of the servers of interest. Upgrade status displays under the Status Message column.
		During the upgrade, the servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31101 (DB Replication To Slave Failure)`
		`Alarm ID = 31106 (DB Merge To Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		`Alarm ID = 31233 (HA Secondary Path Down)`
		`Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)`
		`Alarm ID = 32515 (Server HA Failover Inhibited)`
		However, database (DB) replication failure alarms may be raised during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix L to resolve this issue.
		• The SBR server groups being upgraded with ASG upgrade the standby SBR in iteration 4, and automatically sequence to iteration 5. Monitor these servers for failures, if equipped.

Procedure 33: Upgrade Iteration 4

		• For the DA-MP, SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The Status Message column displays **Success** after approximately 20 to 50 minutes. Do not proceed to iteration 5 until the DA-MP, SS7-MP, and IPFE servers have completed upgrade. If the system does not have SBRs, the server upgrades are complete. Proceed to Section 5.6:Upgrade Iteration 5 Overview.

17. ☐	**Server CLI**: If the upgrade of a server fails	If any upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.
		If the upgrade of a server fails, access the server command line, via 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`

5.6 Upgrade Iteration 5 Overview

Upgrade iteration 5 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 5 consists of upgrading the active SBR(s).

Table 21 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

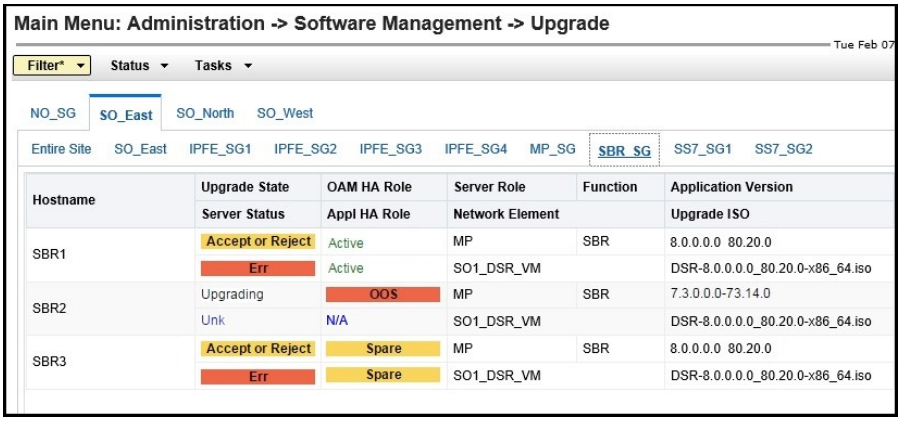
Table 21: Iteration 5 Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 34	0:40-1:00	0:40-1:00	Upgrade Iteration 5	Standby SBR becomes active; previously active SBR is offline for upgrade

5.6.1 Upgrade Iteration 5

Procedure 34 provides the steps to upgrade the active SBRs. The SBRs are automatically upgraded by ASG so the task for iteration 5 is to monitor the upgrade progress. Refer to Table 16 for the hostnames of the servers upgraded in this iteration.

Procedure 34: Upgrade Iteration 5

S T E P #	This procedure upgrades a portion of the C-level servers for iteration 5. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Iteration 5	At iteration 5, the active SBR is upgraded and causes the standby to become active. 

Procedure 34: Upgrade Iteration 5

2. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress.
		See step 3 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 displays as **FAILED**.
		The execution time may be shorter or longer depending on the point in the upgrade where there was a problem.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		• Select the SOAM tab of the site being upgraded.
		• Sequence through the server group tabs for the server groups being upgraded. Observe the Upgrade State of the servers of interest. Upgrade status displays under the Status Message column.
		During the upgrade, the servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31101 (DB Replication To Slave Failure)`
		`Alarm ID = 31106 (DB Merge To Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		`Alarm ID = 31233 (HA Secondary Path Down)`
		`Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)`
		`Alarm ID = 32515 (Server HA Failover Inhibited)`
		However, database (DB) replication failure alarms may be raised during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix L to resolve this issue.
		• Wait for the SBR upgrades to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes.

Procedure 34: Upgrade Iteration 5

3. ☐	**Server CLI**: If the upgrade of a server fails:	If any upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.
		If the upgrade of a server fails, access the server command line (via 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`

5.7 Site Post-Upgrade Procedures

THE FOLLOWING PROCEDURES MUST BE EXECUTED AT THE COMPLETION OF EACH SOAM SITE UPGRADE:

- Procedure 35: Allow Site Provisioning
- Procedure 36: Site Post-Upgrade Health Check

AFTER ALL SOAM SITES IN THE TOPOLOGY HAVE COMPLETED UPGRADE, THE UPGRADE MAY BE ACCEPTED USING THE FOLLOWING PROCEDURE:

- Procedure 49: Accept Upgrade

The post-upgrade procedures consist of procedures that are performed after all of the site upgrades are complete. The final health check of the system collects alarm and status information to verify the upgrade did not degrade system operation. After an appropriate soak time, the upgrade is accepted.

5.7.1 Allow Site Provisioning

This procedure enables site provisioning for the site just upgraded.

CAUTION **ANY PROVISIONING CHANGES MADE TO THIS SITE BEFORE THE UPGRADE IS ACCEPTED ARE LOST IF THE UPGRADE IS BACKED OUT.**

Procedure 35: Allow Site Provisioning

S T E P #	This procedure allows provisioning for SOAM and MP servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Enable site provisioning	Enable site provisioning. • Log into the SOAM GUI of the site just upgraded using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Site Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Disable Site Provisioning**.
2. ☐	**Active SOAM VIP**: Enable the signaling firewall	Enable the signaling firewall for the upgraded site. • Navigate to **Diameter -> Maintenance -> Signaling Firewall**. • Select the signaling node that was just upgraded. • Click **Enable**. • Click **OK** to confirm the action. Verify the Admin State changes to **Enabled**. ***Note***: There may be a short delay while the firewall is enabled on the site.

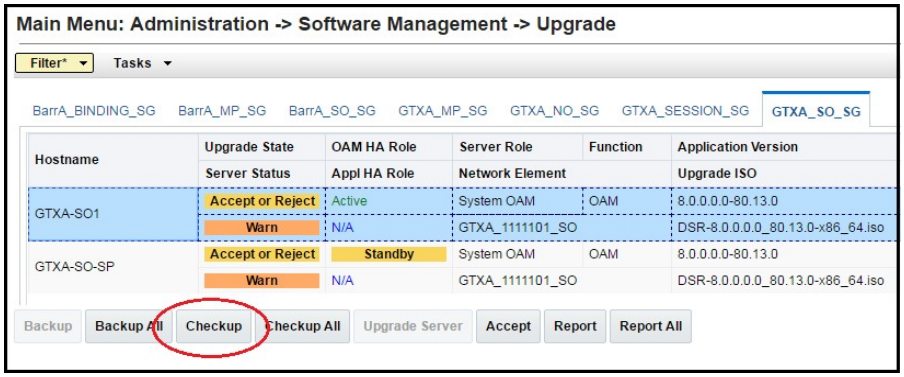
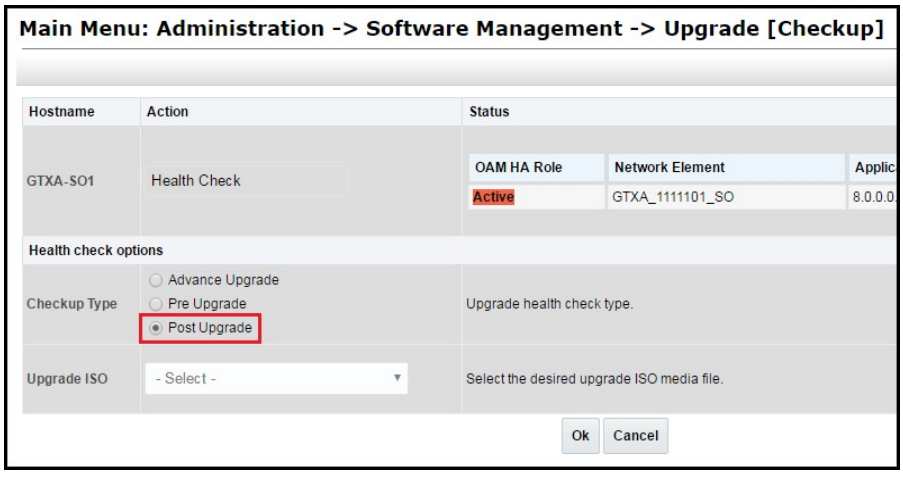
5.7.2 Site Post-Upgrade Health Checks

This section provides procedures to verify the validity and health of the site upgrade.

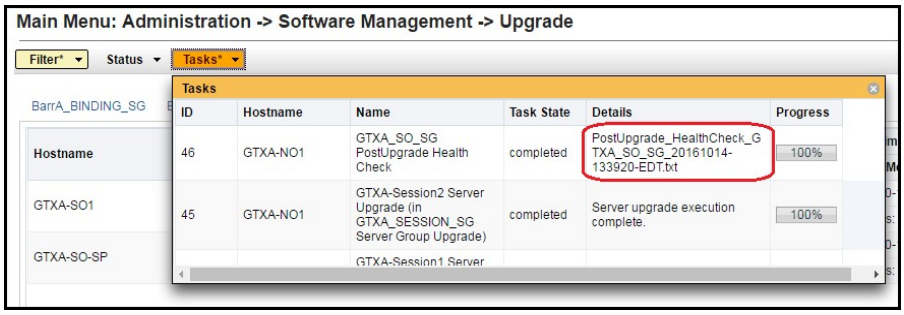
5.7.2.1 Site Post-UpgradeHealth Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

Procedure 36: Site Post-Upgrade Health Check

S T E P #	This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**	This procedure runs the automated post-upgrade health checks. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. • Select the SOAM server group link for the site being upgraded. • Select the active SOAM.  • Click **Checkup**. • Under Healtch Check options, select the **Post Upgrade** option. • Click **OK**. Control returns to the Upgrade screen. 

Procedure 36: Site Post-Upgrade Health Check

2. ☐	**Active NOAM VIP**: Monitor health check progress	Monitor for the completion of the health check. • Click the **Tasks** list to display the currently executing tasks. The Health Check task name displays as <SOServerGroup> PostUpgrade Health Check. • Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. • Click the hyperlink to download the Health Check report. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M. If the health check log contains the **Unable to execute Health Check on <active NOAM hostname>** message, perform the health checks in Procedure 37: Alternate SOAM Post-Upgrade Health Check.
4. ☐	**Active SOAM VIP**: Export and archive the Diameter configuration data	Export Diameter configuration data. • Navigate to **Main Menu -> Diameter Common -> Export**. • Capture and archive the Diameter data by selecting **ALL** from the **Export Application** list. • Click **OK**. • Verify the data export is complete using the tasks button at the top of the screen. • Navigate to **Main Menu -> Status & Manage -> Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine. • Navigate to **Diameter -> Maintenance -> Applications**. • Verify Operational Status is **Available** for all applications.

Procedure 36: Site Post-Upgrade Health Check

5. ☐	**Active SOAM Server**: Check if the setup previously has a customer supplied Apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	If the setup had a customer-supplied Apache certificate installed and protected with passphrase before the start of the upgrade (refer to Procedure 2), then rename the certificate back to the original name.
6. ☐	Compare data to the pre-upgrade health check to verify if the system has degraded after the second maintenance window.	Verify the health check status of the upgraded site as collected from Steps 1 through 4 is the same as the pre-upgrade health checks taken in Section 5.1.2. If system operation is degraded, it is recommended you contact My Oracle Customer Support.

5.7.2.2 Alternate SOAM Post-Upgrade Health Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers. This procedure is an alternative to the normal post upgrade health check in Procedure 36.

Procedure 37: Alternate SOAM Post-Upgrade Health Check

S T E P #	This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active SOAM CLI**: Verify SOAM post-Upgrade Status	Run SOAM post-upgrade health check.
		• Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the command:
		`$ upgradeHealthCheck postUpgradeHealthCheckOnSoam`
		This command creates files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`

Procedure 37: Alternate SOAM Post-Upgrade Health Check

		If any alarms are present in the system:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The same command used for pre-upgrade healthchecks `preUpgradeHealthCheckOnSoam` is also used to verify post upgrade health status.
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		• If the **Server <hostname> needs operator attention before upgrade** message displays, inspect the Server Status Report to determine the reason for the message. If the following message displays in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended you contact My Oracle Customer Support for guidance.
		• Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

2. ☐	**Active SOAM CLI**: Capture Diameter maintenance status	Capture Diameter Maintenance status. • Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command displays a series of messages providing Diameter Maintenance status. Capture this output and save for later use. ***Note***: The output is also captured in **/var/TKLC/db/filemgmt/UpgradeHealthCheck.log**. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
3. ☐	**Active SOAM CLI**: View DA-MP status	Capture DA-MP status. • Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. • Verify all peer MPs are available. • Note the number of Total Connections Established _____

Procedure 37: Alternate SOAM Post-Upgrade Health Check

4. ☐	Compare data to the pre-upgrade health check to verify if the system has degraded after the second maintenance window	Verify the health check status of the upgraded site as collected in this procedure is the same as the pre-upgrade health checks taken in 5.1.2 Site Pre-Upgrade Health Checks. If system operation is degraded, it is recommended you report it to My Oracle Customer Support.

Note: If another site is to be upgraded, all procedures specified by Table 12 must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.

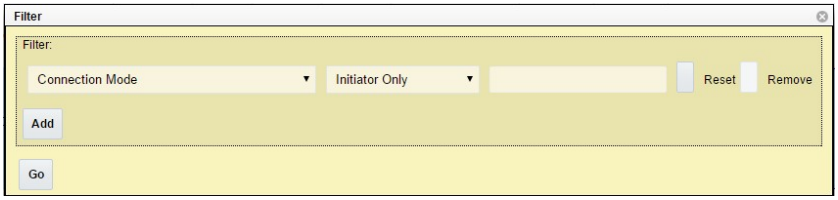
5.7.3 Post-Upgrade Procedures

The procedures in this section are to be executed after the site upgrade is verified to be valid and healthy. These procedures should be executed in the maintenance window.

Procedure 38: Post-Upgrade Procedures

S T E P #	This procedure performs additional actions that are required after the upgrade is successfully completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM VIP**: Enable the signaling firewall	Enable the signaling firewall for the upgraded site. The firewall enables the DSR to dynamically determine and customize the Linux firewall on each DA-MP server in the DSR signaling node to allow only the essential network traffic pertaining to the active signaling configuration. • Navigate to **Diameter -> Maintenance -> Signaling Firewall**. • Select the signaling node that was just upgraded. • Click **Enable**. • Click **OK** to confirm the action. Verify the Admin State changes to **Enabled**. ***Note***: There may be a short delay while the firewall is enabled on the site.

Procedure 38: Post-Upgrade Procedures

2. ☐	**Active SOAM VIP**: Toggle initiator connections. For Source Release 7.0 only.	This step is required only if the source release is DSR 7.0.
		• Navigate to **Diameter -> Maintenance -> Connections**.
		• Use the filter settings to search for **Initiator Only** connections.
		 
		• If the resulting list is empty, this step is complete; otherwise, for the connections in the search results:
		  • Select one or more connections
		  Note: The following steps momentarily disrupt traffic flow for the selected connections.
		  • Click **Disable**.
		  • Click **Enable**.
		  • Verify the Admin State changes to **Enabled**.

6. Backout Procedure Overview

The procedures provided in this section return the individual servers and the overall DSR system to the source release after an upgrade is aborted. The backout procedures support two options for restoring the source release:

- Emergency backout
- Normal backout

The emergency backout overview is provided in Table 22. These procedures back out the target release software in the fastest possible manner, without regard to traffic impact.

The normal backout overview is provided in Table 23. These procedures back out the target release software in a more controlled manner, sustaining traffic to the extent possible.

All backout procedures are executed inside a maintenance window.

The backout procedure times provided in Table 22 and Table 23 are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done.

Note: While not specifically covered by this procedure, it may be necessary to re-apply patches to the source release after the backout. If patches are applicable to the source release, verify all patches are on-hand before completing the backout procedures.

Table 22: Emergency Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 39	0:10-0:30	0:10-0:30	Backout Health Check: The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	None
Procedure 40	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 41	See Note	See Note	Emergency Site Backout: NOTE: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.
Procedure 46	See Note	See Note	Backout Multiple Servers: NOTE: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.
Procedure 42	See Note	See Note	Emergency NOAM Backout: NOTE: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.

Table 23: Normal Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 39	0:10-0:30	0:10-0:30	Backout Health Check: The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	None.
Procedure 40	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 43	See Note	See Note	Normal Site Backout: ***Note***: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.
Procedure 46	See Note	See Note	Backout Multiple Servers: ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.
Procedure 44	See Note	See Note	Normal NOAM Backout: ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.

6.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to My Oracle Customer Support by referring to Appendix M of this document. Before executing any of these procedures, it is recommended you contact My Oracle Customer Support.

Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.

Warning

Before attempting to perform these backout procedures, it is

recommended to first contact My Oracle Customer Support as described in Appendix M.

Warning

Backout procedures cause traffic loss.

Note: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 8.0 release to the previously installed 7.0.w release). Backout of an initial installation is not supported.

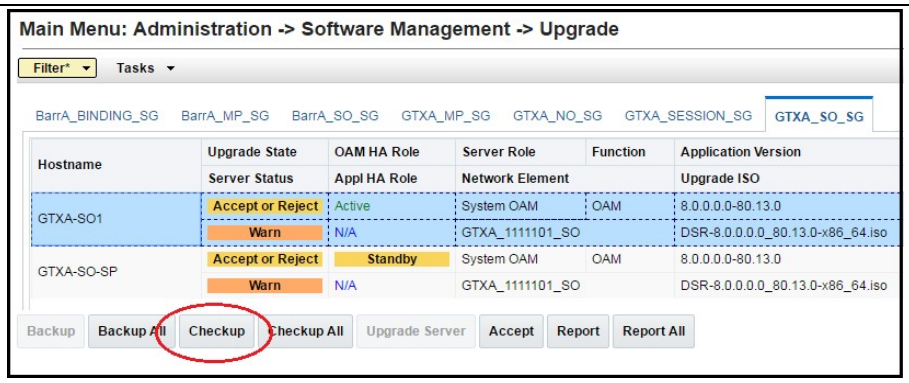
6.2 Backout Health Check

This section verifies the DSR is ready for backout. The site post-upgrade health check performs the backout health check.

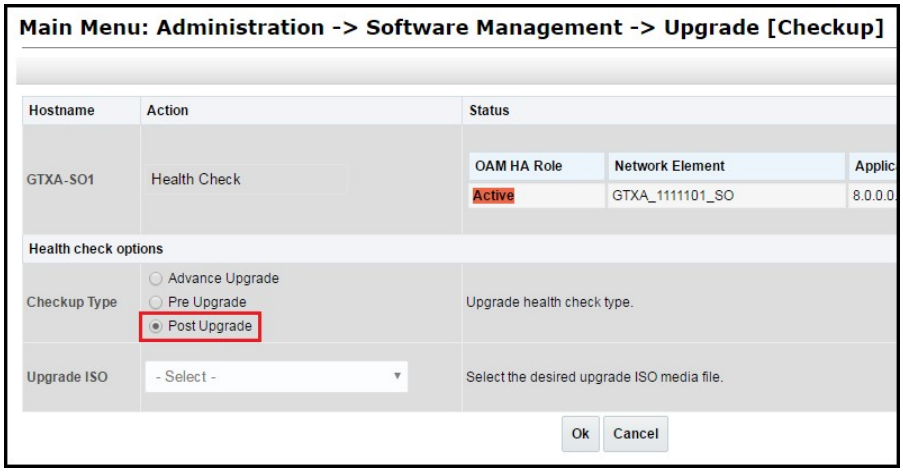
Procedure 39: Backout Health Check

S T E P #	This procedure performs a health check on the site before backing out the upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**	This procedure runs the automated post-upgrade health checks for backout. • Navigate to **Administration > Software Management > Upgrade**. • Select the SOAM tab of the site being backed out. • Select the SOAM server group link for the site being backed out. • Select the active SOAM.

Procedure 39: Backout Health Check

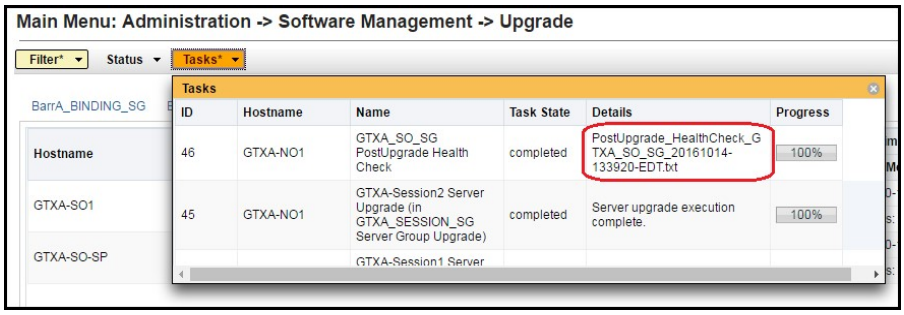
<table>
<tr>
<td></td>
<td></td>
<td>


Click Checkup.
Under Healtch Check options, select the Post Upgrade option.
Click OK. Control returns to the Upgrade screen.



</td>
</tr>
<tr>
<td>2.
☐</td>
<td>Active NOAM VIP: Monitor health check progress</td>
<td>
Monitor for the completion of the health check.

Click the Tasks list to display the currently executing tasks. The Health Check task name displays as <SOServerGroup> PostUpgrade Health Check.
Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report.
Click the hyperlink to download the Health Check report. Open the report and review the results.



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

Procedure 39: Backout Health Check

3. ☐	**Active NOAM VIP**: Analyze health check results	Analyze the Health Check report for failures. If the Health Check report status is anything other than **Pass**, then analyze the Health Check logs to determine if the upgrade can proceed. • Navigate to **Status & Manage -> Files**. • Select the **UpgradeHealthCheck.log** file and click **View**. • Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended you contact My Oracle Customer Support for guidance as described in Appendix M.
4. ☐	**Active NOAM VIP**: Identify IP addresses of servers to be backed out	• Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select each server group link, making note of the application version of each server. • Based on the Application Version column, identify all the hostnames that need to be backed out. • Navigate to **Configuration -> Servers**. • Using the data recorded in Table 5, note the XMI/iLO/LOM IP addresses of all the hostnames to be backed out. These are required to access the server when performing the backout. The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended you contact My Oracle Customer Support as stated in the **Warning** box above.

5. ☐	**Active NOAM VIP**: Verify backup archive files	• Navigate to **Status & Manage -> Files**.
		• For each server to be backed out, select the server tab on the Files screen. Verify the two backup archive files, created in Section 3.4.5, are present on every server that is to be backed out. These archive files have the following format:
		`Backup.<application>.<server>.FullDBParts.<role>.<date_time>.UPG.tar.bz2`
		`Backup.<application>.<server>.FullRunEnv.<role>.<date_time>.UPG.tar.bz2`

Procedure 39: Backout Health Check

6. ☐	Active NOAM CLI: Verify disk usage	Starting with the active SOAM, log into each server to be backed out to verify the disk usage is within acceptable limits.
		• Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM.
		`ssh admusr@<server IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Enter the following command:
		`[admusr@EVO-NO-1 ~]$ df`
		Sample Output (abridged):
		`Filesystem 1K-blocks Used Available Use% Mounted on`
		`/dev/mapper/vgroot-plat_root`
		`999320 294772 652120 32% /`
		`tmpfs 12303460 0 12303460 0% /dev/shm`
		`/dev/vda1 245679 41967 190605 19% /boot`
		`/dev/mapper/vgroot-plat_tmp`
		`999320 1548 945344 1% /tmp`
		`/dev/mapper/vgroot-plat_usr`
		`5029504 2962552 1804824 63% /usr`
		`/dev/mapper/vgroot-plat_var`
		`999320 558260 388632 59% /var`
		`/dev/mapper/vgroot-plat_var_tklc`
		`3997376 2917284 870380 78% /var/TKLC`
		• Observe the line for the **/var** partition. If the **Use%** column is 74% or less, this procedure is complete. Continue with the backout per Table 22 (Emergency) or Table 23 (Normal).
		If the Use% of the /var partition is at 75% or greater, search the partition for files that can be safely deleted. Use extreme caution in choosing files to be deleted. The deletion of critical system files could severely impair the DSR functionality.
		• Repeat sub-steps 1 thru 3 for all servers to be backed out.

6.3 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures no changes are made to the database while the NOAMs and sites are backed out. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 40. Disable Global Provisioning

S T E P #		
	This procedure disables provisioning for the NOAM servers, before upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Disable global provisioning and configuration	Disable global provisioning and configuration updates on the entire network: • Log into the active NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Disable Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Enable Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`

6.4 Perform Emergency Backout

EMERGENCY SITE BACKOUT

Use this section to perform an emergency backout of a DSR upgrade.

The procedures in this section perform a backout of all servers to restore the source release. An emergency backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended you contact My Oracle Customer Support, as stated in the warning box in Section 6.1, to verify all corrective setup steps have been taken.

6.4.1 Emergency Site Backout

The procedures in this section backout all servers at a specific site without regard to traffic impact.

!! WARNING!! **EXECUTING THIS PROCEDURE RESULTS IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR. TRAFFIC BEING PROCESSED BY THE MATE DSR IS NOT AFFECTED.**

Procedure 41: Emergency Site Backout

S T E P #		
	This procedure backs out the DSR application software from multiple B- and C-level servers for a specific site. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Identify all servers that require backout	Identify all servers that require backout (within a site). • Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select each server group link, making note of the application version of the servers. • Identify the servers in the respective server groups with the target release **Application Version**. These servers were previously upgraded but now require Backout. • Make note of these servers. They have been identified for backout. • Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. ☐	**Active SOAM VIP**: Disable site provisioning for the site to be backed out	Disable site provisioning. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Disable Site Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Enable Site Provisioning**. A yellow information box displays at the top of the view screen that states: **[Warning Code 004] – Site provisioning has been manually disabled**. The active SOAM server will have the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`
		**!WARNING!** **STEP 4 RESULTS IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR.**
3. ☐	Backout all C-level servers, as applicable	For all configurations. • Backout all C-level servers (IPFEs, SBRs, SBRs, DA-MPs, and SS7-MPs) identified in step 1: • Execute Section 6.7, Backout Multiple Servers.

Procedure 41: Emergency Site Backout

4. ☐	Backout the standby and spare SOAM servers, as applicable	Backout the standby and spare DSR SOAM servers. If standby and spare SOAM servers are present: • Execute Section 6.7, Backout Multiple Servers. If only a spare SOAM server is present: • Execute Section 6.6. Backout Single Server.
5. ☐	Backout the active SOAM	Backout the active DSR SOAM server. • Execute Section 6.6, Backout Single Server.
6. ☐	**Active SOAM VIP**: Enable site provisioning	Enable site provisioning. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Site Provisioning**. • Click OK to confirm the operation. • Verify the button text changes to **Disable Site Provisioning**.

Note: If another site is to be backed out, follow all procedures in Table 22 in another maintenance window.

6.4.2 Emergency NOAM Backout

This section backs out the NOAM servers.

Procedure 42: Emergency NOAM Backout

S T E P #	This procedure performs an emergency backout of the DSR application software from the NOAM servers. This procedure backs out the application software as quickly as possible without regard to operational impact. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Backout standby DR NOAM server (if equipped)	Backout the standby DR NOAM server. Execute Section 6.6 Backout Single Server.
2. ☐	Backout active DR NOAM server (if equipped)	Backout the other DR NOAM server (now the standby). Execute Section 6.6 Backout Single Server.
3. ☐	Backout standby DSR NOAM server (as applicable)	Backout the standby DSR NOAM server. Execute Section 6.6 Backout Single Server.
4. ☐	Backout active DSR NOAM server	Backout the other DSR NOAM server (now the standby). Execute Section 6.6 Backout Single Server.

Procedure 42: Emergency NOAM Backout

5. ☐	**Active NOAM VIP**: Enable global provisioning	Enable global provisioning and configuration updates on the entire network • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database** • Click **Enable Provisioning**. • Verify the button text changes to **Disable Provisioning**.
6. ☐	**Active NOAM VIP**: Remove **Ready** state for any backed out server	Remove **Ready** state. • Navigate to **Status & Manage -> Server**s. • If any backed-out server Application Status is **Disabled**, then select the server row and click **Restart**. • Navigate to **Administration -> Software Management -> Upgrade**. • If any backed-out server shows an Upgrade State of **Ready** or **Success**, then select that server and click **Complete Upgrade**. Otherwise, skip this step. • Click **OK**. This removes the forced standby designation for the backed-out server. ***Note***: Due to backout being initiated from the command line instead of through the GUI, the following SOAP error may display in 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. • Verify the **Application Version** for servers has been downgraded to the original release version.

6.5 Perform Normal Backout

NORMAL SITE BACKOUT

Use this section to perform a normal backout of a DSR upgrade.

The following procedures to perform a normal backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended you contact My Oracle Customer Support as stated in the warning box in Section 6.1, to verify all corrective setup steps have been taken.

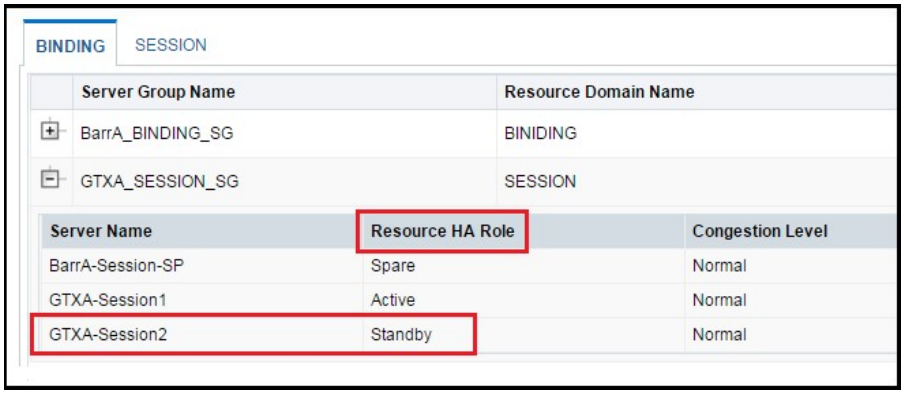
6.5.1 Normal Site Backout

The procedures in this section backout all servers at a specific site.

Procedure 43: Normal Site Backout

S T E P #	This procedure backs out an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Identify all servers that require backout	Identify all servers that require Backout (within a Site): • Log into the NOAM GUI using the VIP. • Navigate to **Administration ->Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select each server group link, making note of the application version of each server. • Identify the servers in the respective server groups with the target release **Application Version**. These servers were previously upgraded but now require Backout. • Make note of these servers. They have been identified for Backout. • Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. ☐	**Active SOAM VIP**: Disable Site Provisioning for the site to be backed out	Disable Site Provisioning • Log into the active SOAM using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Disable Site Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Enable Site Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 004] – Site provisioning has been manually disabled**. The active SOAM server has the following expected alarm: `Alarm ID = 10008 (Provisioning Manually Disabled)`

Procedure 43: Normal Site Backout

3. ☐	Backout the first set of C-level servers as applicable	***Note***: In a PCA system, the spare SBR server is located at the mated site of the site being backed out. Backout the first set of servers. The following servers can be backed out in parallel (as applicable): • Standby DA-MP for 1+1 (active/standby) configuration, or • ½ of all DA-MPs for N+0 (multi-active) configuration • Standby SBR(s) • Spare SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs Execute 6.6 – Backout Single Server for each standby/spare C-level server identified above.
		**!WARNING! Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact**
4. ☐	**Active NOAM VIP**: Verify standby SBR server status	If the server being backed out is the standby SBR, execute this step. Otherwise, continue with step 5. • Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Status**. Open the tab of the server group being upgraded. • Do not proceed to step 5 until the Resource HA Role for the standby server has a status of standby. 

Procedure 43: Normal Site Backout

5. ☐	**Active NOAM VIP**: Verify bulk download is complete.
	For PCA installations only
		Verify bulk download is complete between the active SBR in the server Group to the standby and spare SBRs.
		From the active NOAM GUI:
		• Navigate to **Main Menu > Alarm & Event > View History**.
		• Export the Event Log using the following filter:
		Server Group: Choose the SBR group that is in upgrade
		Display Filter: Event ID = 31127 – DB Replication Audit Complete
		Collection Interval: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time.
		• Wait for the following instances of Event 31127:
		  • 1 for the standby binding SBR server
		  • 1 for the standby session SBR server
		  • 1 for the spare binding SBR server
		  • 1 for the spare session SBR server
		  • 1 for the 2nd spare binding SBR server, if equipped
		  • 1 for the 2nd spare session SBR server, if equipped
		Note: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.

6. ☐	Backout remaining C-level servers, as applicable	Back out the next set of servers. The following servers can be backed out in parallel (as applicable). • Active DA-MP for 1+1 (active/standby) configuration, or • ½ of all DA-MPs for N+0 (multi-active) configuration • Active SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs Execute 6.6, Backout Single Server for each C-level server identified above.
7. ☐	Backout the standby SOAM server	Backout the standby DSR SOAM server: • Execute Section 6.6 Backout Single Server.
8. ☐	Backout active SOAM server	Backout the active DSR SOAM server: • Execute Section 6.6 Backout Single Server.
9. ☐	Backout spare SOAM server (if applicable)	***Note***: The spare server is located at the mated site of the site being backed out. Backout the spare SOAM server: • Execute Section 6.6 Backout Single Server.

Procedure 43: Normal Site Backout

10. ☐	**Active SOAM VIP**: Enable site provisioning	Enable site provisioning. • Log into the SOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Site Provisioning**. • Click **OK** to confirm the operation. • Verify the button text changes to **Disable Site Provisioning**.

Note: If another site is to be backed out, follow all procedures in Table 23 in another maintenance window.

6.5.2 Normal NOAM Backout

The section backs out the NOAM servers.

Procedure 44: Normal NOAM Backout

S T E P #	This procedure performs a normal backout of the DSR application software from the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Backout standby DR NOAM server (if equipped)	Backout the standby DR NOAM server: • Execute Section 6.6 Backout Single Server.
2. ☐	Backout other DR NOAM server (if equipped)	Backout the other DR NOAM server (now the standby): • Execute Section 6.6 Backout Single Server.
3. ☐	Backout standby DSR NOAM server (as applicable)	Backout the standby DSR NOAM server: • Execute Section 6.6 Backout Single Server.
4. ☐	Backout active DSR NOAM server	Backout the active NOAM server: • Execute Section 6.6 Backout Single Server.
5. ☐	**Active NOAM VIP**: Enable Global Provisioning	Enable global provisioning and configuration updates on the entire network • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Database**. • Click **Enable Provisioning**. • Verify the button text changes to **Disable Provisioning**.

6.6 Backout Single Server

This section provides the procedures to backout the application software on a single server.

CAUTION

This procedure is executed as a component of the Emergency Backout Procedure (Section 6.4) or the Normal Backout Procedure (Section 6.5). This procedure should never be executed as a standalone procedure.

Procedure 45: Backout Single Server

S T E P #	This procedure backs out the upgrade of DSR 7.x application software. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Prepare the server for backout. For active NOAM on release 7.1 or later only	Perform the following steps to prepare the server for backout. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select the server group link containing the server to be backed out. Verify the Upgrade State is **Accept or Reject**. Make the server **Backout Ready** as follows: • Navigate to **Status & Manage -> HA**. • Click **Edit**. • Select the server to be backed out and choose a Max Allowed HA Role value of standby (unless it is a Query server, in which case the value should remain set to Observer). ***Note***: When the active NOAM is the server being backed out, clicking **OK** initiates an HA switchover and causes the GUI session to log out. • Click **OK**. ***** Critical *** Do NOT omit this step** • Log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. ***** Critical *** Do NOT omit this step** • The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. • Navigate to **Status & Manage -> Server**. • Select the server to be backed out and click **Stop**. Click **OK** to confirm the operation and verify the Appl State changes to **Disabled**. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select the link of the server group containing the server to be backed out.

Procedure 45: Backout Single Server

		Verify the Upgrade State is now Backout Ready. *Note*: It may take a couple of minutes for the status to update.

2. ☐	**Server CLI**: SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		Note: If direct access to the IMI is not available, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

3. ☐	**Server CLI**: Execute the backout	Execute following command to find the state of the server to be backed out..
		`$ ha.mystate`
		In the example output below, the HA state is standby.
		`[admusr@SO2 ~]# ha.mystate`
		resourceId role node subResources lastUpdate
		DbReplication Stby B2435.024 0 0127:113603.435
		VIP Stby B2435.024 0 0127:113603.438
		SbrBBaseRepl OOS B2435.024 0 0127:113601.918
		SbrBindingRes OOS B2435.024 0 0127:113601.918
		SbrSBaseRepl OOS B2435.024 0 0127:113601.918
		SbrSessionRes OOS B2435.024 0 0127:113601.918
		CacdProcessRes OOS B2435.024 0 0127:113601.918
		DA_MP_Leader OOS B2435.024 0 0127:113601.917
		DSR_SLDB OOS B2435.024 0-63 0127:113601.917
		VIP_DA_MP OOS B2435.024 0-63 0127:113601.917
		EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917
		DSR_Process OOS B2435.024 0-63 0127:113601.917
		CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272
		DSROAM_Proc OOS B2435.024 0 0128:081123.951
		If the server being backed out is on release 7.0.1, and the state of the server is active, then go back to step 1.
		`$ sudo /var/TKLC/backout/reject`
		Note: If backout prompts to continue, answer y.
		The reject command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.
		Sample output of the reject script:
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

Procedure 45: Backout Single Server

4. ☐	Backout proceeds	Many informational messages are output to the terminal screen as the backout proceeds. Finally, after backout is complete, the server automatically reboots.

5. ☐	**Server CLI**: SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

6. ☐	**Server CLI**: Restore the full DB run environment	• Execute the backout_restore utility to restore the full database run environment:
		`$ sudo /var/tmp/backout_restore`
		Note: If prompted to proceed, answer **y**.
		Note: In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory, resulting in the following error message:
		`/var/tmp/backout_restore: No such file or directory`
		If this message occurs, copy the file from **/usr/TKLC/appworks/sbin** to **/var/tmp** and repeat sub-step 1.
		The backout_restore command creates a no-hang-up shell session, so that the command continues to execute if the user session is lost.
		If the restore was successful, the following displays:
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		If an error is encountered and reported by the utility. It is recommended you consult with My Oracle Customer Support by referring to Appendix M of this document for further instructions.

7. ☐	**Server CLI**: Verify the backout	• Examine the output of the following commands to determine if any errors were reported:
		`$ sudo verifyUpgrade`
		Note: The verifyUpgrade command detects errors that occurred in the initial upgrade, as well as errors that occurred during the backout. Disregard the initial upgrade errors.
		Note: Disregard the following TKLCplat.sh error:
		`[root@NO1 ~]# verifyUpgrade`
		`ERROR: TKLCplat.sh is required by upgrade.sh!`
		`ERROR: Could not load shell library!`
		`ERROR: LIB: /var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh`
		`ERROR: RC: 1`
		The following command displays the current sw rev on the server:

Procedure 45: Backout Single Server

		`$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the server is on release 7.0.x or later, enter:
		`$ sudo verifyBackout`
		The verifyBackout command searches the upgrade log and reports all errors found.
		• If the backout was successful (no errors or failures reported), then proceed to step 8.
		• If the backout failed with the following error, this error can be ignored and the backout may continue.
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1485165801::ERROR: <rpm name>-7.2.14-7.2.0.0.0_72.23.0: Failure running`
		`command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'`
		• If the backout failed with the following error:
		`ERROR: The upgrade log does not exist!`
		Examine the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for errors that occurred during the backout.
		• If the backout failed due to errors found in the upgrade log, it is recommended you contact My Oracle Customer Support by referring to Appendix I of this document for further instructions.

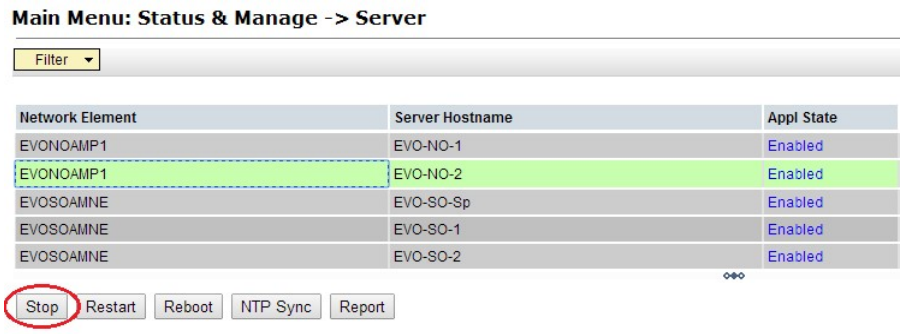
8. ☐	**Server CLI**: Reboot the server	Enter the following command to reboot the server: `$ sudo init 6` This step can take several minutes.

Procedure 45: Backout Single Server

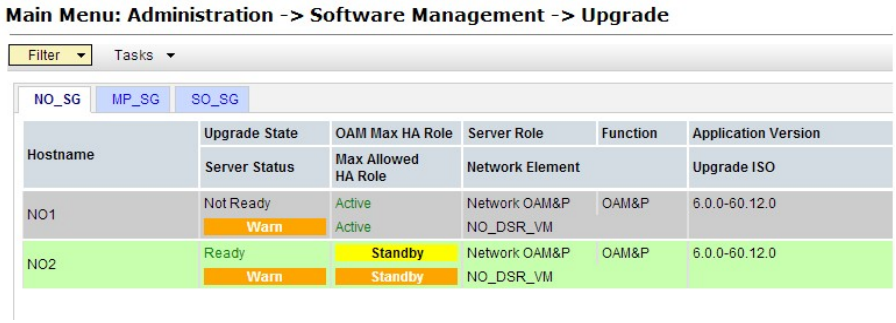
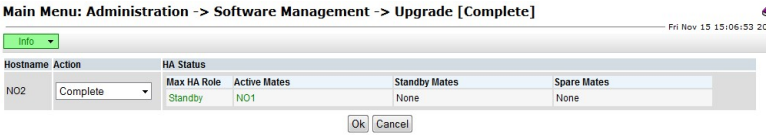
9. ☐	**Server CLI**: Verify services restart
	(NOAM/SOAM only)
		If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 9.
		Verify OAM services have restarted.
		• Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		• SSH to the server and log in.
		`login as: admusr`
		`password: <enter password>`
		• Execute the following command to verify the httpd service is running:
		`$ sudo service httpd status`
		• The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		`httpd <process IDs will be listed here> is running...`
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document for further instructions.

10. ☐	**Active NOAM VIP**: Verify server states	Verify server state. • Navigate to **Administration -> Software Management -> Upgrade** to observe the server upgrade status. • Select the SOAM tab of the site being backed out. • Select the link of the server group containing the server being backed out. If the active NOAM is on release 7.1.x and later: • If the server status is **Not Ready**, proceed to step 11; otherwise proceed to step 14. If the active NOAM is on release 6.0 or 7.0.x: • If the server status is **Ready**, proceed to step 12; otherwise proceed to step 14.

Procedure 45: Backout Single Server

11. ☐	**Active NOAM VIP**: Correct Upgrade State on backed out server For active NOAM on release 7.1.x or later	Modify the backed out server to transition the Upgrade State to **Ready**. • Navigate to **Status & Manage -> HA**. • Click **Edit**. • Select the backed out server 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**. • The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. • Navigate to **Status & Manage -> Server**. • Select the server being backed out and click Restart. Click Ok to confirm the operation. Verify the Appl State updates to Enabled. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the tab of the server group containing the server that was backed out. Verify the Upgrade State is now Ready. ***Note***: It may take a couple of minutes for the status to update. Proceed to step 13 to complete this procedure.
12. ☐	**Active NOAM VIP**: Remove Upgrade Ready status For active NOAM on release 7.0.1 only	Remove Upgrade Ready status. • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Server**. • If the server just backed-out shows an Appl State of **Enabled**, then select the server row and click **Stop**. 

Procedure 45: Backout Single Server

13. ☐	**Active NOAM VIP**: Correct Upgrade State on backed out server For active NOAM on release 7.0.1 only	Change the upgrade state for the backed out server. • Navigate to **Administration -> Software Management -> Upgrade**. • If the server just backed-out shows an Upgrade State of **Ready** or **Success**, then select the backed-out server and click **Complete**. Otherwise, skip to step 13.  • The Upgrade [Complete] screen displays. Leave the Action set to hte default value of **Complete**. • Click **OK**. This updates the Max Allowed HA Role of the backed-out server to active, which causes the server's Upgrade State to move to **Not Ready**.  The following SOAP error may display in 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.
14. ☐	**Active NOAM VIP**: Verify application version	Verify the application version is correct for the backed out server. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being backed out. • Select the Server Group tab for the server that was backed out. • Verify the **Application Version** for this server has been downgraded to the original release version.
15. ☐	Procedure Complete	The single server backout is now complete. Return to the overall DSR backout procedure step that directed the execution of this procedure.

6.7 Backout Multiple Servers

This section provides the procedures to backout the application software on multiple servers.

This procedure is executed as a component of the Emergency Backout Procedure (Section 6.4) or the Normal Backout Procedure (Section 6.5). This procedure should never be executed as a standalone procedure.

Procedure 46: Backout Multiple Servers

S T E P #	This procedure backs out the upgrade of DSR 8.0 application software for multiple servers. Any server requiring backout can be included: DA-MPs, SS7-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Prepare the server for backout. For active NOAM on release 7.1.1 and later	If the active NOAM is on release 7.1.1 and later, perform this step; otherwise, proceed to step 2. Perform the following steps to prepare the server for backout. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the server group tab containing the server to be backed out. Verify the Upgrade State is **Accept or Reject**. Make the server **Backout Ready** as follows: • Navigate to **Status & Manage -> HA**. • Click **Edit**. • Select the server to be backed out and choose a Max Allowed HA Role value of standby (unless it is a Query server, in which case the value should remain set to Observer). Note: When the active NOAM is the server being upgraded, clicking **OK** initiates an HA switchover causing the GUI session to log out. Before logging into the active OAM again, close and re-open the browser using the VIP address for the NOAM, and clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. • Click **OK**. • The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. • Navigate to **Status & Manage -> Server**. • Select the server to be backed out and click **Stop**. Click **OK** to confirm the operation, then verify the Appl State updates to Disabled. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now Backout Ready. ***Note***: It may take a couple of minutes for the status to update.

Procedure 46: Backout Multiple Servers

2. ☐	Server CLI:
	Log into the server(s)
		Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		Note: If direct access to the IMI is not available, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

3. ☐	**Server CLI**:
	Execute the backout
		Determine the state of the server to be backed out. The server role must be either **Standby** or **Spare**. Execute following command to find the state.
		`$ ha.mystate`
		In the example output below, the HA state is standby.
		`[admusr@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		If the state of the server is active, then return to step 1 above.
		`$ sudo /var/TKLC/backout/reject`
		Note: If backout prompts to continue, answer **y**.
		The reject command creates a no-hang-up shell session, so that the command continues to execute if the user session is lost.
		Sample output of the reject script:
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

Procedure 46: Backout Multiple Servers

4. ☐	**Server CLI**: Backout proceeds	Many informational messages are output to the terminal screen as the backout proceeds. Finally, after backout is complete, the server automatically reboots.
5. ☐	Repeat for each server to be backed out.	Repeat steps 1 through 4 for each server to be backed out.

6. ☐	Log into the server	Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

7. ☐	**Server CLI**: Restore the full DB run environment	• Execute the backout_restore utility to restore the full database run environment:
		`$ sudo /var/tmp/backout_restore`
		Note: If prompted to proceed, answer **y**.
		Note: In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory resulting in the following error message:
		`/var/tmp/backout_restore: No such file or directory`
		If this message occurs, copy the file from **/usr/TKLC/appworks/sbin** to **/var/tmp** and repeat sub-step 1.
		The backout_restore command creates a no-hang-up shell session, so that the command continues to execute if the user session is lost.
		If the restore was successful, the following displays:
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		If an error is encountered and reported by the utility, It is recommended you consult with My Oracle Customer Support by referring to Appendix M of this document for further instructions.

8. ☐	**Server CLI**: Verify the backout	• Examine the output of the following commands to determine if any errors were reported:
		`$ sudo verifyUpgrade`
		Note: The verifyUpgrade command detects errors that occurred in the initial upgrade, as well as errors that occurred during the backout. Disregard the initial upgrade errors.
		Note: Disregard the following TKLCplat.sh error:
		`[root@NO1 ~]# verifyUpgrade`
		`ERROR: TKLCplat.sh is required by upgrade.sh!`
		`ERROR: Could not load shell library!`
		`ERROR: LIB:`

Procedure 46: Backout Multiple Servers

		/var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh
		ERROR: RC: 1
		The following command displays the current sw rev on the server:
		$ appRev
		Install Time: Wed Feb 25 02:52:47 2015
		Product Name: DSR
		Product Release: 7.1.0.0.0_71.10.0
		Base Distro Product: TPD
		Base Distro Release: 7.0.0.0.0_86.14.0
		Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso
		ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso
		OS: OracleLinux 6.5
		If the server is on release 7.0.x or later, enter:
		$ sudo verifyBackout
		The verifyBackout command searches the upgrade log and reports all errors found.
		• If the backout was successful (no errors or failures reported), then proceed to step 9.
		• If the backout failed with the following error, this error can be ignored and the backout may continue.
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!
		ERROR: 1485165801::ERROR: <rpm name>-7.2.14-7.2.0.0.0_72.23.0: Failure running
		command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'
		• If the backout failed with the following error:
		ERROR: The upgrade log does not exist!
		Examine the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for errors that occurred during the backout.
		• If the backout failed due to errors found in the upgrade log, it is recommended you contact My Oracle Customer Support by referring to Appendix M of this document for further instructions.

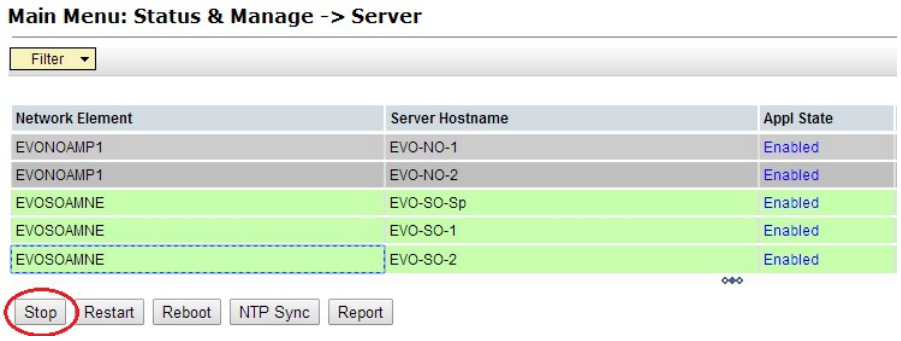
9. ☐	**Server CLI**: Reboot the server	Enter the following command to reboot the server: $ sudo init 6 This step can take several minutes.

Procedure 46: Backout Multiple Servers

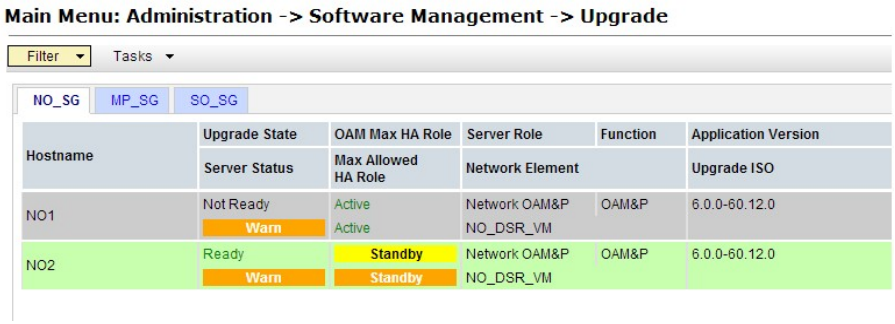
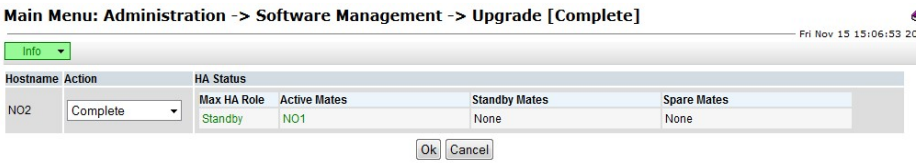
10. ☐	**Server CLI**: Verify services restart
	(NOAM/SOAM only)
		If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 11.
		Verify OAM services have restarted:
		• Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		• SSH to the server and log in.
		`login as: admusr`
		`password: <enter password>`
		• Execute the following command to verify the httpd service is running.
		$ sudo service httpd status
		• The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		`httpd <process IDs will be listed here> is running...`
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document for further instructions.

11. ☐	Repeat for each server backed out	**Repeat** steps 6 through 10 for each server backed out.
12. ☐	**Active NOAM VIP**: Verify server states	Verify server state is correct after the backout. • Navigate to **Administration -> Software Management -> Upgrade** to observe the server upgrade status. If the active NOAM is on release 7.1.1 or later: • If the server status is **Not Ready**, proceed to step 13; otherwise proceed to step 16. If the active NOAM is on release 7.0.1: • If the server status is **Ready**, proceed to step 14; otherwise proceed to step 16.

Procedure 46: Backout Multiple Servers

13 ☐	**Active NOAM VIP**: Correct Upgrade State on backed out server	Modify the backed out server to transition the Upgrade State to Ready. • Navigate to **Status & Manage -> HA**. • Click **Edit**. • Select the backed out server 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**. • The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. • Navigate to **Status & Manage -> Server**. • Select the server being backed out and click Restart. Click Ok to confirm the operation. Verify the Appl State updates to Enabled. • Navigate to **Administration -> Software Management -> Upgrade**; • Select the tab of the server group containing the server that was backed out. Verify the Upgrade State is now Ready ***Note***: It may take a couple of minutes for the status to update.) Proceed to step 16 to complete the procedure.
14. ☐	**Active NOAM VIP**: Remove Upgrade Ready status	Remove Upgrade Ready status. • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Server**. • If the servers just backed-out show an Appl State of **Enabled**, then multi-select the server rows and click **Stop**. • Click **OK** on the confirmation screen. 

Procedure 46: Backout Multiple Servers

15. ☐	**Active NOAM VIP**: Correct upgrade state on backed out server	Correct the upgrade status on the backed out server. • Navigate to **Administration -> Software Management -> Upgrade**. • If the servers just backed-out show an Upgrade State of **Ready** or **Success**, then select the backed-out server and click **Complete**. • If the servers just backed out show an Upgrade State of **Not Ready**, then proceed to step 16.  • The Upgrade [Complete] screen displays. Leave the Action set to hte default value of Complete. • Click **OK**. This updates the Max Allowed HA Role of the backed-out server to active, which causes the server's Upgrade State to move to **Not Ready**.  The following SOAP error may displays in 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.
16. ☐	**Active NOAM VIP**: Verify application version	Verify the application version of the backed out server. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the Server Group tab for the server that was backed out. • Verify the **Application Version** for this server has been downgraded to the original release version.
17. ☐	Procedure complete	The multiple server backout procedure is now complete. Return to the overall DSR backout procedure step that directed the execution of this procedure.

6.8 Post-Backout Health Check

This procedure determines the health and status of the DSR network and servers following the backout of the entire system.

Procedure 47: Post-Backout Health Check

S T E P #	This procedure performs a basic health check of the DSR to verify the health of the system following a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Verify server status is normal	Verify Server Status is Normal. • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Server**. • Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB), and Processes (Proc). • Do not proceed with the upgrade if any server status is not Norm. • Do not proceed with the upgrade if there are any Major or Critical alarms. ***Note***: It is recommended to troubleshoot if any server status is not Norm. A backout should return the servers to their pre-upgrade status.
2. ☐	**Active NOAM VIP**: Log all current alarms	Log all current alarms in the system: • Navigate to **Alarms & Events -> View Active**. • Click **Report** to generate an Alarms report. • Save the report and print the report. Keep these copies for future reference.

6.9 IDIH Backout

The procedures in this section back out the Oracle, Application, and Mediation servers to the previous release.

6.9.1 Oracle Server Backout

This procedure backs out the Oracle server.

This procedure is required only if backing out to IDIH release 7.0 or earlier. Do not back out the Oracle server if backing out to Release 7.1 or later.

Procedure 48: Oracle Server Backout

S T E P #		
	This procedure performs a backout of the Oracle server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Oracle Server CLI**: Log into the server	Use an SSH client to connect to the Oracle server (e.g., ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

2. ☐	**Oracle Server CLI**: Backout the server	Execute the following commands to back out the server.
		`sudo /opt/xIH/plat/bin/db_rollback.sh MED`
		`sudo /opt/xiH/plat/bin/db_rollback.sh APP`

6.9.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [6] Cloud DSR 8.0 Disaster Recovery Guide, E76332, Oracle.

Appendix A. Post Upgrade Procedures

The procedures in this section are executed only **AFTER** the upgrade of **ALL** servers in the topology is completed.

Appendix A.1 Accept Upgrade

Detailed steps for accepting the upgrade are shown in the procedure below. TPD requires that upgrades be accepted or rejected before any subsequent upgrades may be performed. Alarm 32532 (Server Upgrade Pending Accept/Reject) displays for each server until one of these two actions is performed.

An upgrade should be accepted only after it is determined to be successful as the Accept is final. This frees up file storage but prevents a backout from the previous upgrade.

Note: Once the upgrade is accepted for a server, that server is not allowed to back out to a previous release.

Note: This procedure must be performed in a Maintenance Window.

!! WARNING!!

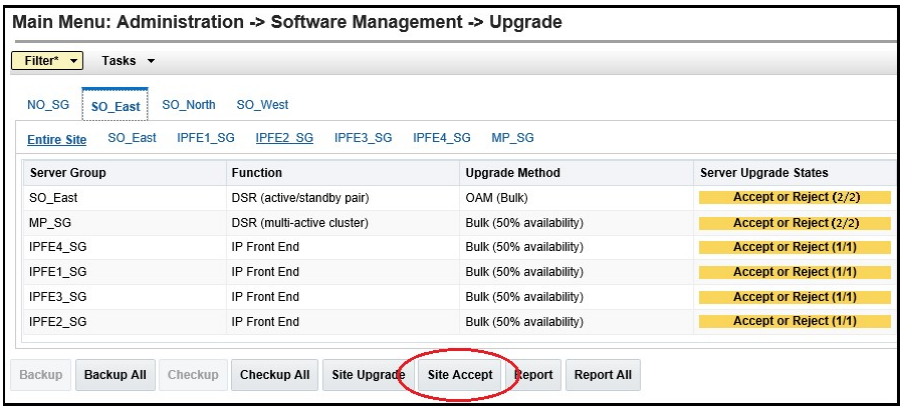
UPGRADE ACCEPTANCE MAY ONLY BE EXECUTED WITH AUTHORIZATION FROM THE CUSTOMER.

THE USER SHOULD BE AWARE THAT ONCE UPGRADE HAS BEEN ACCEPTED, IT IS NOT POSSIBLE TO BACK OUT TO THE PREVIOUS RELEASE.

Procedure 49: Accept Upgrade

S T E P #	This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	It is recommended that this procedure be performed two weeks after the upgrade	Verify the upgraded system has been stable for two weeks or more. ***Note***: It is not possible to back out after this is procedure is executed.
2. ☐	**Active NOAM VIP**: Execute this Step if accepting a NOAM server. Log all current alarms present at the NOAM.	Log all alarms before accepting the NOAM upgrade. • Log into the NOAM GUI. • Navigate to **Alarms & Events -> View Active**. • Click **Report** to generate an Alarms report. • Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: `Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
3. ☐	**Active SOAM VIP**: Execute this Step if accepting a SOAM server. Log all current alarms present at the SOAM.	Log all alarms before accepting the SOAM upgrade. • Log into the SOAM GUI. • Navigate to **Alarms & Events -> View Active**. • Click **Report** to generate an Alarms report. • Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: `Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`

Procedure 49: Accept Upgrade

4. ☐	**Active NOAM VIP**: Accept upgrade for multiple servers	Accept the upgrade of multiple servers. • Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the SOAM tab of the site being upgraded. ***Note***: **Site Accept** accepts the upgrade for every upgraded server at the selected site. This is the most efficient way to accept an upgrade. A manual alternative to this is to select the link of each server group in the site and click **Accept** to accept the upgrade of only the servers in the selected server group. • Click Site Accept.  A confirmation screen warns that once accepted, the server is not able to revert back to the previous image state. • Click **OK**. The Upgrade Administration screen re-displays. • Navigate to Alarms & Events -> View Active. As upgrade is accepted on each server, the corresponding Alarm ID – **32532 (Server Upgrade Pending Accept/Reject)** should automatically clear and server status transitions to **Backup Needed**.

Appendix A.2 Undeploy ISO

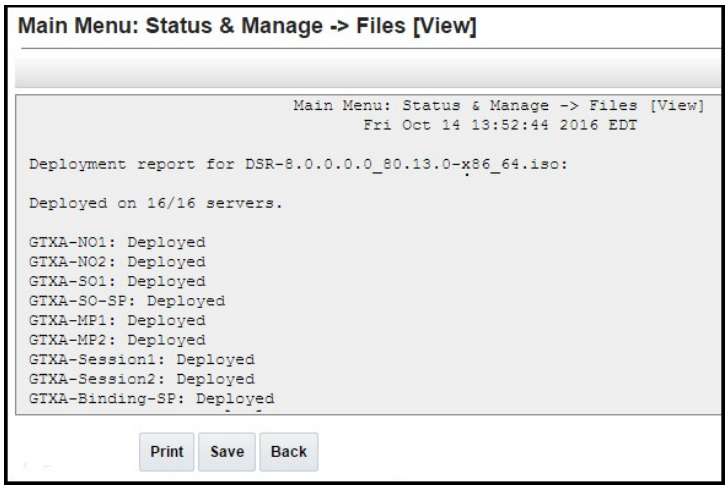
This procedure is run after the upgrade has been Accepted to undeploy all deployed ISOs. When an ISO is undeployed, the ISO is deleted from all servers in the topology except for the active NOAM. On the active NOAM, the ISO remains in the File Management Area.

This procedure can be run at anytime after the upgrade has been accepted.

Procedure 50: Undeploy ISO

S T E P #	This procedure undeploys an ISO from the DSR servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: View files	View the files in the File Management Area on the active NOAM. • Log into the NOAM GUI using the VIP. • Navigate to **Status & Manage -> Files**.
2. ☐	**Active NOAM VIP**: Start ISO undeploy	Start the ISO undeploy sequence. • Select an ISO that is stored in the isos directory of the File Management Area. The ISO filename has the format: `isos/DSR-8.0.0.0.0_80.12.0-x86_64.iso` • Click **Undeploy ISO**. • Click **OK** on the confirmation screen to start the undeploy sequence and refresh the screen.

Procedure 50: Undeploy ISO

3. ☐	**Active NOAM VIP**: Monitor progress	Monitor the ISO undeploy progress. • Select the ISO being deployed in step 2. • Click **View ISO Deployment Report**. • If some servers show the ISO as **Deployed**, click **Back** on the Files [View] page. • Periodically repeat sub-steps 1 through 3 until all servers indicate **Not Deployed**. 
4. ☐	**Active NOAM VIP**: Repeat as necessary	If there are additional ISOs in the File Management Area that need to be undeployed, repeat steps 2 and 3 as necessary.

Appendix A.3 PCA Post Upgrade Procedures

The procedures in this section are executed after the upgrade has been accepted.

Procedure 51: PCA Post Upgrade Procedure

S T E P #	This procedure performs miscellaneous actions that are required to be executed after the upgrade is accepted. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM CLI**: Reset COMCOL compatibility flag	This step is required only if the source release is pre-8.0.
		• Use an SSH client to connect to the active NOAM:
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the following command to reset the COMCOL backward compatibility flag. Backward compatibility is no longer required when all of the servers in the topology have been upgraded to release 8.0 or later.
		`$ iset -fvalue=0 LongParam where "name='cm.cm6compat'"`
		Sample output:
		`=== changed 1 records ===`
		• Verify the changed value:
		`$ iqt -zp -fvalue LongParam where "name='cm.cm6compat'"`
		`value`
		`0`

Appendix A.4 PCA Post Upgrade Procedure

CAUTION **THIS PROCEDURE IS FOR PCA SYSTEMS ONLY!**

Procedure 52 must be executed on PCA systems after the upgrade to DSR 8.0 is Accepted. Do not run this procedure until **after** Procedure 49 has been completed. This procedure executes the PCA top level activation script to remedy a potential PCA activation issue from earlier releases.

Procedure 52: PCA Post Upgrade Procedure

S T E P #	This procedure executes the PCA top level activation script. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM CLI**: Log into the active NOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM: `ssh admusr@<NOAM_VIP>`

2. ☐	**Active NOAM CLI**: Run PCA activation script	Execute the top level PCA script:
		`/usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivationTopLevel`
		At the completion of the activation script, the following message is output:
		`Execution of PCA Activation Script complete.`

3. ☐	**Active NOAM CLI**: Clear cache	Execute the following command to reset the initialization caches: `clearCache`

Appendix B. Increase Maximum Number of Open Files

This procedure increases the maximum number of files that can be opened for reading and writing. As the number of servers in the topology grows, so does the need for additional files to handle merging data to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files.

Note: Following procedure is for one NOAM server. Repeat this procedure for other NOAM servers.

Procedure 53: Increase Max Number of Open Files

S T E P #	This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM CLI**: Currently open file count	Determine the number of files currently open.
		• Use an SSH client to connect to the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• Enter the following command to retrieve the pid of idbsvc. The pid is highlighted in blue in the sample output below:
		`$ ps -ef | grep -i idbsvc`
		`root 4369 idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2`
		• The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 2 above in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1278`
		Record the number of files currently open (the output of sub-step 3):
		_____
		• Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below:
		`$ ps -ef | grep -i tpdProvd`
		`tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd`
		• The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 4 above in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1280`
		Record the number of files currently open (the output of sub-step 5):
		_____

Procedure 53: Increase Max Number of Open Files

2. ☐	**Active NOAM CLI**: Max number of open files	Display the maximum number of open files for idbsvc.
		• Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  32768  32768  files`
		The output of the cat command displays the maximum number of files that can be open by the idbsvc process.
		Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____
		This system has over 1024 open files but its current ulimit for idbsvc is high enough during normal operation that the amount of open files does not pose a problem. But when attempt an upgrade another process (tpdProvd) updates idbsvc max # of open files to 1024, therefore causing the upgrade to fail.
		Display the maximum number of open files for tpdProvd.
		• Use the highlighted value from step 1, sub-step 4 for tpdProvd in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  1024  4096  files`
		The output of the cat command displays the maximum number of files that can be open by the tpdProvd process.
		Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____

3. ☐	Check if current number of open files (used by idbsvc) is in safe limit 	If the number of currently open files (step 1, sub-step 3) of idbsvc is less than the maximum allowed (step 2, sub-step 2 Soft Limit for tpdProvd), this procedure is complete, i.e., number of currently open files (used by idbsvc) is less than 1024. Then further steps are not required to be executed on this NOAM Server. If the number of currently open files are more than the (step 2, sub-step 2 Soft Limit for tpdProvd), i.e., 1024, go to Step 4 below. Repeat this procedure and below steps (if required) for other NOAM Server.
4. ☐	Check if max number of open files for tpdProvd is already set 	If the maximum number of open files value (step 2, sub-step 2 – Soft Limit) for tpdProvd is already set to 32768, this procedure is complete. Then further steps are not required to be executed on this NOAM Server. If maximum value is not already set, then go to Step 5 below. Repeat this procedure and below steps (if required) for other NOAM Server.

Procedure 53: Increase Max Number of Open Files

5. ☐	**Active NOAM CLI**: Increase max number of open files	Increase max number of open files.
		• Using a text editor with sudo, edit the **/etc/init/tpdProvd.conf** file to add the following two lines:
		`# increase open file limit`
		`limit nofile 32768 32768`
		Just before the comment line in the **/etc/init/tpdProvd.conf** file that reads **Start the daemon**.
		Insight of file as example:
		`#`
		`# restart tpdProvd up to 10 times within a 100 second period.`
		`# If tpdProvd fails to start 10 times within a 100 second period then`
		`# it most likely has a deeper problem that restarting will not overcome.`
		`respawn limit 10 100`
		`# increase open file limit`
		`limit nofile 32768 32768`
		`#`
		`# Start the daemon`
		`script`
		• Save the file and close the editor.
		Caution: Don't edit any other line in this file. You can take a backup of the file if required.

6. ☐	**Active NOAM CLI**: Restart service	Restart tpdProvd process
		• Enter the following command to stop tpdProvd:
		`$ sudo initctl stop tpdProvd`
		• Enter the following command to restart tpdProvd
		`$ sudo initctl start tpdProvd`
		Sample output:
		`tpdProvd start/running, process 186743`

7. ☐	**Active NOAM CLI**: Recheck open file max limit	Check the max file limit is set for tpdProvd.
		• Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below:
		`$ ps -ef | grep -i tpdProvd`
		`tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd`
		• Use the highlighted value from sub-step 1 just above in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files 32768 32768 files`
		• Verify the output of sub-step 2 indicates that the max number of open files is 32768. If the value is NOT 32768, it is recommended you contact My Oracle Customer Support per Appendix M.

Appendix C. PCRF Pooling Migration Check

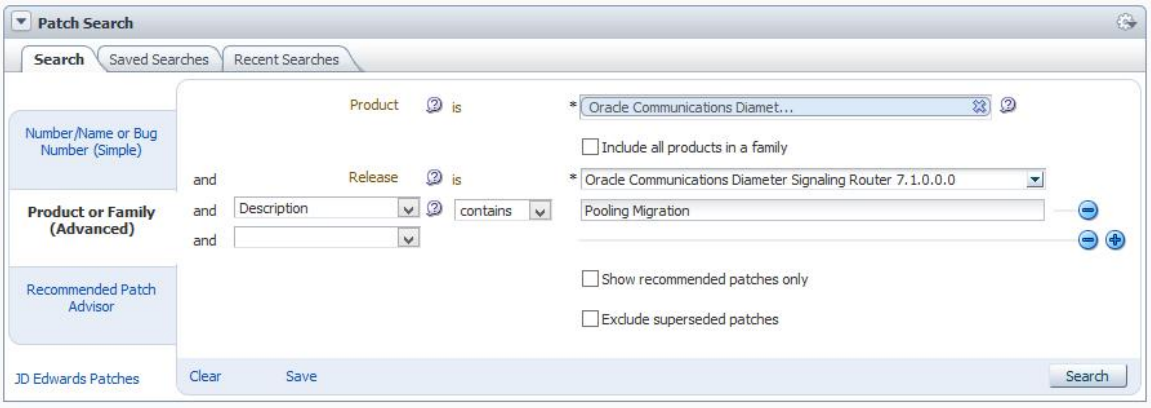
If the PCA application has been activated and the PDRA feature has been enabled, a check of the PCRF pooling migration is **REQUIRED** before the start of a major upgrade to DSR 8.0.

The PCRF pooling migration check is NOT required for a DSR 8.0 incremental upgrade.

Follow the steps in Procedure 54 to execute the PCRF Pooling Migration Check.

Note: If the PCRF pooling migration is NOT complete, this check must be repeated until PCRF Pooling Migration Tool indicates that the migration is complete.

Procedure 54: PCRF Pooling Migration Check

S T E P #		
	This procedure checks the PCRF pooling migration status to determine if the migration is complete. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Download PCRF pooling migration tool	Download the PCRF Pooling Migration Tool from MOS. The tool determines the status of the PCRF pooling migration. • Navigate to the MOS site at **https://support.oracle.com/** and sign in. • Select the Patches & Updates tab. • In the Patch Search screen, select the Product or Family (Advanced) tab on left. • Use the following search criteria to locate and download the migration tool (as shown in the figure below): **Product**: Oracle Communications Diameter Signaling Router (DSR) **Release**: Oracle Communications Diameter Signaling Router (DSR) 7.1.0.0.0 ***Note***: The 7.1 Migration Tool is also valid for DSR 8.0. **Description**: Pooling Migration 
2. ☐	Copy the PCRF pooling migration tool	Copy the PCRF Pooling Migration Tool to the active NOAM. `scp -p <patchfilename> admusr@<active_NOAM>`

Procedure 54: PCRF Pooling Migration Check

3. ☐	SSH to the active NOAM	Using a SSH tool, log into the active NOAM server. `ssh admusr@<NOAM_VIP>`
4. ☐	**Active NOAM CLI**: Move the patch file	Move the patch file to the working directory: `sudo mv <patchfilename> /usr/TKLC/dsr/tools`
5. ☐	**Active NOAM CLI**: Change directory to the PCA tool directory	Change directories using the following command: `cd /usr/TKLC/dsr/tools/`
6. ☐	**Active NOAM CLI**: Unzip the patch	Unzip the PCRF Pooling Migration Tool using the **unzip** command. Example: `sudo unzip <patchfilename>`

7. ☐	**Active NOAM CLI**: Check the PCRF pooling migration status	Check the PCRF Pooling Migration Status using the following command:
		`./verifyPCRFPoolingMigration.sh --checkPCRFPoolingMigrationStatus`
		Sample output:
		`Preparing log directory ...`
		`Creating log directory...`
		`Logging is started in /var/TKLC/log/migrationStatusToolLogs/migrationStatusTool.log`
		`Preparation of log directory done.`
		`============ Execution of PCRF Pooling Migration Verification Tool Started ===============`
		`Checking host server status whether it is active NOAMP server or not.`
		`This server is active NOAMP server.`
		`Application Release is 7.0.1.0.0`
		`PDRA/PCA application is activated on this system.`
		`'PCRFPooling' feature is enabled on this system.`
		`PCRF Pooling Migration is not required. No need to check PCRF pool migration status. Exiting ...`
		`PCRF Pooling Migration is completed or not required on all servers.`
		`Execute tool again with option --verifyUpgradeAllowed to check if upgrade is allowed or not.`
		`============ Execution of PCRF Pooling Migration Verification Tool Completed =============`

Procedure 54: PCRF Pooling Migration Check

8. ☐	**Active NOAM CLI**: Verify PCRF pooling migration is complete	After executing the PCRF Pooling Migration tool, determine if the PCRF pooling migration has completed using the following command:
		`./verifyPCRFPoolingMigration.sh --verifyUpgradeAllowed`
		Note: This command informs the user if the PCRF Pooling Migration has completed.
		If PCRF pooling migration is complete, the command displays the following:
		`Upgrade is allowed.`
		If PCRF pooling migration is **NOT** complete, the command displays the following:
		`Upgrade is not allowed.`

9. ☐	**Active NOAM CLI**: Estimate PCRF pooling migration completion (Optional)	If the PCRF pooling migration is not complete, the user may get an estimate of when the PCRF pooling migration will be complete.
		Execute the PCRF Pooling Migration Completion Estimate tool using the following command:
		`./verifyPCRFPoolingMigration.sh --estimateMigrationCompletionTime`
		Note: Once complete, this command displays the estimated PCRF pooling migration in days, hours, minutes, and seconds.
		Example:
		`Estimated total time for migration completion for all binding servers is: 3 days 4 hours 45 minutes 34 seconds.`

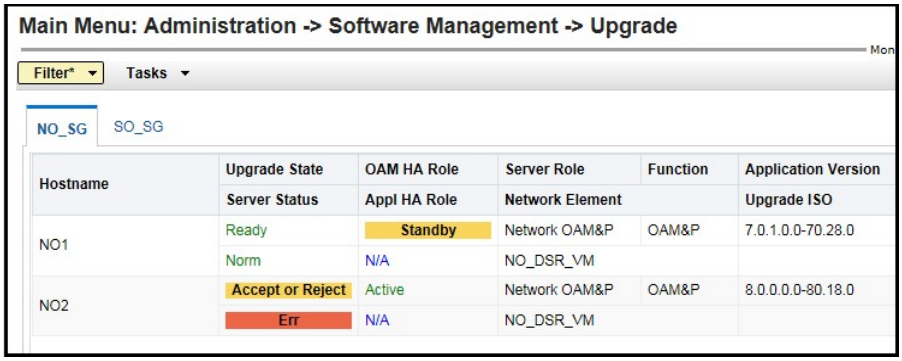
Appendix D. Upgrade Single Server – DSR 8.x

This appendix provides the procedure for upgrading a single DSR server of any type (NOAM, SOAM, MP, etc.) when the active NOAM is on DSR 8.x.

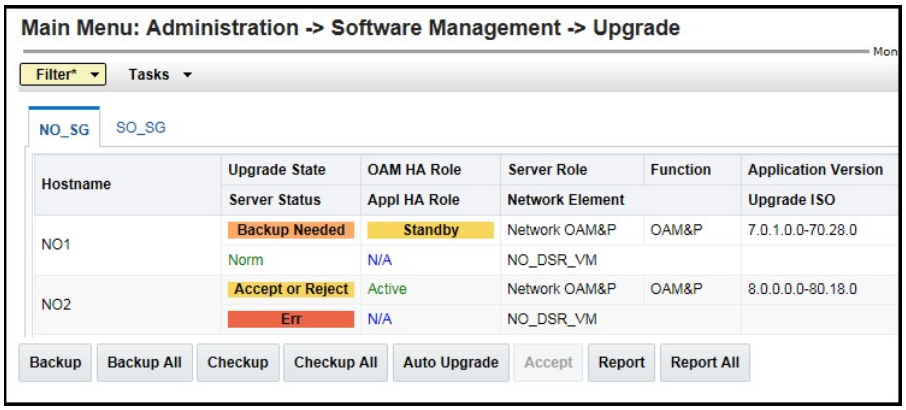
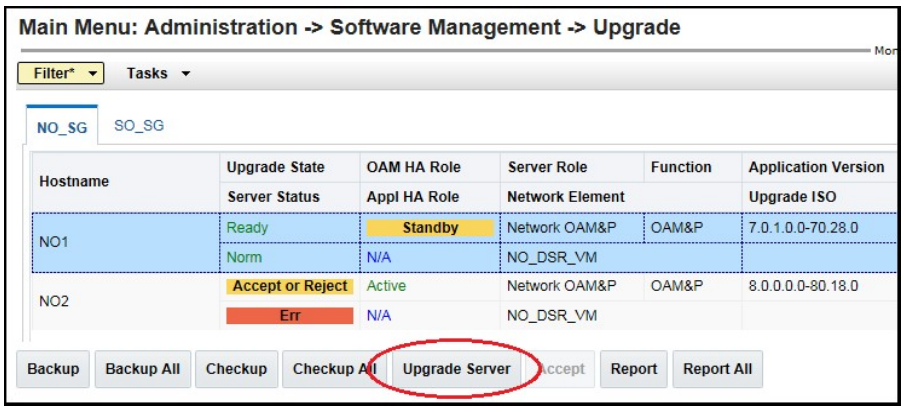
Note that this procedure may be executed multiple times during the overall upgrade, depending on the number of servers in the DSR and the chosen upgrade methodology. Make multiple copies of Appendix D to mark up, or keep another form of written record of the steps performed.

Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x

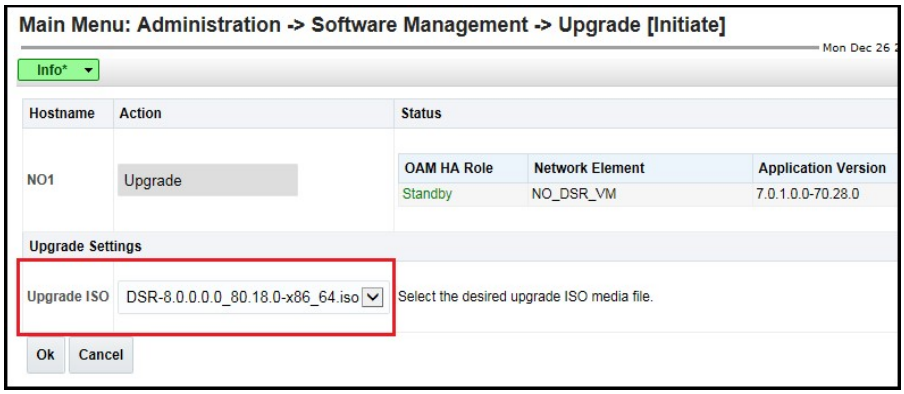
S T E P #		
	This procedure executes the Upgrade Single Server – Upgrade Administration steps for an active NOAM on Release 8.0. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM VIP**: View the pre-upgrade status of Servers	View the pre-upgrade status.
		• Log into the NOAM GUI using the VIP.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		• Select the **Network Element** of the server to be upgraded (NOAM or site).
		 
		Main Menu: Administration -> Software Management -> Upgrade
		Filter* Tasks
		NO_SG SO_SG
		Hostname / Server Status / Upgrade State / Appl HA Role / OAM HA Role / Network Element / Server Role / Function / Upgrade ISO / Application Version
		NO1: Ready / Norm / Standby / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 7.0.1.0.0-70.28.0
		NO2: Accept or Reject / Err / Active / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 8.0.0.0.0-80.18.0
		The active NOAM server may have some or all of the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`

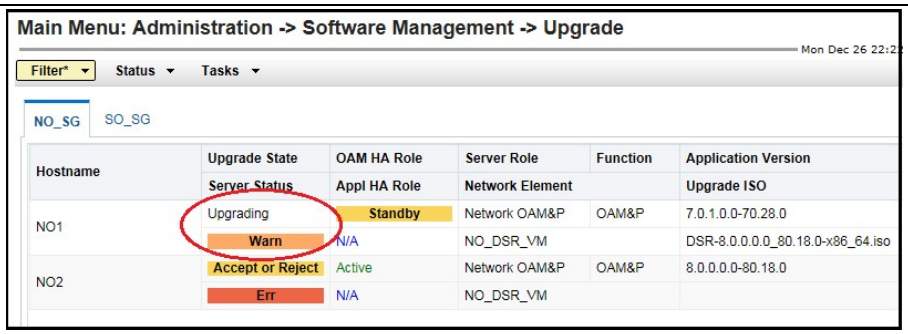
Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x

2. ☐	**Active NOAM VIP**: Verify status of Server to be upgraded	For the server to be upgraded: • Identify the server to be upgraded (NOAM, SOAM, MP, etc.) _____(record hostname) • Verify the **Application Version** is the expected software release version. • If the server is in the **Backup Needed** state, select the server and click **Backup**. On the Upgrade [Backup] screen, click **OK**. The Upgrade State changes to **Backup in Progress**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_SG Hostname / Server Status / Upgrade State / Appl HA Role / OAM HA Role / Network Element / Server Role / Function / Application Version / Upgrade ISO NO1: Backup Needed / Norm / Standby / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 7.0.1.0.0-70.28.0 NO2: Accept or Reject / Err / Active / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 8.0.0.0.0-80.18.0 Backup Backup All Checkup Checkup All Auto Upgrade Accept Report Report All When the backup is complete, verify the server state changes to **Ready**.
3. ☐	**Active NOAM VIP**: Initiate upgrade	Initiate the server upgrade. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_SG Hostname / Server Status / Upgrade State / Appl HA Role / OAM HA Role / Network Element / Server Role / Function / Application Version / Upgrade ISO NO1: Ready / Norm / Standby / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 7.0.1.0.0-70.28.0 NO2: Accept or Reject / Err / Active / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 8.0.0.0.0-80.18.0 Backup Backup All Checkup Checkup All Upgrade Server Accept Report Report All

Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x

4. ☐	**Active NOAM VIP**: Select upgrade ISO	Initiate the server upgrade. • In the Upgrade Settings – **Upgrade ISO** list, select the ISO to use in the server upgrade, ***Note***: When the active NOAM is the server being upgraded, selecting **OK** initiates an HA switchover and causes the GUI session to log out. ***Note***: If the selected server is the active server in an active/standby pair, the OAM Max HA Role column displays **Active** with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the Make Ready action causes an HA switchover. • Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.  ***** Critical *** Do NOT omit this step** • Log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. ***** Critical *** Do NOT omit this step**
5. ☐	**Active NOAM VIP**: View in-progress status	View the Upgrade Administration form to monitor upgrade progress. See step 6 for an optional method of monitoring upgrade progress. See step 7 below for instructions if the Upgrade fails. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. • The upgrade status of the site can be observed on the Upgrade Administration screen by selecting the **Entire Site** link. An upgrade status summary of each server group in the site displays in the Server Upgrade States column.

Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x



Servers may have a combination of the following expected alarms.

Note: Not all servers have all alarms:

```
Alarm ID = 10008 (Provisioning Manually Disabled)

Alarm ID = 10075 (The server is no longer providing
services because application processes have been
manually stopped)

Alarm ID = 10073 (Server Group Max Allowed HA Role
Warning)

Alarm ID = 32515 (Server HA Failover Inhibited)

Alarm ID = 31228 (HA Highly available server failed to
receive mate heartbeats) or (Lost Communication with
Mate Server)

Alarm ID = 31283 (Highly available server failed to
receive mate heartbeats)

Alarm ID = 31106 (DB Merge To Parent Failure)

Alarm ID = 31107 (DB Merge From Child Failure)

Alarm ID = 31233 (HA Secondary Path Down)

Alarm ID = 31101 (DB Replication To Slave Failure)

Alarm ID = 31104 (DB Replication over SOAP has failed
```

- Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes.

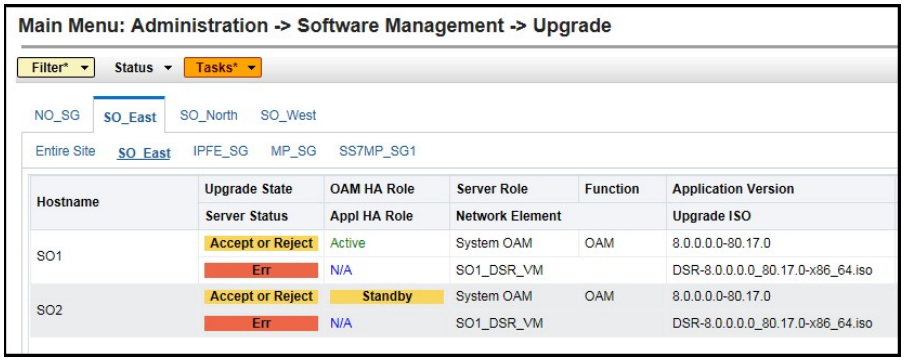
If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x

6. ☐	**Server CLI**: View In-Progress Status from command line of server (Optional)	An optional method to view upgrade progress from the command line:
		To view the detailed progress of the upgrade, access the server command line (via ssh or console), and type:
		`$ tail -f /var/TKLC/log/upgrade/upgrade.log`
		This command displays the upgrade log entries as the events occur. Once the upgrade is complete, the server reboots. It takes a couple of minutes for the DSR application processes to start.
		This command displays the current rev on the server:
		`[admusr@NO2 ~]$ appRev`
		`Install Time: Thu Dec 15 00:05:46 2016`
		`Product Name: DSR`
		`Product Release: 8.0.0.0.0_80.17.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.3.0.0.0_88.30.0`
		`Base Distro ISO: TPD.install-7.3.0.0.0_88.30.0-OracleLinux6.8-x86_64.iso`
		`ISO name: DSR-8.0.0.0.0_80.17.0-x86_64.iso`
		`OS: OracleLinux 6.8`
		If the upgrade fails – **do not proceed**. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

7. ☐	**Server CLI**: If the upgrade fails	If a server upgrade fails, access the server command line, via ssh or console, and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x

8. ☐	**Active NOAM VIP**: Verify post upgrade status	• Navigate to **Administration -> Software Management -> Upgrade**. • Select the tab of the NOAM or site being upgraded. • Verify the **Application Version** for this server has been updated to the target software release version. • Verify the Upgrade State of the upgraded server is **Accept or Reject**. 

9. ☐	**Active NOAM/SOAM VIP**: Verify the server was successfully upgraded	View the Post-Upgrade status of the server:
		• Navigate to **Alarm & Events -> View Active**.
		The active alarms screen displays.
		The active NOAM or SOAM server may have some or all the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10010 (Stateful database not yet synchronized with mate database)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31000 (Program impaired by S/W Fault)`
		`Alarm ID = 31201 (Process Not Running) for eclipseHelp process`
		`Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)`
		The active NOAM or SOAM has the following expected alarm until both NOAMs/SOAMs are upgraded:
		`Alarm ID = 31233 – HA Secondary Path Down`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
		Note: Do Not Accept the upgrade at this time. This alarm is OK.

10. ☐	Procedure complete	The single server upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of this procedure.

Appendix E. Upgrade Single Server – Pre DSR 8.0

This appendix provides the procedure for upgrading a single DSR server when the active NOAM is on DSR 6.x.y or 7.x.y. This procedure upgrades the standby NOAM only. The remaining servers are upgraded using Procedure 55.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

S T E P #	This procedure executes the upgrade single server when the active NOAM is on a release before DSR 8.0. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

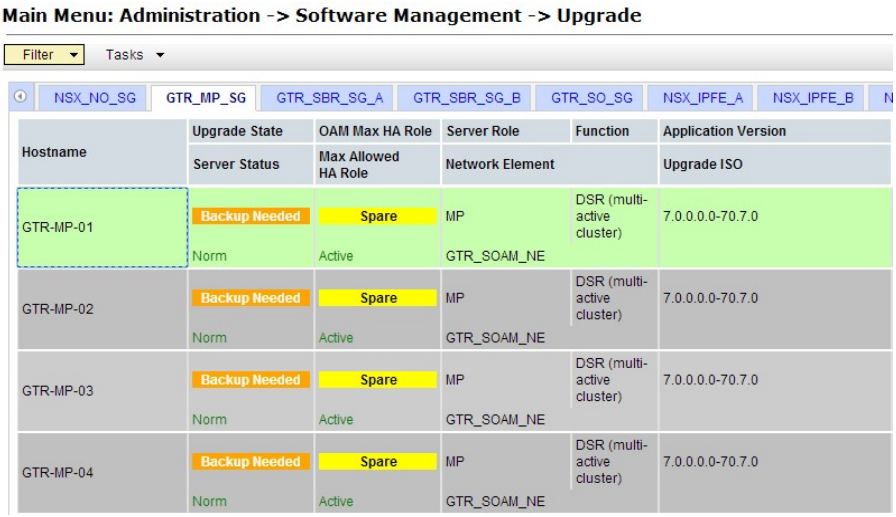
1. ☐	**Active NOAM VIP**: View the pre-upgrade status of Servers	View the pre-upgrade status
		• Log into the NOAM GUI using the VIP.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		The active NOAM server may have some or all of the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
		Main Menu: Administration -> Software Management -> Upgrade

Filter ▾ Tasks ▾

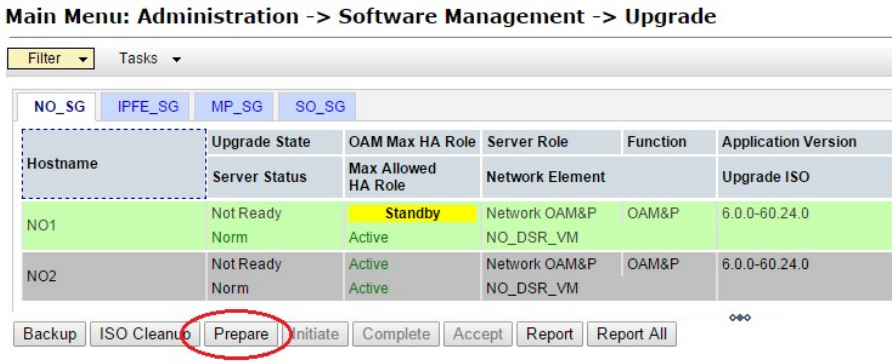
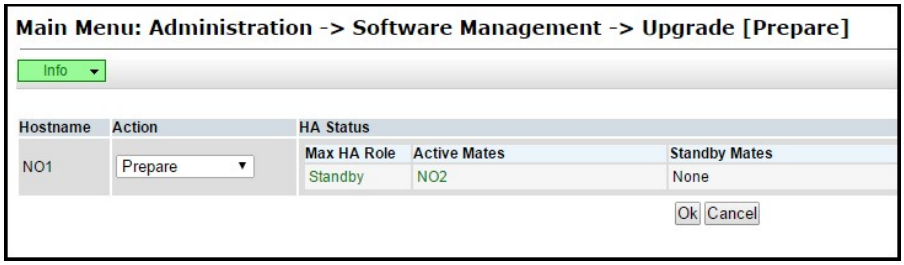
NSX_NO_SG | GTR_MP_SG | GTR_SBR_SG_A | GTR_SBR_SG_B | GTR_SO_SG | NSX_IPFE_A | NSX_IPFE_B

Hostname	Upgrade State / Server Status	OAM Max HA Role / Max Allowed HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO
GTR-MP-01	Backup Needed / Norm	Spare / Active	MP / GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0.0-70.7.0
GTR-MP-02	Backup Needed / Norm	Spare / Active	MP / GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0.0-70.7.0
GTR-MP-03	Backup Needed / Norm	Spare / Active	MP / GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0.0-70.7.0
GTR-MP-04	Backup Needed / Norm	Spare / Active	MP / GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0.0-70.7.0

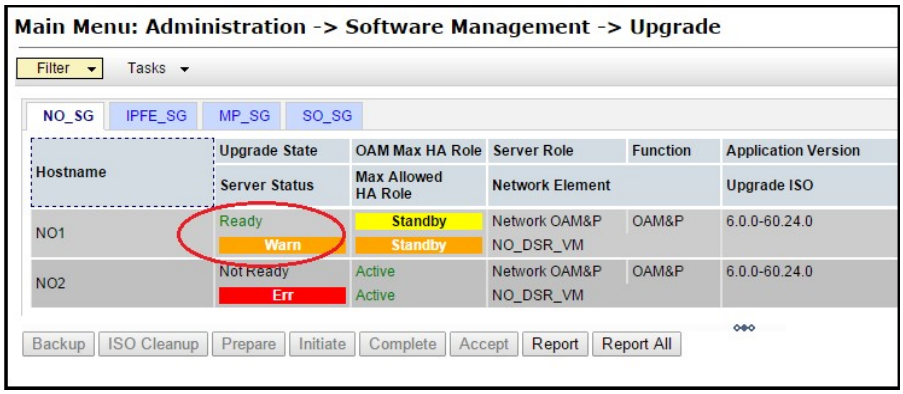
Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

2. ☐	**Active NOAM VIP**: Verify status of server to be upgraded	For the server to be upgraded:
		• Identify the server (NOAM, SOAM, MP, etc.) _____(record name)
		• Verify the **Application Version** is the expected software release version.
		• From the Administration -> Software Management -> Upgrade screen, select the server group of the server to be upgraded.
		 
		• If the server is in the **Backup Needed** state, select the server and click **Backup**. On the Upgrade [Backup] screen, click **OK**. The Upgrade State changes to **Backup in Progress**.
		• Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.
		  • For active NOAM on release 7.0.x:
		  When the backup is complete, verify the server state changes to **Not Ready**, perform steps 3 thru 10.
		  • For active NOAM on release 7.1.x and later:
		  When the backup is complete, verify the server state changes to **Ready**, proceed to step 11.

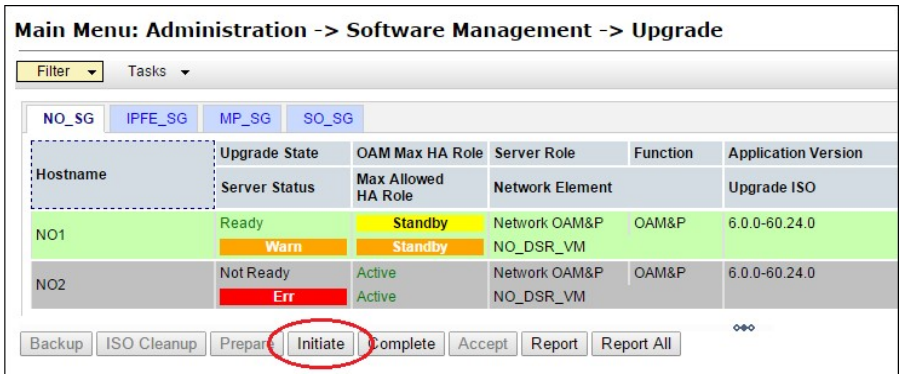
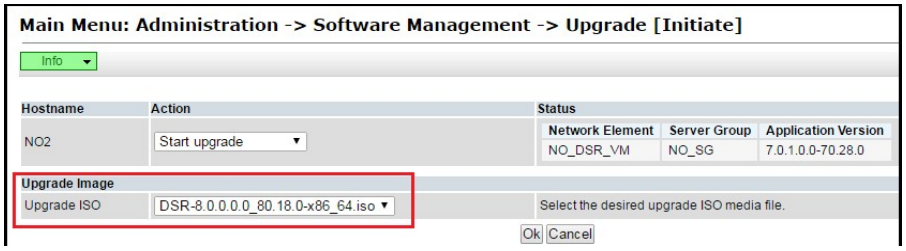
Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

3. ☐	**Active NOAM VIP**: Prepare server for upgrade (step 1) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. On the Upgrade form, make the server **Upgrade Ready** by selecting the server to be upgraded and clicking **Prepare**. In this example, an NOAM with name **NO2** is made ready for Upgrade. 
4. ☐	**Active NOAM VIP**: Prepare server for upgrade (step 2) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. The Upgrade [Prepare] form displays.  For the Max HA Role: • Verify the selected server status is the expected condition (either standby or active). This depends on the server being upgraded. • If the state of the server to be upgraded is as expected, click **OK**.

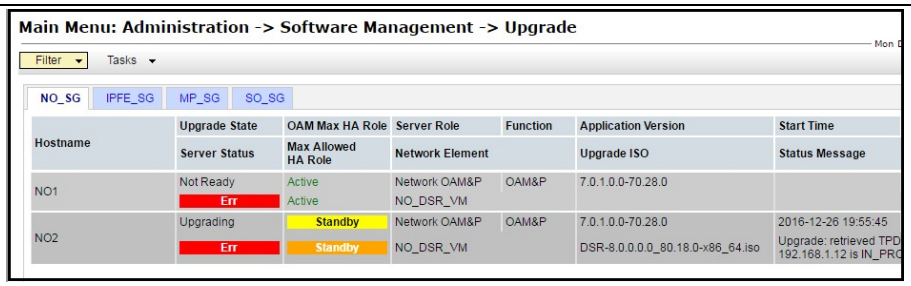
Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

5. ☐	**Active NOAM VIP**: Verify server upgrade status is **Ready**
	
	For active NOAM on release 7.0.x only
		This step is for an active NOAM on release 7.0.x only.
		
		Upon preparing the selected server, the Upgrade Administration form refreshes and the server to be upgraded displays Upgrade State = **Ready**. This may take a minute.
		
		 
		
		Depending on the server being upgraded, new alarms may occur.
		
		Servers may have a combination of the following expected alarms.
		
		Note: Not all servers have all alarms:
		
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		
		`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 = 32515 (Server HA Failover Inhibited)`
		
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		
		`Alarm ID = 31106 (DB Merge to Parent Failure)`

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

6. ☐	**Active NOAM VIP**: Initiate upgrade on the server (part 1) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. From the Upgrade Administration screen, select the server to be upgraded. Click **Initiate**. 
7. ☐	Active NOAM VIP: Initiate upgrade on the server (part 2) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. The Initiate Upgrade form displays: Navigate to **Administration -> Software Management -> Upgrade [Initiate]**. • In the Upgrade Image – **Upgrade ISO** list, select the ISO to use in the server upgrade, • Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen. 
8. ☐	**Active NOAM VIP**: View in-progress status (monitor) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. • View the Upgrade Administration form to monitor upgrade progress. See step 15 for an optional method of monitoring upgrade progress. See step 16 below 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 displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. • Observe the Upgrade State of the server of interest. Upgrade status displays under the Status Message column.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x



Servers may have a combination of the following expected alarms.

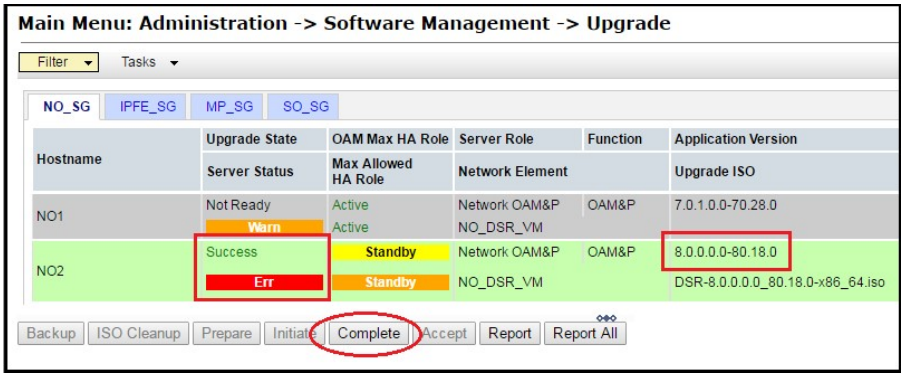
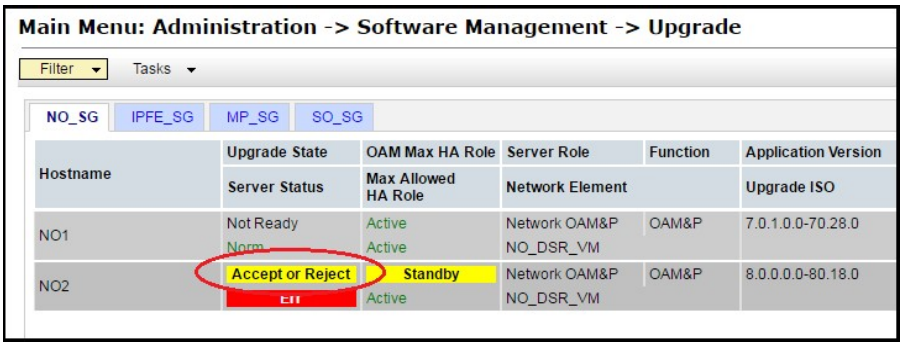
Note: Not all servers have all alarms:

```
Alarm ID = 10008 (Provisioning Manually Disabled)

Alarm ID = 10075 (The server is no longer providing
services because application processes have been
manually stopped)

Alarm ID = 10073 (Server Group Max Allowed HA Role
Warning)

Alarm ID = 32515 (Server HA Failover Inhibited)

Alarm ID = 31228 (HA Highly available server failed to
receive mate heartbeats) or (Lost Communication with
Mate Server)

Alarm ID = 31283 (Highly available server failed to
receive mate heartbeats)

Alarm ID = 31106 (DB Merge To Parent Failure)

Alarm ID = 31107 (DB Merge From Child Failure)

Alarm ID = 31233 (HA Secondary Path Down)

Alarm ID = 31101 (DB Replication To Slave Failure)

Alarm ID = 31104 (DB Replication over SOAP has failed
```

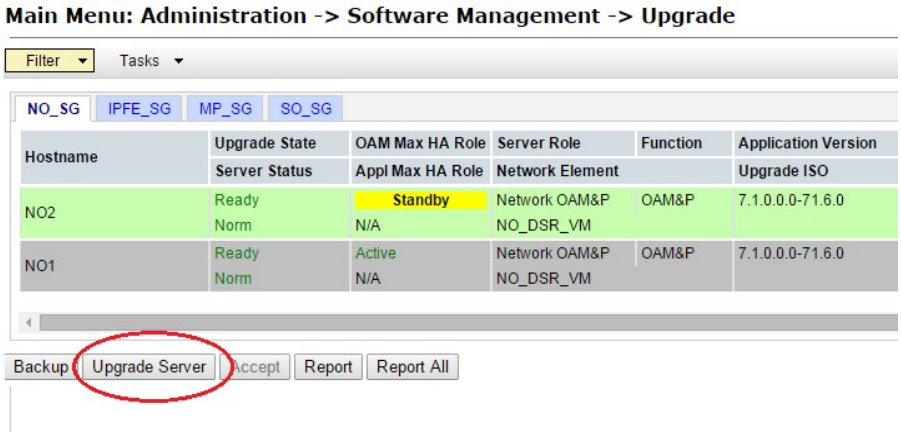
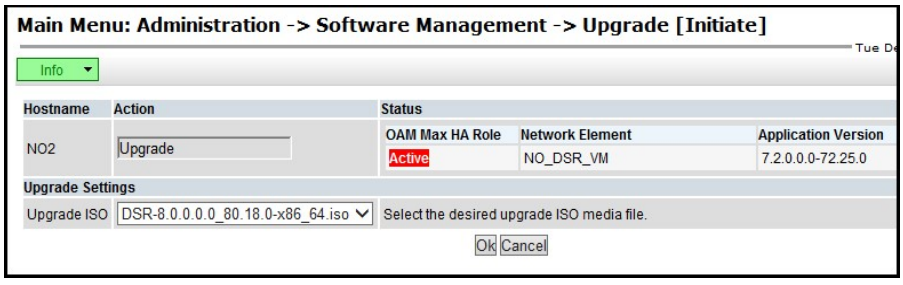
- Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes.

If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

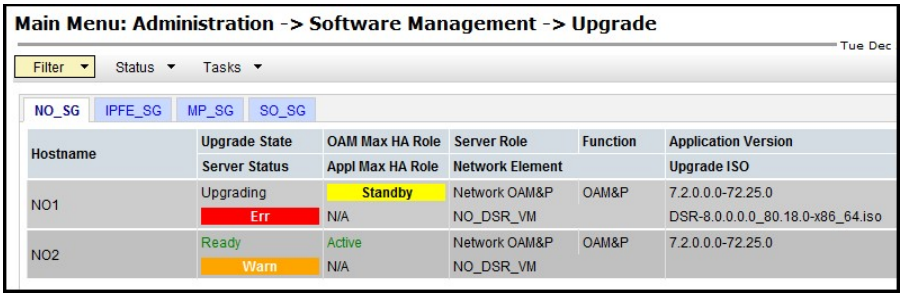
9. ☐	**Active NOAM VIP**: Take the upgraded server out of the upgrade **SUCCESS** state (part 1) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type. • Navigate to **Administration -> Software Management -> Upgrade**. • Verify the **Application Version** for this server has been updated to the target software release version. • Verify the Upgrade State of the server that was upgraded is **Success**. • Select the server that was upgraded. • Click **Complete**. 
10. ☐	**Active NOAM VIP**: Take the upgraded server out of the upgrade **SUCCESS** state (part 2) For active NOAM on release 7.0.x only	This step is for an active NOAM on release 7.0.x only. The Upgrade[Complete] screen displays.  • Click **OK**. This completes the upgrade action on the server. The Upgrade Administration screen displays. Wait for the screen to refresh and show the Upgrade State as **Accept or Reject**. It may take up to 2 minutes for the Upgrade State to change to **Accept or Reject**.  Proceed to step 18 to complete this procedure.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

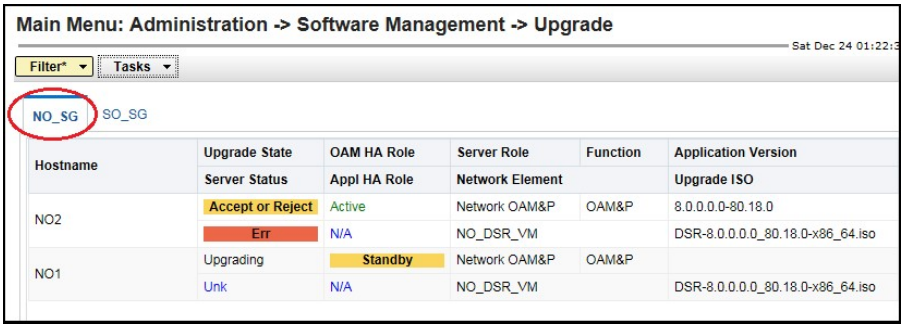
11. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 1) For active NOAM on release 7.1.x and later	This step is for an active NOAM on release 7.1.x or later. • From the Upgrade Administration screen, select the server to be upgraded. • Click **Upgrade Server**.  The Initiate Upgrade form displays: • Navigate to **Administration -> Software Management -> Upgrade [Initiate]**.
12. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 2) – select ISO form. For active NOAM on release 7.1.x and later	This step is for an active NOAM on release 7.1.x or later. • In the Upgrade Settings – **Upgrade ISO** list, select the ISO to use in the server upgrade, ***Note***: When the active NOAM is the server being upgraded, selecting **OK** initiates an HA switchover and causes the GUI session to log out. ***Note***: If the selected server is the active server in an active/standby pair, the OAM Max HA Role column displays **Active** with a red background. This is NOT an alarm condition. This indicator is to make the user aware that this causes an HA switchover. • Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.  ***** Critical *** Do NOT omit this step** • If the server being upgraded is the active NOAM and clicking **OK** initiated a role change, log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

		may exhibit incorrect behaviors if the browser cache is not cleared. • Proceed to step 14 to monitor upgrade status. ***** Critical *** Do NOT omit this step** • If the server being upgraded is not the active NOAM, continue with step 13 to monitor upgrade status.

13.
☐
	Active NOAM VIP:
	View in-progress status (monitor)
		• View the Upgrade Administration form to monitor upgrade progress.
		See step 15 for an optional method of monitoring upgrade progress.
		See step 16 below 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 displays as **FAILED**.
		The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.
		• Observe the Upgrade State of the server of interest. Upgrade status displays under the Status Message column.
		 
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		`Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)`
		`Alarm ID = 31106 (DB Merge To Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31233 (HA Secondary Path Down)`

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

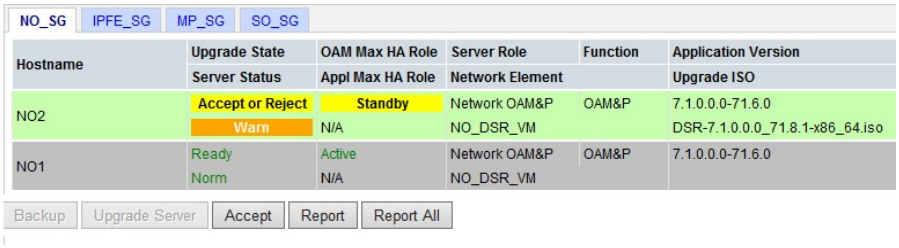
		Alarm ID = 31101 (DB Replication To Slave Failure) Alarm ID = 31104 (DB Replication over SOAP has failed • Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes. If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures. Proceed to step 17 to continue the upgrade.
14. ☐	**Active NOAM VIP**: View in-progress status For active NOAM on DSR 8.0 only	This step is for monitoring upgrade status of the formerly active NOAM after a role change. The NOAM that was active when the upgrade was initiated is now the standby NOAM. Monitoring from this point on is from the new active NOAM on DSR 8.0. • View the Upgrade Administration form to monitor upgrade progress. See step 15 for an optional method of monitoring upgrade progress. See step 16 below for instructions if the Upgrade fails. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. • The upgrade status of the standby NOAM can be observed on the Upgrade Administration screen by selecting the NOAM server group tab.  • Wait for the upgrade to complete. The Upgrade State column displays **Success**. This step takes approximately 20 to 50 minutes. If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures. Proceed to step 18 to continue the upgrade.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

15. ☐	**Server CLI**: View in-progress status from command line of server (Optional)	An optional method to view Upgrade progress from the command line:
		• To view the detailed progress of the upgrade , access the server command line (via SSH or Console), and enter:
		`$ tail -f /var/TKLC/log/upgrade/upgrade.log`
		Once the server has upgraded, it reboots. It takes a couple of minutes for the DSR application processes to start up.
		This command displays the current rev on the server:
		`$ appRev`
		`Install Time: Tue Jun 17 08:20:57 2014`
		`Product Name: DSR`
		`Product Release: 6.0.0_60.14.6`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.7.0.0.1_84.14.0`
		`Base Distro ISO: TPD.install-6.7.0.0.1_84.14.0-OracleLinux6.5-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

16. ☐	**Server CLI**: If the upgrade fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix I of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

Procedure 56: Upgrade Single Server – Upgrade Administration – Pre DSR 8.x

17. ☐	**Active NOAM VIP**: Verify post upgrade status	• Navigate to **Administration -> Software Management -> Upgrade**. • Verify the **Application Version** for this server has been updated to the target software release version. If the active NOAM is on release 7.0.x: • Verify the Status Message indicates **Success**. If the active NOAM is on release 7.1.x or later: • Verify the Upgrade State of the upgraded server is **Accept or Reject**. 

18. ☐	**Active NOAM/SOAM VIP**: Verify the server was successfully upgraded	View the post-upgrade status of the server:
		• Navigate to **Alarm & Events -> View Active**.
		The active alarms screen displays.
		The active NOAM or SOAM server may have some or all the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10010 (Stateful database not yet synchronized with mate database)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31000 (Program impaired by S/W Fault)`
		`Alarm ID = 31201 (Process Not Running) for eclipseHelp process`
		`Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
		Note: Do Not Accept upgrade at this time. This alarm is OK.
		The active NOAM or SOAM has the following expected alarm until both NOAMs/SOAMs are upgraded:
		`Alarm ID = 31233 – HA Secondary Path Down`

19. ☐	Procedure complete	The single server upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of this procedure.

Appendix F. Upgrade Multiple Servers – Upgrade Administration

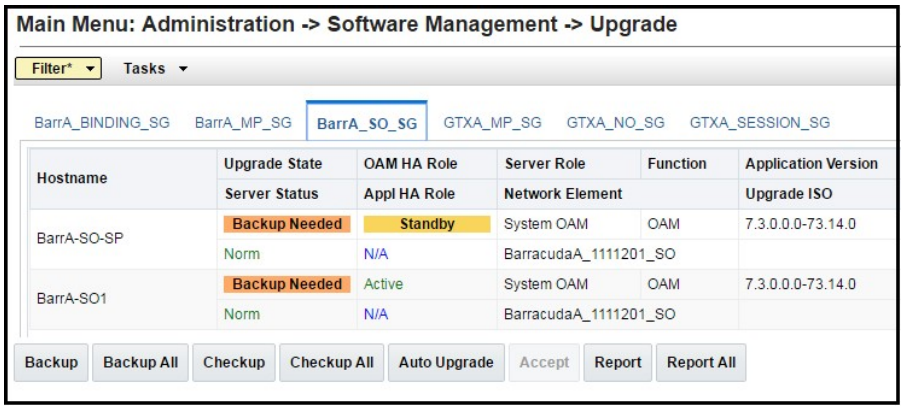
This Appendix provides the procedure for upgrading multiple servers in parallel.

Note: This procedure is executed multiple times during the overall upgrade, depending on the number of servers in your DSR. Make multiple copies of Appendix F to mark up, or keep another form of written record of the steps performed.

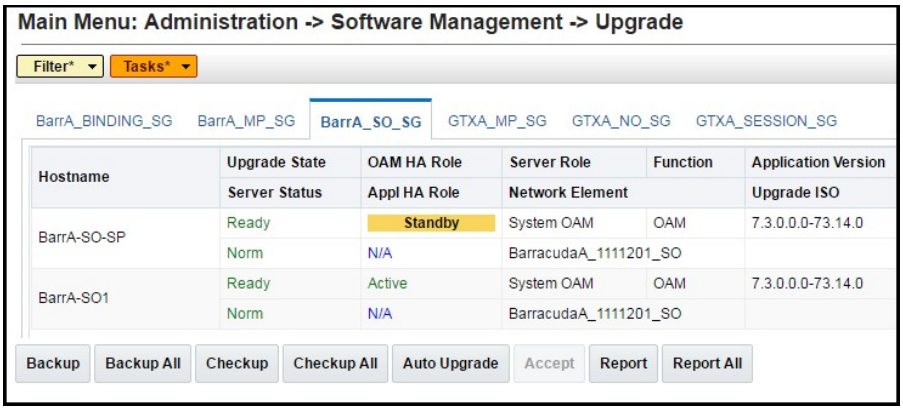
Procedure 57: Upgrade Multiple Servers – Upgrade Administration

S T E P #		
	This procedure executes the upgrade multiple servers – upgrade administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM VIP**: View pre-upgrade status of the servers	• Log into the NOAM GUI using the VIP.
		• Navigate to **Administration -> Software Management -> Upgrade**.
		Active NOAM server may have some or all of the following expected alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`

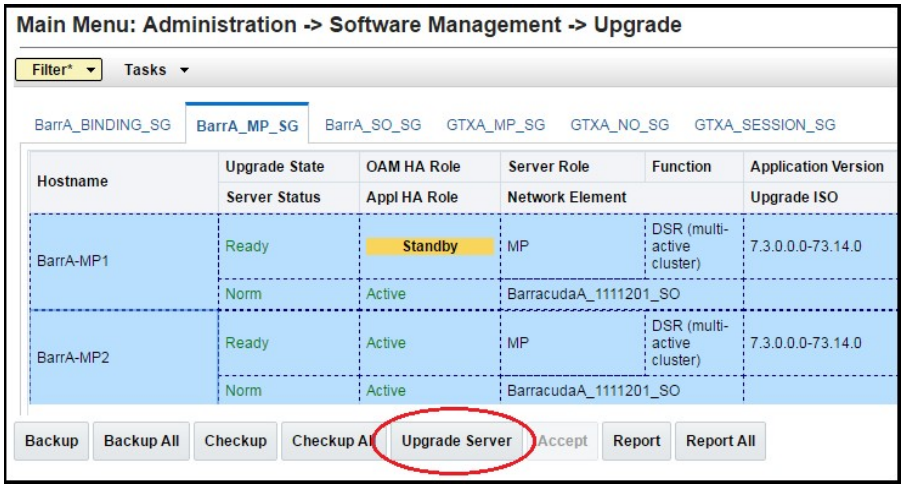
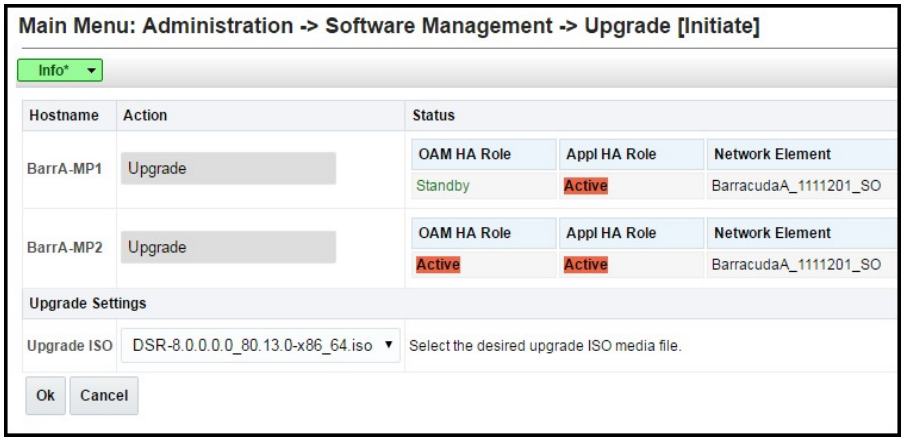
2. ☐	**Active NOAM VIP**: Verify status of servers to be upgraded	• For the servers to be upgraded, Identify the MP servers to be upgraded in parallel _____ (record names) • Verify the **Application Version** is the expected software release version for each MP server to be upgraded. • From the Administration -> Software Management -> Upgrade screen, select the server group of the server to be upgraded.  • If the server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. • Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.

Procedure 57: Upgrade Multiple Servers – Upgrade Administration

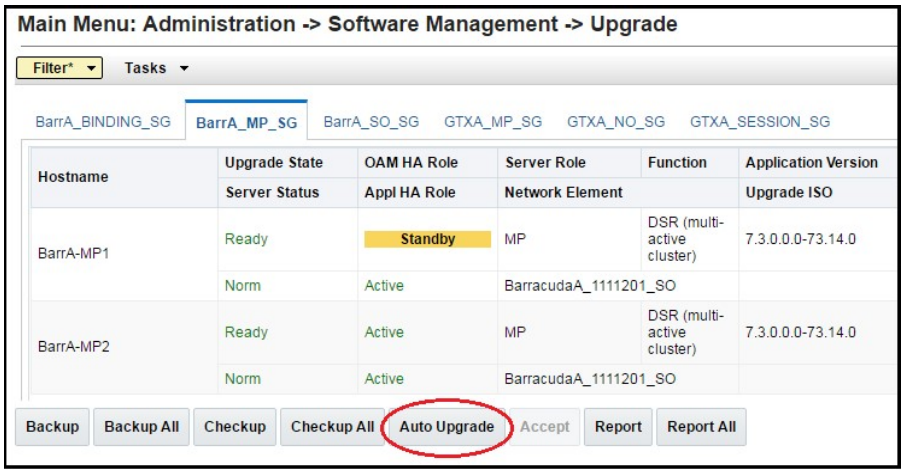
3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	The Upgrade Administration form refreshes and the server to be upgraded displays Upgrade Status = **Ready**. This may take a minute. Depending on the server being upgraded, new alarms may occur.
		The Upgrade Administration screen displays:
		 
		
		Servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`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 = 32515 (Server HA Failover Inhibited)`
		`Alarm ID = 31101 (DB Replication to slave DB has failed)`
		`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)`

4. ☐	Determine upgrade method – manual or automatic	To upgrade multiple servers in parallel using the manual option, execute steps 4 and 5. To upgrade a server group using the Automated Server Group Upgrade option, proceed to step 6.

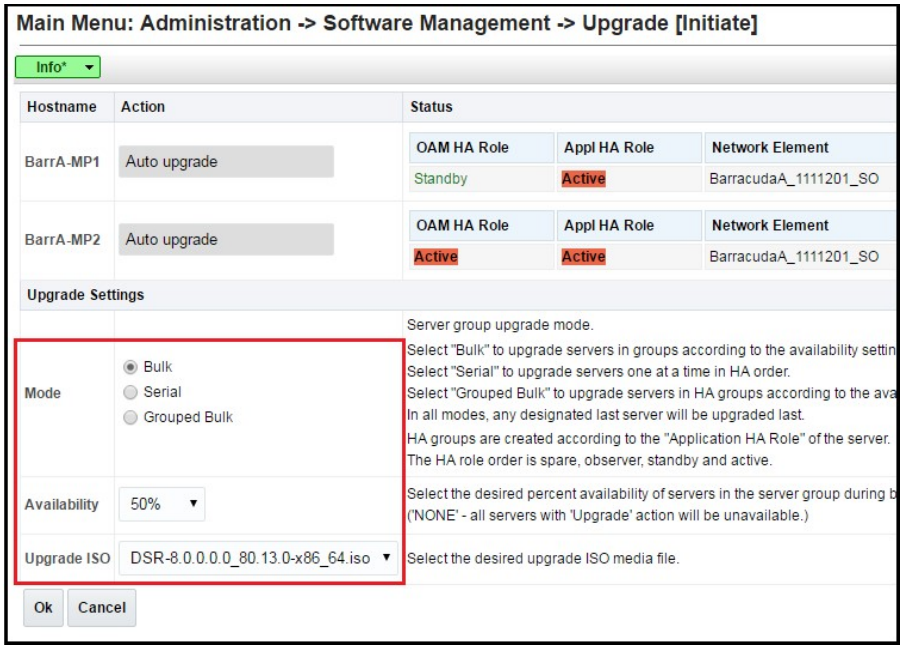
Procedure 57: Upgrade Multiple Servers – Upgrade Administration

5. ☐	**Active NOAM VIP**: Initiate upgrade (initiate) (part 1)	• From the Upgrade Administration screen, select the servers to be upgraded. • Click Upgrade Server.  The Initiate Upgrade form displays: • Navigate to **Administration -> Software Management -> Upgrade [Initiate]**.
6. ☐	**Active NOAM VIP**: Initiate upgrade– Select ISO form (part 2)	• In the Upgrade Settings – **Upgrade ISO** list, select the ISO to use in the server upgrade, • Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.  Proceed to step 8 to complete this procedure.

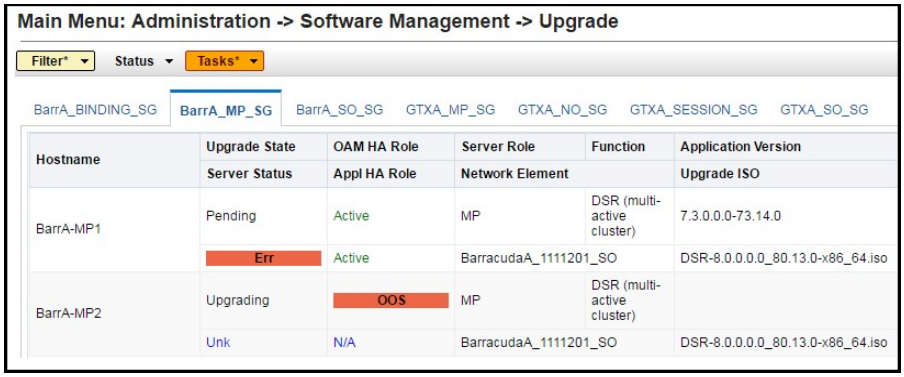
Procedure 57: Upgrade Multiple Servers – Upgrade Administration

7. ☐	**Active NOAM VIP**: Initiate automated server group upgrade (part 1)	• To use the Automated Server Group upgrade option, verify no servers in the server group are selected.  • Click **Auto Upgrade**. The Upgrade [Initiate] screen displays.

Procedure 57: Upgrade Multiple Servers – Upgrade Administration

8. ☐	**Active NOAM VIP**: Initiate automated server group upgrade (part 2)	***Note***: The settings to be used in this step are specified in the calling procedure. • The Upgrade Settings section of the Initiate screen controls the behavior of the automated upgrade. Select the settings that apply to the server type being upgraded. **Bulk**: Select this option for active/standby and multi-active server groups. For servers in an active/standby configuration, the standby server is upgraded first, followed by the active. Servers in a multi-active configuration are upgraded in parallel to the extent allowed by the Availability setting. **Serial**: Select this option to upgrade multiple servers one at a time. **Grouped Bulk**: Select this option for SBR server groups. Grouped bulk always upgrades the spare(s), followed by the standby, followed by the active. **Availability**: This setting determines how many servers remain in service while servers in the server group are upgraded. For example, a setting of 50% ensures that **at least** half of the servers **in the server group** remain in service. ***Note***: The **Serial** upgrade mode is available as an alternative to Bulk and Grouped Bulk for a more conservative upgrade scenario. Serial mode upgrades each server in the server group one at a time, and can be used on any server group type. • Select the appropriate ISO from the **Upgrade ISO** list. • Click **OK** to start the upgrade. 

Procedure 57: Upgrade Multiple Servers – Upgrade Administration

9. ☐	**Active NOAM VIP**: View in-progress status (monitor)	View the Upgrade Administration form to monitor upgrade progress.
		See step 9 for an optional method of monitoring upgrade progress.
		See step 10 below 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 displays as **FAILED**.
		The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.
		• Observe the Upgrade State of the servers of interest. Upgrade status displays under the Status Message column.
		 
		Main Menu: Administration -> Software Management -> Upgrade
		Filter* Status Tasks*
		BarrA_BINDING_SG BarrA_MP_SG BarrA_SO_SG GTXA_MP_SG GTXA_NO_SG GTXA_SESSION_SG GTXA_SO_SG
		Hostname / Server Status / Upgrade State / Appl HA Role / OAM HA Role / Network Element / Server Role / Function / Upgrade ISO / Application Version
		BarrA-MP1 Pending Active MP DSR (multi-active cluster) 7.3.0.0.0-73.14.0
		Err Active BarracudaA_1111201_SO DSR-8.0.0.0.0_80.13.0-x86_64.iso
		BarrA-MP2 Upgrading OOS MP DSR (multi-active cluster)
		Unk N/A BarracudaA_1111201_SO DSR-8.0.0.0.0_80.13.0-x86_64.iso
		During the upgrade, the servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31101 (DB Replication To Slave Failure)`
		`Alarm ID = 31106 (DB Merge To Parent Failure)`
		`Alarm ID = 31107 (DB Merge From Child Failure)`
		`Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)`
		`Alarm ID = 31233 (HA Secondary Path Down)`
		`Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)`
		`Alarm ID = 32515 (Server HA Failover Inhibited)`
		• Wait for the upgrades to complete. The Status Message column displays

Procedure 57: Upgrade Multiple Servers – Upgrade Administration

		Success. This step takes approximately 20 to 50 minutes. When an upgraded SOAM becomes active on Release 8.x, alarm 25607 displays to alert the operator to enable the new Signaling Firewall feature. This alarm is active until the firewall is enabled in Procedure 35. `Alarm ID = 25607 (DSR Signaling Firewall is administratively Disabled)` If the upgrade fails – do not proceed. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

10. ☐	**Server CLI**: View in-progress status from command line	An optional method to view upgrade progress from the command line:
		To view the detailed progress of the upgrade, access the server command line (via ssh or console), and type:
		`$ tail -f /var/TKLC/log/upgrade/upgrade.log`
		This command displays the upgrade log entries as the events occur. Once the upgrade is complete, the server reboots. It takes a couple of minutes for the DSR application processes to start.
		This command displays the current rev on the upgraded servers:
		`[admusr@NO1 ~]$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the upgrade fails – **do not proceed**. It is recommended you consult with My Oracle Customer Support on the best course of action. Refer to Appendix K for failed server recovery procedures.

11. ☐	**Server CLI**: If upgrade fails**:**	If a server upgrade fails, access the server command line, via ssh or console, and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

Procedure 57: Upgrade Multiple Servers – Upgrade Administration

12. ☐	**Active NOAM VIP**: Verify post upgrade status	• Navigate to **Administration -> Software Management -> Upgrade**. • Verify the **Application Version** for the servers has been updated to the target software release version. • Verify the **Status Message** indicates success. • Verify the Upgrade State of the upgraded servers is **Accept or Reject**.

13. ☐	Verify the servers were successfully upgraded	View Post-Upgrade status of the server:
		The active SOAM server may have some or all the following expected alarm(s):
		`Alarm ID = 10008 (Provisioning Manually Disabled)`
		`Alarm ID = 10010 (Stateful database not yet synchronized with mate database)`
		`Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)`
		`Alarm ID = 31000 (Program impaired by S/W Fault)`
		`Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)`
		Note: Do Not Accept upgrade at this time. This alarm is OK.

14. ☐	Procedure complete	The multiple servers upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix F.

Appendix G. Alternate Server Upgrade Procedures

The procedures in this section provide alternative ways of upgrading various server types, using an array of differing methods. All of the procedures in this section are secondary to the upgrade methods provided in Section 4 and Section 5. These procedures should be used only when directed by My Oracle Customer Support or by other procedures within this document.

Appendix G.1 Alternate Pre-Upgrade Backup

This procedure is an alternative to the normal pre-upgrade backup provided in Procedure 22. It is recommended that this procedure be executed only under the direction of My Oracle Customer Support.

Procedure 58: Alternate Pre-Upgrade Backup

S T E P #	This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active SOAM CLI**: SSH to the active SOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active SOAM: `ssh admusr@<SOAM_VIP>`

Procedure 58: Alternate Pre-Upgrade Backup

2. ☐	**Active SOAM CLI**: Start a screen session	Enter the following commands: `# screen` The screen tool creates a no-hang-up shell session, so the command continues to execute if the user session is lost.

3. ☐	**Active SOAM CLI**: Execute a backup of all servers managed from the SOAM to be upgraded	Execute the **backupAllHosts** utility on the active SOAM. This utility remotely accesses each specified server, and runs the backup command for that server.
		The **--site** parameter allows the user to backup all servers associated with a given SOAM site to be upgraded:
		WARNING: Failure to include the **--site** parameter with the **backupAllHosts** command results in overwriting the NOAM backup file created in Section 3.4.5. Backing out to the previous release is not possible if the file is overwritten.
		`$ /usr/TKLC/dpi/bin/backupAllHosts --site=<NEName>`
		where **<NEName>** is the network element name (**NEName**) as seen using the following command:
		`$ iqt NetworkElement`
		The following output is generated upon execution of either of the above options:
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.
		Do not proceed until the backup on each server is completed.
		Output similar to the following indicates successful completion:
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`
		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		Errors also report back to the command line.
		Note: There is no progress indication for this command; only the final report when it completes.

4. ☐	**Active SOAM CLI**: Exit the screen session.	`# exit`
		`[screen is terminating]`
		Note: **screen -ls** shows active screen sessions on a server, and **screen -dr** re-enters a disconnected screen session.

Procedure 58: Alternate Pre-Upgrade Backup

5. ☐	**ALTERNATIVE METHOD** (Optional)
	Server CLI: If needed, the alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following indicates successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

6. ☐	**Active NOAM VIP**: Verify backup files are present on each server	• Log into the active NOAM GUI using the VIP.
		• Navigate to **Status & Manage -> Files**.
		• Select each server tab, in turn.
		• For each server, verify the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		• Repeat sub-steps 1 through 4 for each site.

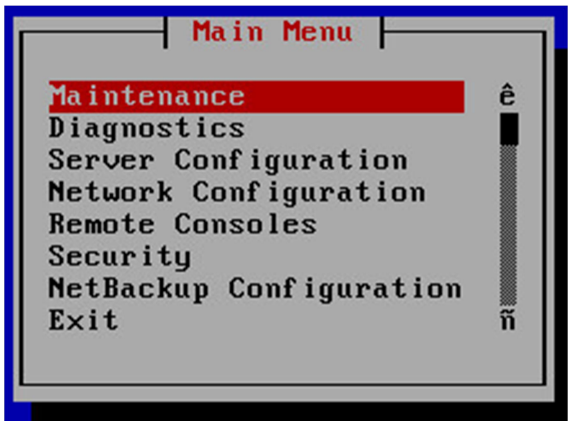
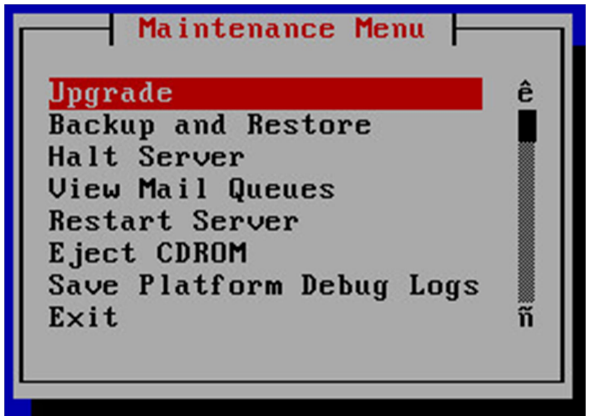
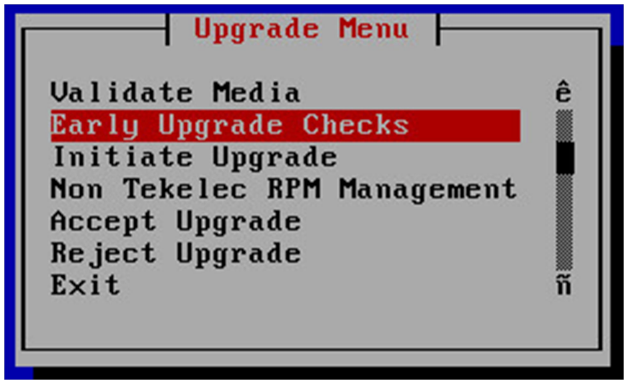
Appendix G.2 Server Upgrade using platcfg

The procedure provided in this appendix enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of My Oracle Customer Support.

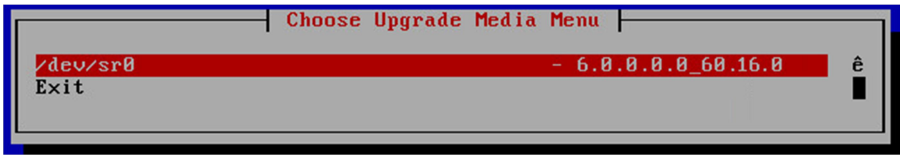
Procedure 59: Server Upgrade Using Platcfg

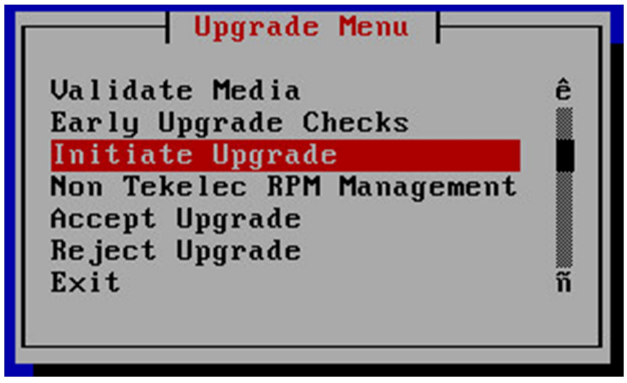
S T E P #	This procedure upgrades a server using the platcfg utility. NOTE: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Log into the server to be upgraded	• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server to be upgraded: `ssh admusr@<server_ip>`

Procedure 59: Server Upgrade Using Platcfg

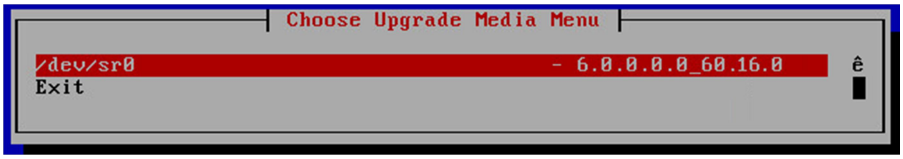
2. ☐	Enter the platcfg menu	• Switch to the platcfg user to start the configuration menu. `$ sudo su - platcfg` • From the Main Menu, select **Maintenance**. 
3. ☐	Select upgrade	• From the Maintenance Menu, select **Upgrade**. 
4. ☐	Select early upgrade checks	• From the Upgrade Menu, select **Early Upgrade Checks**. 

Procedure 59: Server Upgrade Using Platcfg

5. ☐	Select the upgrade media	• From the Choose Upgrade Media Menu, select the desired target media. This initiates the early upgrade checks in the console window.
		 
		Informational messages displays as the checks progress. At the end of a successful test, a message similar to the following displays:
		`Running earlyUpgradeChecks() for Upgrade::EarlyPolicy:: TPDEarlyChecks upgrade policy...`
		• Verified server is not pending accept of previous upgrade.
		`Hardware architectures match`
		`Install products match.`
		`Verified server is alarm free!`
		`Early Upgrade Checks Have Passed!`
		• Verify early upgrade checks pass. In case of errors, it is recommended you contact My Oracle Customer Support.
		• Press **q** to exit the screen session and return to the platcfg menu.
		• From the Choose Upgrade Media Menu, select **Exit**.

6. ☐	Initiate the upgrade	• From the Upgrade Menu, select **Initiate Upgrade**. 

Procedure 59: Server Upgrade Using Platcfg

7. ☐	Select the Upgrade Media	The screen displays a message that it is searching for upgrade media. Once the upgrade media is found, an Upgrade Media selection menu displays similar to the example shown. • From the Choose Upgrade Media Menu, select the desired target media. This initiates the server upgrade.  Many informational messages come across the terminal screen as the upgrade proceeds. Finally, after upgrade is complete, the server reboots. A reboot of the server is required. The server is rebooted in 10 seconds
8. ☐	SSH to the upgraded server	• Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server just upgraded: `ssh admusr@<server_IP>` Answer **yes** if you are asked to confirm the identity of the server.

9. ☐	Check for upgrade errors	• Examine the upgrade logs in the directory /var/TKLC/log/upgrade and verify no errors were reported.
		`grep -i error /var/TKLC/log/upgrade/upgrade.log`
		• Examine the output of the above command to determine if any errors were reported.
		If the upgrade fails, collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/platcfg.log`
		It is recommended you contact My Oracle Customer Support by referring to Appendix M of this document and provide these files.

10. ☐	Verify the upgrade	• Check the upgrade log for the upgrade complete message.
		`grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		• Verify the **UPGRADE IS COMPLETE** message displays. If not, it is recommended you contact My Oracle Customer Support.
		`[admusr@NO2 ~]$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/ upgrade/upgrade.log`
		`1407786220:: UPGRADE IS COMPLETE`

Appendix G.3 Manual DA-MP (N+0) Upgrade Procedure

Procedure 60 manually upgrades a multi-active DA-MP server group. This procedure is an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 60 must be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 60 must be executed four distinct times.

Procedure 60: Manual DA-MP (N+0) Upgrade Procedure

S T E P #	This procedure upgrades a multi-active DA-MP servers using the manual upgrade method. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Identify all the DA-MPs to be upgraded together	From the data captured in Table 5, identify the **DSR (multi-active cluster)** server group to be upgraded.
2. ☐	Upgrade DA-MP servers as identified in step 1	Upgrade up to (½) one half (no more than 50%) of the DA-MP servers in parallel using the Upgrade Multiple Servers procedure. ***Note***: When using the manual server upgrade method, it is recommended that the DA-MP Leader be upgraded in the last group of servers to minimize DA-MP Leader role changes. • Execute Appendix F : Upgrade Multiple Servers. • After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
3. ☐	Repeat for all servers identified in Step 1 of this procedure	Repeat step 2 of this procedure for the remaining DA-MP servers.

Appendix G.4 Manual DA-MP (1+1) Upgrade Procedure

Procedure 61 manually upgrades an active/standby DA-MP server group. This procedure is an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 61: Manual DA-MP (1+1) Upgrade Procedure

S T E P #	This procedure upgrades an active/standby DA-MP servers using the manual upgrade method. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Upgrade the standby DA-MP server	Upgrade the standby DA-MP server using the Upgrade Single Server procedure: • Execute Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x. • After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
2. ☐	Upgrade the active DA-MP server	Upgrade the active DA-MP server using the Upgrade Single Server procedure. • Execute Procedure 55: Upgrade Single Server – Upgrade Administration – DSR 8.x.

Appendix G.5 SG SBR Upgrade Procedure

Procedure 62 upgrades the SBR server group using Automated Server Group upgrade. This procedure is an alternative to the normal SBR upgrade procedures in Section 5.

Procedure 62: ASG SBR Upgrade

S T E P #	This procedure upgrades the SBR server group using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	Identify the SBR server group(s) to upgrade	From the data captured in Table 5, identify the SBR server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously.
2. ☐	Upgrade SBR server group(s) identified in step 1 of this procedure	***Note***: The spare SBRs of this server group is located at different sites. Upgrade the SBR server group using the Upgrade Multiple Servers procedure with the following options: • Use the Automated Server Group Upgrade option • Select the Serial upgrade mode • Execute Appendix F — Upgrade Multiple Servers Procedure

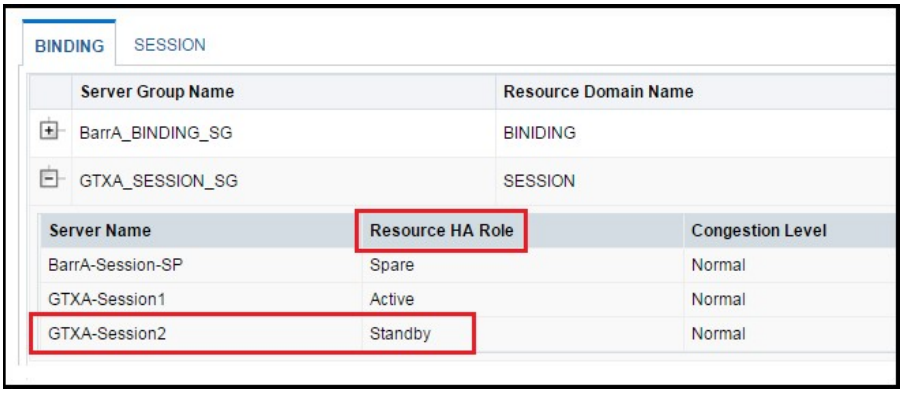
Procedure 62: ASG SBR Upgrade

3. ☐	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2 (and an optional 2nd spare in Site 3)	Repeat step 2 for all remaining binding and session server groups to be upgraded.

Appendix G.6 Manual SBR Upgrade Procedure

Procedure 63: Manual SBR Upgrade Procedure

S T E P #	This procedure upgrades an SBR server group using the manual upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM VIP**: Identify the SBR server group(s) to upgrade	Identify the active, standby, and spare SBR servers.
		From the data captured in Table 5, identify the server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously.
		• Log into the NOAM GUI using the VIP.
		• Navigate to **Main Menu -> Policy and Charging ->Maintenance -> SBR Status**. Open each server group chosen in sub-step 1. Note which server is active, standby, and spare (as designated by the Resource HA Role) for each server group chosen for upgrade. The following figure provides an example:
		`GTXA-Session1 – Active`
		`GTXA-Session2 – Standby`
		`BarrA-Session-SP – Spare`
		 
		BINDING SESSION
		Server Group Name / Resource Domain Name
		BarrA_BINDING_SG / BINIDING
		GTXA_SESSION_SG / SESSION
		Server Name / Resource HA Role / Congestion Level
		BarrA-Session-SP / Spare / Normal
		GTXA-Session1 / Active / Normal
		GTXA-Session2 / Standby / Normal
		Note: SBR servers have two High Availability policies: one for controlling replication of session or binding data, and one for receipt of replicated configuration data from the NOAM and SOAM GUIs. During this upgrade procedure, ONLY the High Availability policy for replication of session or binding data is important. This means that the SBR

Procedure 63: Manual SBR Upgrade Procedure

		Status screen MUST be used to determine the High Availability status (active, standby, or spare) of SBR servers. The HA Status screen and the OAM Max HA Role column on the Upgrade screen must NOT be used because they only show the status of the configuration replication policy. Because the two High Availability policies run independently, it is possible that a given server might be standby or spare for the session and binding replication policy, but active for the configuration replication policy. When this happens, it is necessary to ignore warnings on the Upgrade screen about selecting what it views as the active server (for the configuration replication policy).
2. ☐	**Active NOAM VIP**: Upgrade spare SBR Server identified in step 1 of this procedure	***Note***: The spare SBRs of this server group is located at different sites. Upgrade the spare SBR server using the Upgrade Single Server procedure. • Execute Appendix D—Upgrade Single Server Procedure. • After successfully completing the procedure in Appendix D, return to this point to monitor server status. From the active NOAM GUI: • Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Status**. Open the tab of the server group being upgraded. ***Note***: After executing Appendix D, the spare SBR temporarily disappears from the SBR Status screen. When the server comes back online, it reappears on the screen with a status of **Out of Service**. • Monitor the Resource HA Role status of the spare server. Wait for the status to transition from **Out of Service** to **Spare**. • If the system is equipped with a second spare SBR server, repeat sub-steps 1 thru 3 for the other spare. **Caution**: Do not proceed to step 3 until the **Resource HA Role** of the spare SBR server returns to **Spare**.
3. ☐	Upgrade standby SBR Server identified in step 1 of this procedure	• Upgrade the standby SBR server using Appendix D Upgrade Single Server – DSR 8.x. • After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
		**!WARNING!** **Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact.**

Procedure 63: Manual SBR Upgrade Procedure

4. ☐	**Active NOAM VIP**: Verify standby SBR server status	• Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Status**. Open the tab of the server group being upgraded. ***Note***: After executing Appendix D, the standby SBR temporarily disappeara from the SBR Status screen and the spare server assumea the standby role. When the upgraded server comes back online, it reappeara on the screen with a status of **Out of Service**. • Monitor the Resource HA Role status of the upgraded server. Wait for the status to transition from **Out of Service** to **Standby**. **Caution**: Do not proceed to step 5 until the **Resource HA Role** of the upgraded server transitions to **Standby**.
5. ☐	**Active NOAM VIP**: Verify bulk download completes	Verify the bulk download from the active SBR to the standby and spare SBRs completes. • Navigate to **Main Menu -> Alarm & Event -> View History**. • Export the Event Log using the following filter: **Server Group**: Choose the SBR group that is in upgrade **Display Filter**: Event ID = 31127 – DB Replication Audit Complete **Collection Interval**: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time. • Wait for all instances of Event 31127: 1 for the standby binding SBR 1 for the standby session SBR 1 for the spare binding SBR 1 for the spare session SBR 1 for the 3rd site spare binding SBR (if equipped) 1 for the 3rd site spare session SBR (if equipped) ***Note***: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.
6. ☐	Upgrade active SBR Server as identified in Step 1 of this procedure	Upgrade the active SBR server using the Upgrade Single Server procedure. • Execute Appendix D -- Single Server Upgrade Procedure. • After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
7. ☐	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2	Repeat steps 1 through 6 for all remaining binding and session server groups to be upgraded.

Appendix H. Expired Password Workaround Procedure

This appendix provides the procedures to handle password expiration during upgrade. Procedure 64 is a temporary workaround to allow an expired password to be used on a non-upgrade site. This procedure is provided as a workaround when a password expires after the NOAM has been upgraded and before all sites have been upgraded.

The workaround must be removed using Procedure 65 after the site is upgraded. Failure to remove the workaround inhibits password aging on the server.

Appendix H.1 Inhibit Password Aging

This procedure enacts a workaround that inhibits password aging on the SOAM. This procedure should be used only when the following conditions apply:

- An upgrade is in progress
- The NOAMs have been upgraded, but one or more sites have not been upgraded
- A login password has expired on a non-upgraded site

Once the workaround is enacted, no passwords expire at that site. It is expected that the workaround is removed once the site is upgraded.

Procedure 64: Expired Password Workaround Procedure

S T E P #	This procedure disables password aging on a server, allowing **expired** credentials to be used for login. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active SOAM CLI**: SSH to active SOAM server	Disable password aging.
		• Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Create a text file with the following content (exactly as formatted):
		`[production]`
		`aw.policy.pwchange.isExpired =`
		`aw.policy.db.checkPw =`
		`[development : production]`
		`[test : development]`
		• Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		• Change the file permissions:
		`$ chmod 644 pw.ini`
		• Execute the following command:
		`$ sudo clearCache`
		Note: For each server on which this workaround is enacted, the old **expired**

Procedure 64: Expired Password Workaround Procedure

		password must be used for login. The new password that is used on the NOAM will not work on these servers.
2. ☐	Repeat for standby SOAM	Repeat step 1 for the standby SOAM.
3. ☐	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.

Appendix H.2 Enable Password Aging

This procedure removes the password expiration workaround that is enabled by Procedure 64.

Procedure 65: Expired Password Workaround Removal Procedure

S T E P #	This procedure removes the password aging workaround and re-enables password aging on a server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active SOAM CLI**: SSH to active SOAM server	• Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Delete the pw.ini file:
		`$ sudo rm /var/TKLC/appworks/ini/pw.ini`
		• Execute the following command:
		`$ sudo clearCache`

2. ☐	Repeat for standby SOAM	Repeat step 1 for the standby SOAM.
3. ☐	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.

Appendix H.3 Password Reset

Procedure 66 resets the GUI Admin (guiadmin) password on the NOAM. In a backout scenario where the password expired during the upgrade, it is possible for the customer to get locked out due to global provisioning being disabled. When this happens, this procedure can be used to reset the password to gain access to the GUI.

Procedure 66: Expired Password Reset Procedure

S T E P #	This procedure resets the guiadmin password on the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**Active NOAM CLI**: SSH to active NOAM server	Rest the password.
		• Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active NOAM:
		`ssh admusr@<NOAM_VIP>`
		Answer **yes** if you are asked to confirm the identity of the server.
		• Execute the reset command:
		`$ sudo /usr/TKLC/appworks/sbin/resetPassword guiadmin`
		• At the **Enter new Password for guiadmin** prompt, enter a new password.
		• Attempt to log into the NOAM GUI using the new password. If the login is not successful, it is recommended you contact My Oracle Customer Support for guidance.

Appendix I. Network IDIH Compatibility Procedures

The procedures in this appendix are used to provide IDIH compatibility when upgrading to Release 8.0. Procedure 67 is performed on a Release 8.0 IDIH to make the trace data viewable on prior release IDIH systems, as described in Section 1.7.4. This procedure must be performed on every IDIH 8.0 system from which trace data is expected.

When all IDIH systems have been upgraded to Release 8.0, Procedure 68 must be executed on every IDIH on which Procedure 67 was previously performed.

Procedure 67: Enable IDIH 8.0 Compatibility

S T E P #	This procedure upgrades a server using the platcfg utility. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Appserver CLI**: Log into the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the appserver: `ssh admusr@<server_ip>` Answer **yes** if you are asked to confirm the identity of the server.

Procedure 67: Enable IDIH 8.0 Compatibility

2. ☐	**Appserver CLI**: Change user	Change to the system user tekelec: `sudo su - tekelec`
3. ☐	**Appserver CLI**: Execute command	Execute the following command to enable backward compatibility. `apps/ndih7-compat.sh enable`
4. ☐	Repeat as needed	Repeat this procedure on each IDIH 8.0 appserver as needed.

Procedure 68: Disable IDIH 8.0 Compatibility

S T E P #	This procedure upgrades a server using the platcfg utility. NOTE: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.
1. ☐	**Appserver CLI**: Log into the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the appserver: `ssh admusr@<server_ip>` Answer **yes** if you are asked to confirm the identity of the server.
2. ☐	**Appserver CLI**: Change user	Change to the system user tekelec: `sudo su - tekelec`
3. ☐	**Appserver CLI**: Execute command	Execute the following command to enable backward compatibility `apps/ndih7-compat.sh disable`
4. ☐	Repeat as needed	Repeat this procedure on each IDIH 8.0 appserver as needed.

Appendix J. IDIH Upgrade at a Site

In IDIH release 7.1 and later, the mediation and application instance data is stored in the Oracle Database. This allows the Application and Mediation servers to be upgraded by performing a fresh installation. Upon completion of the upgrade, the mediation and application guests automatically restore the configuration data from the Oracle database.

Table 24 shows the elapsed time estimates for IDIH upgrade.

Table 24: IDIH Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 69	1:15-1:45	1:15-1:45	Oracle Guest Upgrade	None
Procedure 70	0:30-0:45	1:45-2:30	Upgrade the Mediation and Application Guests	None

Appendix J.1 Oracle Guest Upgrade

The Oracle Guest is upgraded first.

Procedure 69: Oracle Guest Upgrade

S T E P #	This procedure performs the IDIH Oracle Guest upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	

1. ☐	**IDIH CLI**: Perform system health check	Perform a system health check on the Oracle guest.
		• Login in to the Oracle guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		• Execute the analyze_server.sh script.
		`$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		Sample output:
		`[admusr@cat-ora ~]$ /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		`13:24:52: STARTING HEALTHCHECK PROCEDURE`
		`13:24:52: date: 03-17-15, hostname: cat-ora`
		`13:24:52: TPD VERSION: 7.0.0.0.0-86.14.0`
		`13:24:52: ----------`
		`13:24:52: Checking disk free space`
		`13:24:52: No disk space issues found`
		`:`
		`:`
		`13:25:02: All tests passed!`
		`13:25:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 0`
		If the output indicates a status failure, do not proceed with the upgrade. It is recommended you contact My Oracle Customer Support for guidance.

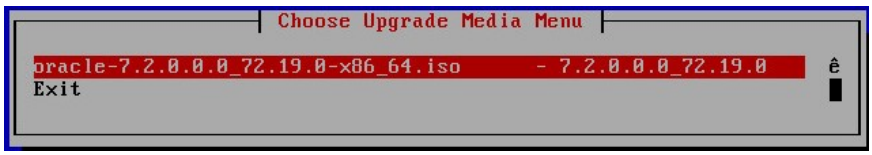
Procedure 69: Oracle Guest Upgrade

2. ☐	**IDIH CLI**: Shutdown Mediation guest	Shut down the Mediation guest in preparation for the Oracle guest upgrade.
		• Log into the Mediation guest as admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		• Shutdown the Mediation guest.
		`$ sudo init 0`
		The active SOAM server may have some or all of the following expected alarms:
		`Alarm ID = 19800 Communication Agent Connection Down`
		`Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname`
		`The active NOAM server may have some or all of the following expected alarms:`
		`Alarm ID = 19800 Communication Agent Connection Down`

3. ☐	**IDIH CLI**: Shutdown Application guest	Shut down the Application guest in preparation for the Oracle guest upgrade.
		• Log into the Application guest as admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		• Shutdown the Application guest.
		`$ sudo init 0`
		The active SOAM server may have some or all of the following expected alarms:
		`Alarm ID = 19800 Communication Agent Connection Down`
		`Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname`
		The active NOAM server may have some or all of the following expected alarms:
		`Alarm ID = 19800 Communication Agent Connection Down`

4. ☐	Move Oracle ISO	• Use a file transfer tool to copy the Oracle ISO to the Oracle guest as admusr. Example: `$ scp oracle-8.0.0.0.0_80.21.0-x86_64.iso admusr@<ora-guest-ip>:/var/TKLC/upgrade`

Procedure 69: Oracle Guest Upgrade

5. ☐	**IDIH CLI**: Start Oracle guest upgrade	The Oracle guest is upgraded using the Platform Configuration utility. • Launch the platform configuration utility. `$ sudo su - platcfg` • In the resulting menu, navigate to **Maintenance -> Upgrade -> Initiate Upgrade**. • At the ISO selection menu, select the target release Oracle ISO and press the Enter key. 
6. ☐	**IDIH CLI**: Monitor upgrade progress	The platform configuration menu exits and the guest reboots when the upgrade completes. • To view the detailed progress of the upgrade, access the server command line (via SSH or Console), and enter: `$ tail -f /var/TKLC/log/upgrade/upgrade.log` Once the server has upgraded, it reboots. It takes a couple of minutes for the Oracle processes to start up.
7. ☐	**IDIH CLI**: Perform system health check	Wait a few minutes to allow the Oracle guest to stabilize after the reboot, and then repeat step 1 to perform the post-upgrade system health check. ***Note***: The following warnings are expected due to the mediation and app servers being shutdown. **Warning**: Mediation server is not reachable (or ping response exceeds 3 seconds). **Warning**: app server is not reachable (or ping response exceeds 3 seconds).

Appendix J.2 Upgrade the Mediation and Application Guests

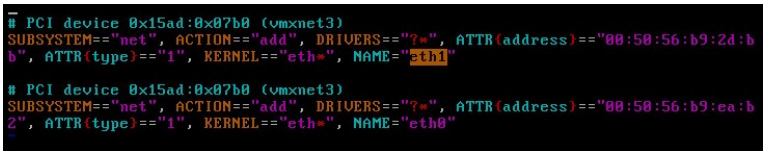
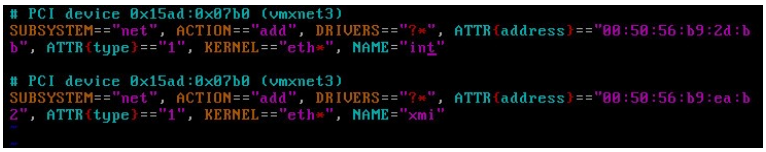
- The Mediation and Application Guest upgrade is similar to the installation procedure.

Procedure 70: Upgrade the Mediation and Application Guests

S T E P #	This procedure performs the IDIH Mediation and Application server upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Cloud GUI**: Remove existing application server	• Use the hpyervisor-specific procedure to remove the current iDIH Application and iDIH Mediation guests.

Procedure 70: Upgrade the Mediation and Application Guests

2. ☐	**Cloud GUI**: Deploy the latest application and mediation guest images	• Use the hypervisor-specific procedure to deploy the latest Application and Mediation guests. • Configure the iDIH Mediation and application guests to reflect the guest profile in the installation document [1].

3. ☐	**IDIH CLI**: Configure the network rules file	• Login in to the iDIH Mediation guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		• Generate the net rules file.
		`$ sudo udevadm trigger --subsystem-match=net`
		• Update the net rules file. Replace the default interface names **eth0** with **xmi** and **eth1** with **int**. For the Mediation guest, rename the third interface from **eth2** to **imi**.
		`$ sudo vi /etc/udev/rules.d/70-persistent-net.rules`
		 
		
		 
		
		• Reboot the server:
		`$ sudo init 6`
		• Repeat sub-steps 1 thru 4 for the application guest.

Procedure 70: Upgrade the Mediation and Application Guests

4. ☐	**IDIH CLI**: Configure the network interfaces for the mediation guest	• Login in to the iDIH Mediation guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		• Configure the xmi network with its ip address and netmask.
		`$ sudo netAdm add -device=xmi -address=x.x.x.x -netmask=x.x.x.x -onboot=yes -bootproto=none`
		• Configure the default route.
		`$ sudo netAdm add -route=default -device=xmi -gateway=x.x.x.x`
		• Configure the int network its ip address and netmask.
		`$ sudo netAdm add -device=int -address=10.254.254.3 -netmask=255.255.255.224 -onboot=yes -bootproto=none`
		• Ping the oracle guest to verify network connectivity
		`$ ping oracle`
		• Configure the imi network with its ip address and netmask. *(mediation guest only)
		`$ sudo netAdm add -device=imi -address=x.x.x.x -netmask=x.x.x.x -onboot=yes -bootproto=none`
		• Repeat sub-steps 1 thru 5 for the application guest.

5. ☐	**IDIH CLI**: Configure the network time protocol for the mediation and application guests	• On the iDIH Mediation guest, launch the platform configuration menu. `$ sudo su - platcfg` • From the platform configuration menu, configure ntpserver1 with the ip address supplied for NTP. Navigate to **Network Configuration -> NTP -> Edit -> ntpserver1**. Select **Yes** when asked to restart NTP. • Exit the network configuration menu. • To configure the Oracle VM hostname, navigate to **Server Configuration -> Hostname -> Edit**. ***Note***: The Mediation and Application guest hostnames should follow the format **xxxx-med** and **xxxx-app**, where **xxxx** can be any valid hostname characters. • Exit the platform configuration menu. • Repeat sub-steps 1 through 5 for the iDIH Application guest.
6. ☐	**PM&C CLI**: Reset the guest creation timeout	Reset the guest creation timeout value. `$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=2000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"';`
7. ☐	**IDIH CLI**: Run the application guest post installation scipt.	• On the iDIH application guest, run the post installation script and monitor the script until it completes. $ sudo /opt/xIH/apps/install.sh

Procedure 70: Upgrade the Mediation and Application Guests

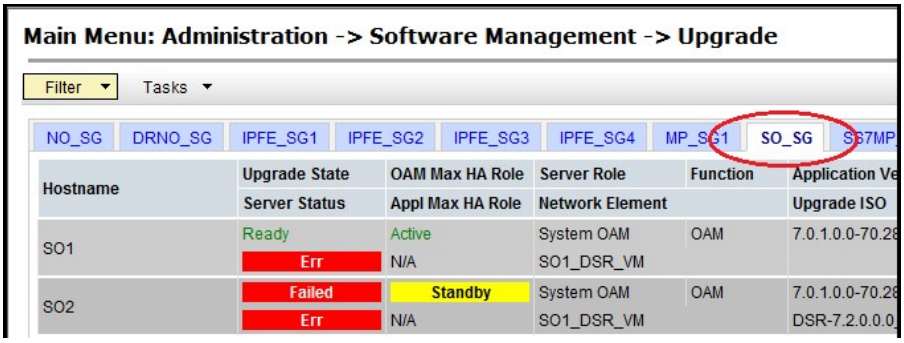
8. ☐	**IDIH CLI**: Run the mediation post installation script	• On the iDIH mediation guest, run the post installation script and monitor the script until it completes.
		`$ sudo /opt/xIH/mediation/install.sh`
		• Reconfigure the hostname in the comcol database.
		`$ sudo su - tekelec`
		`$ sudo iset -fnodeName=`hostname` -fhostName=`hostname` NodeInfo where 1=1`

9. ☐	**IDIH CLI**: Run the healthcheck scripts on the mediation and application guests	After the post installation script has completed on the application guests, run the healthcheck script on the application and mediation guests. `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`

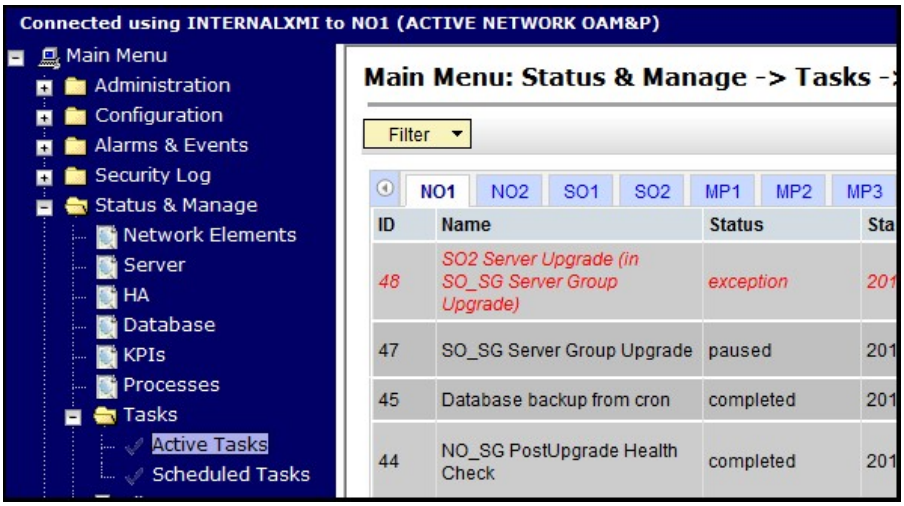
Appendix K. Recovering From A Failed Upgrade

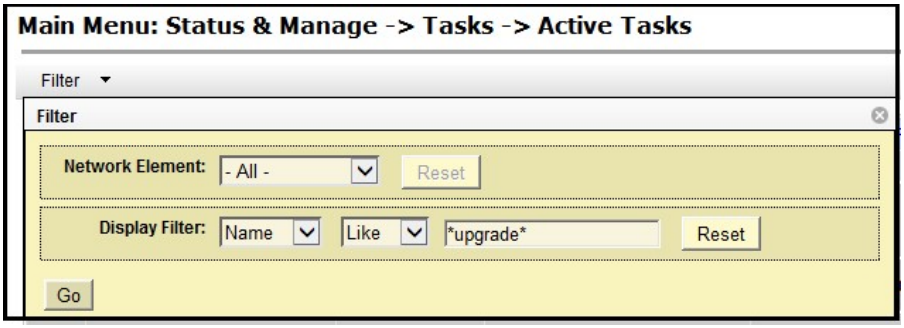
This procedure provides the steps required to recover a server after a failed upgrade. Due to the complexity of the DSR system and the nature of troubleshooting, it is recommended you contact My Oracle Customer Support for guidance while executing this procedure.

Procedure 71: Recovering from a Failed Upgrade

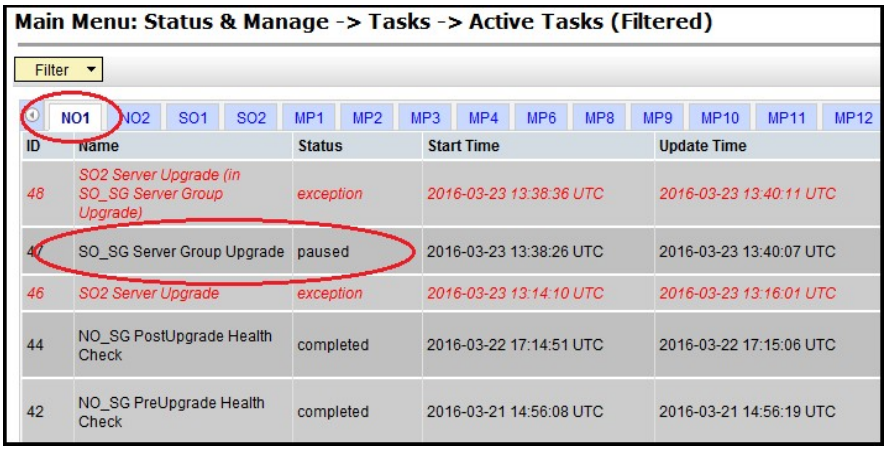
S T E P #	This procedure returns a server to a normal state after an upgrade failure. Note that the server is returned to the source release by this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Active NOAM VIP**: Select affected server group	From the Upgrade screen, select the server group containing the failed server. • Log into the NOAM GUI using the VIP. • Navigate to **Administration -> Software Management -> Upgrade**. • Select the server group tab for the server to be recovered.  If the failed server was upgraded using the **Upgrade Server** option, then skip to step 7 of this procedure If the failed server was upgraded using the **Auto Upgrade** option, then continue with step 2 of this procedure.

Procedure 71: Recovering from a Failed Upgrade

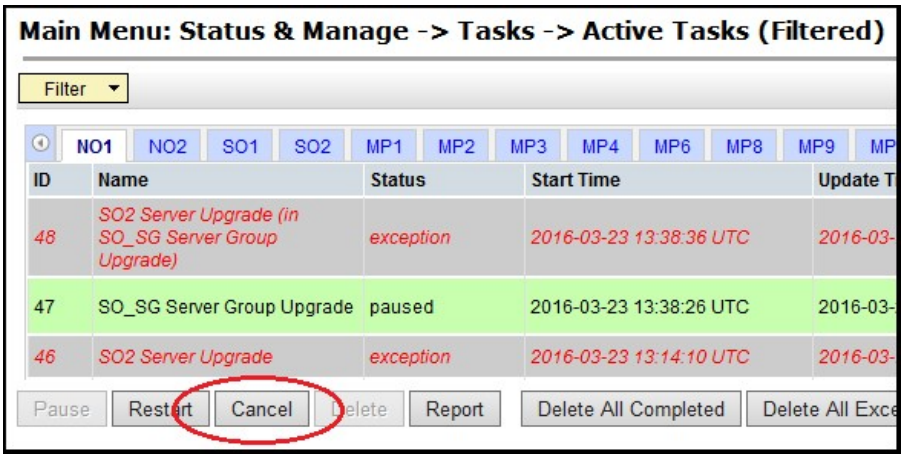
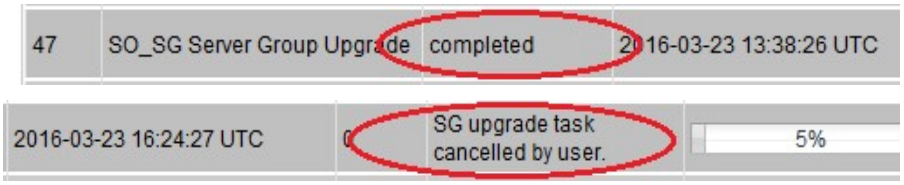
2. ☐	**Active NOAM VIP**: View active tasks	• Navigate to **Status & Manage -> Tasks -> Active Tasks**. 

3. ☐	**Active NOAM VIP**: Search for upgrade task	Use the filter to locate the server group upgrade task.
		From the active NOAM GUI:
		• Click the **Filter** list and enter the following filter values:
		  • **Network Element**: All
		  • **Display Filter**: Name
		  Like
		  upgrade
		• Click **Go**.
		 

Procedure 71: Recovering from a Failed Upgrade

4. ☐	**Active NOAM VIP**: Identify the upgrade task	In the search results list, locate the **Server Group Upgrade** task. • If not already selected, select the tab displaying the hostname of the active NOAM server. • Locate the task for the **Server Group Upgrade**. It displays a status of **paused**.  ***Note***: Consider the case of an upgrade cycle where it is seen that the upgrade of one or more servers in the server group have status as exception (i.e., 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, please cancel the running (upgrade) task for that server group before reattempting ASU for the same. **Caution**: Before clicking **Cancel** for server group uprade task, please ensure that the upgrade status of the individual servers in that particular server group should have status as completed or exception (i.e., failed for some reason). Make sure you are not cancelling any task that has some servers still in running state.

Procedure 71: Recovering from a Failed Upgrade

5. ☐	Active NOAM VIP: Cancel the upgrade task	Cancel the Server Group Upgrade task. • Click the **Server Group Upgrade** task to select it. It is highlighted on the screen. • Click **Cancel** to cancel the task. • Click **OK** on the confirmation dialog box to confirm the cancellation. 
6. ☐	**Active NOAM VIP**: Verify task cancellation	Verify the Server Group Upgrade task is cancelled. • On the active Tasks screen, verify the task that was cancelled in step 5 shows a status of **completed**. 

7. ☐	**Failed server CLI**: Inspect upgrade log	Log into the failed server to inspect the upgrade log for the cause of the failure.
		• Use an SSH client to connect to the failed server:
		`ssh <XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		• View or edit the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for clues to the cause of the upgrade failure.
		• If the upgrade log contains a message similar to the following, inspect the early upgrade log at /var/TKLC/log/upgrade/earlyChecks.log for additional clues.
		`1440613685::Early Checks failed for the next upgrade`
		`1440613691::Look at earlyChecks.log for more info`

Procedure 71: Recovering from a Failed Upgrade

<table>
<tr><td colspan="3"> 

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 you contact My Oracle Customer Support as described in Appendix M.
DO NOT PROCEED TO STEP 8 OF THIS PROCEDURE UNTIL THE ALARM CONDITION HAS BEEN CLEARED!
</td></tr>
<tr><td>8.
☐</td><td>Failed Server CLI: Verify Platform alarms are cleared</td><td>Verify all Platform alarms have been cleared from the failed server.
• Use the alarmMgr utility to verify all Platform alarms have been cleared from the system.
<code>$ sudo alarmMgr --alarmstatus</code>
Example output:
<code>[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus</code>
<code>SEQ: 2 UPTIME: 827913 BIRTH: 1458738821 TYPE: SET ALARM: TKSPLATMI10|tpdNTPDaemonNotSynchronizedWarning|1.3.6.1.4.1.323.5.3.18.3.1.3.10|32509|Communications|Communications Subsystem Failure</code>
<code>***** user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm *****</code>
<code>[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus</code>
<code>[admusr@SO2 ~]$</code></td></tr>
<tr><td>9.
☐</td><td>Active NOAM VIP: Re-execute the server upgrade</td><td>Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option.
Note: Once a server has failed while using the Automated Server Group Upgrade option, the Auto Upgrade option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the Upgrade Server option.</td></tr>
</table>

Appendix L. Workaround to Resolve DB Site Replication Alarms

This procedure is to resolve DB site replication alarms if encountered during upgrade. Database (DB) replication failure alarms may be raised during an Automated Site Upgrade (ASU) or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved.

Procedure 71 must be performed on the server(s) with the above alarms.

Procedure 72: Restart the inetrep Process on the Affected Server(s).

S T E P #	This procedure restarts the inetrep process on the server that has the DB replication failure alarm. ***Note***:All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Customer Support and ask for assistance.	
1. ☐	**Server CLI**: Log into the server	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server on which the DB replication failure alarm is seen: `ssh admusr@<server_ip>` Answer **yes** if you are asked to confirm the identity of the server.
2. ☐	**Server CLI**: Check for replication links	Check if the replication links are up by executing the below command: `irepstat` If we see that some of the B-C and C-C replication links to be down.
3. ☐	**Server CLI**: Execute command	Execute the following command to resolve the replication issue: `sudo pm.kill inetrep`
4. ☐	Repeat as needed	Repeat this procedure on each of the affected server(s).

Appendix M. My Oracle Customer Support

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

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

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

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

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

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Locate Product Documentation on the Oracle Help Center

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

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page displays. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release 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.