Oracle® Communications

Diameter Signaling Router

DSR Software Upgrade Guide

Release 8.0

E75967-02

May 2017

Oracle® Communications Diameter Signaling Router, DSR 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.

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 a major upgrade from DSR 6.0.x, 7.0.x, 7.1.x, 7.2.x, or 7.3.x to release 8.0, or an incremental upgrade from an earlier DSR 8.0 release to a later 8.0 release. The upgrade of HP C-Class blades, RMS HP servers, and VE-DSR servers 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 software upgrade.

Note: This document does not cover Cloud DSR. Refer to [16] for Cloud upgrades.

The DSR 8.0 software release includes all Oracle CGBU Platform Distribution (TPD) software. Any upgrade of TPD required to bring the DSR to release 8.0 occurs automatically as part of the DSR 8.0 software upgrade. The execution of this procedure assumes that the DSR 8.0 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 software loads. It is recommended to contact MOS for the software loads as described in Appendix S.
- Initial installation of DSR software.
- Firmware upgrade. Refer to [1] (HP) or [2] (Netra).
- PM&C upgrade. Refer to [4].
- SDS upgrade. Refer to [8].

1.2 References

[1] *HP Solutions Firmware Upgrade Pack Release Notes, E76846, Oracle*
[2] *Oracle Firmware Upgrade Pack Upgrade Guide, E70316, Oracle*
[3] *TVOE 3.3 Upgrade Document. E80323, CGBU_019811, Oracle*
[4] *PM&C 6.4 Incremental Upgrade Guide, E82636, CGBU_019931, Oracle*
[5] *DSR 5.x/6.x Software Installation Part 2/2. E52510, Oracle*
[6] *DSR 7.0/7.1 Software Installation Part 2/2, E58954, Oracle*
[7] *DSR 7.2/7.3 Software Installation Part 2/2, E69409, Oracle*
[8] *SDS 8.0 Software Upgrade Guide. E75970, Oracle*
[9] *Maintenance Window Analysis Tool, CGBU_010314, Oracle*
[10] *DSR 6.0 to 7.0 Migration – IPFE Aspects, WI007086, CGBU_770, Oracle*
[11] *Fast Deployment and Configuration Tool*, *TR007249, CGBU_ENG_24_2353, Oracle*
[12] *DSR 7.2/7.3 Disaster Recovery Guide, E69612, Oracle*
[13] *DSR 7.1.x/7.2/7.3 Rack Mount Server Disaster Recovery Guide, E66227, Oracle*
[14] *Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) In DSR 7.1 By Enabling SCTP AUTH Extensions By Default, OSD 2019141.1*
[15] *Oracle Communications Tekelec Platform 7.0.x Configuration Guide, E53486, Oracle*
[16] *DSR 8.0 Cloud Software Upgrade Guide, E75969, CGBU_018978, Oracle*

1.3 Acronyms

Table 1: Acronyms

ASG	Automated Server Group upgrade
CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
cSBR	Charging Session Binding Repository
DA	Diameter Agent
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
iLO	Integrated Lights Out (HP)
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
LOM	Lights Out Manager (Netra)
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NOAM	Network OAM
OA	HP Onboard Administrator
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent

Table 1: Acronyms

PM&C / PMAC	Platform Management and Configuration
RMS	Rack Mount Server
SBR	Session Binding Repository
SDS	Subscriber Database Server
SOAM	System OAM
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualized Operating Environment
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

Upgrade	The process of converting an application from its current release on a system to a newer release.
Major Upgrade	An upgrade from one DSR release to another DSR release. E.g. DSR 6.0 to DSR 8.0.
Incremental Upgrade	An upgrade within a given DSR release e.g. 8.0..x to 8.0.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Source release	Software release to upgrade from.
Target release	Software release to upgrade to.
Single Server Upgrade	The process of converting a DSR 6.0/7.0.x/7.1.x/7.2/7.3 server from its current release to a newer release.
Blade (or Managed Blade) Upgrade	Single Server upgrade performed on a blade. This upgrade requires the use of the PM&C GUI.
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.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.

Primary NOAM Network Element	The network element that contains the Active and Standby NOAM servers in a DSR. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same.
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.
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’.
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’.
Health Check	Procedure used to determine the health and status of the DSR‘s internal network. This includes status displayed from the DSR GUI and PM&C GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
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. The state is defined by the following attributes: A backup file is present in /var/TKLC/db/filemgmt Not in “Accept or Reject” state
UI	User interface. Platcfg UI refers specifically to the Platform Configuration Utility User Interface which is a text-based user interface.
Management Server	Server deployed with HP c-class or RMS used to host PM&C application, to configure Cisco 4948 switches, and to serve other configuration purposes.
PM&C Application	PM&C is an application that provides platform-level management functionality for HPC/RMS system, such as the capability to manage and provision platform components of the system so it can host applications.
1+1	Setup with one Active and one Standby DA-MP.
N+0	Setup with N active DA-MP(s) but no standby DA-MP.
NOAM	Network OAM for DSR.
SOAM	System OAM for DSR.
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (Active/Standby) policy to N+ 0 (Multiple Active) policies.
RMS geographic site	Two rack-mount servers that together host 1) a NOAM HA pair; 2) a SOAM HA pair; 3) two DA-MPs in either a 1+1 or N+0 configuration; 4) optional IPFE(s); 5) optional IDIH
RMS Diameter site	One RMS geographic site implemented as a single Diameter network element.

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.
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.

1.5 How to Use this Document

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

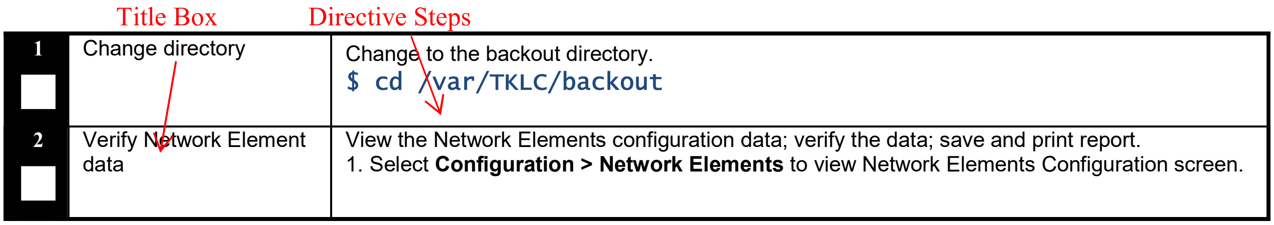
1) Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2) Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
3) If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact MOS for assistance, as described in Appendix S, before attempting to continue.

1.5.1 Executing Procedures

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

- Each step has a checkbox that 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.

Figure 1. Example Procedure steps used in this document


Title Box
Directive Steps

1 □	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2 □	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 1. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

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. However, primary and DR NOAM (if equipped) Network Element servers should be upgraded within the same 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 to contact MOS as directed in Appendix S 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 prior to the start of a major upgrade to DSR 8.0.

!! WARNING!! **THE UPGRADE TO RELEASE 8.0 WILL FAIL 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 will allow the upgrade to proceed.

Refer to Appendix D: 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:

1. The PCA/PDRA application has not been activated
2. When upgrading from release 7.1, 7.2, or 7.3 to 8.0 (in this case, pooling migration has already completed)
3. 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 prior to 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 to contact MOS per Appendix S 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.

1. Verify that all APNs are mapped to the "Default" PCRF Pool
   - This ensures that only one binding exists for a given subscriber even after enabling PCRF Pooling.
2. Configure ingress mediation rule to add a Called-Station-Id AVP (code=30, RFC 4005) to binding dependent session creation Diameter messages (for 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.
3. Configure egress mediation rule to remove the Called-Station-Id AVP if it was added by mediation at ingress.
4. Enable PCRF Pooling and wait for the migration to complete
   - All PCRF Pooling configuration requirements for binding capable interfaces must still be met.
5. 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.

1. Build patches on a customer-to-customer basis.
   a. The patch will:
      - 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.

   b. Verify that all APNs are mapped to the "Default" PCRF Pool
      - This ensures that 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.
2. Upgrade to DSR 8.0

1.7.3 Obsolete Hardware Check

Due to the enhanced processing capabilities and requirements of DSR Release 8.0, HP Gen6 and Gen7 hardware are NOT supported. All Gen6 and Gen7 blades must be replaced with supported hardware before upgrading to release 8.0.

🛑	**!! WARNING!!**	**HP GEN6 AND GEN7 HARDWARE ARE NOT SUPPORTED IN DSR 8.0. ALL GEN6 AND GEN7 BLADES MUST BE REPLACED WITH SUPPORTED HARDWARE PRIOR TO UPGRADING TO 8.0.**

1.7.4 Netbackup 7.7 Support

Netbackup 7.7 requires additional disk space that is not available prior to 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 PRIOR TO UPGRADING TO NETBACKUP 7.7.**

1.7.5 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 79 in Appendix O must be executed to prepare the systems running IDIH Release 8.0 to support IDIH systems running the prior release. After executing Procedure 79, network traces should be viewed only from an IDIH system running the prior IDIH release. Viewing a network trace from an IDIH 8.0 will result in a visualization that is incomplete because the IDIH 8.0 system will fail 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 80 should be executed on each IDIH system where Procedure 79 was previously executed to ensure that no errors occur when viewing network traces.

1.7.6 Review Release Notes

Before starting the upgrade, it is recommended to review the Release Notes for the DSR 8.0 release to understand the functional differences and possible traffic impacts of the upgrade.

2 GENERAL DESCRIPTION

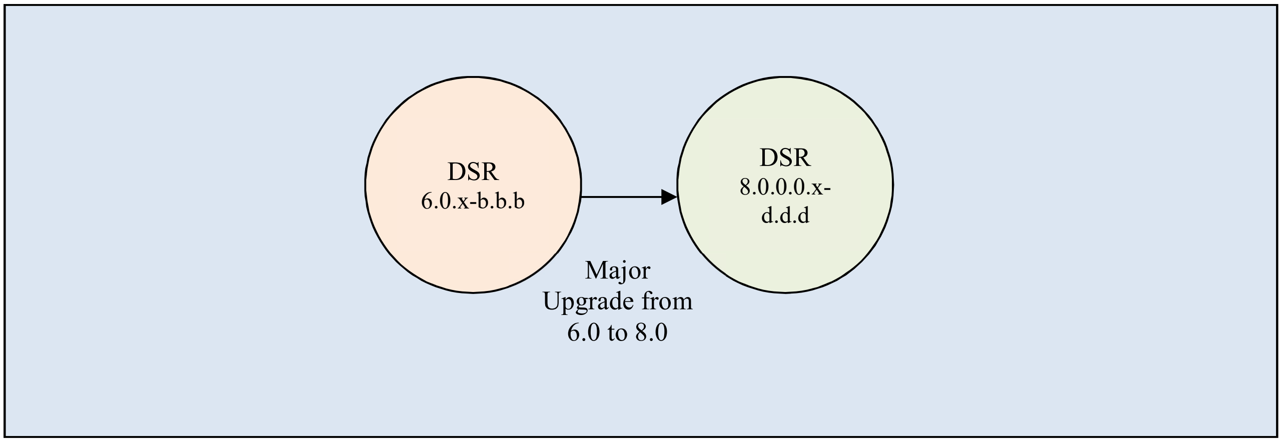
This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from the source release to the target release. An incremental upgrade advances the DSR from an earlier DSR 8.0 source release to later version of the same target release.

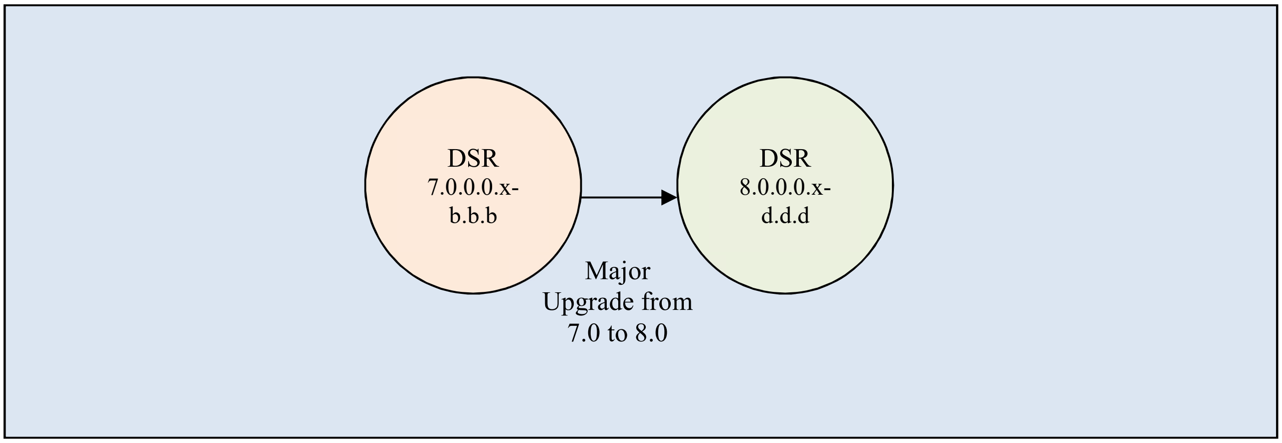
Note that for any incremental upgrade, the source and target releases must have the same value of “x”. For example, advancing a DSR from 8.x.0-80.1.0 to 8.x.0-80.2.0 is an incremental upgrade. But advancing a DSR running a 6.0 release to an 8.0 target release constitutes a major upgrade.

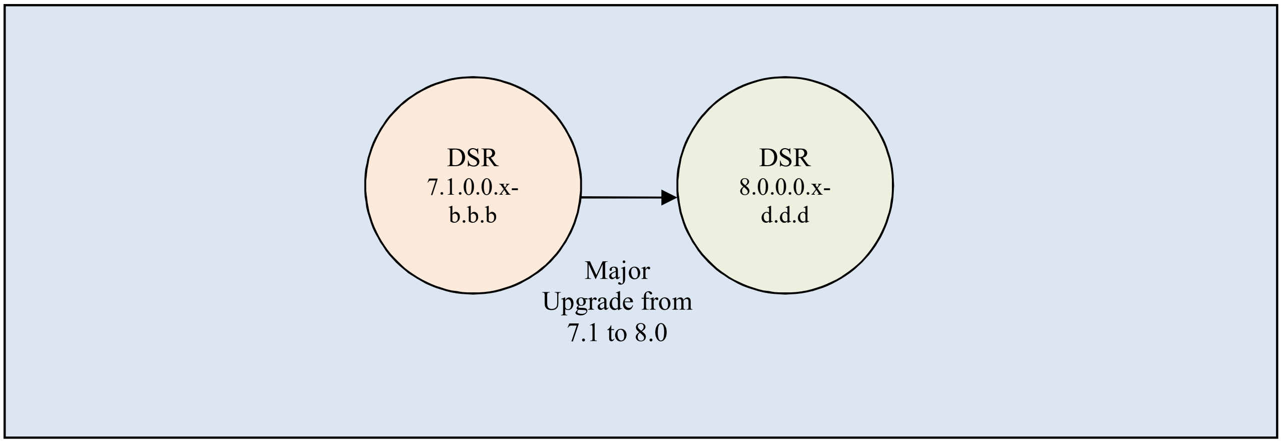
2.1 Supported Upgrade Paths

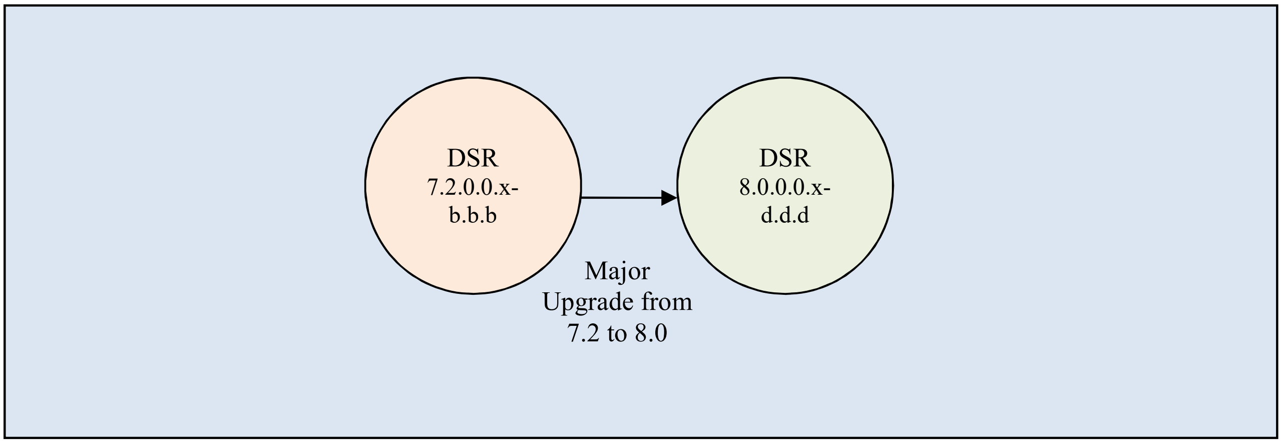
The supported upgrade paths to a DSR 8.0 target release are shown in Figure 2 below.
NOTE: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.

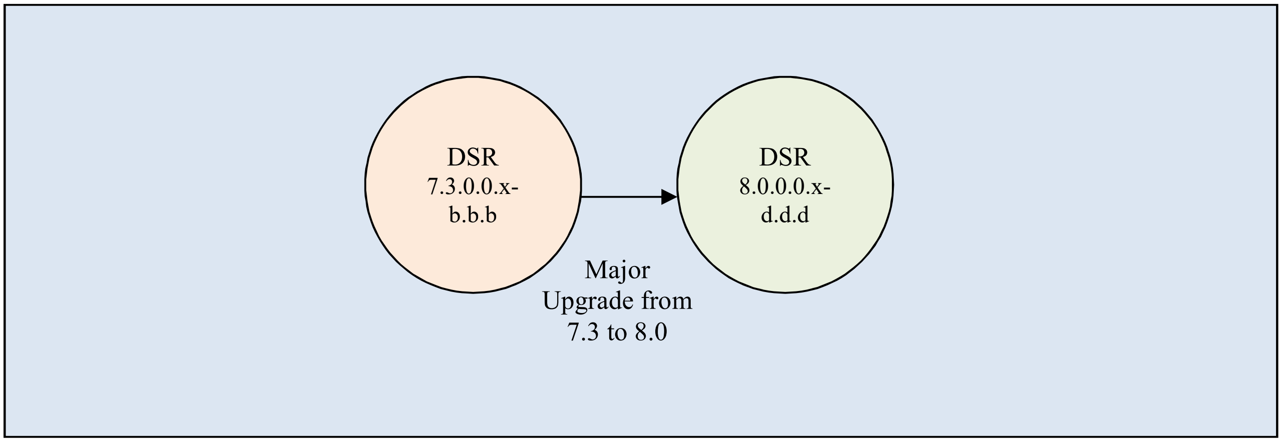
Figure 2. DSR 8.0 Supported Upgrade Paths

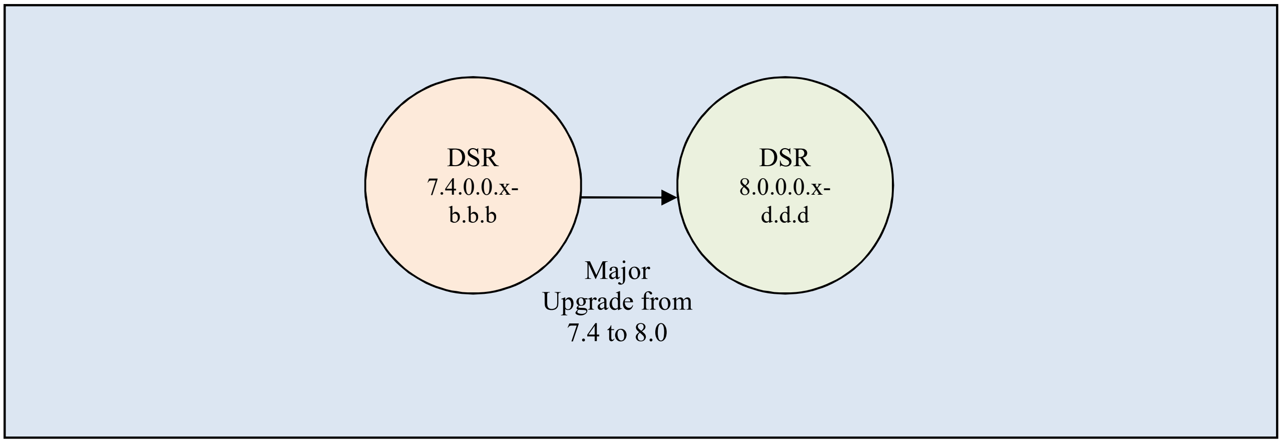


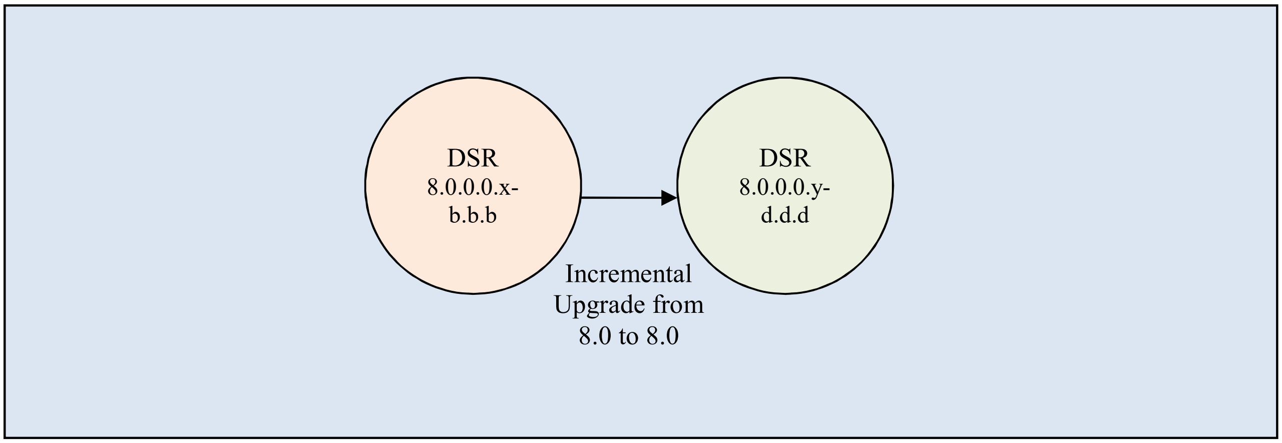



DSR
7.1.0.0.x-
b.b.b
DSR
8.0.0.0.x-
d.d.d
Major
Upgrade from
7.1 to 8.0


DSR
7.2.0.0.x-
b.b.b
DSR
8.0.0.0.x-
d.d.d
Major
Upgrade from
7.2 to 8.0


DSR
7.3.0.0.x-
b.b.b
DSR
8.0.0.0.x-
d.d.d
Major
Upgrade from
7.3 to 8.0


DSR
7.4.0.0.x-
b.b.b
DSR
8.0.0.0.x-
d.d.d
Major
Upgrade from
7.4 to 8.0


DSR
8.0.0.0.x-
b.b.b
DSR
8.0.0.0.y-
d.d.d
Incremental
Upgrade from
8.0 to 8.0

2.2 Supported Hardware

This section is not applicable to Software Centric upgrades.

Due to the enhanced processing capabilities and requirements of DSR Release 8.0, HP Gen6 and Gen7 hardware are NOT supported. All Gen6 and Gen7 blades must be replaced with supported hardware before upgrading to release 8.0.

!! WARNING!! **HP GEN6 AND GEN7 HARDWARE ARE NOT SUPPORTED IN DSR 8.0. ALL GEN6 AND GEN7 BLADES MUST BE REPLACED WITH SUPPORTED HARDWARE PRIOR TO UPGRADING TO 8.0.**

2.3 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.

2.4 Firmware Updates

This section is not applicable to Software Centric upgrades.

Firmware upgrades are not in the scope of this document, but may be required before upgrading DSR. It is assumed that these are completed when needed by the hardware, and there is typically not a dependency between a firmware version and the DSR release. See the DSR Release Notes for any dependencies.

2.5 TVOE Upgrade

TVOE (Virtual Operating Environment) is a hypervisor, which hosts multiple virtual servers on the same hardware. It is typically used to make more efficient use of a hardware server (Rack Mount or Blade), while maintaining application independence, for DSR applications that do not require the full resources of a modern hardware server.

In DSR architecture, TVOE Hosts are typically used to host several functions, including:

- PM&C
- DSR NOAM and SOAM Applications
- SDS SOAM Applications
- IDIH

(TVOE Host servers may also be used to host other DSR functions, including DA-MPs and IPFEs in a small deployment.)

TVOE Host servers (i.e. servers running TVOE + one or more DSR applications) must be upgraded before upgrading the guest applications, to assure compatibility. However, TVOE is backward compatible with older application versions, so the TVOE Host and the applications do not have to be upgraded in the same maintenance window.

The TVOE server hosting PM&C, as well as the PM&C application, must be upgraded before other TVOE host upgrades, since PM&C is used to perform the TVOE upgrades.

There are three supported strategies for site TVOE upgrades (Options A, B and C):

- Option A: Upgrade TVOE environments as a separate activity that is planned and executed days or weeks before the application upgrades (perhaps site-at-a-time)
- Options to Upgrade TVOE and applications in the same maintenance window:

- Option B: Upgrade a TVOE and application, followed by another TVOE and application. For example: for Standby SOAM Upgrade – stop the application, upgrade TVOE, upgrade the application, start the application; then repeat for the Active SOAM.(Preferred)
- Option C: Upgrade multiple TVOE Hosts at a site, and then start upgrading the applications (same maintenance window)

Note that TVOE upgrades require a brief shutdown of the guest application(s) on the server. Note also that the TVOE virtual hosts may be hosting NOAM or SOAM applications. These applications will also be affected, including a forced switchover if the Active NOAM/SOAM is shutdown.
The procedure for upgrading TVOE environments in advance of the application upgrades (Option A) is documented in Section 3.4.6.

2.6 PM&C (Management Server) Upgrades

Each site may have a PM&C (Management Server) that provides support for maintenance activities at the site. The upgrade of the PM&C (and the associated TVOE) is documented in a separate procedure (see Ref [4]). PM&C must be upgraded before the other servers at the site are upgraded.

If a PM&C upgrade is required, this activity will be directed in Section 3.3.1 of this document.

2.7 SDS Upgrade

It is recommended to upgrade the SDS topology (NOAMs, SOAMs, DPs) before the DSR topology. See [8] for SDS upgrade documentation.

2.8 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 [14]. It is highly recommended that customers upgrading to Release 8.0 should prepare clients before the DSR is upgraded. This will ensure the DSR-to-Client SCTP connection will establish 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 that the SCTP connections do not re-establish after the upgrade, follow the Disable/Enable DTLS procedure in [7].

2.9 RMS Deployments

All RMS deployments are 3-Tier. In these smaller deployments, the Message Processing (DA-MP and IPFE) servers are also virtualized (deployed on a Hypervisor Host) to reduce the number of servers required.

When an RMS-based DSR has no geographic redundancy, there is just a single RMS geographic site, functioning as a single RMS Diameter site. The upgrade of this DSR deployment should be done in two maintenance windows: one for the NOAMs, and the second for all remaining servers.

When an RMS-based DSR includes geographic redundancy, there are two RMS geographic sites (but still functioning as a single RMS Diameter site). The primary RMS site contains the NOAM active/standby pair that manages the network element, while the geo-redundant RMS site contains a disaster recovery NOAM pair. Each RMS geographic site includes its own SOAM pair, but only the SOAMs at the primary RMS site are used to manage the signaling network element. The SOAMs at the geo-redundant site are for backup purposes only.

The upgrade of an RMS DSR deployment should be done in three maintenance windows: one for the NOAMs; a second for the SOAMs and MPs (DA-MP and IPFE) at the geo-redundant backup RMS site; and a third for the SOAMs and MPs (DA-MP and IPFE) at the primary RMS site.

2.10 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 will upgrade an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade will automatically prepare the server(s), perform the upgrade, and then sequence 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, Auto Site Upgrade cannot be used to upgrade PMAC, TVOE, or 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 will be upgraded with the Site 1 SOA server group, and SOB-sp will be upgraded with the Site 2 SOB server group. The MP server groups will be upgraded in the same maintenance window as their respective site SOAMs. These sites conform to the **Topological Site** definition of Table 2: Terminology.

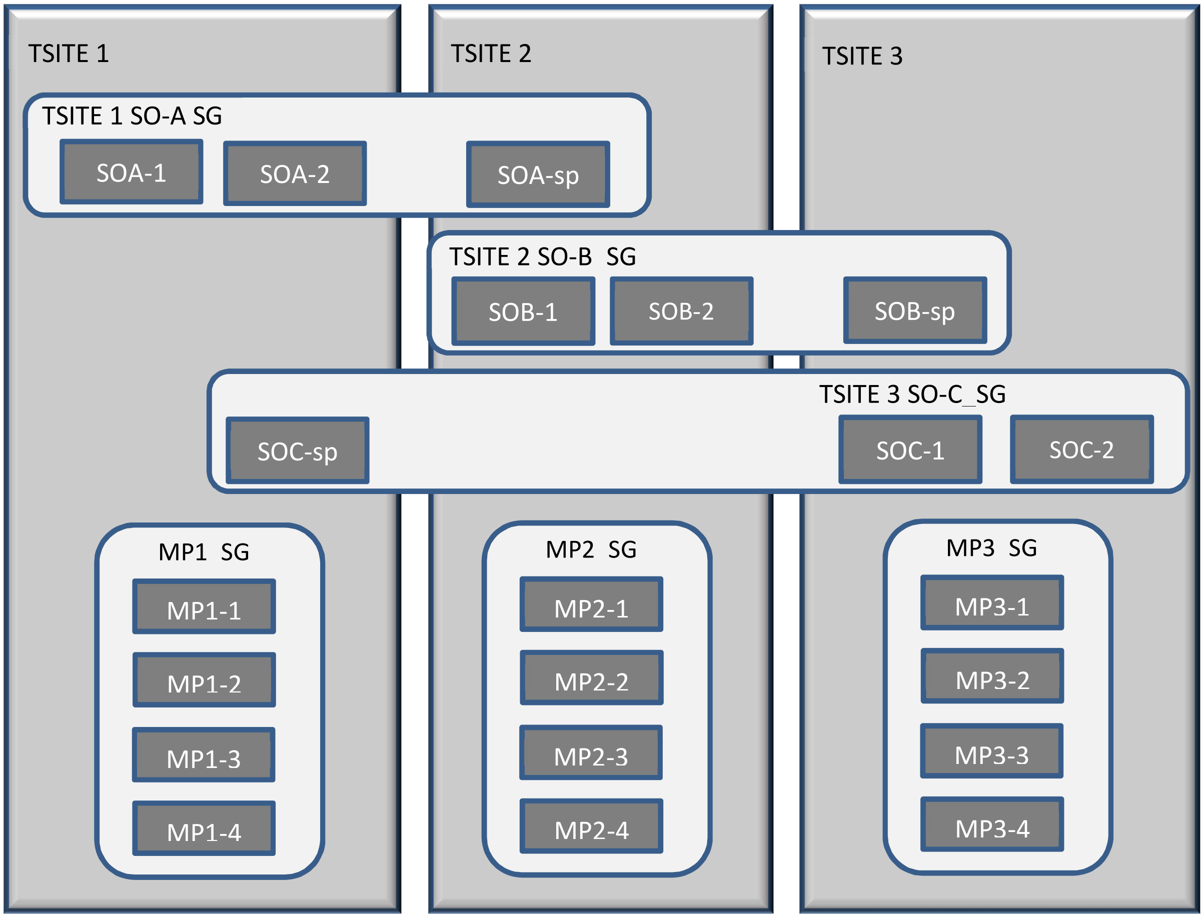
With this feature, a site upgrade can be initiated on SO-A SG and all of its children (in this example, MP1 SG) using a minimum of GUI selections. The upgrade will perform the following actions:

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

Server Groups that span sites (e.g., SOAMs and SBRs) will be upgraded with the Server Group to which the server belongs. This will result 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: Auto Site Upgrade will not automatically initiate the upgrade of TSite 2 in parallel with TSite 1. However, the feature will allow the user to *manually* initiate Auto Site Upgrade of multiple sites in parallel.

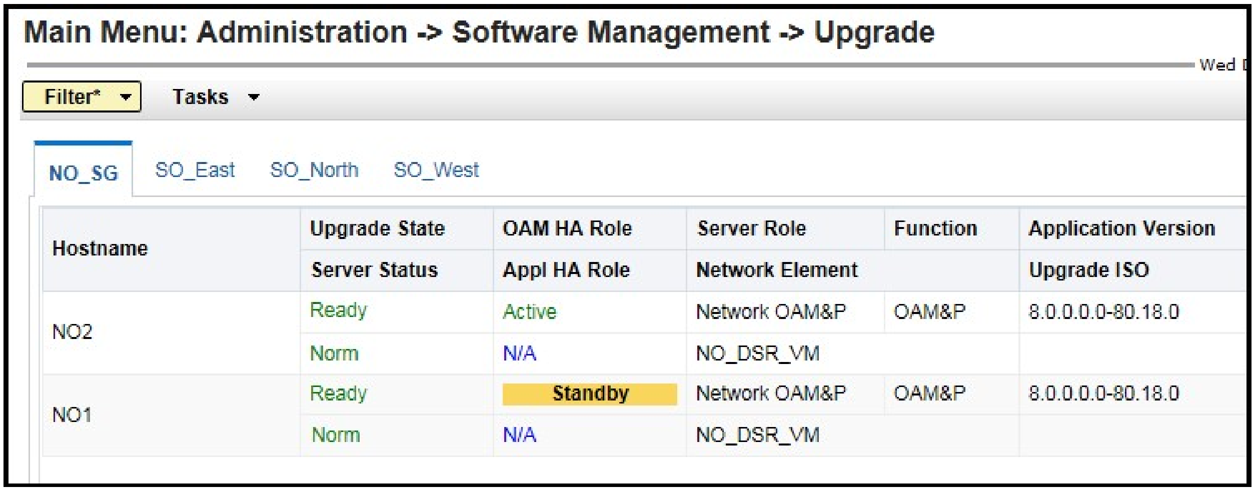
Figure 3. Upgrade Perspective of DSR "Site" Topology.



2.10.1 Site Upgrade Execution

With Auto 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, the **Auto Upgrade** button refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature becomes available once a SOAM server group tab is selected. The SOAM server group tabs correspond to the topological sites (TSites).

Figure 4. Site Upgrade - NOAM View.



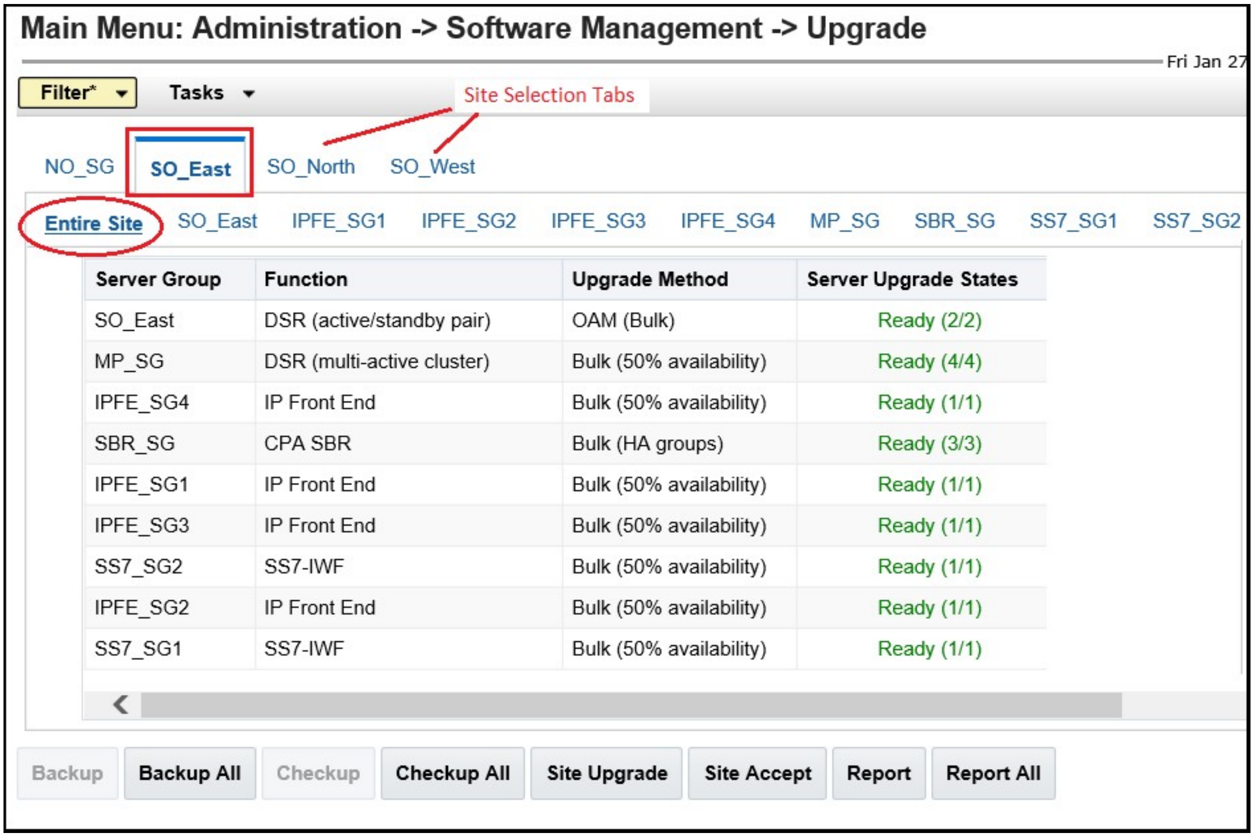
Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO2	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Norm	N/A	NO_DSR_VM		
NO1	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Norm	N/A	NO_DSR_VM		

Upon selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen is displayed (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 2.10.3 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.



Server Group	Function	Upgrade Method	Server Upgrade States
SO_East	DSR (active/standby pair)	OAM (Bulk)	Ready (2/2)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Ready (4/4)
IPFE_SG4	IP Front End	Bulk (50% availability)	Ready (1/1)
SBR_SG	CPA SBR	Bulk (HA groups)	Ready (3/3)
IPFE_SG1	IP Front End	Bulk (50% availability)	Ready (1/1)
IPFE_SG3	IP Front End	Bulk (50% availability)	Ready (1/1)
SS7_SG2	SS7-IWF	Bulk (50% availability)	Ready (1/1)
IPFE_SG2	IP Front End	Bulk (50% availability)	Ready (1/1)
SS7_SG1	SS7-IWF	Bulk (50% availability)	Ready (1/1)

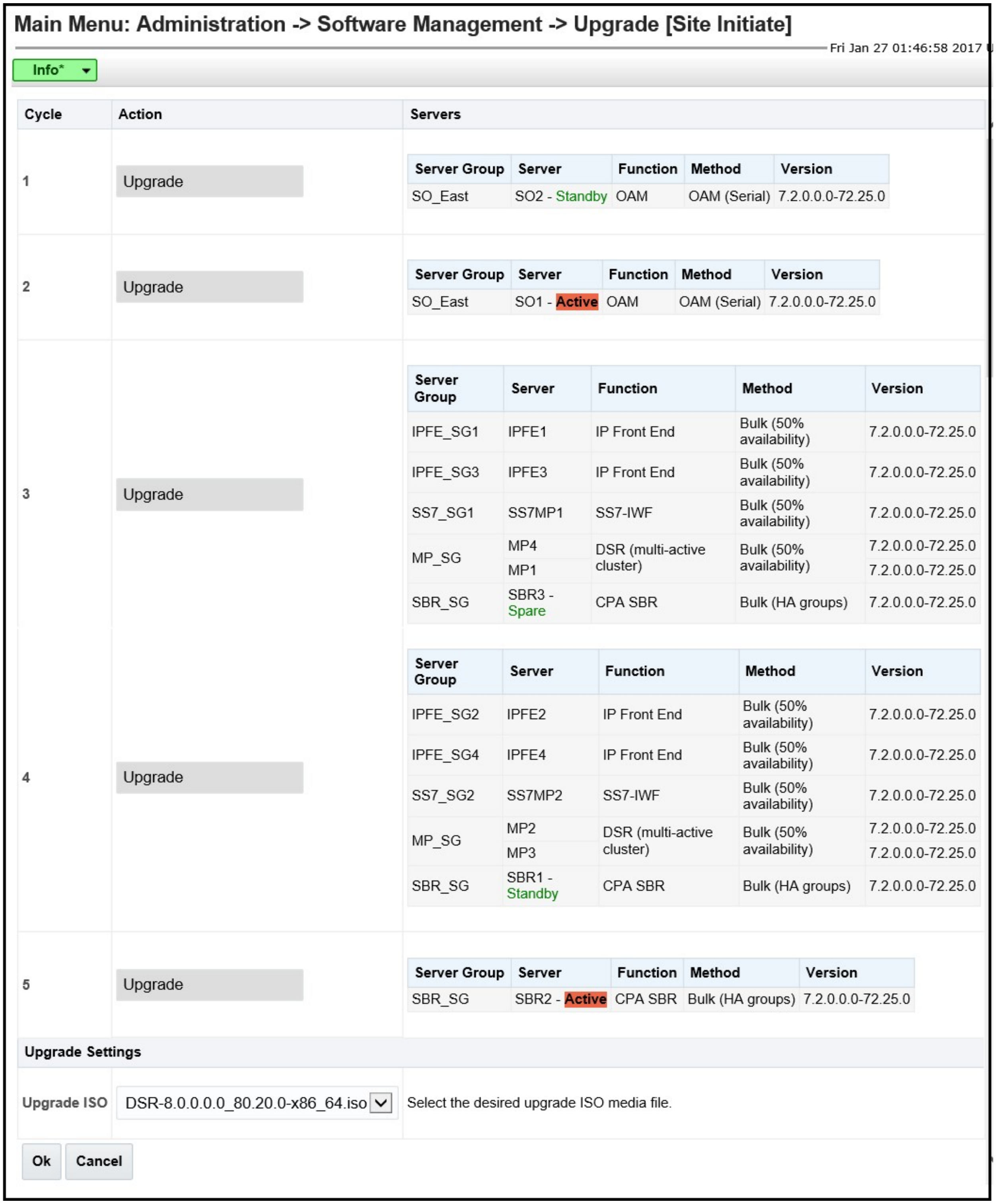
For a server to be considered “Ready” for upgrade, the following conditions must hold true:

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

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

Selecting the **Site Upgrade** button from the **Entire Site** view produces 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 will upgrade the Spare and Standby SOAMs in parallel. (Note: this scenario assumes default settings for the site upgrade options. These options are described in Section 2.10.3.) The specific servers to be upgraded in each cycle are identified in the **Servers** column of the **Site Initiate** display. 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 will not begin until Cycle 2 is complete.

Figure 6. Site Upgrade - [Site Initiate] screen.



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

Fri Jan 27 01:46:58 2017

Cycle	Action	Server Group	Server	Function	Method	Version
1	Upgrade	SO_East	SO2 - Standby	OAM	OAM (Serial)	7.2.0.0.0-72.25.0
2	Upgrade	SO_East	SO1 - Active	OAM	OAM (Serial)	7.2.0.0.0-72.25.0
3	Upgrade	IPFE_SG1	IPFE1	IP Front End	Bulk (50% availability)	7.2.0.0.0-72.25.0
		IPFE_SG3	IPFE3	IP Front End	Bulk (50% availability)	7.2.0.0.0-72.25.0
		SS7_SG1	SS7MP1	SS7-IWF	Bulk (50% availability)	7.2.0.0.0-72.25.0
		MP_SG	MP4 MP1	DSR (multi-active cluster)	Bulk (50% availability)	7.2.0.0.0-72.25.0 7.2.0.0.0-72.25.0
		SBR_SG	SBR3 - Spare	CPA SBR	Bulk (HA groups)	7.2.0.0.0-72.25.0
4	Upgrade	IPFE_SG2	IPFE2	IP Front End	Bulk (50% availability)	7.2.0.0.0-72.25.0
		IPFE_SG4	IPFE4	IP Front End	Bulk (50% availability)	7.2.0.0.0-72.25.0
		SS7_SG2	SS7MP2	SS7-IWF	Bulk (50% availability)	7.2.0.0.0-72.25.0
		MP_SG	MP2 MP3	DSR (multi-active cluster)	Bulk (50% availability)	7.2.0.0.0-72.25.0 7.2.0.0.0-72.25.0
		SBR_SG	SBR1 - Standby	CPA SBR	Bulk (HA groups)	7.2.0.0.0-72.25.0
5	Upgrade	SBR_SG	SBR2 - Active	CPA SBR	Bulk (HA groups)	7.2.0.0.0-72.25.0

Upgrade Settings

Upgrade ISO	DSR-8.0.0.0.0_80.20.0-x86_64.iso	Select the desired upgrade ISO media file.

Cycles 3 through 5 will 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 will allow 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 2.10.2.

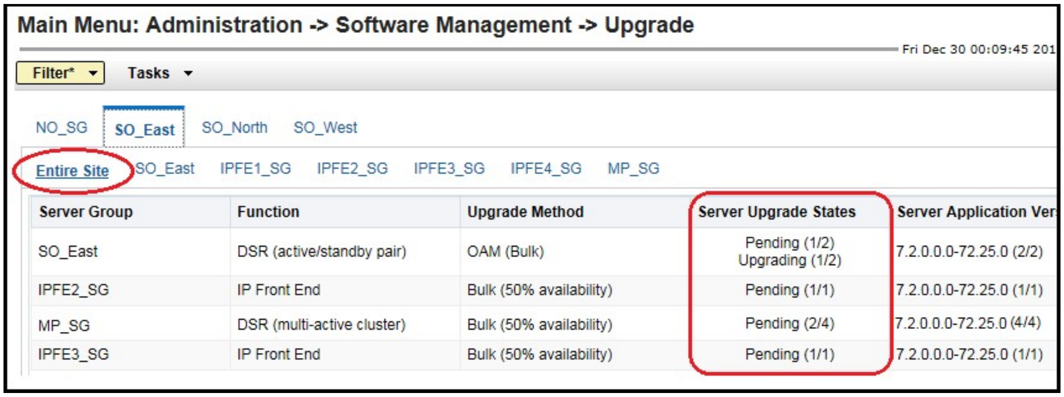
Table 3. Server Selection vs Server Group Function

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 will be 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 Auto 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 2.10.3.
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 will never be upgraded at the same time as IPFE A2. They will always be 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 picklist in the **Upgrade Settings** section of the **[Site Initiate]** screen (Figure 6). Once the **Ok** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 7). With the **Entire Site** link selected, a summary of the upgrade status for the selected site is displayed. 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



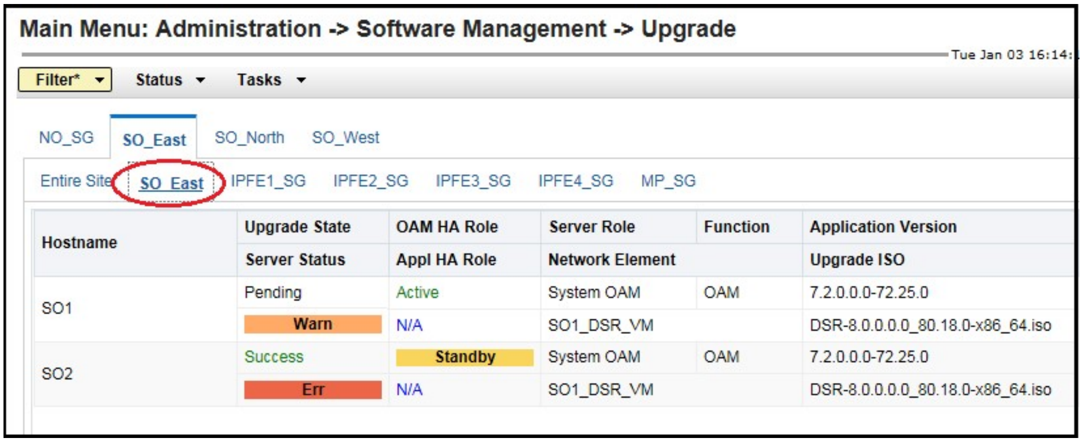
Main Menu: Administration -> Software Management -> Upgrade

Fri Dec 30 00:09:45 201

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Ver
SO_East	DSR (active/standby pair)	OAM (Bulk)	Pending (1/2) Upgrading (1/2)	7.2.0.0.0-72.25.0 (2/2)
IPFE2_SG	IP Front End	Bulk (50% availability)	Pending (1/1)	7.2.0.0.0-72.25.0 (1/1)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Pending (2/4)	7.2.0.0.0-72.25.0 (4/4)
IPFE3_SG	IP Front End	Bulk (50% availability)	Pending (1/1)	7.2.0.0.0-72.25.0 (1/1)

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

Figure 8. Server Group Upgrade Monitoring



Main Menu: Administration -> Software Management -> Upgrade

Tue Jan 03 16:14:

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SO1	Pending	Active	System OAM	OAM	7.2.0.0.0-72.25.0
	Warn	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso
SO2	Success	Standby	System OAM	OAM	7.2.0.0.0-72.25.0
	Err	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso

Upon completion of a successful upgrade, every server in the site will be in the “Accept or Reject” state. See Section 2.10.4 for a description of canceling and restarting the Auto Site Upgrade.

2.10.2 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 will remain in service while four upgrade. However, if there are nine server of type 'X', then the minimum availability requires that five remain in service while four upgrade. The minimum availability calculation automatically rounds up in the event of a non-zero fractional remainder.

To meet the needs of a wide-ranging customer base, the minimum availability percentage is a user-configurable option. The option allows for settings of 50%, 66%, and 75% minimum availability. There is also a setting of 0% for lab upgrade support. This option is described in detail in Section 2.10.3.

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

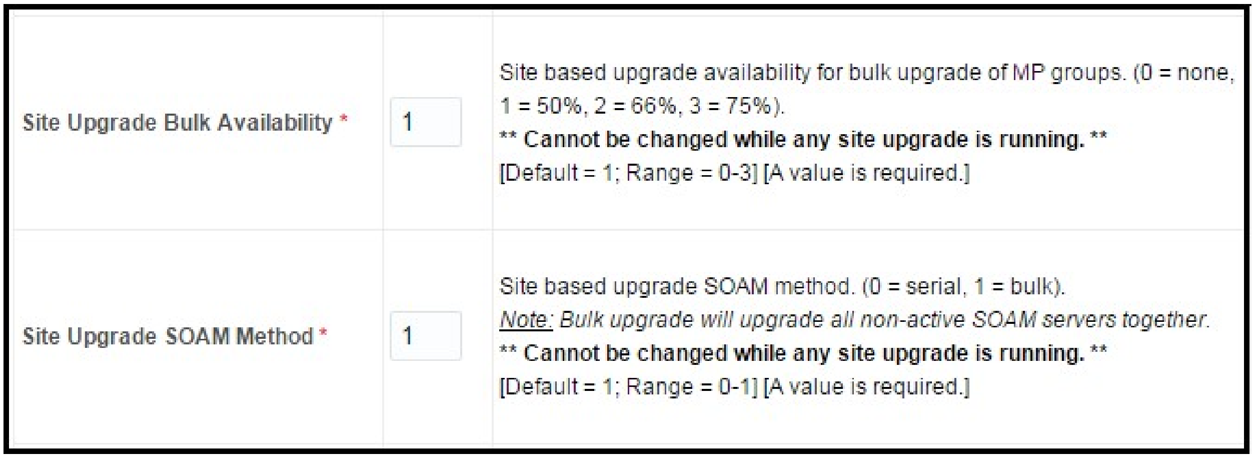
Server Group Function	Server Availability
DSR (multi-active cluster)	In a multi-active cluster, the availability percentage applies to all of the servers in the server group. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.
SBR	Availability 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 will not be upgraded together, and IPFE-B1 and IPFE-B2 will not be 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.

2.10.3 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. Auto Site Upgrade General Options.



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

The first option that affects the upgrade sequence is the "**Site Upgrade SOAM Method**". This option determines the sequence in which the SOAMs will be 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 will always be 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:

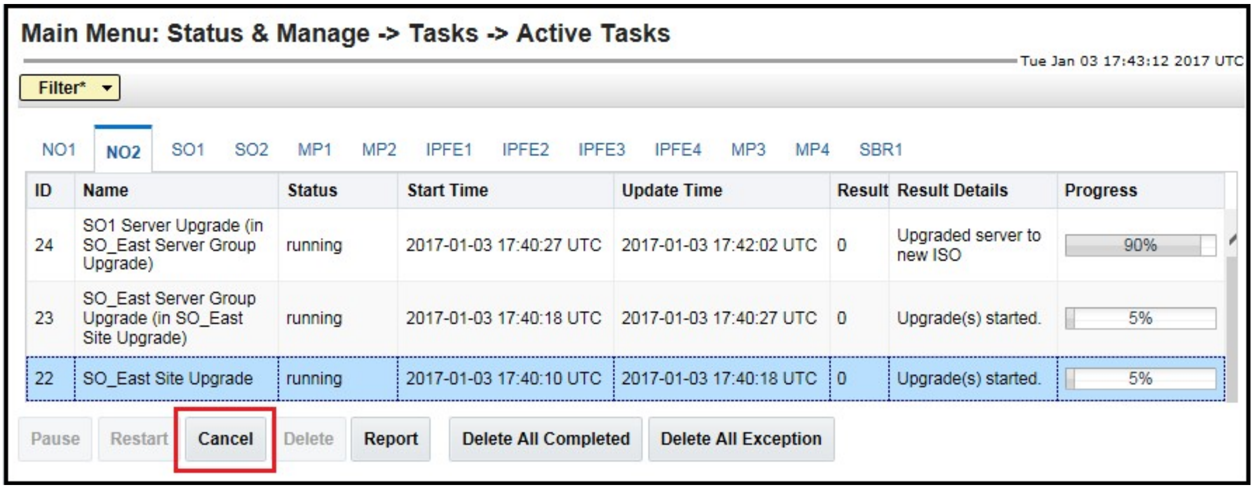
```
[Error Code xxx] - Option cannot be changed because one or more automated
site upgrades are in progress
```

2.10.4 Canceling and Restarting Auto Site Upgrade

When an Auto Site Upgrade is initiated, several tasks are created to manage the upgrade of the individual server groups as well as the servers within the server groups. These tasks can be monitored and managed 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



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

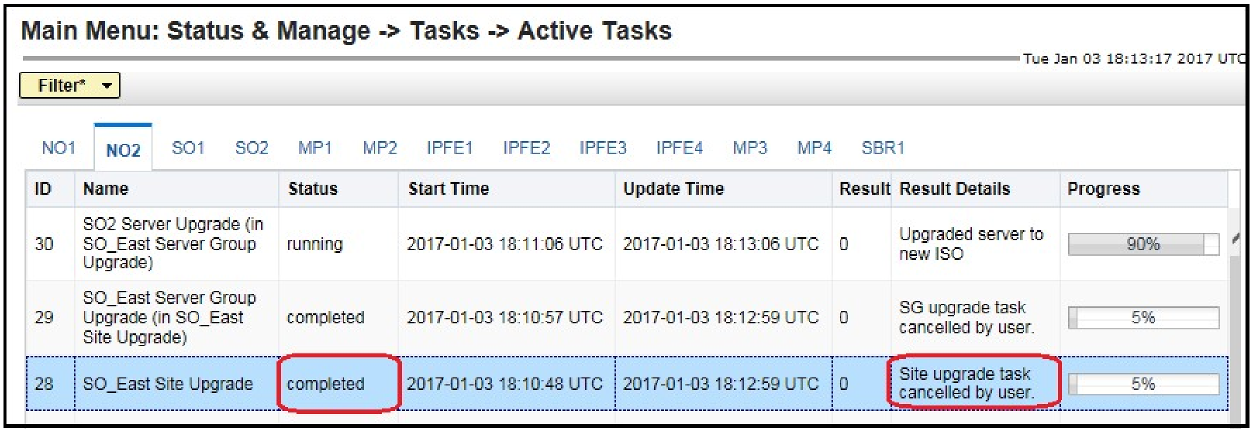
Tue Jan 03 17:43:12 2017 UTC

ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress
24	SO1 Server Upgrade (in SO_East Server Group Upgrade)	running	2017-01-03 17:40:27 UTC	2017-01-03 17:42:02 UTC	0	Upgraded server to new ISO	90%
23	SO_East Server Group Upgrade (in SO_East Site Upgrade)	running	2017-01-03 17:40:18 UTC	2017-01-03 17:40:27 UTC	0	Upgrade(s) started.	5%
22	SO_East Site Upgrade	running	2017-01-03 17:40:10 UTC	2017-01-03 17:40:18 UTC	0	Upgrade(s) started.	5%

To cancel the site upgrade, select the site upgrade task and click the **Cancel** button. A popup dialog box will request 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 will continue to completion. Figure 11 shows the Active Task screen after a site upgrade has been canceled.

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

Figure 11. Canceled Site Upgrade Tasks.



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

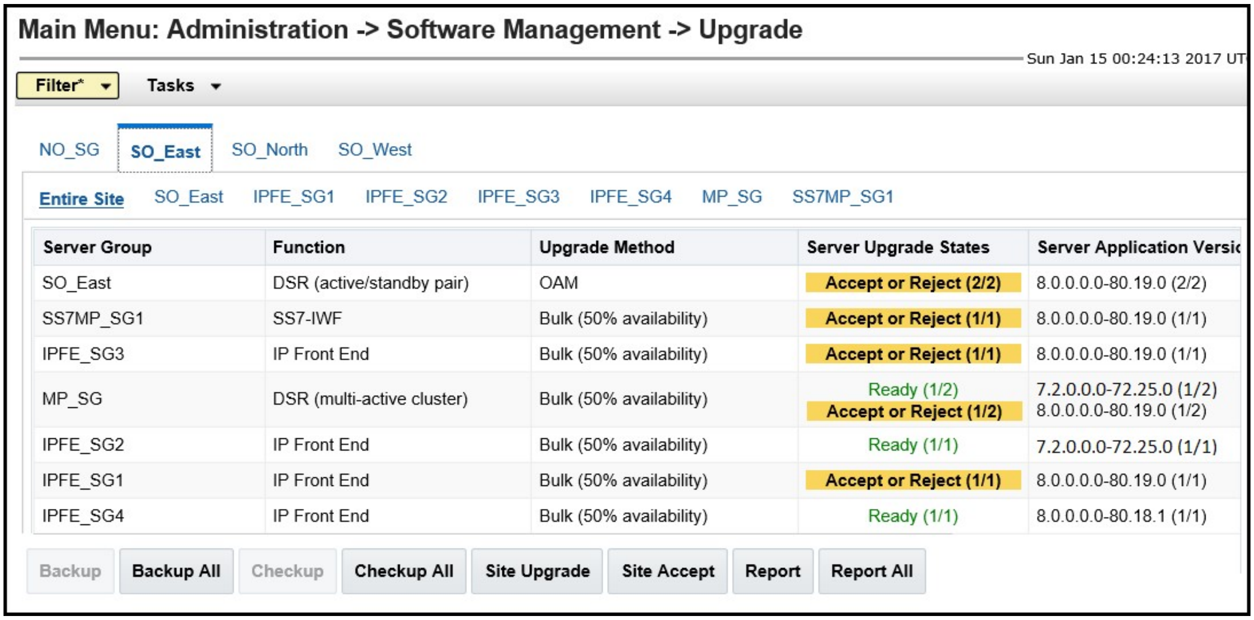
Tue Jan 03 18:13:17 2017 UTC

ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress
30	SO2 Server Upgrade (in SO_East Server Group Upgrade)	running	2017-01-03 18:11:06 UTC	2017-01-03 18:13:06 UTC	0	Upgraded server to new ISO	90%
29	SO_East Server Group Upgrade (in SO_East Site Upgrade)	completed	2017-01-03 18:10:57 UTC	2017-01-03 18:12:59 UTC	0	SG upgrade task cancelled by user.	5%
28	SO_East Site Upgrade	completed	2017-01-03 18:10:48 UTC	2017-01-03 18:12:59 UTC	0	Site upgrade task cancelled by user.	5%

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

To retstart the upgrade all that is required is to verify that the **Entire Site** link is selected, then click the **Site Upgrade** button. The **Upgrade [Site Initiate]** screen is displayed.

Figure 12. Partially Upgraded Site



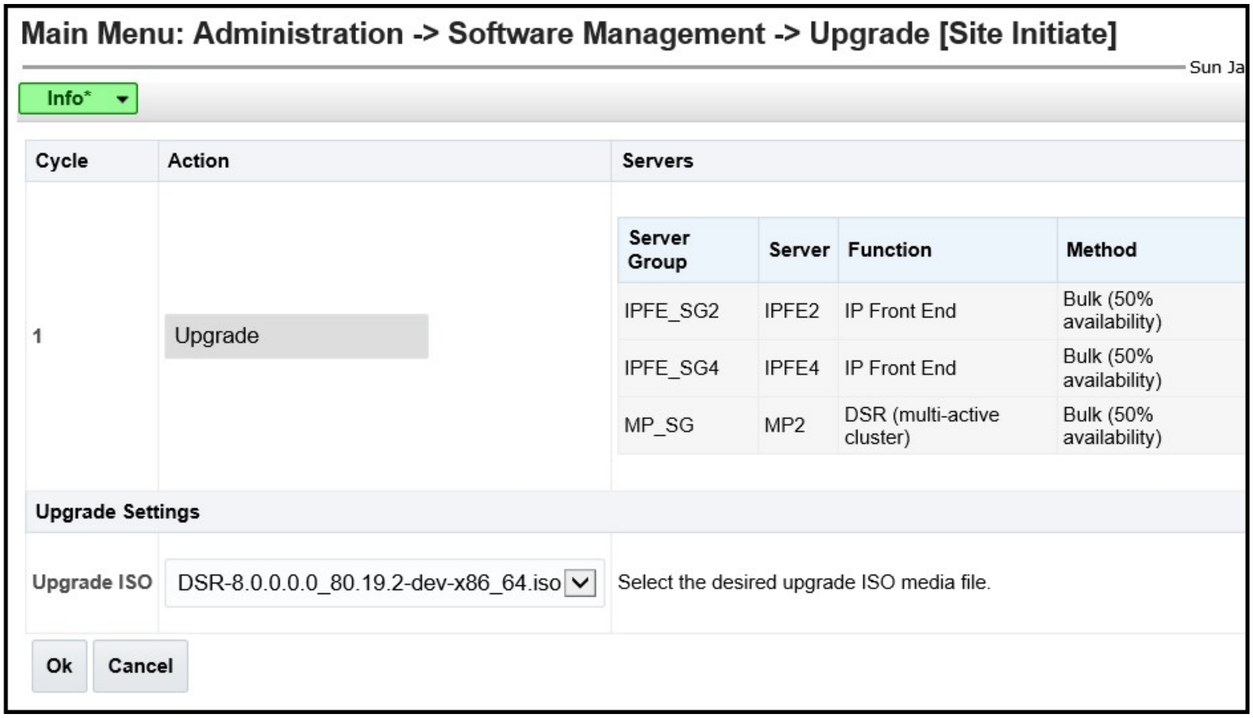
Main Menu: Administration -> Software Management -> Upgrade

Sun Jan 15 00:24:13 2017 UT

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versic
SO_East	DSR (active/standby pair)	OAM	Accept or Reject (2/2)	8.0.0.0.0-80.19.0 (2/2)
SS7MP_SG1	SS7-IWF	Bulk (50% availability)	Accept or Reject (1/1)	8.0.0.0.0-80.19.0 (1/1)
IPFE_SG3	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)	8.0.0.0.0-80.19.0 (1/1)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Ready (1/2) Accept or Reject (1/2)	7.2.0.0.0-72.25.0 (1/2) 8.0.0.0.0-80.19.0 (1/2)
IPFE_SG2	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0.0.0-72.25.0 (1/1)
IPFE_SG1	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)	8.0.0.0.0-80.19.0 (1/1)
IPFE_SG4	IP Front End	Bulk (50% availability)	Ready (1/1)	8.0.0.0.0-80.18.1 (1/1)

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 canceled in Figure 11, only a single cycle is needed since the availability requirements can be met by the servers that have already been upgraded. Once an ISO is selected and the **Ok** button is clicked, the site upgrade continues normally.

Figure 13. Restarting Site Upgrade.



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

Cycle	Action	Servers			
		Server Group	Server	Function	Method
1	Upgrade	IPFE_SG2	IPFE2	IP Front End	Bulk (50% availability)
		IPFE_SG4	IPFE4	IP Front End	Bulk (50% availability)
		MP_SG	MP2	DSR (multi-active cluster)	Bulk (50% availability)

Upgrade Settings

Upgrade ISO: DSR-8.0.0.0.0_80.19.2-dev-x86_64.iso — Select the desired upgrade ISO media file.

2.11 Automated Server Group Upgrade

The Automated Server Group (ASG) upgrade feature allows the user to automatically upgrade 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 impact system operations.

When a server group is selected for upgrade, ASG will upgrade 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, there are some instances in which the manual upgrade method is utilized. In all cases where ASG is used, procedures for a manual upgrade are also provided. **Note that in order to use ASG on a server group, no servers in that server group can be already upgraded – either by ASG or manually**.

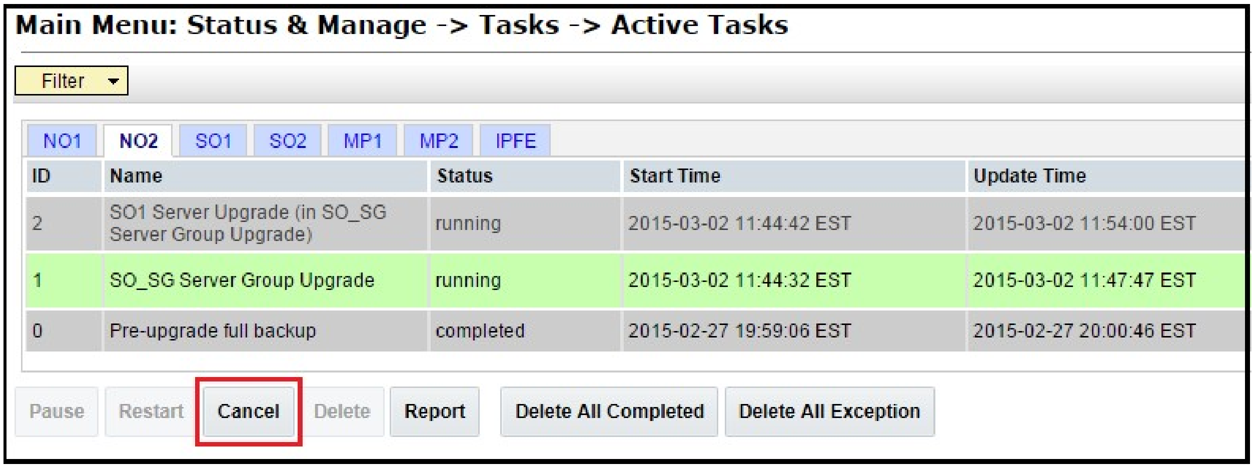
DSR continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

2.11.1 Canceling 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 canceled from the **Status & Manage > Active Tasks** screen (Figure 14) if necessary. Once the task is canceled, it cannot be restarted. However, a new ASG task can be started 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. Canceling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tasks that were started by the ASG task (i.e., task ID #2 in Figure 14). Because the ASG task is canceled, no new server upgrades will be initiated by the task.

Figure 14. Server Group Upgrade Active Tasks



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

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

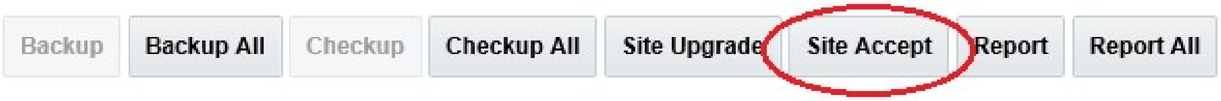
In the event that a server fails upgrade, that server will automatically roll back to the previous release in preparation for backout_restore and fault isolation. Any other servers in that server group that are in the process of upgrading will continue to upgrade to completion. However, the ASG task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

2.11.2 Site Accept

Prior to 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.

The 'Site Accept' button on the upgrade GUI (Figure 15) provides the capability to nearly simultaneously Accept the upgrade of some or all servers for a given site. When the button is selected, a subsequent screen (Figure 16) displays the servers that are ready for the Accept action.

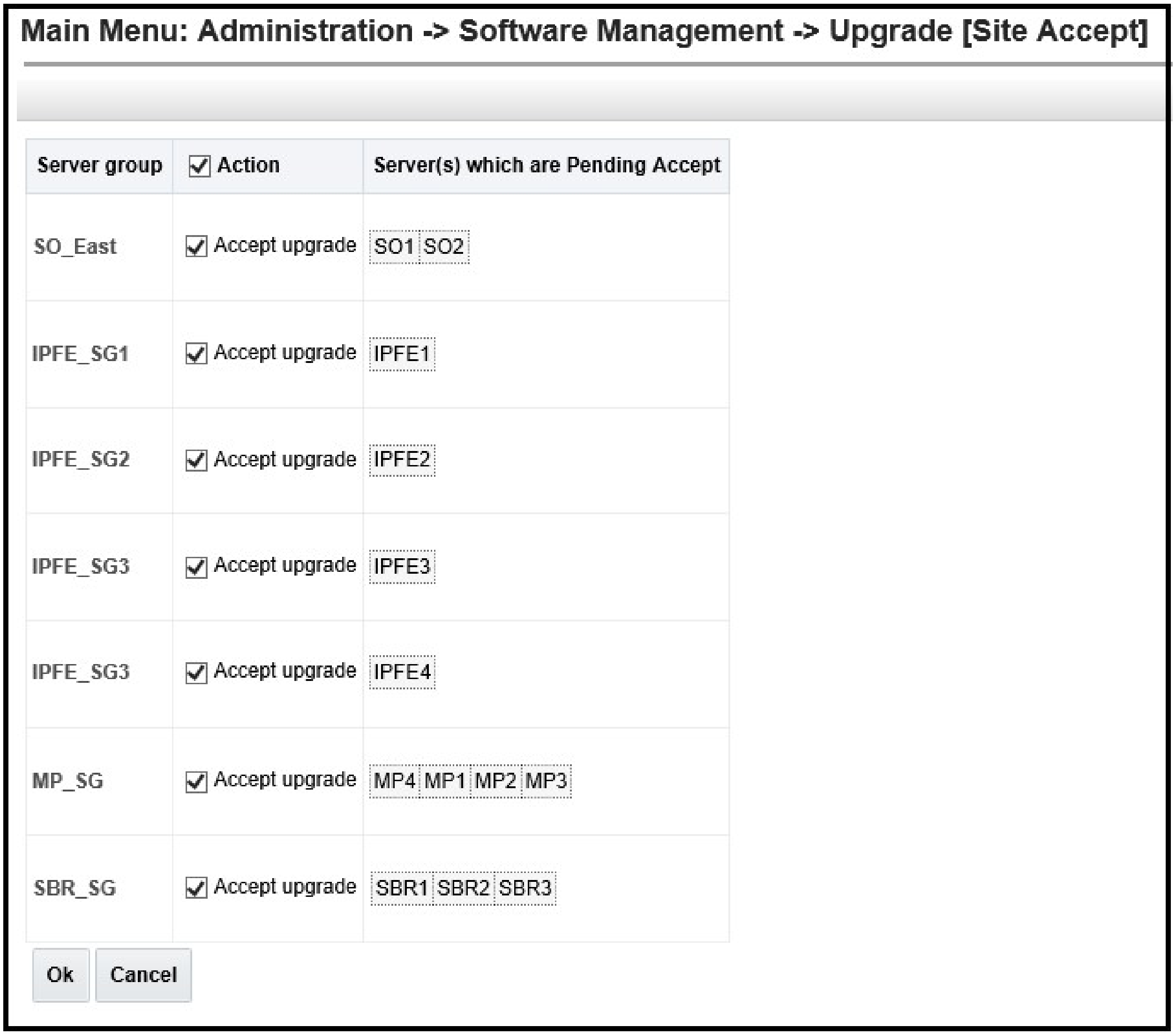
Figure 15. Site Accept Button



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 that the information presented is accurate, clicking the 'Ok' button results in a pop up dialog box that requires confirmation of the intended action. Confirming the action causes the server upgrades to be accepted.

The Accept command will be 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 will transition to "Backup Needed".

Figure 16. Site Accept Screen.


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

Server group	☑ Action	Server(s) which are Pending Accept
SO_East	☑ Accept upgrade	SO1 SO2
IPFE_SG1	☑ Accept upgrade	IPFE1
IPFE_SG2	☑ Accept upgrade	IPFE2
IPFE_SG3	☑ Accept upgrade	IPFE3
IPFE_SG3	☑ Accept upgrade	IPFE4
MP_SG	☑ Accept upgrade	MP4 MP1 MP2 MP3
SBR_SG	☑ Accept upgrade	SBR1 SBR2 SBR3

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 document that help plan the upgrade and estimate how long it will take 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 6.0/7.x/8.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.
- Direct access to the blades/RMS Integrated Lights Out (iLO)/XMI IP addresses (whichever is applicable) from the workstations directly connected to the DSR servers is required.

3.1.1 ISO Image Files / Media

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

The DSR 8.0 ISO image file name will be in the following format:

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

If TVOE is being upgraded, obtain a copy of the TVOE release ISO image file or media. The TVOE ISO image file name will be in the following format:

TVOE-3.3.0.0.0_88.xx.0-x86_64.iso

NOTE: Prior to the execution of this upgrade procedure it is assumed that the ISO image files have already been delivered to the site by the customer. The ISO image files must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image files. If the user performing the upgrade is at a remote location, it is assumed the ISO files are already available before starting the upgrade procedure.

The DSR ISO will be 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 will be 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 that the necessary administration information is available prior to 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 Value
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username[1] GUI Admin Password	
	DSR Root Password[2]	
	DSR admusr Password[2]	
	Blades iLO/LOM Admin Username	
	Blades iLO/LOM Admin Password	
	PM&C GUI Admin Username	
	PM&C GUI Admin Password	
	PM&C root Password	
	PM&C pmacftpusr password	
	OA GUI Username	
	OA GUI Password	
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	
	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)	

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

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

	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	

Item	Description	Recorded Value
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	

Item	Description	Recorded Value
iLO/LOM	NOAM 1 iLO/LOM IP Address	
	NOAM 2 iLO/LOM IP Address	
	SOAM 1 iLO/LOM IP Address	
	SOAM 2 iLO/LOM IP Address	
	MP 1 iLO/LOM IP Address	
	MP 2 iLO/LOM IP Address	
	……..	
	MP (n) iLO/LOM IP Address	
	IPFE MP iLO/LOM IP Address (optional)	
	IPFE MP iLO/LOM IP Address (optional)	
	……..	
	IPFE MP (n) iLO/LOM IP Address (optional)	
	……..	
	DA MP iLO/LOM IP Address (optional)	
	DA MP iLO/LOM IP Address (optional)	
	………	
	DA MP(n) iLO/LOM IP Address (optional)	
PM&C	PM&C Management IP Address(Site 1)	
PM&C	PM&C Management IP Address(Site 2)	
Software	Target Release Number	
	ISO Image (.iso) file name	
Misc.[4]	Miscellaneous additional data	

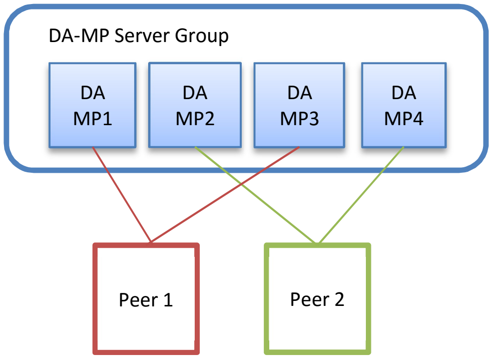
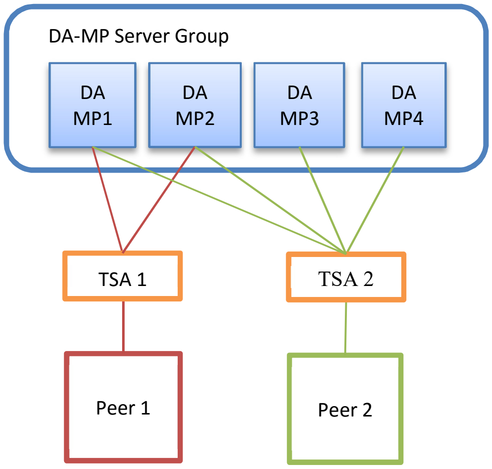
[4] As instructed by Oracle CGBU Customer Service.

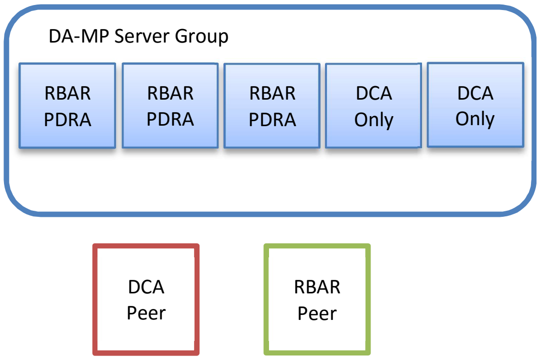
3.2 Site Upgrade Methodology Selection

There are three primary methods for upgrading a DSR site: Auto Site Upgrade, Auto Server Group Upgrade, and manual upgrade. The Auto Site Upgrade is the easiest and most efficient site upgrade method; however, it is not suitable for all customers or all configurations. The Auto Server Group upgrade incorporates many of the conveniences of Auto Site Upgrade, but allows for more customer control of the upgrade process. Again, Auto 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 utilized 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 will be 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?  DA-MP Server Group DA MP1 DA MP2 DA MP3 DA MP4 Peer 1 Peer 2	□	□	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) will be upgraded simultaneously, thereby isolating the peer. Auto Site Upgrade and Auto Server Group Upgrade should not be used for this configuration. **If yes, proceed to step 8.** **If no, continue with step 2.**
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?  DA-MP Server Group DA MP1 DA MP2 DA MP3 DA MP4 TSA 1 TSA 2 Peer 1 Peer 2	□	□	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) will be upgraded simultaneously, thereby isolating the peer. Auto Site Upgrade and Auto Server Group Upgrade should not be used for this configuration. **If yes, proceed to step 8.** **If no, continue with step 3.**

	Criteria	Yes	No	Notes
3	Do any of the site’s DA-MPs have specialized distribution of DSR features, similar to the depiction below?  DA-MP Server Group RBAR PDRA RBAR PDRA RBAR PDRA DCA Only DCA Only DCA Peer RBAR Peer	□	□	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) will be upgraded simultaneously, thereby eliminating service functionality. Auto Site Upgrade and Auto 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 Auto Site Upgrade. The site is a candidate for Auto Server Group upgrade. **If yes, proceed to step 7.** **If no, continue with step 5.**
5	Auto Site Upgrade is a candidate for this system. Auto 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, Auto 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, Auto Site Upgrade requires no additional user input to complete the upgrade. User control is limited to canceling the site upgrade task. **If yes, Auto 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?	□	□	Auto Server Group upgrade allows the user to initiate the upgrade of each server group, while the individual servers within the server group upgrade automatically. **If yes, Auto Server Group upgrade is the recommended upgrade method.** **If no, proceed to step 8.**

	Criteria	Yes	No	Notes
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.**

3.2.1 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 will be 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 will be upgraded.

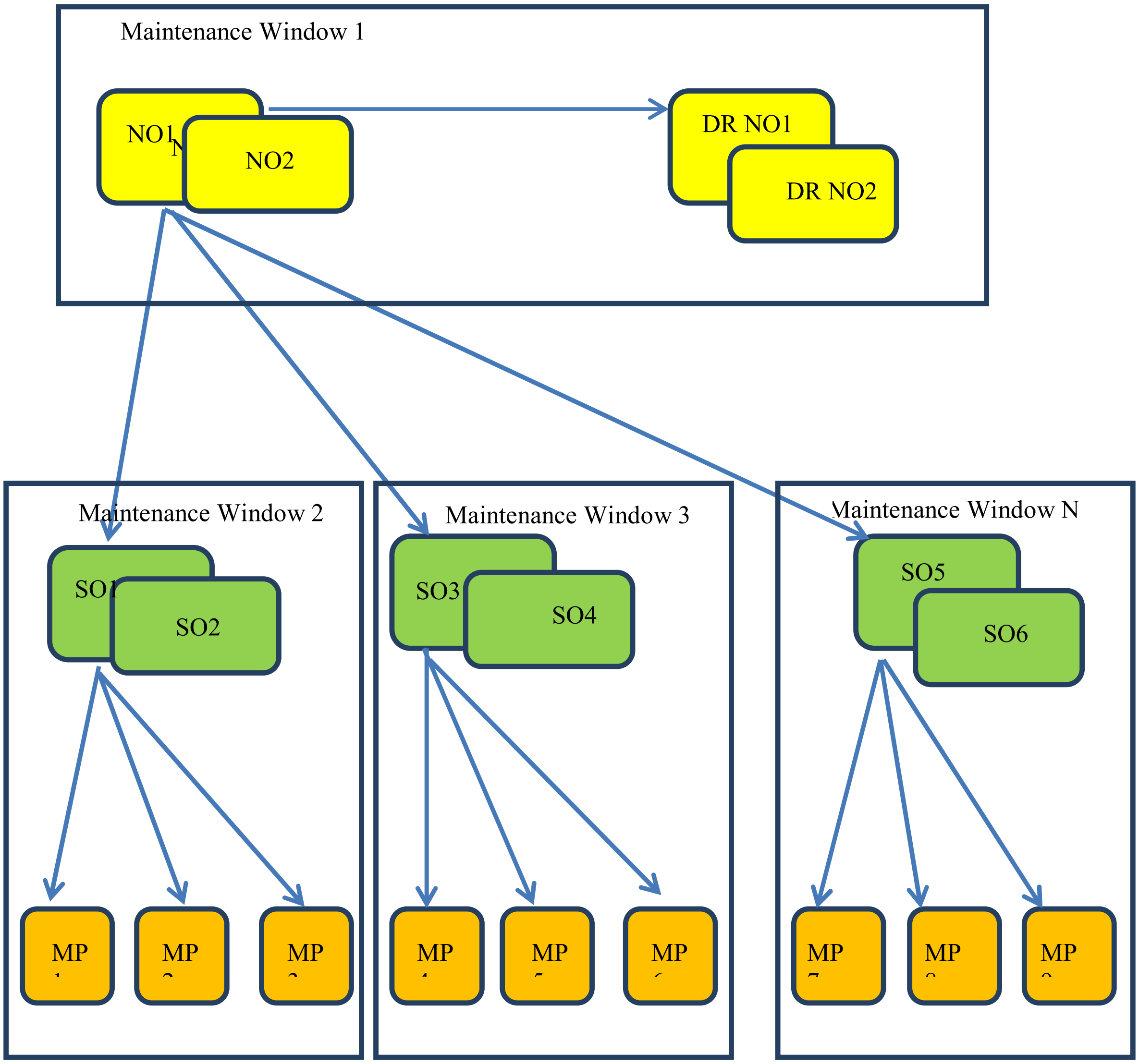
Table 7. DA-MP Upgrade Planning Sheet

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

3.3 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**

3.3.1 Maintenance Window for PM&C and TVOE Upgrades (optional)

This document includes steps to upgrade TVOE as an integrated activity with the upgrade of the DSR application. However, it is an **option** to upgrade TVOE and PM&C (if necessary) as separately planned and executed activities using the following references:

- PM&C Upgrade procedure is provided in reference [4]
- TVOE Host environment upgrade procedures are included in this document and in reference [3].

PM&C and TVOE upgrades are backwards compatible to prior releases of DSR. These upgrades may be done throughout the entire topology, or a site-at-a-time, before upgrading the DSR application.

If PM&C and TVOE are to be upgraded in a separate maintenance window than the DSR application, this activity should be initiated and completed prior to starting Section 4. The procedure for upgrading TVOE is provided in Section 3.4.6. Refer to [4] for PM&C upgrade procedures.

Note: In RMS and VEDSR configurations, the PM&C and DSR servers could be sharing the same TVOE Host. Make the customer aware of all servers affected by the TVOE upgrade.

3.3.2 Calculating Maintenance Window Requirements

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see ref [9]).

This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. Complete DSR upgrade maintenance window details and timings can be found in Reference [9]. Please see the instructions tab of the spreadsheet for more information and details.

3.3.3 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded, and possibly also the PM&C, and the TVOE environments supporting these servers. *(Note that PM&C and/or TVOE environments may be upgraded before Maintenance Window 1, as described in Section 2.5.)*

Maintenance Window 1 ***(NOAM Sites)*** **Date:** ______________ **NOTE 1:** *The **NE Name** may be viewed from the DSR NOAM GUI under* **[Main Menu → Configuration → Network Elements].** *** NOTE 2:** *In order to save time, It is suggested that PM&C servers be upgraded outside/ahead of DSR maintenance window 1 as this activity is seen as non-intrusive to DSR operation.*	1. Record the Site **NE Name** of the PM&C, DSR NOAM and the DR Provisioning Site to be upgraded during Maintenance Window 1 in the space provided below: 2. **"Check off"** the associated **Check Box** as upgrade is completed for each server. □ * DR PM&C *(Guest)*: ____________________ □ TVOE for DR NOAM-B: ______________________ □ TVOE for DR NOAM-A: ______________________ □ * Primary PM&C *(Guest)*: __________________________ □ TVOE for Primary NOAM-B: ______________________ □ TVOE for Primary NOAM-A: ______________________ □ DR Standby NOAM *(Guest)*: _______________________ □ DR Active NOAM *(Guest)*: __________________________ □ Primary Standby NOAM *(Guest)*: ____________________ □ Primary Active NOAM *(Guest)*: ______________________

3.3.4 Maintenance Window 2 and beyond (SOAM Site Upgrades)

During maintenance window 2, all servers associated with the first SOAM site 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), the following form should be copied and used for the subsequent SOAM site upgrades.

⚠ WARNING *It is strongly recommended that mated pair SOAM sites are NOT upgraded in the same maintenance window.*

Maintenance Window ***(SOAM Sites)*** **Date:** ______________ **NOTE 1:** *For 1+1 configuration, only 2 DA-MP(s) will be present, one is Active while the other is Standby.* * **NOTE 2:** *In order to save time, It is suggested that PM&C servers be upgraded outside/ahead of DSR maintenance window 1 as this activity is seen as non-intrusive to DSR operation.*	1. Record the Site **NE Name** of the DSR SOAM and the MP(s) to be upgraded during maintenance window 2 in the space provided. 2. **"Check off"** the associated **Check Box** as upgrade is completed for each server. SOAM Site: _______________ □ * PM&C : __________________ □ * TVOE for PM&C: _________________ □ TVOE for SOAM-B: _________________ □ TVOE for SOAM-A: _________________ □ Spare SOAM1 *(Guest)*: _______________ *(If equipped)* □ Spare SOAM2 *(Guest)*: _______________ *(If equipped)* □ Standby SOAM *(Guest)*: _________________ □ Active SOAM *(Guest)*: _________________
	□ 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.

INCREASE MAX NUMBER OF OPEN FILES

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 3 or Procedure 4 or Procedure 5 or 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 6.0, 7.0.x 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	0:20-3:00[1]	1:00-6:00	DSR ISO Administration	None
Procedure 8	0:05	1:05-6:05	ISO Link Correction	None
Procedure 9 or Procedure 10	0:10-2:00	1:15-8:05	Full Backup of DB Run Environment for Release 6.0, 7.0.x or Full Backup of DB Run Environment for Release 7.1.x and later	None

[1] The ISO transfer process changed in DSR 7.1. Due to this change, 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 prior to, 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE 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 that all information in Sections 3.2 and 3.3 is filled-in and accurate.
3 □	Contact MOS	It is recommended to contact MOS and inform them of plans to upgrade this system. See Appendix S for instructions. Note that obtaining a new online support account can take up to 48 hours.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 (TVOE, PM&C, etc).

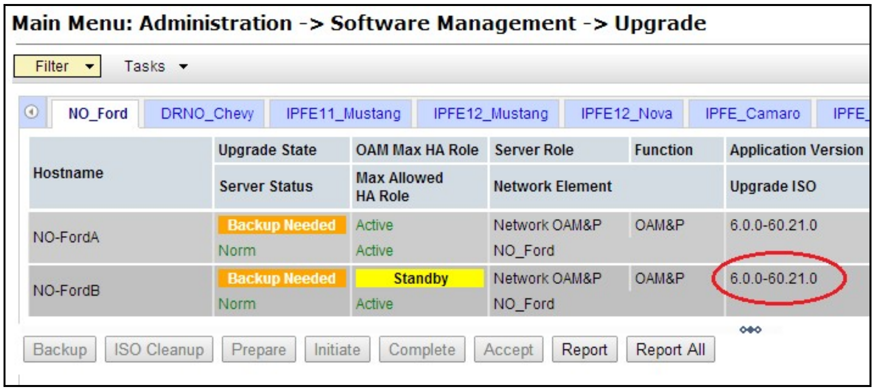
3.4.2.1 Verification of Configuration Data

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

Procedure 2: Verification of Configuration Data

<table>
<tr>
<td>S
T
E
P
#</td>
<td colspan="2">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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK <u>FOR UPGRADE ASSISTANCE</u></b></td>
</tr>
<tr>
<td>1
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Verify application version</td>
<td>
1. Select <b>Administration > Software Management > Upgrade</b>.
2. Verify that the Upgrade path to the target release is supported as documented in Section 2.1 (Supported Upgrade Paths).
3. Select the NOAM Server Group and verify the Application Version

<b>Main Menu: Administration -> Software Management -> Upgrade</b>

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM Max HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Max Allowed HA Role</th><th colspan="2">Network Element</th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">NO-FordA</td><td>Backup Needed</td><td>Active</td><td>Network OAM&P</td><td>OAM&P</td><td>6.0.0-60.21.0</td></tr>
<tr><td>Norm</td><td>Active</td><td colspan="2">NO_Ford</td><td></td></tr>
<tr><td rowspan="2">NO-FordB</td><td>Backup Needed</td><td>Standby</td><td>Network OAM&P</td><td>OAM&P</td><td>6.0.0-60.21.0</td></tr>
<tr><td>Norm</td><td>Active</td><td colspan="2">NO_Ford</td><td></td></tr>
</table>

</td>
</tr>
<tr>
<td>2
□</td>
<td><b><u>Active NOAM CLI:</u></b>

Check if the setup has customer supplied Apache certificate installed and protected with a passphrase.</td>
<td>
1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM
<pre>
ssh admusr@<NOAM_VIP>
password: <enter password>
</pre>
(Answer ‘yes’ if you are prompted to confirm the identity of the server.)

2. cd to <code>/etc/httpd/conf.d</code> and open the file named <code>ssl.conf</code>.
3. Locate the line beginning with the phrase “<code>SSLCertificateFile</code>”
4. The path that follows ”SSLCertificateFile“ is the location of the Apache certificate. If the path is <code>/usr/TKLC/appworks/etc/ssl/server.crt</code>,
then the certificate is supplied by Oracle and no further action is required. Continue with the next step.
5. If the path is anything other than <code>/usr/TKLC/appworks/etc/ssl/server.crt</code>, then a customer-supplied Apache certificate is likely installed. Rename the certificate, but note the original certificate pathname for use in Section 5.7.2.
</td>
</tr>
</table>

Procedure 2: Verification of Configuration Data

3 □	Check if a new Firmware Release may be required for the system.	**This step is not applicable to Software Centric installations/upgrades.** It is recommended to contact MOS by referring to Appendix S to determine the minimum supported firmware release required for the target DSR release. NOTE: New Firmware Releases for the DSR platform are typically released every 6 months. Target Firmware Rev: _______________________________ Example: FW rev. 2.2.7 Acquire the Firmware Release Notes and Firmware Upgrade Pack procedures for the target Firmware Revision. Use the Firmware Upgrade Pack procedures to determine which specific system components (Switches, OAs, Servers, etc.) may require an upgrade. Plan for additional Maintenance Windows if Firmware Upgrade is required. Please note that Firmware Upgrade activity is typically performed before the DSR Upgrade.
4 □	Check the existing PM&C version and identify if PM&C upgrade is required. **NOTE:** *If required, PM&C upgrade should be performed as a prerequisite to DSR upgrade.*	**This step is not applicable to Software Centric installations/upgrades.** *This step applies to all servers that have a PM&C guest (VM) installed.* Identify any PM&C servers requiring upgrade. 1. Determine the PM&C version installed by logging into PM&C GUI. 2. Refer to the Release Notes to determine the minimum supported PM&C version required for the target DSR release. If a PM&C upgrade is required, obtain the required PM&C upgrade document [4] and plan for additional Maintenance Windows to execute PM&C upgrades.

Procedure 2: Verification of Configuration Data

5 □

Check the TVOE Host server software version

This step is not applicable to Software Centric installations/upgrades.

This step applies to all RMS & Blade servers that have TVOE installed.

1. Find the target DSR release from Table 5.

2. Refer to the Release Notes to determine the minimum supported TVOE OS version required for the target DSR release.

   Required TVOE Release: ________________________

Example: 872-2525-101-2.5.0_82.22.0-TVOE-x86_64.iso

3. Verify the current TVOE HOST OS version for each TVOE Hosts by comparing the “Product Release” field from the “appRev” command to the “Required TVOE Release” field shown above.

```
# appRev
        Install Time: Thu Nov  6 14:31:08 2014
        Product Name: TVOE
     Product Release: 2.7.0.0.0_84.20.0
 Base Distro Product: TPD
 Base Distro Release: 6.7.0.0.1_84.20.0
     Base Distro ISO: TPD.install-6.7.0.0.1_84.20.0-
OracleLinux6.5-x86_64.iso
                  OS: OracleLinux 6.5
```

IMPORTANT: If TVOE Hosts are not on the correct release, refer to Section 3.3.1 to plan for TVOE Host upgrades.

THIS PROCEDURE HAS BEEN COMPLETED.

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:
6.0 or 7.0.x	Procedure 3: Data Collection for Source Release 6.0, 7.0.x
7.1.x	Procedure 4: Data Collection for Source Release 7.1.x
7.2 or 7.3	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 6.0, 7.0.x

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 6.0 or 7.0.x.

Procedure 3: Data Collection for Source Release 6.0, 7.0.x

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK <u>FOR UPGRADE ASSISTANCE</u>**	

1
□
	<u>Active SOAM CLI:</u>
	Database consistency check
		Check the transport connections tables.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		2. 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`
		3. 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 to consult with MOS before continuing.

Procedure 3: Data Collection for Source Release 6.0, 7.0.x

2 □

Server CLI:

Verify uptime for each server in the topology

Starting with the Active NOAM, execute the following procedure.

1. Use the SSH command (on UNIX systems - or putty if running on windows) to login to the server using the server XMI IP Address.

   ```
   ssh admusr@<target_server_XMI_IP>
   ```

   (Answer 'yes' if you are prompted to confirm the identity of the server.)

2. 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
```

3. Record the hostname of any server with an "uptime" value > 200 days.

4. Inform the customer that a "**Cold Reboot**" will be required for all servers with an "uptime" value > 200 days prior to beginning any upgrade activity.

NOTE: ***This is required response due to Red Hat Bug 765720. It is recommended to contact MOS if instruction is needed on how to gracefully perform a "Cold Reboot".***

5. Repeat steps 1 through 4 for each server in the topology.

3 □

Active SOAM VIP:

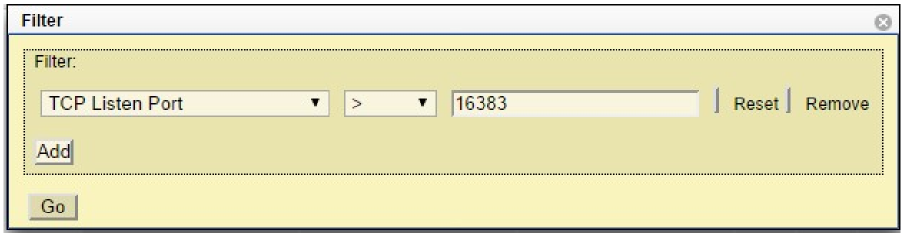
Verify Local Node port ranges

For source release 6.0 only

Perform this step only if the source release is 6.0; otherwise proceed to step 5.

Verify the Local Node port numbers are within the allowed range.

1. Login to the SOAM GUI using the VIP.
2. Navigate to **Diameter > Configuration > Local Nodes**.
3. Click **Filter** to open the filter selection box.
4. Enter the following values and click **Go**.



TCP Listen Port > 16383

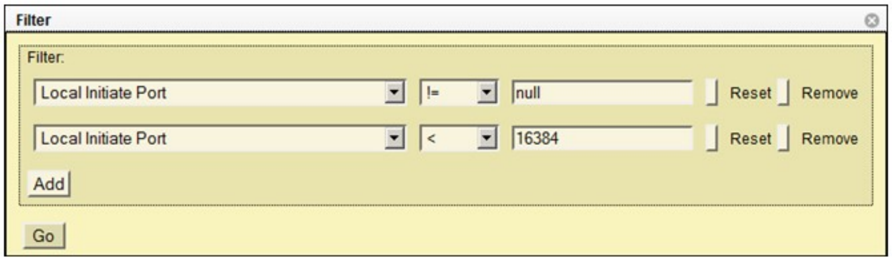
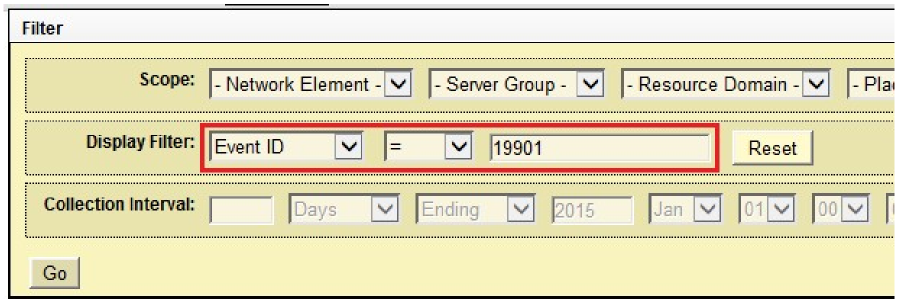
5. Repeat steps 3 and 4 for the following filter values:
   - "TCP Listen Port < 1024"
   - "SCTP Listen Port > 16383"
   - "SCTP Listen Port < 1024"

If the filters produce no results, then continue with the next step.

Otherwise, record the results and report to the customer that the current port configuration is not within recommended best practices.

NOTE: *Only the customer may modify the port configurations. Refer to Reference [10] for further instruction.*

Procedure 3: Data Collection for Source Release 6.0, 7.0.x

4 □	**Active SOAM VIP:** Verify Initiator connection port ranges **For source release 6.0 only**	**Perform this step only if the source release is 6.0; otherwise proceed to step 5.** Verify the Initiator connection port numbers are within the allowed range. 1. Navigate to **Diameter > Configuration > Connections**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  Filter Filter: Local Initiate Port != null Reset Remove Local Initiate Port < 16384 Reset Remove Add Go 4. Repeat sub-step 2 and 3 for the following filter values: • “Local Initiate Port != null” AND “Local Initiate Port > 24575” **If the filters produce no results, continue with the next Step. Otherwise, record the results and report to the customer that the current port configuration is not within recommended best practices.** **NOTE:** *Only the customer may modify the port configurations. Refer to Reference [10] for further instruction.*
5 □	Repeat checks	Repeat steps 1 through 4 for each SOAM site in the topology.
6 □	**Active NOAM VIP:** Alarm Check	Check for the presence of alarm 19901 – CFG-DB Validation Error. 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  Filter Scope: - Network Element - - Server Group - - Resource Domain - - Pla Display Filter: Event ID = 19901 Reset Collection Interval: Days Ending 2015 Jan 01 00 Go 4. 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 to consult with MOS for guidance if the alarm does not clear within 60 minutes.

Procedure 3: Data Collection for Source Release 6.0, 7.0.x

7 □	**Active NOAM VIP:** Verify IPFE Server Groups	Verify the IPFE Server Groups are properly configured. 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE Server Group. Verify that each IPFE Server Group is configured with one, **and only one**, IPFE server. 4. If any IPFE Server Group contains more than one IPFE server, refer to the Server Group Configuration procedure of ref [5] (DSR 6.0), [6] (DSR 7.0.x/7.1.x), or [7] (DSR 7.2/7.3) to correct the configuration.
8 □	**Active NOAM VIP:** Verify and collect Network Element Configuration data	1. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
9 □	**Active NOAM VIP:** Verify and collect Server Group Configuration data	1. Select **Configuration > Server Groups** to view the Server Group screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
10 □	**Active NOAM VIP:** Verify and collect Server Configuration data	1. Select **Configuration > Servers** to view the Server screen 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
11 □	**Active NOAM VIP:** Verify and collect Services Configuration data	1. Select **Configuration > Services** to view Services screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
12 □	**Active NOAM VIP:** Verify and collect Signaling Network Configuration data for DSR	1. Select **Configuration > Network** to view the Signaling Networks. 2. Click "**Report**" at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference. 5. Select **Configuration > Network > Devices**. 6. Click "**Report All**" at the bottom of the table to generate a report for all entries. 7. Save the report and/or print the report. Keep these copies for future reference. 8. Select **Configuration > Network > Routes**. 9. 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.
13 □	**Active NOAM VIP:** Verify Server Status is Normal	1. Select **Status & Manage > Server.** The Server Status screen is displayed. 2. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 3. Do not proceed with the upgrade if any server status displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms.
14 □	**Active NOAM VIP:** Log all current alarms at NOAM.	1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. 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.

Procedure 3: Data Collection for Source Release 6.0, 7.0.x

15 □	**Active NOAM VIP:** View Communication Agent status	1. Select **Communication Agent > Maintenance > Connection Status** The Communication Agent > Connection Status screen is displayed. 2. Verify the Connection Status of each connection is InService.
16 □	**Active NOAM VIP:** View SBR status (if equipped)	View SBR status if PDRA/PCA is enabled. **If the Active NOAM is on release 6.0:** 1. Select **Policy DRA > Maintenance > Policy SBR Status** The Policy SBR Status screen is displayed. 2. Expand each Server Group. Verify Congestion Level is 'Normal' for all servers. **If the Active NOAM is on release 7.0.x, 7.1.x:** 1. Select **Policy and Charging > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding** tab. 3. Expand each Server Group. 4. Verify Congestion Level is 'Normal' for all servers. 5. Repeat sub-steps 3 and 4 for the **PDRA Mated Triplet** tab. **If the Active NOAM is on release 7.2 and later:** 1. Select **SBR > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding** tab. 3. Expand each Server Group. 4. Verify Congestion Level is '**Normal**' for all servers. 5. Repeat sub-steps 3 and 4 for the **PCA Mated Triple**t tab
17 □	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA which will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 16 of this procedure. 2. It is recommended to plan for MP upgrades by consulting Section 3.2 to assess the impact of out-of-service MP servers 3. Determine the exact sequence in which MP servers will be upgraded for each site.
		THIS PROCEDURE HAS BEEN COMPLETED.

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 □	**Active NOAM VIP:** Verify IPFE Server Groups	Verify the IPFE Server Groups are properly configured. 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE Server Group. Verify that 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 to consult with MOS before continuing.

Procedure 4: Data Collection for Source Release 7.1.x

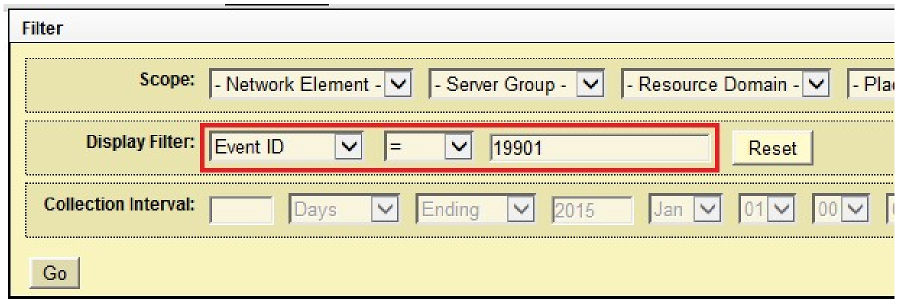
2 □

Active NOAM VIP:

Alarm Check

Check for the presence of alarm 19901 – CFG-DB Validation Error.

1. Navigate to **Alarms & Events > View Active**.
2. Click **Filter** to open the filter selection box.
3. Enter the following values and click **Go**.



Filter

Scope: - Network Element - | - Server Group - | - Resource Domain - | - Pla

Display Filter: Event ID | = | 19901 | Reset

Collection Interval: Days | Ending | 2015 | Jan | 01 | 00

Go

4. 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 to consult with MOS for guidance if the alarm does not clear within 60 minutes.

3 □

Active NOAM CLI:

Verify NOAM pre-Upgrade Status

Execute the following commands on the Active DSR NOAM and Active DR NOAM servers.

1. Use an SSH client to connect to the Active NOAM:

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

Note: The static XMI IP address for each server should be available in Table 5.

2. 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 message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears 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 to contact MOS for guidance.

4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

Procedure 4: Data Collection for Source Release 7.1.x

<table>
<tr><td>4
□</td><td><b><u>Server CLI:</u></b>
Verify uptime for each server in the topology</td><td>Starting with the Active NOAM, execute the following procedure.
1. Use the SSH command (on UNIX systems - or putty if running on windows) to login to the server using the server XMI IP Address.
<code>ssh admusr@<target_server_XMI_IP&gt;</code>
(Answer ‘yes’ if you are prompted to confirm the identity of the server.)
2. Execute the “uptime” command:
<code>[admusr@ipfe-freeport-a1 ~]$ uptime</code>
<code> 02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83</code>
3. Record the hostname of any server with an “uptime” value > 200 days.
4. Inform the customer that a “<b>Cold Reboot</b>” will be required for all servers with an “uptime” value > 200 days prior to beginning any upgrade activity.
<b>NOTE:</b> <b><i>This is required response due to Red Hat Bug 765720. It is recommended to contact MOS if instruction is needed on how to gracefully perform a “Cold Reboot”.</i></b>
5. Repeat steps 1 through 4 for each server in the topology.</td></tr>
<tr><td>5
□</td><td><b><u>Active SOAM CLI:</u></b>
Database consistency check</td><td>Check the transport connections tables.
1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM
<code>ssh admusr@<NOAM_VIP&gt;</code>
(Answer ‘yes’ if you are prompted to confirm the identity of the server.)
2. Enter the following commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
<code>iqt -zhp ConnectionAdmin | wc -l</code>
<code>iqt -zhp TransportConnection | wc -l</code>
Sample output:
<code>[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l</code>
<code>7196</code>
<code>[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l</code>
<code>7196</code>
3. If the entry counts match, <b>proceed to step 6</b>.
<b>If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, DO NOT PROCEED WITH THE UPGRADE. It is recommended to consult with MOS before continuing.</b></td></tr>
</table>

Procedure 4: Data Collection for Source Release 7.1.x

6
□
	Active SOAM CLI:
	Log SOAM Alarm Status
		1. 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.
		2. 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 message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. If the following message appears 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**.
		3. Verify all Peer MPs are available
		4. Note the number of Total Connections Established ____________
		5. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

7 □	**Active SOAM CLI:** Verify PCA status (if equipped)	1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. 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 will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 8 of this procedure. 2. It is recommended to plan for MP upgrades by consulting Section 3.2 to assess the impact of out-of-service MP servers 3. Determine the exact sequence in which MP servers will be upgraded for each site.
		THIS PROCEDURE HAS BEEN COMPLETED.

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.

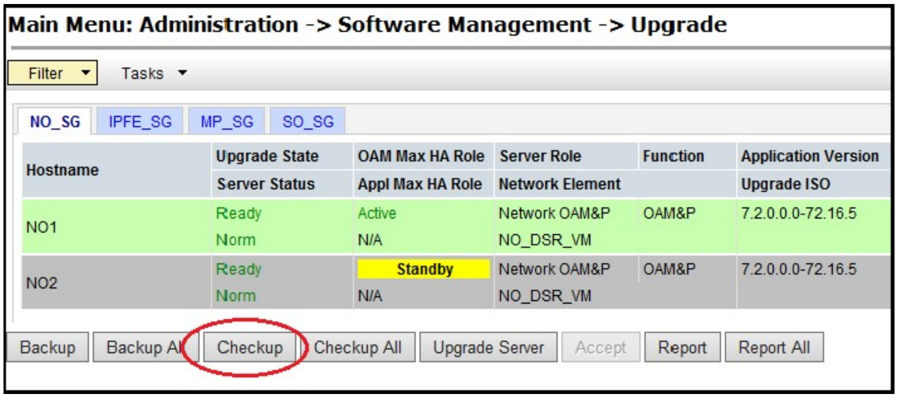
Procedure 5: Data Collection for Source Release 7.2, 7.3, 7.4

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK <u>FOR UPGRADE ASSISTANCE</u>**

1 □ **Active NOAM VIP:**

This procedure will run the automated Health Checks on the Active NOAM.

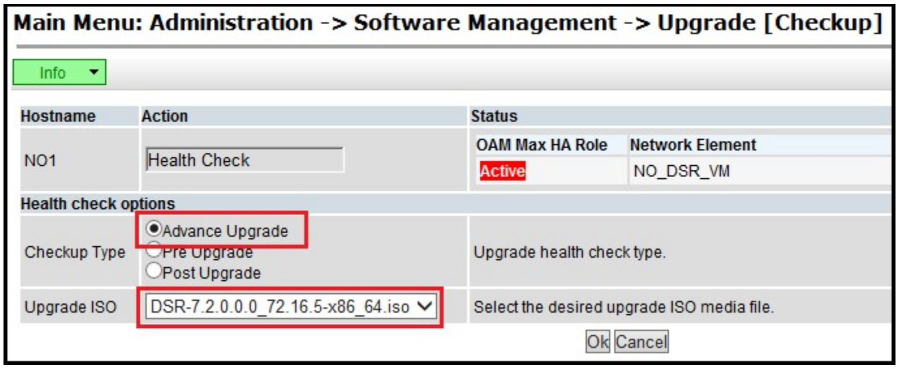
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the Active NOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Ready Norm	Active N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.16.5
NO2	Ready Norm	Standby N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.16.5

3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. In the 'Health check options' section, select the **Advance Upgrade** option.
5. If the ISO Administration procedure has already been performed for the target ISO, use the Upgrade ISO pulldown to select the target release ISO. Otherwise, do not select an ISO.
6. Click **Ok**. Control returns to the Upgrade screen.



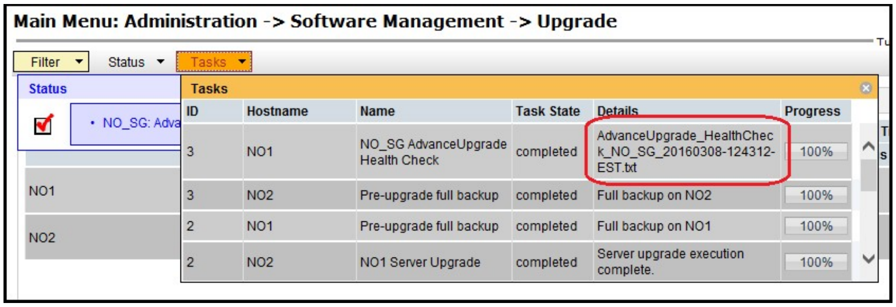
Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status	
		OAM Max HA Role	Network Element
NO1	Health Check	Active	NO_DSR_VM

Health check options

Checkup Type	● Advance Upgrade ○ Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-7.2.0.0.0_72.16.5-x86_64.iso	Select the desired upgrade ISO media file.

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

<table>
<tr>
<td>2
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Monitor health check progress</td>
<td>Monitor for the completion of the Health Check.
1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <NOServerGroup&gt; <b>AdvanceUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The Details column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.


Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>3</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160308-124312-EST.txt</td><td>100%</td></tr>
<tr><td>3</td><td>NO2</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on NO2</td><td>100%</td></tr>
<tr><td>2</td><td>NO1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on NO1</td><td>100%</td></tr>
<tr><td>2</td><td>NO2</td><td>NO1 Server Upgrade</td><td>completed</td><td>Server upgrade execution complete.</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>3
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Analyze any Health Check failure</td>
<td>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.
1. Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.
2. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
3. Locate the log entries for the most recent health check.
4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.</td>
</tr>
</table>

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

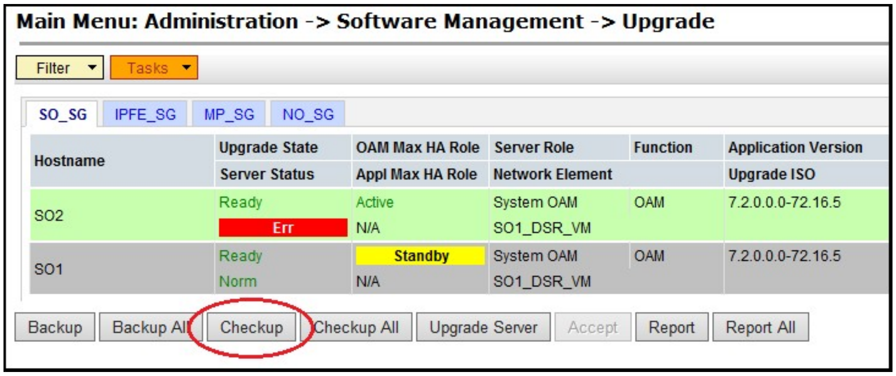
4 ☐

Active NOAM VIP:

Initiate SOAM health check

This procedure will run the automated Health Checks on the Active SOAM.

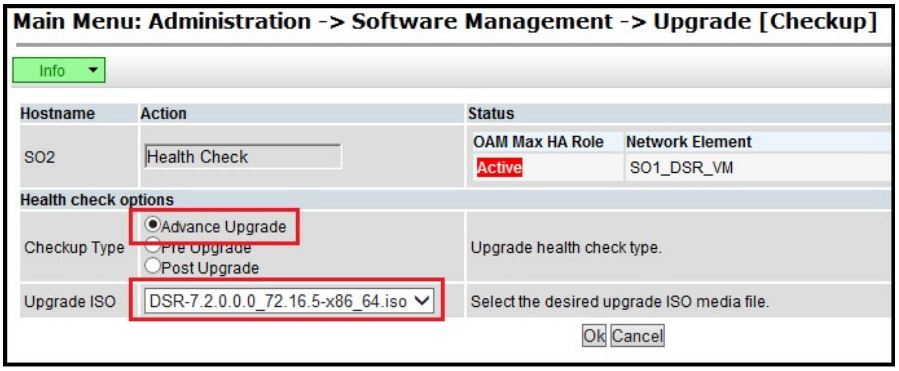
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the SOAM server group tab.
3. Select the Active SOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
SO2	Ready Err	Active N/A	System OAM SO1_DSR_VM	OAM	7.2.0.0.0-72.16.5
SO1	Ready Norm	Standby N/A	System OAM SO1_DSR_VM	OAM	7.2.0.0.0-72.16.5

4. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
5. In the 'Health check options' section, select the **Advance Upgrade** option.
6. For a major upgrade, use the Upgrade ISO pulldown to select the target release ISO. Do not select an ISO for an incremental upgrade.
7. Click **Ok**. Control returns to the Upgrade screen.



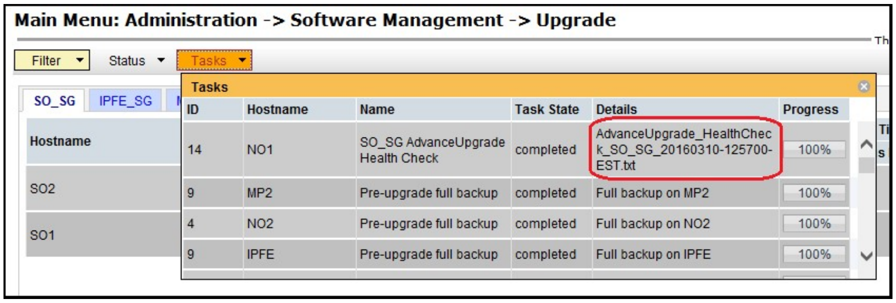
Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status	
		OAM Max HA Role	Network Element
SO2	Health Check	Active	SO1_DSR_VM

Health check options

Checkup Type	● Advance Upgrade ○ Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-7.2.0.0.0_72.16.5-x86_64.iso	Select the desired upgrade ISO media file.

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

<table>
<tr>
<td>5
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Monitor health check progress</td>
<td>Monitor for the completion of the Health Check.
1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <SOServerGroup&gt; <b>AdvanceUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The Details column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.

Main Menu: Administration -&gt; Software Management -&gt; Upgrade

Tasks
<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>14</td><td>NO1</td><td>SO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_SO_SG_20160310-125700-EST.txt</td><td>100%</td></tr>
<tr><td>9</td><td>MP2</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP2</td><td>100%</td></tr>
<tr><td>4</td><td>NO2</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on NO2</td><td>100%</td></tr>
<tr><td>9</td><td>IPFE</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on IPFE</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>6
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Analyze Health Check failure</td>
<td>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.
1. Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.
2. Select the Active SOAM tab.
3. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
4. Locate the log entries for the most recent health check.
5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.
If the health check log contains the message “Unable to execute Health Check on <Active SOAM hostname>”, perform health checks in accordance with Procedure 4.</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 will be out-of-service during the upgrade sequence.
1. 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 <b>Status & Manage &gt; Files</b> on the Active SOAM.
2. It is recommended to plan for MP upgrades by consulting MOS to assess the impact of out-of-service MP servers
3. Determine the manner in which the MP servers will be upgraded: Manually or Automated Server Group Upgrade. If the MPs will be upgraded manually, determine the exact sequence in which MP servers will be upgraded for each site.</td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td>
</tr>
</table>

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK <u>FOR UPGRADE ASSISTANCE</u>**

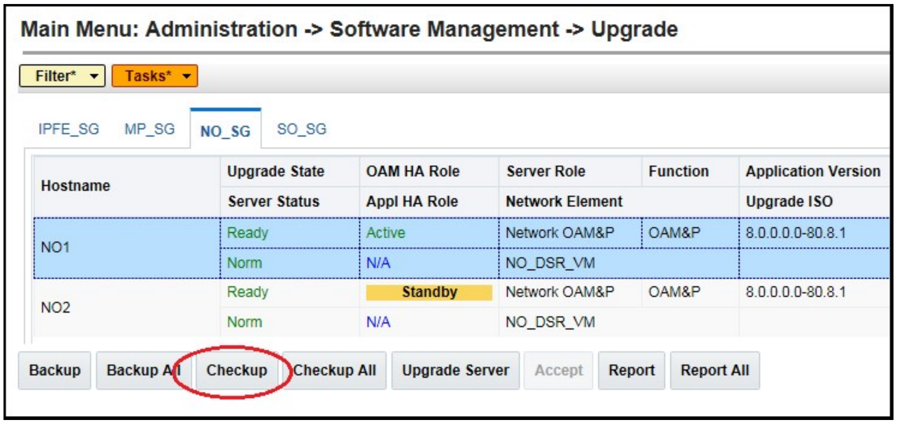
Procedure 6: Data Collection for Source Release 8.0 and later

1 □

Active NOAM VIP:

This procedure will run the automated Health Checks on the Active NOAM.

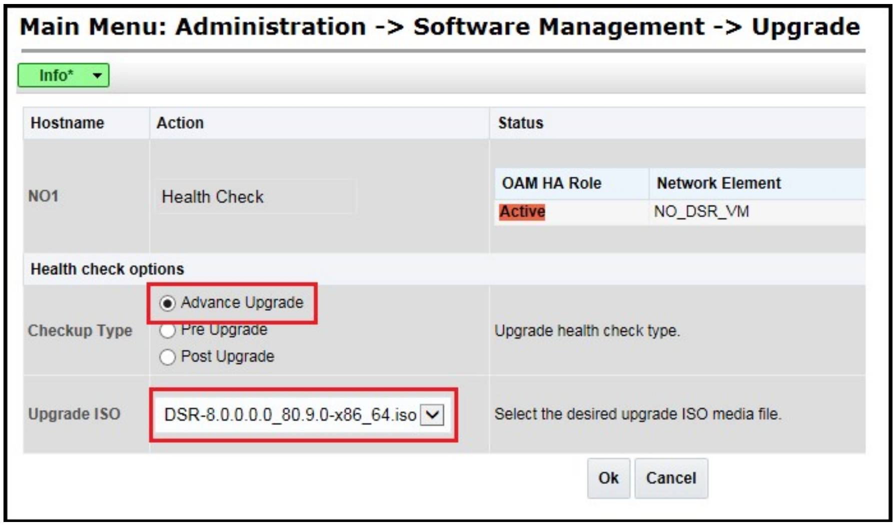
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the Active NOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.8.1
	Norm	N/A	NO_DSR_VM		
NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.8.1
	Norm	N/A	NO_DSR_VM		

3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. In the 'Health check options' section, select the **Advance Upgrade** option.
5. If the ISO Administration procedure has already been performed for the target ISO, use the Upgrade ISO pulldown to select the target release ISO. Otherwise, do not select an ISO.
6. Click **Ok**. Control returns to the Upgrade screen.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Action	Status	
		OAM HA Role	Network Element
NO1	Health Check	Active	NO_DSR_VM

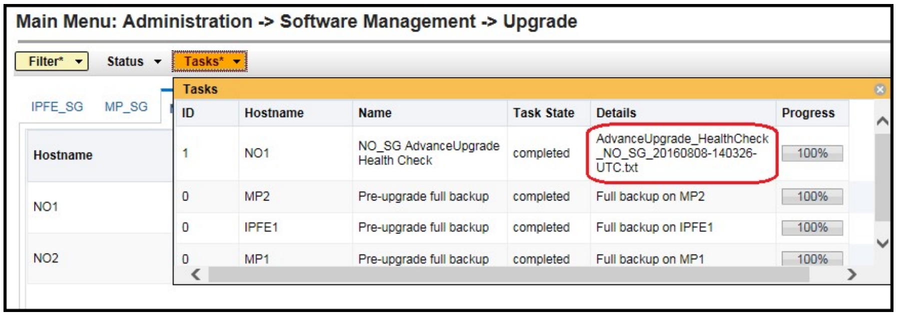
Health check options

Checkup Type	● Advance Upgrade ○ Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-8.0.0.0.0_80.9.0-x86_64.iso	Select the desired upgrade ISO media file.

Procedure 6: Data Collection for Source Release 8.0 and later

<table>
<tr>
<td>2
□</td>
<td><b><u>Active NOAM VIP:</u></b></td>
<td>Monitor for the completion of the Health Check.

1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <NOServerGroup&gt; <b>AdvanceUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The Details column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.


Main Menu: Administration -> Software Management -> Upgrade

Tasks
<table>
<tr><th>Hostname</th></tr>
<tr><td>NO1</td></tr>
<tr><td>NO2</td></tr>
</table>
<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>1</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160808-140326-UTC.txt</td><td>100%</td></tr>
<tr><td>0</td><td>MP2</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP2</td><td>100%</td></tr>
<tr><td>0</td><td>IPFE1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on IPFE1</td><td>100%</td></tr>
<tr><td>0</td><td>MP1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP1</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>3
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Analyze any Health Check failure</td>
<td>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.

1. Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.
2. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
3. Locate the log entries for the most recent health check.
4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.</td>
</tr>
</table>

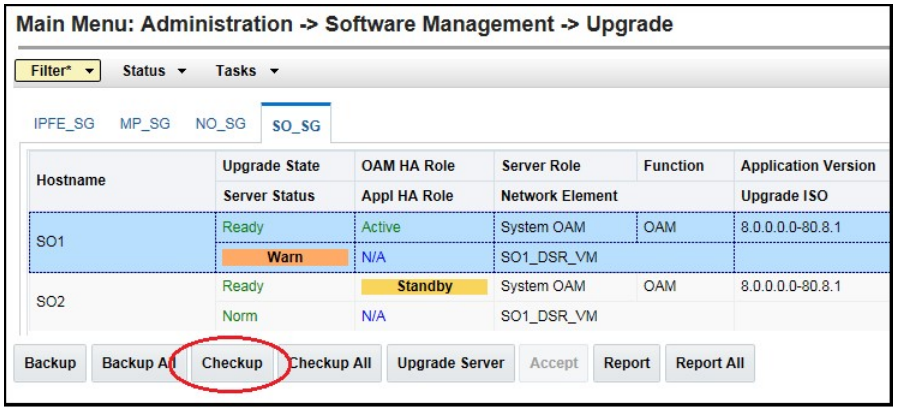
Procedure 6: Data Collection for Source Release 8.0 and later

4 □

Active NOAM VIP:

This procedure will run the automated Health Checks on the Active SOAM.

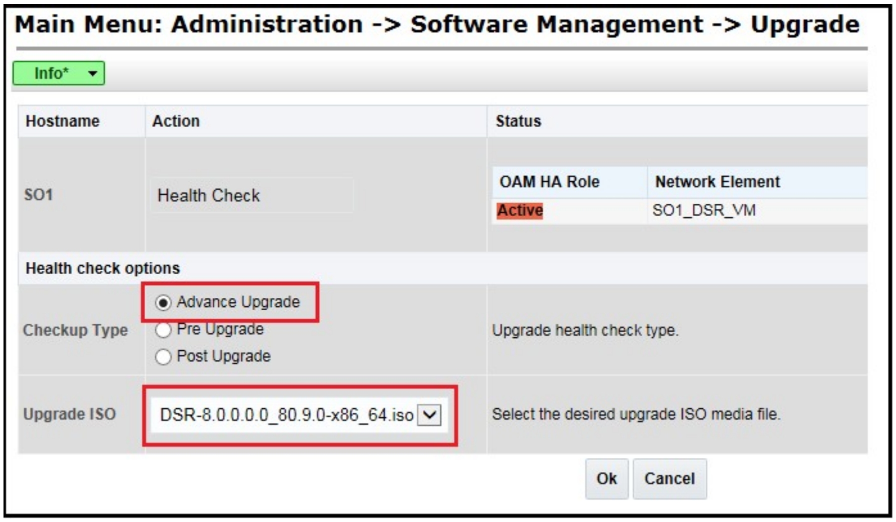
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the SOAM server group tab.
3. Select the Active SOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
SO1	Ready Warn	Active N/A	System OAM SO1_DSR_VM	OAM	8.0.0.0-80.8.1
SO2	Ready Norm	Standby N/A	System OAM SO1_DSR_VM	OAM	8.0.0.0-80.8.1

4. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
5. In the 'Health check options' section, select the **Advance Upgrade** option.
6. For a major upgrade, use the Upgrade ISO pulldown to select the target release ISO. Do not select an ISO for an incremental upgrade.
7. Click **Ok**. Control returns to the Upgrade screen.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Action	Status
SO1	Health Check	OAM HA Role: Active Network Element: SO1_DSR_VM

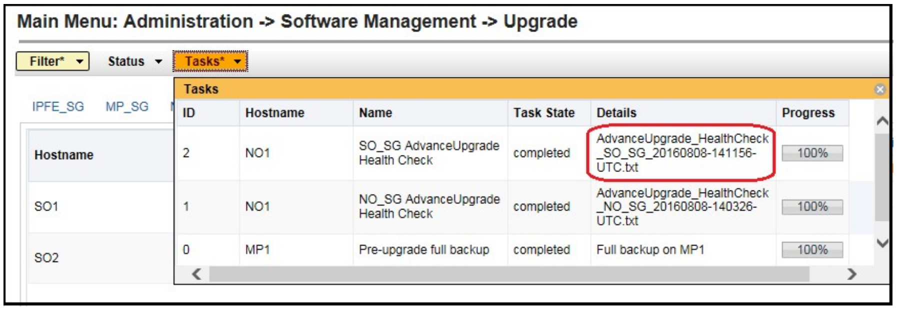
Health check options

Checkup Type	● Advance Upgrade ○ Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-8.0.0.0.0_80.9.0-x86_64.iso	Select the desired upgrade ISO media file.

Procedure 6: Data Collection for Source Release 8.0 and later

<table>
<tr>
<td>5
□</td>
<td><b><u>Active NOAM VIP:</u></b></td>
<td>Monitor for the completion of the Health Check.

1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <SOServerGroup&gt; <b>AdvanceUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The Details column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.



Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th>Hostname</th></tr>
<tr><td>SO1</td></tr>
<tr><td>SO2</td></tr>
</table>
Tasks
<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>2</td><td>NO1</td><td>SO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_SO_SG_20160808-141156-UTC.txt</td><td>100%</td></tr>
<tr><td>1</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160808-140326-UTC.txt</td><td>100%</td></tr>
<tr><td>0</td><td>MP1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP1</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>6
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Analyze Health Check failure</td>
<td>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.

1. Select <b>Status & Manage > Files</b>.
The Files screen is displayed.
2. Select the Active SOAM tab.
3. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
4. Locate the log entries for the most recent health check.
5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.

If the health check log contains the message “Unable to execute Health Check on <Active SOAM hostname>”, perform health checks in accordance with Procedure 4.</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 will be out-of-service during the upgrade sequence.

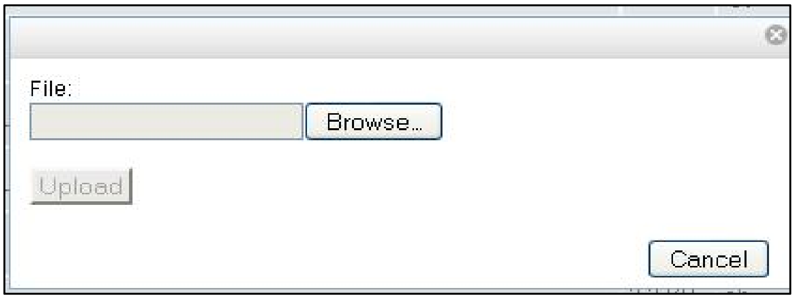
1. Analyze system topology data gathered in Section 3.4.2.1 and steps 1 through 6 of this procedure. The Health Check reports from steps 3 and 6 can be found in <b>Status & Manage > Files</b> on the Active NOAM.
2. It is recommended to plan for MP upgrades by consulting MOS to assess the impact of out-of-service MP servers
3. Determine the manner in which the MP servers will be upgraded: Manually or Automated Server Group Upgrade. If the MPs will be upgraded manually, determine the exact sequence in which MP servers will be upgraded for each site.</td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></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 prior to, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 7: DSR ISO Administration

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">This procedure transfers the target ISO to all servers in the topology.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u></b></td></tr>
<tr><td><b>1</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
Upload ISO to Active NOAM server</td><td>There are two methods to upload the application ISO to the Active NOAM based on the type of the media: Execute either:
<b>Option 1</b> (Use NOAM GUI Upload function for ISO file transfer over the network)
<b>Proceed to step 2.</b>
<b><u>OR</u></b>
<b>Option 2</b> (Local site media ISO transfer, using PM&C).
<b>Proceed to step 6.</b></td></tr>
<tr><td><b>2</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
Option 1 - Transfer via NOAM GUI</td><td><b><u>OPTION 1:</u></b> 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:
1. Log into the Active NOAM GUI.
2. Select <b>Status & Manage > Files</b>
The Files menu is displayed
3. Click the Active NOAM tab to display all files stored in the file management storage area of this server.
4. 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 that they are the same and the status is <b>ACTIVE</b> in the session banner.
5. Click the <b>Upload</b> button. The Browse window will open:
Note: actual screens may vary from those shown below, depending on the browser and browser version used.

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

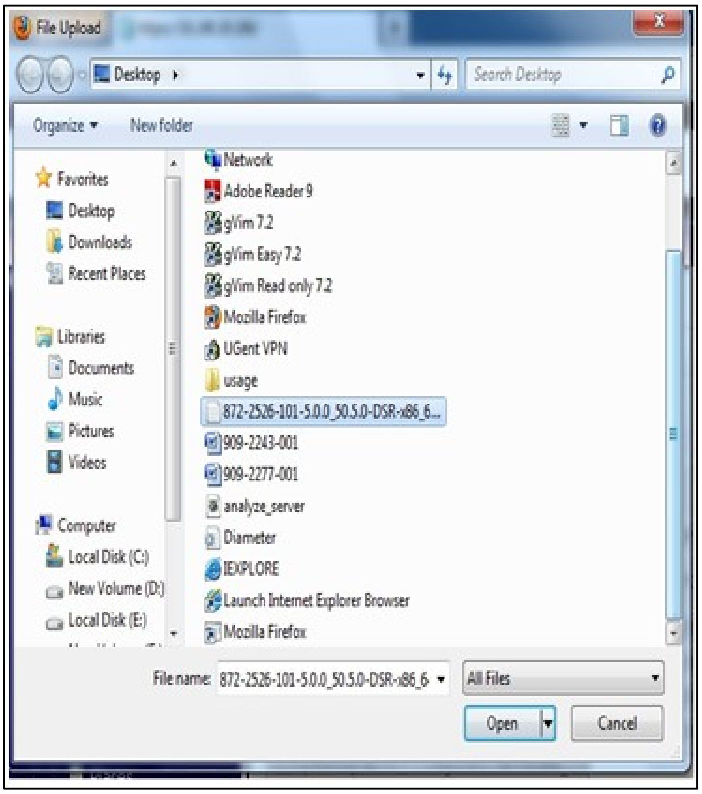
Procedure 7: DSR ISO Administration

3 □

Active NOAM VIP:

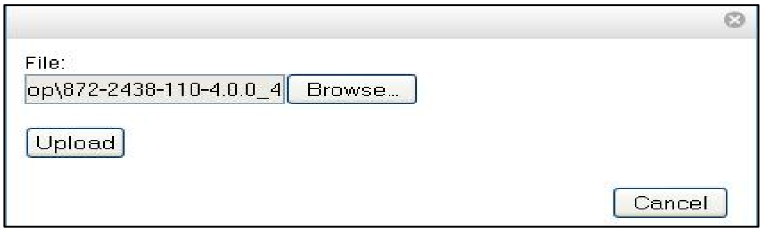
Option 1 (cont)

1. Click **Browse** to select the file to upload.
2. The Choose File window displays, allowing selection of the file to upload.



File name: 872-2526-101-5.0.0_50.5.0-DSR-x86_6

3. Select the target release ISO image file and click **Open**.
4. The selected file and its path display on the screen.



File: op\872-2438-110-4.0.0_4

5. Click **Upload.**
   The ISO file begins uploading to the file management storage area.
6. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This will usually take between 2 to 10 minutes, but more if the network upload speed is slow.

Procedure 7: DSR ISO Administration

4
☐
	Active NOAM VIP:
	Option 1 (cont)
		1. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This will usually take between 2 to 10 minutes, but more if the network upload speed is slow.
		2. To back up the ISO file to the PM&C, SSH to the Active NOAM and execute the following command. Refer to [4] for creating space on PM&C if desired space is not available on the PM&C:
		1) cd to the directory on the Active NOAM where the ISO image is located
		`$ cd /var/TKLC/db/filemgmt`
		2) Using sftp, connect to the PM&C management server
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		3) After the image transfer is 100% complete, close the connection
		`$ quit`
		NOTE: *UserId and password should already be recorded in Table 5.*

5
☐
	Active NOAM VIP:
	Option 1 (cont) - Copy ISO to the Standby NOAM
	For an Active NOAM on release 6.0 or 7.0.x
		If the Active NOAM is on release 6.0 or 7.0.x, perform this step; otherwise, proceed to step 11.
		Copy the ISO file to the Standby NOAM.
		1. Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM:
		`ssh admusr@<NOAM_VIP>`
		`password:    <enter password>`
		2. 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`
		3. Execute Steps 3 to 7 of Appendix F to add the ISO image to the PM&C software inventory.
		Proceed to step 8 to complete this procedure

6
☐
	PM&C Guest:
	Option 2 - Transfer via PM&C
		OPTION 2 (Local site media ISO transfer, using PM&C):
		Using a Media containing the application (recommended for slow network connections between the client computer and the DSR frame
		1. Execute Appendix F to load the ISO onto the PM&C server at the site.
		2. SSH into the PM&C server and SCP the ISO to the Active NOAM using the following commands:
		`sudo scp -p /var/TKLC/smac/image/repository/`
		`<DSR_ISO_Filename>`
		`admusr@<Active_NOAM_IP>:/var/TKLC/db/filemgmt`

Procedure 7: DSR ISO Administration

7 □

Active NOAM CLI:

Option 2 (cont) - Copy ISO to Standby NOAM

1. Log into the Active NOAM and execute the following command :

```
sudo chmod 644 /var/TKLC/db/filemgmt/<DSR_ISO_Filename>
```

2. If the Active NOAM is on release 6.0 or 7.0.x,, copy the ISO file to the Standby NOAM using the following command:

```
sudo scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename>
admusr@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt
```

8 □

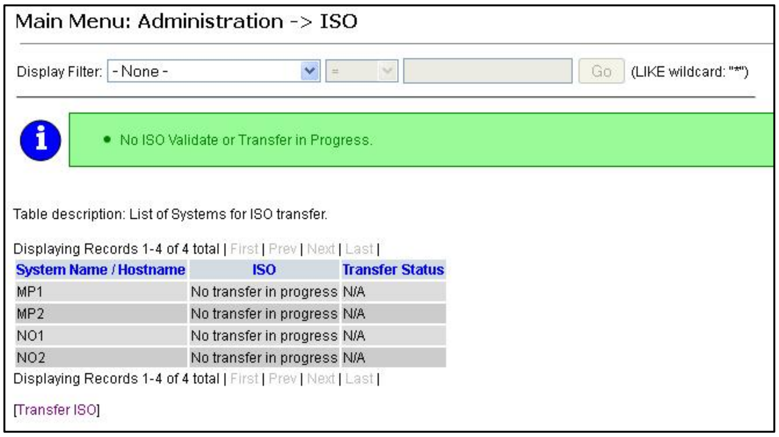
Active NOAM VIP:

Using NOAM GUI, transfer ISO to all servers to be upgraded.

For Active NOAM on release 6.0 or 7.0.x

Transfer the target release ISO image file from the Active NOAM to all other DSR servers.

1. Navigate to **Administration >Software Management > ISO Deployment**
2. Click "**Transfer ISO"**



Main Menu: Administration -> ISO

Display Filter: - None - = Go (LIKE wildcard: "*")

- No ISO Validate or Transfer in Progress.

Table description: List of Systems for ISO transfer.

Displaying Records 1-4 of 4 total | First | Prev | Next | Last |

System Name / Hostname	ISO	Transfer Status
MP1	No transfer in progress	N/A
MP2	No transfer in progress	N/A
NO1	No transfer in progress	N/A
NO2	No transfer in progress	N/A

Displaying Records 1-4 of 4 total | First | Prev | Next | Last |

[Transfer ISO]

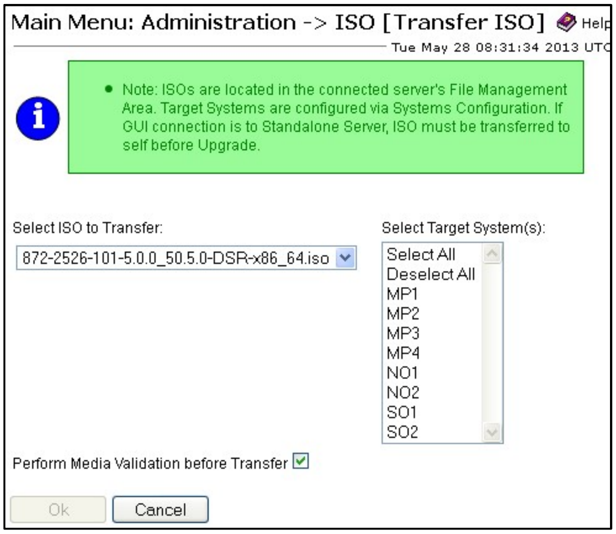
9 □

Active NOAM VIP:

Using NOAM GUI, transfer ISO to all servers to be upgraded.

For Active NOAM on release 6.0 or 7.0.x

1. Under **Select ISO to Transfer:** drop down menu, select the DSR 8.0 ISO. Under **Select Target System(s):** click **Select All**.
2. Select the checkbox next to **Perform Media Validation before Transfer**.



Main Menu: Administration -> ISO [Transfer ISO] Help

Tue May 28 08:31:34 2013 UTC

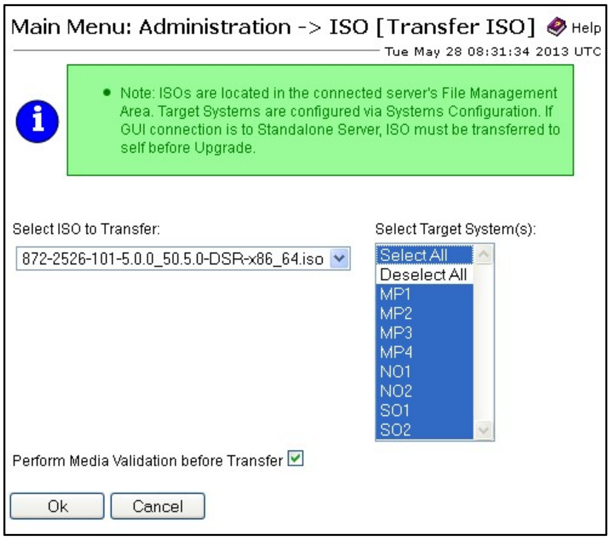
- Note: ISOs are located in the connected server's File Management Area. Target Systems are configured via Systems Configuration. If GUI connection is to Standalone Server, ISO must be transferred to self before Upgrade.

Select ISO to Transfer: 872-2526-101-5.0.0_50.5.0-DSR-x86_64.iso

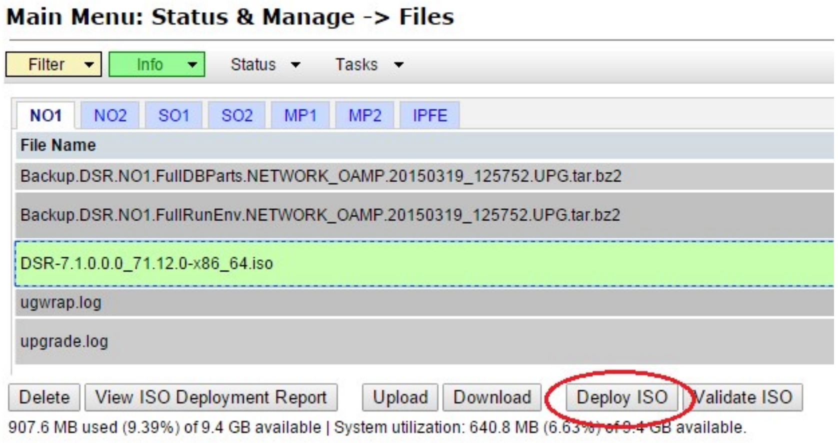
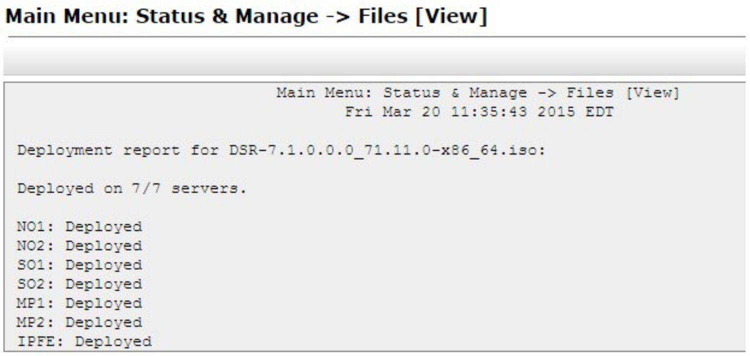
Select Target System(s): Select All, Deselect All, MP1, MP2, MP3, MP4, NO1, NO2, SO1, SO2

Perform Media Validation before Transfer ☑

Procedure 7: DSR ISO Administration

10 □	**Active NOAM VIP:** ISO transfer continued **For Active NOAM on release 6.0 or 7.0.x**	1. Click **Ok** 2. Control will return 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.  Main Menu: Administration -> ISO [Transfer ISO] Tue May 28 08:31:34 2013 UTC • Note: ISOs are located in the connected server's File Management Area. Target Systems are configured via Systems Configuration. If GUI connection is to Standalone Server, ISO must be transferred to self before Upgrade. Select ISO to Transfer: 872-2526-101-5.0.0_50.5.0-DSR-x86_64.iso Select Target System(s): Select All, Deselect All, MP1, MP2, MP3, MP4, NO1, NO2, SO1, SO2 Perform Media Validation before Transfer ☑ 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 to contact MOS for assistance.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Procedure 7: DSR ISO Administration

11 □	**Active NOAM VIP:** Using NOAM GUI, deploy ISO to all servers to be upgraded. **For Active NOAM on release 7.1.x and later**	**This step is for an Active NOAM on release 7.1.x and later.** Deploy ISO to all servers. 1. Select **Status & Manage > Files** The Files menu is displayed 2. Click the Active NOAM server tab. All files stored in the file management storage area of this server display on the screen. 3. Select the DSR 8.0 ISO, and click the **View ISO Deployment Report** button. 4. In the resulting report, determine if the ISO has been deployed to all servers in the system. 5. If the ISO has been deployed to all servers, proceed to the next procedure; otherwise, complete the remaining steps in this procedure. 6. Select the 8.0 DSR ISO in the file list, and click the **Validate ISO** button. Click **Ok** on the resulting confirmation dialog box. 7. 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 to contact MOS. 8. If the ISO is valid, select the ISO, and click the **Deploy ISO** button. Click **Ok** on the resulting confirmation dialog box.  Main Menu: Status & Manage -> Files Filter Info Status Tasks NO1 NO2 SO1 SO2 MP1 MP2 IPFE Delete View ISO Deployment Report Upload Download Deploy ISO Validate ISO File Name Backup.DSR.NO1.FullDBParts.NETWORK_OAMP.20150319_125752.UPG.tar.bz2 Backup.DSR.NO1.FullRunEnv.NETWORK_OAMP.20150319_125752.UPG.tar.bz2 DSR-7.1.0.0.0_71.12.0-x86_64.iso ugwrap.log upgrade.log 907.6 MB used (9.39%) of 9.4 GB available | System utilization: 640.8 MB (6.63%) of 9.4 GB available.
12 □	**Active NOAM VIP:** Monitor ISO deployment **For Active NOAM on release 7.1.x and later**	The deployment progress can be monitored by viewing the tasks dropdown list on the **Status & Manage > Files** screen. 1. Select the target release ISO, and click the **View ISO Deployment Report** button. Monitor deployment progress until 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

Procedure 7: DSR ISO Administration

THIS PROCEDURE HAS BEEN COMPLETED.

3.4.4 ISO Link Correction

This procedure is required when upgrading from Release 7.1, 7.2, or 7.3 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, in order to support the Storage Reclamation feature used in DSR 8.0, in preparation for future Dual Image Upgrade, the symlinks to the ISO image in the /var/TKLC/db/filemgmt/isos directory must be removed and replaced with direct copies of the ISO image in the /var/TKLC/upgrade directory. This must be executed after the application ISO has been deployed but before the software upgrade in Section 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 6.0, 7.0, or 8.x.

!! WARNING!! **FAILURE TO PERFORM THIS PROCEDURE MAY CAUSE THE UPGRADE TO FAIL**

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. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
1 □	Verify this procedure should be run.	Verify that this procedure should be run: 1. Is the topology of servers to be upgraded currently running DSR release 7.1, 7.2, 7.3, or 7.4? 2. Has the DSR 8.0 ISO been deployed? If “Yes” to the above questions, then proceed to step 2. If “No”, this procedure is complete.
2 □	**Active NOAM GUI:** Undeploy all unneeded ISO images.	Use the **Undeploy ISO** button on the **Status & Manage > Files** screen to **remove all unneeded old** ISO images from the /var/TKLC/upgrade directory. Keep deployed the ISO image file being used for this upgrade. This will save space in the /var/TKLC/upgrade directory. 1. Select **Status & Manage > Files** The Files screen displays. 2. Select the ISOs to be undeployed and click the ‘**Undeploy ISO**’ button. 3. 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 pull-down Tasks menu message box at the top of the Files page displays the status of the undeployment for each server. In addition, an ISO Deployment report can be viewed by selecting the ISO and clicking **View ISO Deployment Report**
3 □	**Active NOAM CLI:** Log into the Active NOAM	Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM: `ssh admusr@<NOAM_VIP>`

Procedure 8: ISO Link Correction

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.

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 will use 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 will occur 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 to contact MOS for guidance.

THIS PROCEDURE HAS BEEN COMPLETED.

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 WILL BE LOST

3.4.5.1 Full Backup of DB Run Environment for Release 6.0, 7.0.x

This procedure is used to backup the DB run environment when the Active NOAM is on release 6.0 or 7.0.x.

Procedure 9: Full Backup of DB Run Environment for Release 6.0, 7.0.x

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND** **ASK FOR UPGRADE 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 will create a no-hang-up shell session, so that the command will continue 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 will remotely access each server managed by the NOAM, and run 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 will indicate successful completion:

```
Script Completed. Status:
HOSTNAME                          | STATUS
--------------------------------------------
HPC3blade02                       | PASS
HPC3blade01                       | PASS
HPC3blade03                       | PASS
HPC3blade04                       | PASS
```

(Errors will 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” is used to show active screen sessions on a server, and “screen -dr” is used to re-enter a disconnected screen session.

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 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 will indicate 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 that backup files are present on each server.

1. Log into the Active NOAM.
2. Select **Status & Manage > Files**
   The **Files** menu is displayed
3. Click on each server tab, in turn
4. For each server, verify that 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>.U
PG.tar.bz2
```

THIS PROCEDURE HAS BEEN COMPLETED.

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

This procedure is used to backup the DB run environment when the Active NOAM is on release 7.1.x and later.

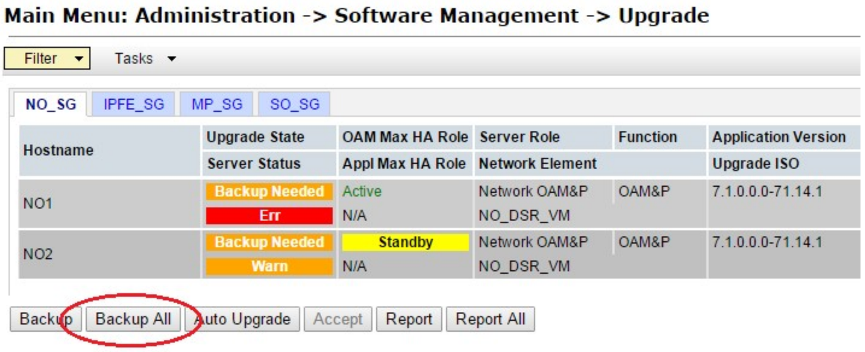
Procedure 10: Full Backup of DB Run Environment for Release 7.1.x and later

<table>
<tr><td>S
T
E
P
#</td><td colspan="2">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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u></b></td></tr>
<tr><td>1
□</td><td><b><u>Active NOAM VIP:</u></b>

Start backup of all servers</td><td>1. Login to the NOAM GUI using the VIP.
<b>2.</b> Navigate to <b>Administration > Software Management > Upgrade.</b>
3. Click the <b>Backup All</b> button.

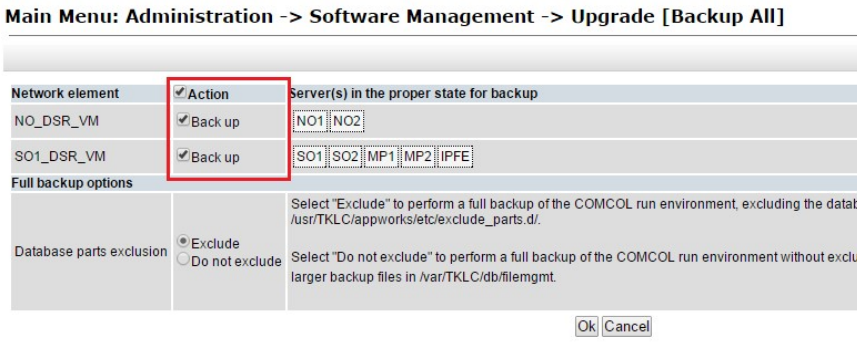

<b>Main Menu: Administration -> Software Management -> Upgrade</b>

Filter
Tasks
NO_SG
IPFE_SG
MP_SG
SO_SG
<table>
<tr><td>Hostname</td><td>Upgrade State
Server Status</td><td>OAM Max HA Role
Appl Max HA Role</td><td>Server Role
Network Element</td><td>Function</td><td>Application Version
Upgrade ISO</td></tr>
<tr><td>NO1</td><td>Backup Needed
Err</td><td>Active
N/A</td><td>Network OAM&P
NO_DSR_VM</td><td>OAM&P</td><td>7.1.0.0.0-71.14.1</td></tr>
<tr><td>NO2</td><td>Backup Needed
Warn</td><td>Standby
N/A</td><td>Network OAM&P
NO_DSR_VM</td><td>OAM&P</td><td>7.1.0.0.0-71.14.1</td></tr>
</table>
Backup
Backup All
Auto Upgrade
Accept
Report
Report All

</td></tr>
<tr><td>2
□</td><td><b><u>Active NOAM VIP:</u></b>

Select network elements to backup</td><td>The Upgrade [Backup All] screen is displayed. This screen displays the various Network Elements, and identifies which servers are ready for backup.

1. In the <b>Action</b> column, select the <b>Back up</b> checkbox for each Network Element.
2. Ensure the ‘Exclude’ radio button is selected.
3. Click the <b>Ok</b> button. This initiates a full backup on each eligible server.


<b>Main Menu: Administration -> Software Management -> Upgrade [Backup All]</b>
<table>
<tr><td>Network element</td><td>☑ Action</td><td>Server(s) in the proper state for backup</td></tr>
<tr><td>NO_DSR_VM</td><td>☑ Back up</td><td>NO1 NO2</td></tr>
<tr><td>SO1_DSR_VM</td><td>☑ Back up</td><td>SO1 SO2 MP1 MP2 IPFE</td></tr>
<tr><td colspan="3">Full backup options</td></tr>
<tr><td>Database parts exclusion</td><td>● Exclude
○ Do not exclude</td><td>Select "Exclude" to perform a full backup of the COMCOL run environment, excluding the datab
/usr/TKLC/appworks/etc/exclude_parts.d/.

Select "Do not exclude" to perform a full backup of the COMCOL run environment without exclu
larger backup files in /var/TKLC/db/filemgmt.</td></tr>
</table>
</td></tr>
</table>

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

STEP #

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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**

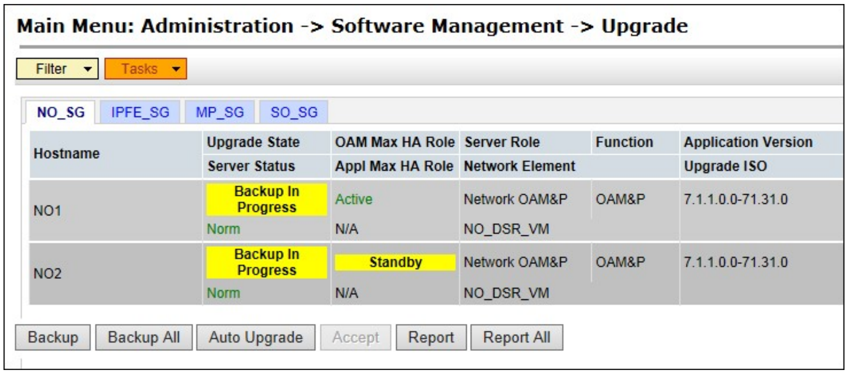
3 □

Active NOAM VIP:

Monitor backup progress

Monitor the upgrade progress.

1. Select each server group tab and verify that each server transitions from ‘Backup in Progress’ to ‘Ready’.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO
NO1	Backup In Progress	Active	Network OAM&P	OAM&P	7.1.1.0.0-71.31.0
	Norm	N/A	NO_DSR_VM		
NO2	Backup In Progress	Standby	Network OAM&P	OAM&P	7.1.1.0.0-71.31.0
	Norm	N/A	NO_DSR_VM		

4 □

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 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 will indicate 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.
```

5 □

Active NOAM VIP:

Verify that backup files are present on each server.

1. Log into the Active NOAM.
2. Select **Status & Manage > Files**
   The Files menu is displayed
3. Click on each server tab, in turn
4. For each server, verify that 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.t
ar.bz2
```

THIS PROCEDURE HAS BEEN COMPLETED.

3.4.6 Upgrade TVOE Hosts at a Site

This procedure applies if the TVOE Hosts at a site will be upgraded BEFORE the start of the DSR 8.0 upgrade. Performing the TVOE upgrade BEFORE reduces the time required for DSR and IDIH Application Upgrade procedures during the maintenance window. This procedure should be initiated and completed prior to starting the DSR upgrade procedures in Section 4.

NOTE: *If the TVOE Hosts will be upgraded in the same maintenance windows as the DSR and IDIH servers, then this procedure does not apply.*

PRECONDITION: *The PM&C application at each site (and the TVOE Host running the PM&C virtual server, must be upgraded before performing TVOE Host OS upgrade for servers that are managed by this PM&C. Refer to [4] for PM&C upgrade procedures. If any DSR applications are hosted on the same server as the PM&C application, restart the DSR applications after the PM&C upgrade is complete (see Procedure 64 step 5).*

IMPACT: *TVOE Host upgrades require that the DSR, SDS, or IDIH applications running on the host be shut down for up to 30 minutes during the upgrade.*

Note: In RMS and VEDSR configurations, the PM&C and DSR servers could be sharing the same TVOE Host. Make the customer aware of all servers affected by the TVOE upgrade.

Table 10: TVOE Upgrade Execution Overview

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 11	60 min per TVOE Host*	1:00-16:00	Upgrade TVOE Hosts	DSR and IDIH servers running as virtual guests on the TVOE host will be stopped and unable to perform their role while the TVOE Host is being upgraded.

* **WARNING:** Depending on the risk tolerance of the customer, it is possible to execute multiple TVOE Upgrades in parallel. Detailed steps are shown in the procedure on the next page.

Procedure 11: Upgrade TVOE Hosts

S T E P #	This procedure upgrades the TVOE Hosts for a site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.	
1. □	Record site	Record Site to be upgraded _____________________

Procedure 11: Upgrade TVOE Hosts

2. □	Select order of TVOE server upgrades	Record the TVOE Hosts to be upgraded, in order: (It is best to upgrade Standby servers before Active servers, to minimize failovers. Otherwise, any order is OK.) ______________________ ______________________ ______________________ ______________________ ______________________ ______________________ **NOTE:** *The site PM&C, "Software Inventory" form, will typically list the TVOE Hosts at a site, and their versions.*
3. □	Upload TVOE ISO to PM&C	Execute Appendix F to add the TVOE ISO to the PM&C software inventory.

4.
□
	Determine if there are SDS Applications on the TVOE Hosts	Log into the TVOE Hosts and display the guests.
		1. SSH to the TVOE and log in.
		If the TVOE version is 2.5.2:
		`ssh root@<TVOE_ip>`
		`password:  <enter password>`
		If the TVOE version is 2.7 or later:
		`ssh admsur@<TVOE_ip>`
		`password:  <enter password>`
		2. Execute the following command to display all the VM guests running:
		If the TVOE version is 2.5.2:
		`# virsh list --all`
		If the TVOE version is 2.7 or later:
		`$ sudo virsh list --all`
		If the application list includes SDS SOAM applications, then make this team aware of possible failovers, and expected alarms due to running in simplex mode during the TVOE upgrade.

5. □	Upgrade the TVOE hosting a DSR or IDIH server	Upgrade the TVOE Host of the first server. **Execute Error! Reference source not found. to shutdown the TVOE Host to be upgraded** **Execute Appendix K.1 to upgrade the TVOE Host** **NOTE: This step may cause a failover of the DSR or other active applications on the TVOE.**
6. □	Repeat for other TVOE Hosts at a site	Repeat step 5 for each TVOE Host at the site requiring upgrade.
	THIS PROCEDURE HAS BEEN COMPLETED	

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 will 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 K.2 and may be performed at any time after Procedure 12.

Table 11. IDIH Upgrade Preparation Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
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 FD config scripts for the Mediation and Application guests.

Procedure 12: IDIH Upgrade Preparation

STEP #	This procedure prepares the FD config scripts that will be used to create the Mediation and Application guests. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**	

1
□
	PM&C CLI:
	Login to the PM&C server
		Login in to the PM&C server as the admusr user.
		`ssh <PM&C IP address>`
		`login as:    admusr`
		`password:    <enter password>`

2
□
	PM&C CLI:
	Copy the ISOs to PM&C
		1. Add the Application ISO images (Mediation, Application, and Oracle) and the TPD ISO to the PM&C, this can be done in one of three ways:
		a. Insert the Application CD required by the application into the removable media drive.
		b. Attach the USB device containing the ISO image to a USB port.
		c. Copy the Application iso file to the PM&C server into the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
		cd into the directory where your ISO image is located on the TVOE Host (not on the PM&C server)
		Using sftp, connect to the PM&C server:
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		2. Execute Appendix F to add the ISO to the PM&C software inventory.
		3. Repeat the above steps for the Application, Mediation, Oracle and TPD ISOs.
		4. After the all images are transferred, close the connection:
		`$ quit`
		Note: If there is insufficient disk space in the PMAC pmacftpuser local directory, refer to section “Configure PM&C Application Guest isoimages Virtual Disk” of [15] to increase the storage allocation.

Procedure 12: IDIH Upgrade Preparation

3 □

IDIH CLI:

Perform a system health check on the guest

Perform a system health check.

1. Login in to the Oracle guest as the admusr user.

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

2. 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 to contact MOS for guidance.

THIS PROCEDURE HAS BEEN COMPLETED

3.5 Software Upgrade Execution Overview

It is recommended to contact MOS as described in Appendix S *prior* to 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 will be upgraded first.

If alarms are present on the server, it is recommended to contact MOS 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 MOS 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? ____________

  What DSR applications are running in a TVOE Host environment? ________________

  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? _____________

3.6 Accepting 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 **Appendix A** are performed in a separate Maintenance Window to finalize the upgrade. Procedure 53 “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 will be disabled before upgrading the NOAM servers. Provisioning activities at the NOAM and SOAM servers will have certain limitations during the period where the NOAMs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in table below specifies the time with and without TVOE upgrade.
If the TVOE Host upgrades are not needed, or were previously performed, then the time estimates without TVOE upgrade will apply. All times are estimates.

Table 12: NOAM Upgrade Execution Overview

Procedure	**Elapsed Time (hr:min)**		**Procedure Title**	**Impact**
	This Step	**Cumulative**		
Procedure 13	0:05	0:05	NOAM Pre-Upgrade Health Checks	None
Procedure 14	0:30-1:00	0:35-1:05	NOAM Health Check for Source Release 6.0	None
or Procedure 15	0:30-0:45	0:35-0:50	NOAM Health Check for Source Release 7.0.x, 7.1.x	None
or Procedure 16	0:20-0:30	0:25-0:35	NOAM Health Check for Source Release 7.2, 7.3	None
or Procedure 17	0:20-0:30	0:25-0:35	NOAM Health Check for Source Release 8.0	None
Procedure 18	0:05-0:10	0:30-1:15	NOAM Pre-Upgrade Backup	None
Procedure 19	0:01-0:05	0:31-1:20	Disable Global Provisioning	Global Provisioning Disabled
Procedure 20[1]	0:40-1:20	1:11-2:40	NOAM Upgrade	No Traffic Impact
Procedure 21	0:01-0:05	1:12-2:45	PCA Topology Hiding Configuration	No Traffic Impact
Procedure 22	0:05-0:15	1:17-3:00	Verify NOAM Post Upgrade Status	None
Procedure 23	0:05-0:10	1:22-3:10	Allow Provisioning	Global Provisioning Enabled

[1] **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 8.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 8.0 Application upgrade, then see* ***[****Table 10****]*** *for additional time estimates associated with TVOE upgrade.*

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 prior to Procedure 20.

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 Pre-Upgrade Health Checks

This procedure performs the pre-upgrade health checks that are common to all source releases.

Procedure 13: NOAM Pre-Upgrade Health Checks

S T E P #	This procedure makes a record of the TVOE software versions and verifies that a recent backup exists for all servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	Verify that NOAM TVOE Host upgrades have been completed (before starting DSR upgrade).	**IMPORTANT:** Verify the revision level of the TVOE Host systems for the NOAM and DR-NOAM servers. If they are not on the required release, then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix J for the steps to verify the TVOE Host revision level. (This can also be done from the PM&C Software Inventory screen.) Complete this information: NOAM-A TVOE Host Rev ____________________ NOAM-B TVOE Host Rev ____________________ DR-NOAM-A TVOE Host Rev _________________ DR-NOAM-B TVOE Host Rev _________________ Will TVOE Upgrades be performed during the DSR Application Upgrades? __________

Procedure 13: NOAM Pre-Upgrade Health Checks

2.
□
	Active NOAM VIP:
	Verify that backups are created for all servers
		Verify that a recent COMCOL Environment backup has been performed.
		1. Select **Status and Manage > Files.**
		2. Select each server tab, in turn.
		3. 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`
		See **Section 3.4.5** to perform (or repeat) a full Backup, if needed.
		4. Repeat sub-steps 1 through 3 for each site.

	THIS PROCEDURE HAS BEEN COMPLETED.	

4.1.2 NOAM Health Check for Source Release 6.0

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 6.0. This procedure must be executed on the Active NOAM.

🛑	**!WARNING!**	**THE NOAM AND DR-NOAM SITES MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.** **SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, WITH MATED SITES IN SEPARATE MAINTENANCE WINDOWS.**

Procedure 14: NOAM Health Check for Source Release 6.0

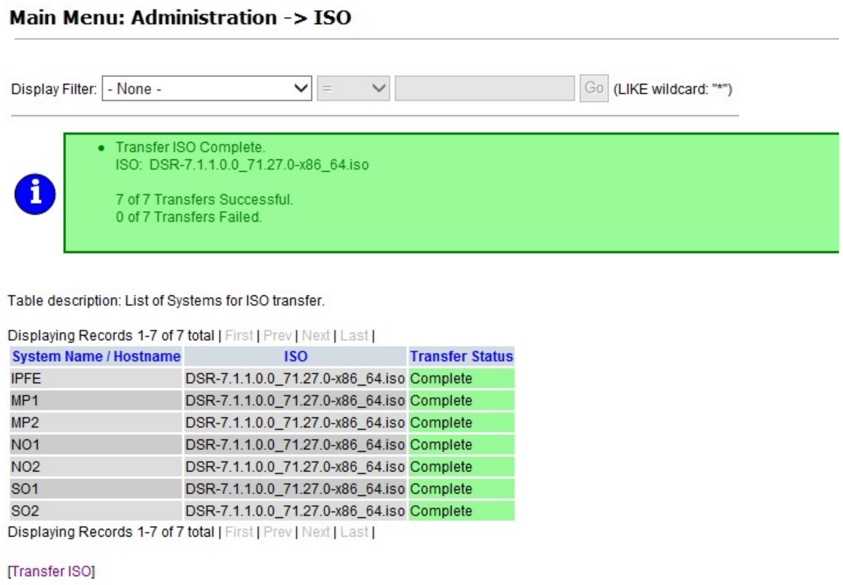
S **T** **E** **P** **#**	This procedure performs a Health Check of the system prior to upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.

Procedure 14: NOAM Health Check for Source Release 6.0

<table>
<tr><td>1
☐</td><td>**Active NOAM VIP:**

Verify ISO for Upgrade has been deployed</td><td>Verify the DSR ISO file has been transferred to all servers.

1. Navigate to **Administration > Software Management > ISO Deployment**
2. Verify the “**Transfer Status**” is “**Complete**” for each server in the topology.
3. If any server shows “**Not Complete**”, perform Section 3.4.3 DSR ISO Administration


Main Menu: Administration -> ISO

Display Filter: - None - = Go (LIKE wildcard: "*")

• Transfer ISO Complete.
ISO: DSR-7.1.1.0.0_71.27.0-x86_64.iso

7 of 7 Transfers Successful.
0 of 7 Transfers Failed.

Table description: List of Systems for ISO transfer.

Displaying Records 1-7 of 7 total | First | Prev | Next | Last |
<table>
<tr><th>System Name / Hostname</th><th>ISO</th><th>Transfer Status</th></tr>
<tr><td>IPFE</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>MP1</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>MP2</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>NO1</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>NO2</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>SO1</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
<tr><td>SO2</td><td>DSR-7.1.1.0.0_71.27.0-x86_64.iso</td><td>Complete</td></tr>
</table>
Displaying Records 1-7 of 7 total | First | Prev | Next | Last |

[Transfer ISO]</td></tr>
<tr><td>2
☐</td><td>**Active NOAM VIP:**

Verify Server Status is Normal - NOAM</td><td>Verify server status is normal for all servers.

1. Select **Status & Manage > Server.**
The Server Status screen is displayed.
2. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc).
3. Do not proceed with the upgrade if any server status displayed is not **Norm**.
4. Do not proceed if there are any Major or Critical alarms.

The following expected alarm will occur after the first NOAM upgrade, and will clear after the second NOAM is upgraded:

Alarm ID = **31233 (HA Secondary Path Down)**

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.</td></tr>
<tr><td>3
☐</td><td>**Active NOAM VIP:**

Log all current alarms at NOAM</td><td>View active alarms.

1. Select **Alarms & Events > View Active.**
The Alarms & Events > View Active screen is displayed.
2. Click the **Report** button to generate an Alarms report.
3. Save the report and/or print the report. Keep these copies for future reference.</td></tr>
<tr><td>4
☐</td><td>**Active NOAM VIP:**

View Communication Agent status</td><td>View ComAgent connection status.

1. Select **Communication Agent > Maintenance > Connection Status;**
The Communication Agent > Connection Status screen is displayed.
2. Expand each server entry. Verify the Connection Status of each connection is InService.</td></tr>
</table>

Procedure 14: NOAM Health Check for Source Release 6.0

5 □	**Active NOAM VIP:** View SBR status (if equipped)	View SBR status if PDRA/PCA is enabled. **If the Active NOAM is on release 6.0:** 1. Select **Policy DRA > Maintenance > Policy SBR Status** The Policy SBR Status screen is displayed. 2. Expand each Server Group. Verify Congestion Level is 'Normal' for all servers. **If the Active NOAM is on release 7.0.x, 7.1.x:** 1. Select **Policy and Charging > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding** tab. 3. Expand each Server Group. 4. Verify Congestion Level is 'Normal' for all servers. 5. Repeat sub-steps 3 and 4 for the **PDRA Mated Triplet** tab. **If the Active NOAM is on release 7.2 and later:** 1. Select **SBR > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding Region** tab. 3. Expand each Server Group. 4. Verify Congestion Level is '**Normal**' for all servers. 5. Repeat sub-steps 3 and 4 for the **Mated Site** tab.
6 □	**Active NOAM VIP:** Export and archive the Diameter configuration data	Export the diameter configuration data. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry labeled "**ALL**". 3. Click the '**Ok**' button. 4. Verify the data export is complete using the tasks button at the top of the screen. 5. Browse 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.
7 □	**Active NOAM VIP:** Export and archive Configuration Places data	Export the Configuration Places data. 1. **Main Menu > Configuration > Places** 2. Click the **Report** at the bottom of the table to generate a report for all entries. 3. Save the report and/or print the report. Keep these copies for future reference.
8 □	**Active SOAM VIP:** Log all current alarms at SOAM	Log active site alarms. 1. Log into the SOAM GUI using the VIP. 2. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 3. Click the **Report** button to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference.
9 □	**Active SOAM VIP:** View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established**
10 □	**Active SOAM VIP:** Verify application status	Verify application status 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is 'Available' for all applications

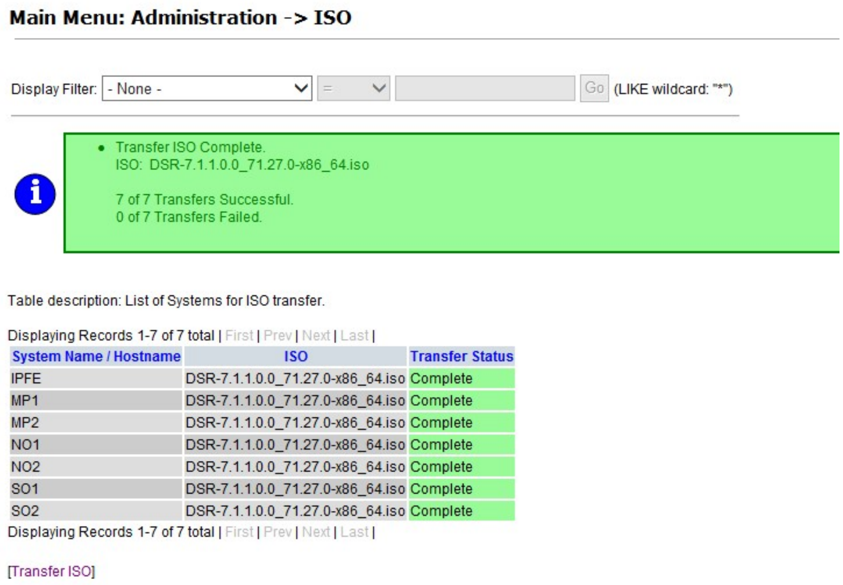
Procedure 14: NOAM Health Check for Source Release 6.0

11 □	Repeat for each Network Element	Repeat **Steps 8 - 10** for each SOAM site in the topology.
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.1.3 NOAM Health Check for Source Release 7.0.x, 7.1.x

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 7.0.x or 7.1.x. This procedure must be executed on the Active NOAM.

Procedure 15: NOAM Health Check for Source Release 7.0.x, 7.1.x

STEP #	This procedure performs a Health Check of the system prior to upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.	
1 □	**Active NOAM VIP:** Verify upgrade ISO has been deployed **For Active NOAM on release 7.0.x only**	**This step is for an Active NOAM on release 7.0.x. 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. 1. Navigate to **Administration > Software Management > ISO Deployment** 2. Verify the **Transfer Status** is "**Complete**" for each server in the topology. 3. If any server shows "**Not Complete**", perform Section 3.4.3 DSR ISO Administration  **Proceed to step 3 to complete this procedure.**

Main Menu: Administration -> ISO

- Transfer ISO Complete.
  ISO: DSR-7.1.1.0.0_71.27.0-x86_64.iso

  7 of 7 Transfers Successful.
  0 of 7 Transfers Failed.

Table description: List of Systems for ISO transfer.

Displaying Records 1-7 of 7 total | First | Prev | Next | Last |

System Name / Hostname	ISO	Transfer Status
IPFE	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
MP1	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
MP2	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
NO1	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
NO2	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
SO1	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete
SO2	DSR-7.1.1.0.0_71.27.0-x86_64.iso	Complete

Displaying Records 1-7 of 7 total | First | Prev | Next | Last |

Procedure 15: NOAM Health Check for Source Release 7.0.x, 7.1.x

2 □

Active NOAM VIP:

Verify ISO for upgrade has been deployed

For Active NOAM on release 7.1.x only

This step is for an Active NOAM on release 7.1.x.

Verify the DSR ISO file has been transferred to all servers.

1. Navigate to **Status & Manage > Files**
2. Select the target release DSR ISO and click "**View ISO Deployment Report**".
3. 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
```

3 □

Active NOAM CLI:

Verify NOAM pre-Upgrade Status

Execute the following commands on the Active DSR NOAM and Active DR NOAM servers.

1. 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.

2. 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 message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears 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 to contact MOS for guidance.

4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

Procedure 15: NOAM Health Check for Source Release 7.0.x, 7.1.x

4 □	**Active NOAM VIP:** Export and archive the Diameter configuration data	Export Diameter configuration data. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry labeled “**ALL**”. 3. Verify the data export is complete using the tasks button at the top of the screen. 4. Browse 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.

5
□
	Active SOAM CLI:
	Pre-upgrade health checks
		Execute SOAM pre-upgrade alarm status health checks.
		1. 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.
		2. 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 message “**FIPS integrity verification test failed**” may be output when the upgradeHealthCheck command runs. This message can be ignored.
		3. Keep this report for future reference. This report will be 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. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message “**FIPS integrity verification test failed**” may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. 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. 1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. Note: The message “**FIPS integrity verification test failed**” may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify Operational Status is ‘**Available**’ for all applications

Procedure 15: NOAM Health Check for Source Release 7.0.x, 7.1.x

8 □	Repeat for each Network Element	Repeat **Steps 5 - 7** for each SOAM site in the topology.
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.1.4 NOAM Health Check for Source Release 7.2, 7.3

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 7.2 or later. This procedure must be executed on the Active NOAM.

Procedure 16: NOAM Health Check for Source Release 7.2, 7.3

S T E P #	This procedure performs a Health Check of the system prior to upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT** **MOS AND** **ASK FOR** **UPGRADE ASSISTANCE.**	

1
□
	Active NOAM VIP:
	Verify Upgrade ISO has been deployed
		Verify the DSR ISO file has been transferred to all servers.
		1. Navigate to **Status & Manage > Files**
		2. Select the target release DSR ISO and click “**View ISO Deployment Report**”.
		3. 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. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing “**ALL**” for the Export Application dropdown. 3. Verify the data export is complete using the tasks button at the top of the screen. 4. Browse 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 16: NOAM Health Check for Source Release 7.2, 7.3

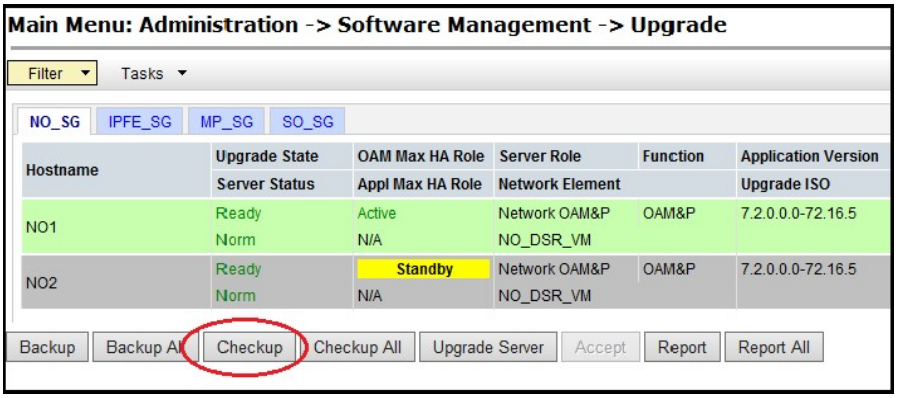
3 □

Active NOAM VIP:

Initiate NOAM health checks

This procedure runs the automated pre-upgrade Health Checks.

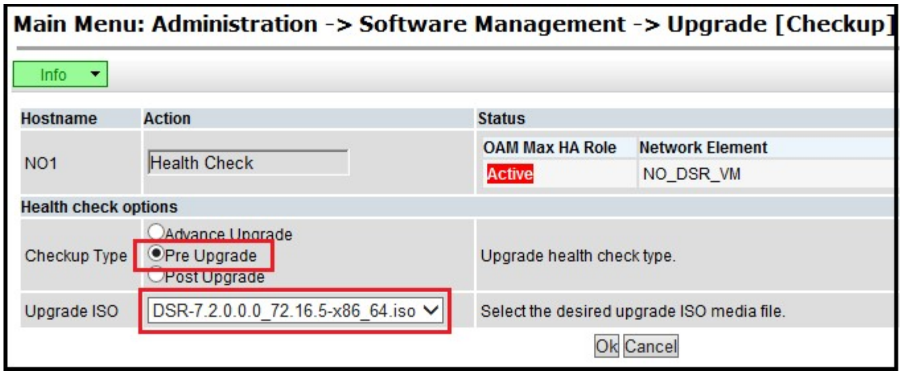
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the Active NOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Ready Norm	Active N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.16.5
NO2	Ready Norm	Standby N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.16.5

3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. Under Health check options, select the **Pre Upgrade** option.
5. Use the **Upgrade ISO** pulldown to select the target release ISO.
6. Click **Ok**. Control returns to the Upgrade screen.



Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status	
		OAM Max HA Role	Network Element
NO1	Health Check	Active	NO_DSR_VM

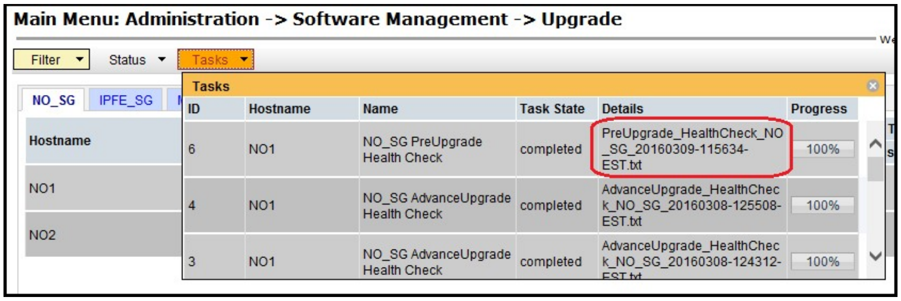
Health check options

Checkup Type	○ Advance Upgrade ● Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-7.2.0.0.0_72.16.5-x86_64.iso ▾	Select the desired upgrade ISO media file.

Procedure 16: NOAM Health Check for Source Release 7.2, 7.3

<table>
<tr>
<td>4
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Monitor health check progress</td>
<td>Monitor for the completion of the Health Check.

1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <b>&lt;NOServerGroup> PreUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The <b>Details</b> column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.


Main Menu: Administration -> Software Management -> Upgrade

Filter
Status
Tasks
NO_SG
IPFE_SG
Hostname
NO1
NO2

Tasks
<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>6</td><td>NO1</td><td>NO_SG PreUpgrade Health Check</td><td>completed</td><td>PreUpgrade_HealthCheck_NO_SG_20160309-115634-EST.txt</td><td>100%</td></tr>
<tr><td>4</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160308-125508-EST.txt</td><td>100%</td></tr>
<tr><td>3</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160308-124312-EST.txt</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>5
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Analyze health check results</td>
<td>Analyze Health Check report for failures. If the Health Check report status is anything other than “Pass”, the Health Check logs must be analyzed to determine if the upgrade can proceed.

1. Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.
2. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
3. 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 to contact MOS for guidance as described in Appendix S.

If the health check log contains the message “Unable to execute Health Check on <Active NOAM hostname>”, perform health checks in accordance with Procedure 14 or Procedure 15.</td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td>
</tr>
</table>

4.1.5 NOAM Health Check for Source Release 8.0 and later

This procedure is used to determine 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 17: NOAM Health Check for Source Release 8.0

STEP #	This procedure performs a Health Check of the system prior to upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.	

1
□
	Active NOAM VIP:
	Verify Upgrade ISO has been deployed
		Verify the DSR ISO file has been transferred to all servers.
		1. Navigate to **Status & Manage > Files**
		2. Select the target release DSR ISO and click "**View ISO Deployment Report**".
		3. 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. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry labeled "**ALL**". 3. Verify the data export is complete using the tasks button at the top of the screen. 4. Browse 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 17: NOAM Health Check for Source Release 8.0

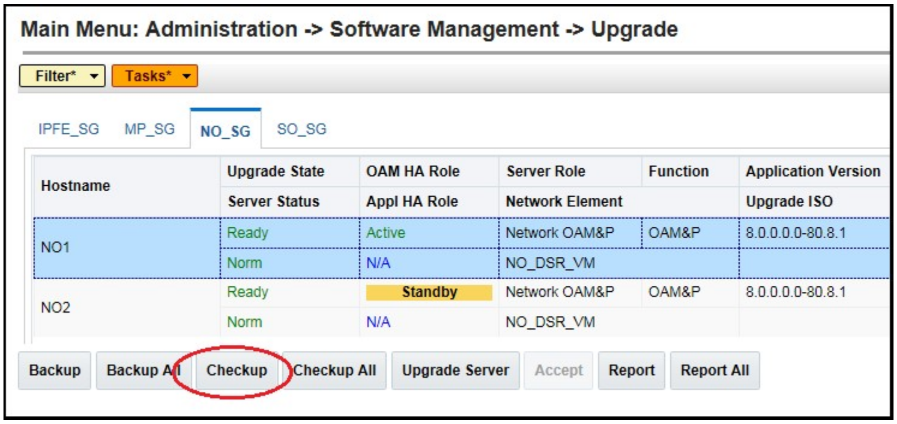
3 □

Active NOAM VIP:

Initiate NOAM health checks

This procedure runs the automated pre-upgrade Health Checks.

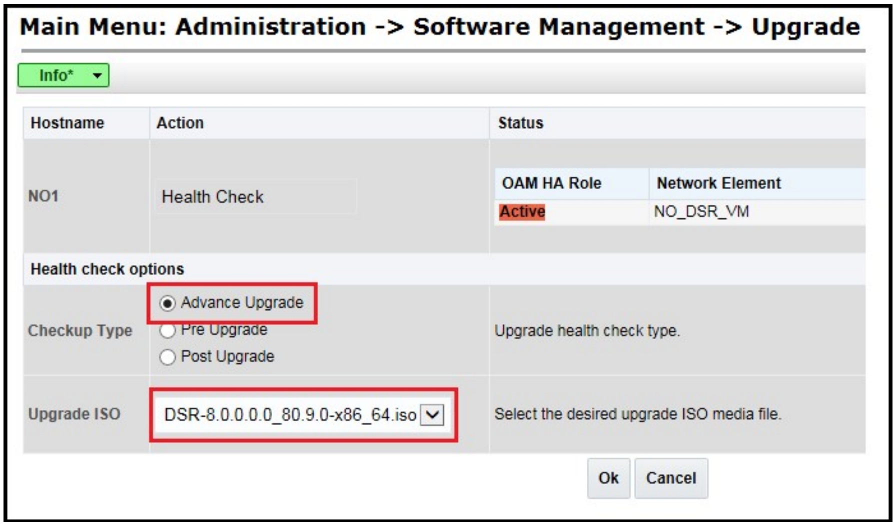
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the Active NOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.8.1
	Norm	N/A	NO_DSR_VM		
NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.8.1
	Norm	N/A	NO_DSR_VM		

3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. Under Health check options, select the **Pre Upgrade** option.
5. Use the **Upgrade ISO** pulldown to select the target release ISO.
6. Click **Ok**. Control returns to the Upgrade screen.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Action	Status
NO1	Health Check	OAM HA Role: Active Network Element: NO_DSR_VM

Health check options

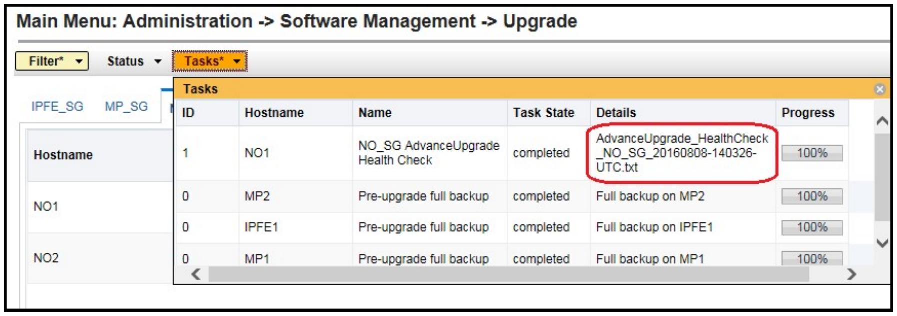
Checkup Type	● Advance Upgrade ○ Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-8.0.0.0.0_80.9.0-x86_64.iso	Select the desired upgrade ISO media file.

Procedure 17: NOAM Health Check for Source Release 8.0

<table>
<tr>
<td>4
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Monitor health check progress</td>
<td>
Monitor for the completion of the Health Check.

1. Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <b>&lt;NOServerGroup> PreUpgrade Health Check</b>.
2. Monitor the Health Check task until the Task State is <b>completed</b>. The <b>Details</b> column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.



Main Menu: Administration -> Software Management -> Upgrade

Tasks
<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>1</td><td>NO1</td><td>NO_SG AdvanceUpgrade Health Check</td><td>completed</td><td>AdvanceUpgrade_HealthCheck_NO_SG_20160808-140326-UTC.txt</td><td>100%</td></tr>
<tr><td>0</td><td>MP2</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP2</td><td>100%</td></tr>
<tr><td>0</td><td>IPFE1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on IPFE1</td><td>100%</td></tr>
<tr><td>0</td><td>MP1</td><td>Pre-upgrade full backup</td><td>completed</td><td>Full backup on MP1</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>5
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Analyze health check results</td>
<td>
Analyze Health Check report for failures. If the Health Check report status is anything other than “Pass”, the Health Check logs must be analyzed to determine if the upgrade can proceed.

1. Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.
2. Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.
3. 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 to contact MOS for guidance as described in Appendix S.

If the health check log contains the message “Unable to execute Health Check on <Active NOAM hostname>”, perform health checks in accordance with Procedure 14, Procedure 15 or Procedure 16.
</td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td>
</tr>
</table>

4.1.6 NOAM Pre-Upgrade Backup

This procedure takes a backup of the NOAM servers just prior to the upgrade.

Procedure 18: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.	
1 □	**Active NOAM VIP:** Backup all global configuration databases for NOAM **IMPORTANT: Required for Disaster Recovery**	Backup NOAM database. 1. Select **Status & Manage > Database** to return to the Database Status screen. 2. Click to highlight the **Active NOAM** server; click **Backup. NOTE: the Backup button will only be enabled when the Active server is selected.** The Database [Backup] screen is displayed. 3. Select the **Configuration** checkbox**.** 4. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 5. Enter **Comments** (optional) 6. Click **OK**. **NOTE:** On the **Status & Manage >Database** screen, the Active NOAM server will display the word **“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. 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active NOAM server tab**.** 3. Select the configuration database backup file and click the **Download** button. 4. If a confirmation window is displayed, click **Save**. 5. If the **Choose File** window is displayed, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a **Download Complete** confirmation is displayed, click **Close**.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 will be re-enabled once the NOAM upgrade is complete.

Procedure 19: Disable Global Provisioning

STEP #	This procedure disables provisioning for the NOAM (and DR-NOAM) servers, prior to upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active NOAM VIP:** Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: 1. Log into the Active NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.3 NOAM Upgrade

This procedure is used to upgrade the NOAM and DR NOAM servers, including the TVOE host if TVOE was not upgraded previously, as recommended in Section 3.4.6 - Upgrade TVOE Hosts at a Site**.**

Procedure 20: NOAM Upgrade

STEP #	This procedure upgrades the TVOE host of the NOAM servers (optional) and upgrades NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1. □	RMS Check	If the Active DSR NOAM or Standby DSR NOAM is a guest on RMS servers, perform Appendix C to update the NOAM guest VM configuration. **Note: This step is not applicable to VE-DSR systems.** **WARNING: Appendix C is mandatory and also depends on the amount of physical RAM deployed on the server. The appendix can be run on any server type if the physical RAM is available.**
2. □	TVOE Upgrade (if applicable)	Before proceeding with the primary DSR Standby NOAM upgrade, execute Appendix J to upgrade the TVOE Host if the Standby NOAM is a TVOE guest.
3. □	Upgrade primary DSR Standby NOAM	1. Upgrade the primary DSR Standby NOAM server using the Upgrade Single Server procedure: If the Active NOAM is on DSR 8.0: **Execute Appendix G** -- Single Server Upgrade Procedure - DSR 8.x Otherwise: **Execute Appendix H** -- Single Server Upgrade Procedure - pre DSR 8.x 2. After successfully completing the single server upgrade procedure, return to this point and continue with the next 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 = **31226 (HA Availability Status Degraded)** Alarm ID = **31233 (HA Path Down)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** After being upgraded, the Standby DR NOAM will display the following expected alarm: Alarm ID = **31225 (HA Service Start Failure)** **If the Active NOAM is on release 7.1.x or later, proceed to step 5.**

Procedure 20: NOAM Upgrade

4. □	**Active NOAM VIP:** Prepare the primary DSR Active NOAM for upgrade **For Active NOAM on release 6.0 or 7.0.x only**	**This step is for a primary DSR Active NOAM on release 6.0 or 7.0.x only.** Prepare the primary DSR Active NOAM for Upgrade. 1. Select **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select the NOAM Server Group: 3. Select the **Active** NOAM. 4. On the upgrade form, make the Active NOAM 'Upgrade Ready', by selecting the **Prepare** button. 5. On the Upgrade [Prepare] form, select '**Prepare**' in the **Action** dropdown list. Click the **Ok** button. This starts the Prepare action on the Active NOAM and forces an HA failover. *** Critical *** Do NOT omit this step 6. **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 the source release to release 8.0. 7. Select **Status & Manage > HA.** The HA status screen is displayed. 8. Click the **Edit** button. 9. For the NOAM to be upgraded (now the Standby), set the **Max Allowed HA Role** to Active, and click **Ok**. 10. Select **Status & Manage > Server**. The server status screen is displayed. 11. Select the Standby NOAM and click the **Restart** button. 12. Click **Ok** and verify the **Appl State** changes to **Enabled**.
5. □	TVOE Upgrade (if applicable)	Before proceeding with the primary DSR Active NOAM upgrade, execute Appendix J to upgrade the TVOE Host if the Active NOAM is a TVOE guest.
6. □	Upgrade second DSR NOAM	Upgrade the second DSR NOAM server using the Upgrade Single Server procedure: If the Active NOAM is on DSR 8.0: **Execute Appendix G** -- Single Server Upgrade Procedure - DSR 8.x Otherwise: **Execute Appendix H** -- Single Server Upgrade Procedure - pre DSR 8.x After successfully completing the single server upgrade procedure, return to this point and continue with the next step.
7. □	RMS Check	If the Active DR NOAM or Standby DR NOAM is a guest on RMS servers, perform Appendix C to update the NOAM guest VM configuration. **Note: This step is not applicable to VE-DSR systems.** **WARNING: Appendix C is mandatory and also depends on the amount of physical RAM deployed on the server. The appendix can be run on any server type if the physical RAM is available.**
8. □	TVOE Upgrade (if applicable)	Before proceeding with the Standby DR NOAM upgrade, execute Appendix J to upgrade the TVOE Host if the Standby DR NOAM is a TVOE guest.

Procedure 20: NOAM Upgrade

9. □	Upgrade Standby DR NOAM	Upgrade the Standby DR NOAM server using the Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure - DSR 8.x After successfully completing the procedure in Appendix G, return to this point and continue with the next step.
10. □	TVOE Upgrade (if applicable)	Before proceeding with the Active DR NOAM upgrade, execute Appendix J to upgrade the TVOE Host if the Active DR NOAM is a TVOE guest.
11. □	Upgrade Active DR NOAM	Upgrade the Active DR NOAM server using the Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure - DSR 8.x After successfully completing the procedure in Appendix G, return to this point and continue with the next procedure per Table 12.
		THIS PROCEDURE HAS BEEN COMPLETED.

4.3.1 PCA 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 will 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 6.0 to DSR 7.1 and later.

NOTE: The network-wide Topology Hiding settings at the NOAM will 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.

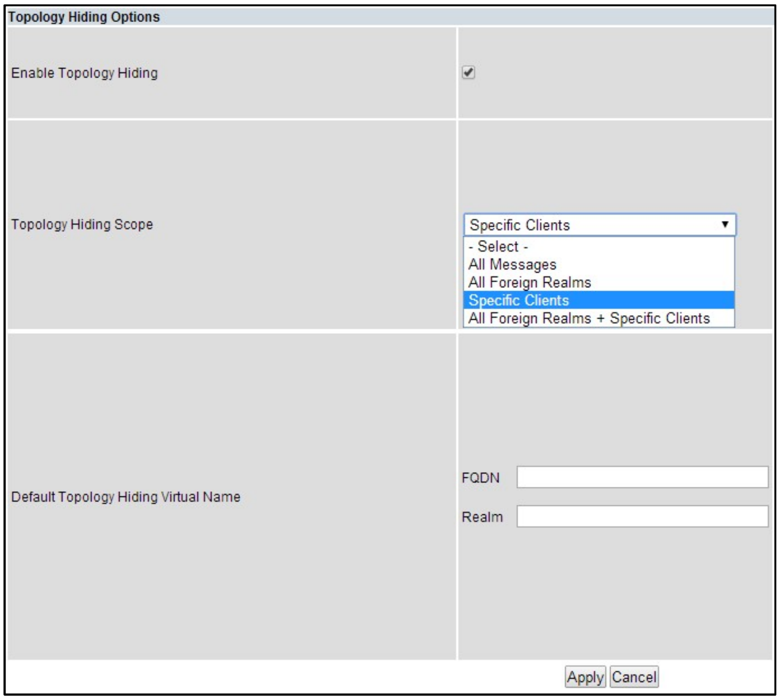
Procedure 21: PCA Topology Hiding Configuration

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active NOAM VIP:** Enable Global Provisioning	Before the Topology Hiding configuration can be modified, Global Provisioning must be enabled temporarily. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.

Procedure 21: PCA Topology Hiding Configuration

<table>
<tr>
<td>2.
□</td>
<td><u><b>Active NOAM VIP:</b></u>
Configure Topology Hiding settings</td>
<td>Configure the topology hiding settings.

1. Navigate to <b>Policy and Charging > Configuration > Policy DRA > Network-Wide Options</b>.
2. In the Topology Hiding Options section, select the <b>Enable Topology Hiding</b> checkmark.
3. Select the appropriate Topology Hiding Scope setting.
4. Enter a Default Topology Hiding Virtual Name – FQDN and Realm. These default values will be used if specific values have not been set at a site.
5. Select <b>Apply</b>.


Topology Hiding Options
Enable Topology Hiding ☑
Topology Hiding Scope: Specific Clients

- Select -
All Messages
All Foreign Realms
Specific Clients
All Foreign Realms + Specific Clients
Default Topology Hiding Virtual Name
FQDN
Realm
Apply
Cancel

</td>
</tr>
<tr>
<td>3.
□</td>
<td><u><b>Active NOAM VIP:</b></u>
Disable global provisioning</td>
<td>Disable global provisioning.

1. Select <b>Status & Manage > Database.</b>
The Database Status screen is displayed
2. Click the <b>Disable Provisioning</b> button.
3. Confirm the operation by clicking <b>Ok</b> in the popup dialog box.
4. Verify the button text changes to <b>Enable Provisioning</b>. A yellow information box should also be displayed at the top of the view screen which states: <b>[Warning Code 002] - Global provisioning has been manually disabled</b>.

The Active NOAM server will have the following expected alarm:
Alarm ID = <b>10008 (Provisioning Manually Disabled)</b></td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td>
</tr>
</table>

4.4 Verify NOAM Post Upgrade Status

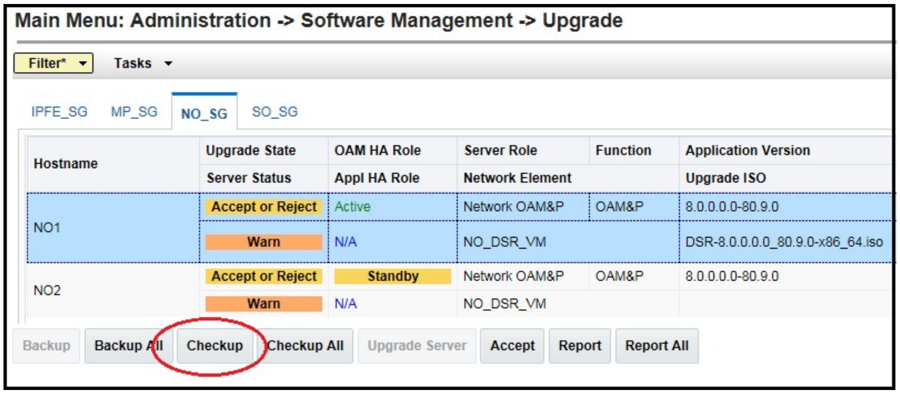
This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

Procedure 22: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**.	
1 □	**Active NOAM VIP:** Post-upgrade health checks	This procedure will run the automated post-upgrade Health Checks.

This procedure will run the automated post-upgrade Health Checks.

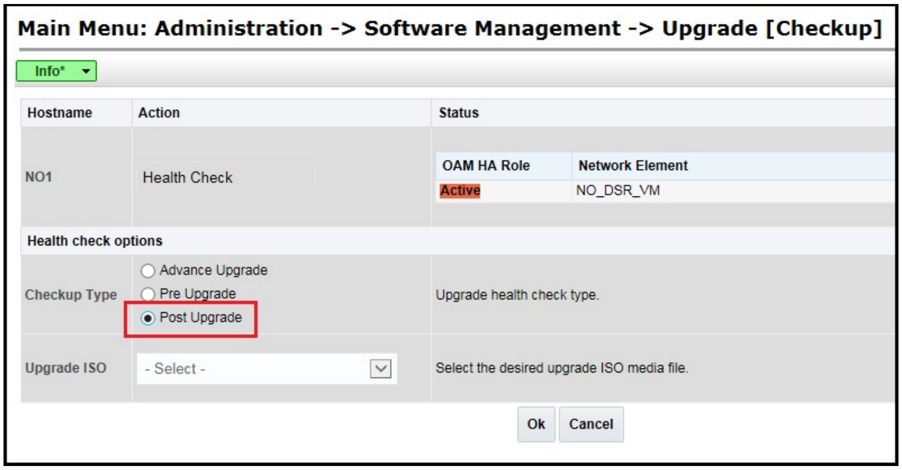
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the Active NOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.9.0
	Warn	N/A	NO_DSR_VM		DSR-8.0.0.0.0_80.9.0-x86_64.iso
NO2	Accept or Reject	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.9.0
	Warn	N/A	NO_DSR_VM		

3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. Under Health check options, select the **Post Upgrade** option.
5. Click **Ok**. Control returns to the Upgrade screen.



Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status
NO1	Health Check	OAM HA Role: Active Network Element: NO_DSR_VM
Health check options		
Checkup Type	○ Advance Upgrade ○ Pre Upgrade ● Post Upgrade	Upgrade health check type.
Upgrade ISO	- Select -	Select the desired upgrade ISO media file.

Procedure 22: Verify NOAM Post Upgrade Status

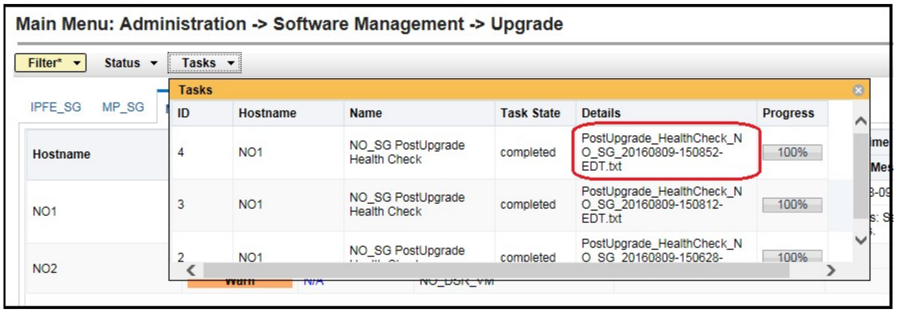
2 □

Active NOAM VIP:

Monitor health check progress

Monitor for the completion of the Health Check.

1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **PostUpgrade Health Check**.
2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.



Main Menu: Administration -> Software Management -> Upgrade

Tasks

ID	Hostname	Name	Task State	Details	Progress
4	NO1	NO_SG PostUpgrade Health Check	completed	PostUpgrade_HealthCheck_NO_SG_20160809-150852-EDT.txt	100%
3	NO1	NO_SG PostUpgrade Health Check	completed	PostUpgrade_HealthCheck_NO_SG_20160809-150812-EDT.txt	100%
2	NO1	NO_SG PostUpgrade	completed	PostUpgrade_HealthCheck_NO_SG_20160809-150628-	100%

3 □

Active NOAM VIP:

Analyze health check results

Analyze Health Check failure. If the Health Check report status is anything other than "Pass", the Health Check logs must be analyzed to determine if the upgrade can proceed.

1. Select **Status & Manage > Files**.
   The Files screen is displayed.
2. Select the file named "UpgradeHealthCheck.log" and click **View**.
3. Locate the log entries for the most recent health check.
4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.

THIS PROCEDURE HAS BEEN COMPLETED

4.5 Allow Provisioning *(Post NOAM Upgrade)*

The following procedure enables Global Provisioning for all Network Elements.

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

Procedure 23: Allow Provisioning

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active NOAM VIP:** Enable global provisioning and configuration.	Enable global provisioning and configuration updates on the entire network. 1. Log into the Active NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Provisioning.**
	Note: After enabling provisioning at the NOAM, the SOAM GUI(s) may 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 will be 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 will require 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 7.3 Installation Procedures ([6], [7]) 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 will add a new DSR SOAM site under the existing NOAM(s).
	THIS PROCEDURE HAS BEEN COMPLETED.	

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. Use the procedures in this section if Automated Site Upgrade was recommended in Section 3.2 Site Upgrade Methodology Selection.

The manual site upgrade procedures are in Section 5.3. Use the procedures in this section if Automated Server Group Upgrade or manual upgrade was recommended in Section 3.2 Site Upgrade Methodology Selection.

5.1 Site Pre-Upgrade Activities

SITE 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 13 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 13 as a guide for determining the order in which the procedures are to be executed.

Table 13. Site Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 24	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 25 or Procedure 26 or Procedure 27	0:05-0:10 0:10-0:15 0:10-0:20	0:15-0:30 0:20-0:35 0:20-0:40	Site Pre-Upgrade Health Check for Release 8.0 and later Site Pre-Upgrade Health Check for Release 7.x/8.0 Site Pre-Upgrade Health Check for Release 6.0	None None None
Procedure 29	0:01-0:05	0:16-0:45	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 31	0:05-0:10	0:21-0:55	Site Upgrade Pre-Checks	

Procedure 32	2:40-4:00	3:01-4:55	Automated Site Upgrade	Traffic is not serviced by servers that are actively upgrading.
Procedure 39	0:02	3:03-4:57	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 40	0:10-0:15	3:13-5:12	Site Post-Upgrade Health Check	None

5.1.1 Site Pre-Upgrade Backups

This procedure is non-intrusive and is used to perform 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 prior to the start of the upgrade.

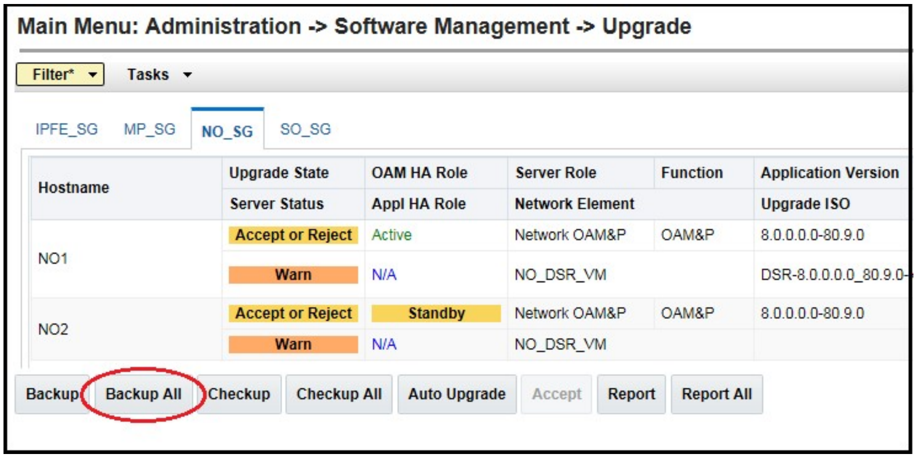
Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 69 is an alternate procedure that can be used to backup a site using the command line. Procedure 69 should only be used by direction of MOS.

Procedure 24: Site Pre-Upgrade Backups

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. □	**Active SOAM VIP:** Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup SOAM database. 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database** to return to the Database Status screen. 3. Click to highlight the **Active SOAM** server, click **Backup. NOTE: the Backup button will only be enabled when the Active server is selected.** The Database [Backup] screen is displayed. 4. Select the **Configuration** checkbox. 5. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 6. Enter **Comments** (optional). 7. 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. 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active SOAM server tab**.** 3. Select the configuration database backup file and click the **Download** button. 4. If a confirmation window is displayed, click **Save**. 5. If the **Choose File** window is displayed, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a **Download Complete** confirmation is displayed, click **Close**.

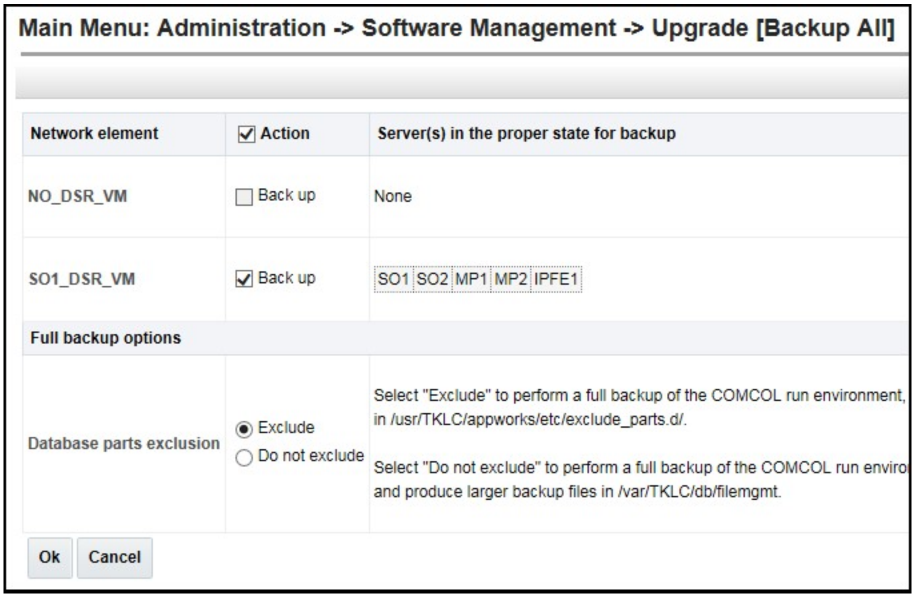
Procedure 24: Site Pre-Upgrade Backups

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT** **MOS AND** **ASK FOR** **UPGRADE ASSISTANCE**	
3. □	**Active NOAM VIP:** Backup DB run environment	Backup run environment for site being upgraded. 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade.** 3. Click the **Backup All** button. 

Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.9.0
	Warn	N/A	NO_DSR_VM		DSR-8.0.0.0.0_80.9.0-
NO2	Accept or Reject	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.9.0
	Warn	N/A	NO_DSR_VM		

Procedure 24: Site Pre-Upgrade Backups

<table>
<tr><td>S
T
E
P
#</td><td colspan="2">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.
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u></b></td></tr>
<tr><td><b>4.</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
Set backup parameters</td><td>The <b>Upgrade [Backup All]</b> screen is displayed. This screen displays the various Network Elements, and identifies which servers are ready for backup.
1. In the <b>Action</b> column, select the <b>Back up</b> checkbox for the Network Element to be upgraded.
2. Verify the check box for the NOAM server group is NOT checked.
Note: Backing up the NOAM servers at this point will overwrite the pre-upgrade backup files that are needed for backing out the target release. Do NOT backup the NOAM servers.
3. In the <b>Full backup options</b> section, verify the ‘Exclude’ option is selected.
4. Click the <b>Ok</b> button. This initiates a full backup on each eligible server.

Main Menu: Administration -> Software Management -> Upgrade [Backup All]<table>
<tr><th>Network element</th><th>☑ Action</th><th>Server(s) in the proper state for backup</th></tr>
<tr><td>NO_DSR_VM</td><td>□ Back up</td><td>None</td></tr>
<tr><td>SO1_DSR_VM</td><td>☑ Back up</td><td>SO1 SO2 MP1 MP2 IPFE1</td></tr>
<tr><td colspan="3">Full backup options</td></tr>
<tr><td>Database parts exclusion</td><td>● Exclude
○ Do not exclude</td><td>Select "Exclude" to perform a full backup of the COMCOL run environment, in /usr/TKLC/appworks/etc/exclude_parts.d/.
Select "Do not exclude" to perform a full backup of the COMCOL run enviro and produce larger backup files in /var/TKLC/db/filemgmt.</td></tr>
</table> </td></tr>
</table>

Procedure 24: 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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>**

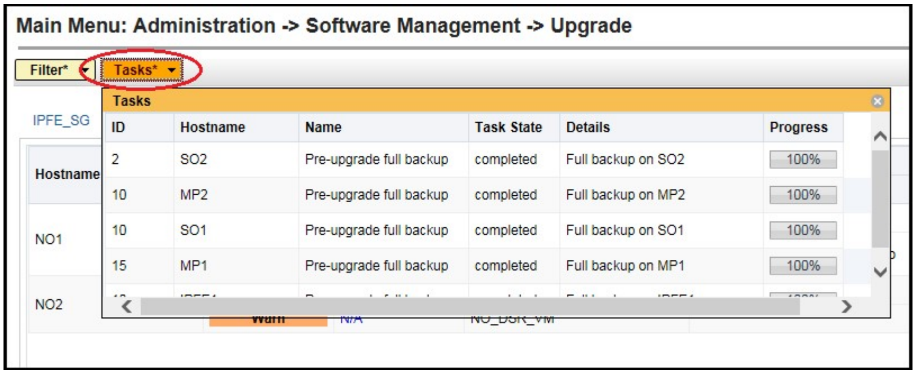
5. □

<u>Active NOAM VIP:</u>

Monitor for backup completion

Monitor the backup tasks

1. From the Upgrade screen, select the **Tasks** pulldown.
2. Monitor the progress of the backups until the Network Element(s) selected in step 4 are complete.



Main Menu: Administration -> Software Management -> Upgrade

Tasks

ID	Hostname	Name	Task State	Details	Progress
2	SO2	Pre-upgrade full backup	completed	Full backup on SO2	100%
10	MP2	Pre-upgrade full backup	completed	Full backup on MP2	100%
10	SO1	Pre-upgrade full backup	completed	Full backup on SO1	100%
15	MP1	Pre-upgrade full backup	completed	Full backup on MP1	100%

6. □

<u>Active NOAM VIP:</u>

Verify that backup files are present on each server.

1. Log into the Active NOAM or SOAM GUI.
2. Select **Status & Manage > Files** *(The **Files** menu is displayed)*
3. Click on each Server tab, in turn
4. For each Server, verify that 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
```

5. Repeat sub-steps 1 through 4 for each site being upgraded.

THIS PROCEDURE HAS BEEN COMPLETED.

5.1.2 Site Pre-Upgrade Health Checks

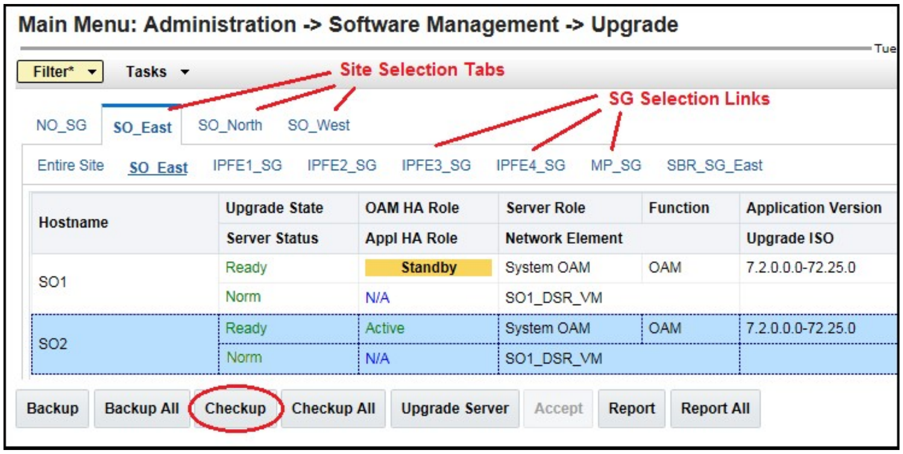
This section provides procedures to verify the health of the SOAM site prior to upgrade. Procedure 25 is the primary procedure to be executed when the Active NOAM is on Release 8.0 and later. Alternate release-specific procedures are also provided, to be used as directed.

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 prior to upgrading.

Procedure 25: Site Pre-Upgrade Health Check for Release 8.0 and later

S T E P #	This procedure performs a Health Check prior to upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1 □	**<u>Active NOAM VIP:</u>** Run site health checks (part 1)	Select the SOAM on which health checks will be run. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the tab of the site to be upgraded. 3. Select the SOAM server group link. 4. Select the Active SOAM. 5. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed.



Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SO1	Ready	Standby	System OAM	OAM	7.2.0.0.0-72.25.0
	Norm	N/A	SO1_DSR_VM		
SO2	Ready	Active	System OAM	OAM	7.2.0.0.0-72.25.0
	Norm	N/A	SO1_DSR_VM		

Procedure 25: Site Pre-Upgrade Health Check for Release 8.0 and later

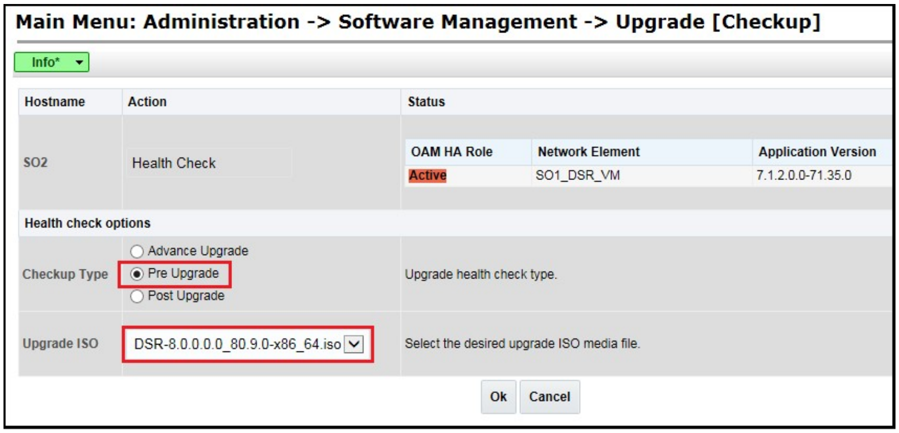
2 □

Active NOAM VIP:

Run site health checks (part 2)

Initiate the health checks.

1. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
2. In the **Health check options** section, select the **Pre Upgrade** option.
3. Use the **Upgrade ISO** pulldown to select the target release ISO.
4. Click **Ok** to initiate the health check. Control returns to the Upgrade Administration screen.



Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status		
		OAM HA Role	Network Element	Application Version
SO2	Health Check	Active	SO1_DSR_VM	7.1.2.0.0-71.35.0

Health check options

Checkup Type	○ Advance Upgrade ● Pre Upgrade ○ Post Upgrade	Upgrade health check type.
Upgrade ISO	DSR-8.0.0.0.0_80.9.0-x86_64.iso	Select the desired upgrade ISO media file.

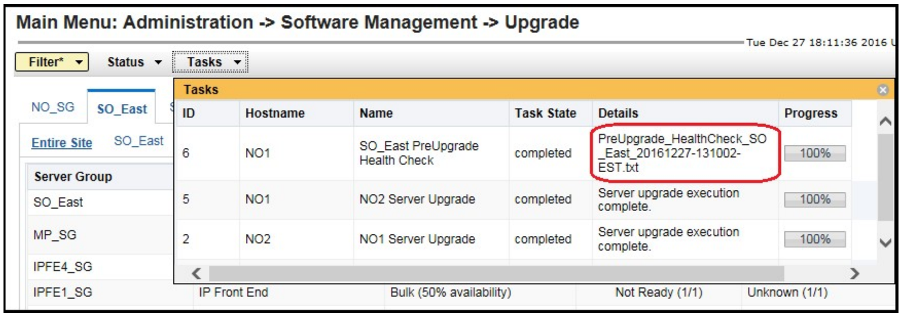
3 □

Active NOAM VIP:

Monitor health check progress

Monitor for the completion of the Health Check.

1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PreUpgrade Health Check**.
2. Monitor the Health Check task until the Task State is **completed**. The **Details** column will display a hyperlink to the Health Check report.
3. Click the hyperlink to download the Health Check report. Open the report and review the results.



Main Menu: Administration -> Software Management -> Upgrade

Tue Dec 27 18:11:36 2016

Tasks

ID	Hostname	Name	Task State	Details	Progress
6	NO1	SO_East PreUpgrade Health Check	completed	PreUpgrade_HealthCheck_SO_East_20161227-131002-EST.txt	100%
5	NO1	NO2 Server Upgrade	completed	Server upgrade execution complete.	100%
2	NO2	NO1 Server Upgrade	completed	Server upgrade execution complete.	100%

Server Group				
SO_East				
MP_SG				
IPFE4_SG				
IPFE1_SG	IP Front End	Bulk (50% availability)	Not Ready (1/1)	Unknown (1/1)

Procedure 25: Site Pre-Upgrade Health Check for Release 8.0 and later

4 □	**Active SOAM VIP:** Analyze health check results	Analyze Health Check report for failures. If the Health Check report status is anything other than "Pass", the Health Check logs must be analyzed to determine if the upgrade can proceed. The Health Check log is located in the File Management area of the Active SOAM. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named "UpgradeHealthCheck.log" and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S. **If the health check log contains the message "Unable to execute Health Check on <Active SOAM hostname>", perform an alternate health check procedure as follows:** **If the Active SOAM release is 7.x/8.0:** Execute Procedure 26: Site Pre-Upgrade Health Check for Release 7.x/8.0 **If the Active SOAM release is 6.0:** Execute Procedure 27: Site Pre-Upgrade Health Check for Release 6.0
5 □	**ACTIVE SOAM VIP:** Capture Diameter Configuration on Active SOAM GUI	Export Diameter configuration. 1. Select **Main Menu > Diameter Common > Export**. 2. Capture and archive the Diameter data by setting the **Export Application** drop down entry to "**ALL**". 3. Click **Ok**. 4. Verify the requested data is exported using the tasks button at the top of the screen. 5. Select the **File Management** button 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.**
		THIS PROCEDURE HAS BEEN COMPLETED.

5.1.2.2 Site 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 SOAMs are on Release 7.x. The procedure is non-intrusive and performs a health check of the site prior to upgrading.
Do not perform this procedure unless directed in Procedure 25 step 4.

Procedure 26: Site Pre-Upgrade Health Check for Release 7.x/8.0

S T E P #	This procedure performs a Health Check prior to upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1.
□
	ACTIVE SOAM CLI:
	Perform health checks
		Run health checks on the Active SOAM.
		1. 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.
		2. 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:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears 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 to contact MOS for guidance.
		4. ep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

2. □	**ACTIVE SOAM CLI:** Capture Diameter Maintenance Status	Capture Diameter Maintenance status. 1. Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command will output 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 message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

Procedure 26: Site Pre-Upgrade Health Check for Release 7.x/8.0

3. □	**ACTIVE SOAM CLI:** View DA-MP Status	Capture DA-MP status. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established ____________
4. □	**ACTIVE SOAM VIP:** Capture Diameter Configuration on Active SOAM GUI	Export Diameter configuration. 1. Select **Main Menu > Diameter Common > Export**. 2. Capture and archive the Diameter data by setting the **Export Application** drop down entry to "**ALL**". 3. Click **Ok**. 4. Verify the requested data is exported using the tasks button at the top of the screen. 5. Select the **File Management** button 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.
5.	**Active SOAM VIP:** Capture measurements data	DSR 8.0 introduces Alarm 22077 – Excessive Request Reroute Threshold Exceeded. This alarm indicates that 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. Prior to upgrading a site, measurement stats are collected from the DA-MPs to serve as a baseline for post-upgrade comparisons. 1. Select **Main Menu > Measurements > Report** 2. Click the "**Go to Export**" button. 3. On the **Report [Export]** screen, make the following selections: a. Report Scope => <Site SOAM NE> b. Report Groups => **Diameter Rerouting** c. Time Interval => **Fifteen Minute** d. Time Range => **1 Day** e. Export Frequency => **Once** f. Task Name => leave as is 4. Click the **Ok** button to initiate the export. 5. When the export task is complete, select **Status & Manage > Files**. 6. 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.**

THIS PROCEDURE HAS BEEN COMPLETED.

5.1.2.3 Site Pre-Upgrade Health Check for Release 6.0

This procedure is an alternate health check that is used when upgrading to Release 8.0 and the Active SOAM is on Release 6.0. The procedure is non-intrusive and performs a health check of the site prior to upgrading. Do not perform this procedure unless directed in Procedure 25 step 4.

Procedure 27: Site Pre-Upgrade Health Check for Release 6.0

S T E P #	This procedure performs a Health Check prior to upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active SOAM VIP:** Verify Server Status is Normal	Verify server status 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed. 3. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 4. Do not proceed with the upgrade if any server status is not **Norm**. 5. Do not proceed if there are any Major or Critical alarms. 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.
2. □	**Active SOAM VIP:** Log all current alarms	Capture active alarms 1. Select **Alarms & Events > View Active**. The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
3. □	**Active SOAM VIP:** Capture the Diameter Maintenance Status	Capture Diameter Maintenance status. 1. Select **Main Menu > Diameter > Maintenance** 2. Select the **Maintenance > Route Lists** screen. 3. Filter out all the Route Lists with **Route List Status** as **"Is Not Available"** and **"Is Available".** 4. Record the number of "Not Available" and "Available" Route Lists. 5. Select **Maintenance >Route Groups** screen. 6. Filter out all the Route Groups with "**PeerNode/Connection Status** as **"Is Not Available"** and **"Is Available".** 7. Record the number of "Not Available" and "Available" Route Groups. 8. Select **Maintenance >Peer Nodes** screen. 9. Filter out all the Peer Nodes with "**Peer Node Operational Status"** as **"Is Not Available"** and **"Is Available".** 10. Record the number of "**Not Available**" and "**Available**" peer nodes. 11. Select **Maintenance >Connections** screen. 12. Filter out all the Connections with "**Operational Status"** as **"Is Not Available"** and **"Is Available".** 13. Record the number of "**Not Available**" and "Available" connections. 14. Select **Maintenance >Applications** screen. 15. Filter out all the Applications with "**Operational State"** as **"Is Not Available" and "Is Available".** 16. Record the number of "**Not Available**" and "**Available**" applications. 17. Save recorded data on the client machine.

Procedure 27: Site Pre-Upgrade Health Check for Release 6.0

4. □	**Active SOAM VIP:** View DA-MP Status	Capture DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**
5. □	**Active SOAM VIP:** Capture Transport Manager configuration (if MD-IWF equipped) **NOTE:** *Perform this step only if the MD-IWF feature is provisioned.*	Capture Transport Manager configuration. 1. Select **Main Menu > Transport Manager > Configuration > Adjacent Node** 2. Capture and archive a screen capture of the screen. 3. Select **Configuration Sets**. 4. Capture and archive a screen capture of the screen. 5. Select **Transport** 6. Click the **Report** at the bottom of the table to generate a report for all entries. 7. Save the report and/or print the report. Keep these copies for future reference.
6. □	**Active SOAM VIP:** Capture SS7/Sigtran Configuration on Active SOAM GUI (if MD-IWF equipped) **NOTE:** *Perform this step only if the MD-IWF feature is provisioned.*	If the MD-IWF feature is enabled, capture SS7/Sigtran configure. 1. Select **Main Menu > SS7/Sigtran > Configuration > Adjacent Server Groups.** 2. Capture and archive a screen capture of the screen. 3. Select **Local Signaling Points.** 4. Click the **Report** button. 5. Download and archive the report on the client machine. 6. Select **Local SCCP Users.** 7. Click the **Report** button. 8. Download and archive the report on the client machine. 9. Select **Remote Signaling Points.** 10. Click the **Report** button. 11. Download and archive the report on the client machine. 12. Select **Remote MTP3 Users**. 13. Capture and archive a screen capture of the screen. 14. Select **Link Sets**. 15. Click the **Report** button. 16. Download and archive the report on the client machine. 17. Select **Links**. 18. Click the **Report** button. 19. Download and archive the report on the client machine. 20. Select **Routes**. 21. Click the **Report** button. 22. Download and archive the report on the client machine. 23. Select **SCCP Options**. 24. Capture and archive a screen capture of the screen. 25. Select **MTP3 Options**. 26. Capture and archive a screen capture of the screen. 27. Select **M3UA Options**. 28. Capture and archive a screen capture of the screen. 29. Select **Local Congestion Options**. 30. Capture and archive a screen capture of the screen. 31. Select **Capacity Constraint Options**. 32. Capture and archive a screen capture of the screen.

Procedure 27: Site Pre-Upgrade Health Check for Release 6.0

7.	**Active SOAM VIP:** Capture measurements data	DSR 8.0 introduces Alarm 22077 – Excessive Request Reroute Threshold Exceeded. This alarm indicates that 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. Prior to upgrading a site, measurement stats are collected from the DA-MPs to serve as a baseline for post-upgrade comparisons. 1. Select **Main Menu > Measurements > Report** 2. Click the "**Go to Export**" button. 3. On the **Report [Export]** screen, make the following selections: a. Report Scope => <Site SOAM NE> b. Report Groups => **Diameter Rerouting** c. Time Interval => **Fifteen Minute** d. Time Range => **1 Day** e. Export Frequency => **Once** f. Task Name => leave as is 4. Click the **Ok** button to initiate the export. 5. When the export task is complete, select **Status & Manage > Files**. 6. 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.
8. □	Capture Data for each SOAM Site	**Repeat steps 1 through 6 for each configured SOAM Site to be upgraded.**
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 2.10.3. Prior to 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 Auto Site Upgrade. The options have no effect on manual upgrades or Automated Server Group upgrades.

Procedure 28: Site Upgrade Options Check

S T E P #	This procedure is used to review 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**

Procedure 28: Site Upgrade Options Check

1. □	**Active NOAM VIP:** View options	View Auto Site Upgrade options. 1. Log into the Active NOAM GUI 2. Select **Administration > General Options.** The General Options screen is displayed. 3. Scroll down to the "**Site Upgrade Bulk Availability"** option. 4. Review the existing value of this option and determine if changes are needed. If the option is changed, click the "**Ok**" button to save the change. 5. Scroll down to the "**Site Upgrade SOAM Method**" option. 6. Review the existing value of this option and determine if changes are needed. If the option is changed, click the "**Ok**" button to save the change.
THIS PROCEDURE HAS BEEN COMPLETED.		

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 29: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1. □	**<u>Active SOAM VIP:</u>** Disable Site Provisioning	Disable Site Provisioning at the SOAM. 1. Log into the SOAM GUI of the site to be upgraded. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which 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)**
2. □	Repeat for each SOAM Site	**Repeat step 1 for each configured SOAM Site to be upgraded.**
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.2 Automated Site Upgrade

	!! WARNING!!	**THE FOLLOWING PROCEDURES MUST BE COMPLETED BEFORE THE START OF AUTOMATED SITE UPGRADE:** Procedure 24; [Procedure 25, Procedure 26, or Procedure 27**]**; Procedure 29; Procedure 31

5.2.1 TVOE Upgrade Check

When using the Auto Site Upgrade feature, it is not possible to upgrade the TVOE hosts with the application, as the application upgrades are performed continuously to completion. Therefore, all TVOE hosts in the target site must be upgraded, if necessary, prior to initiating the site upgrade sequence. Refer to Section 3.4.6 for TVOE host upgrade procedures. Once the TVOE hosts upgrades are complete, return to this section to continue the site upgrade.

The TVOE version check is especially applicable to VEDSR systems, wherein all of the DSR applications run as guests of a TVOE host. In particular, consideration must be given to Spare SBRs, which may be located at a different physical location, but will be upgraded with the server group to which the Spare SBR belongs.

5.2.2 VEDSR VM Update

Before Auto Site Upgrade can be used to upgrade a VEDSR site, the guest VMs may need to be be modified to support 8.0 functional requirements. Because Auto Site Upgrade does not allow for operator intervention during the upgrade, the modifications must be implemented on ALL guests before the site upgrade begins.

This procedure modifies the guest VM profile to increase the size of the disk to 70GB due to the increased storage requirements of DSR 8.0.

This procedure is applicable to the VEDSR configuration only.

This procedure is not required if the source release is DSR 8.0 or later.

Procedure 30: VEDSR VM Update

S T E P #	This procedure increases the size of the VM disk to 70GB. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	

1.
□
	Identify guests to modify	**If the source release is DSR 8.0, skip this procedure.**
		Identify a VEDSR server in the site to be upgraded. Log into the TVOE Host of this server and identify the guests that need to be updated.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the TVOE Host of the selected VEDSR server:
		`ssh admusr@<TVOE_HOST>`
		`password:  <enter password>`
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		2. Use the following command to list the guests running on the host:
		`sudo virsh list`
		3. Record the VM guest names of the following DSR applications running on this host:
		SOAMs: ______________________________
		DA-MPs: ______________________________
		______________________________
		SS7-MPs: ______________________________
		SBRs: ______________________________
		IPFEs: ______________________________

	THIS PROCEDURE HAS BEEN COMPLETED.	

5.2.3 Site Upgrade Pre-Checks

This procedure verifies that the system is prepared for Automated Site Upgrade.

Procedure 31: Site Upgrade Pre-Checks

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active SOAM VIP:** Verify Traffic status	View KPIs to verify traffic status. 1. Log into the Active SOAM GUI using the VIP. 2. Select **Status & Manage > KPIs**. 3. Inspect KPI reports to verify traffic is at the expected condition.
2. □	**Active SOAM VIP:** Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 29. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, continue with the next procedure per Table 13, otherwise, execute: Procedure 29: Disable Site Provisioning
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.2.4 Initiate Automated Site Upgrade

This procedure initiates the Auto Site Upgrade sequence.

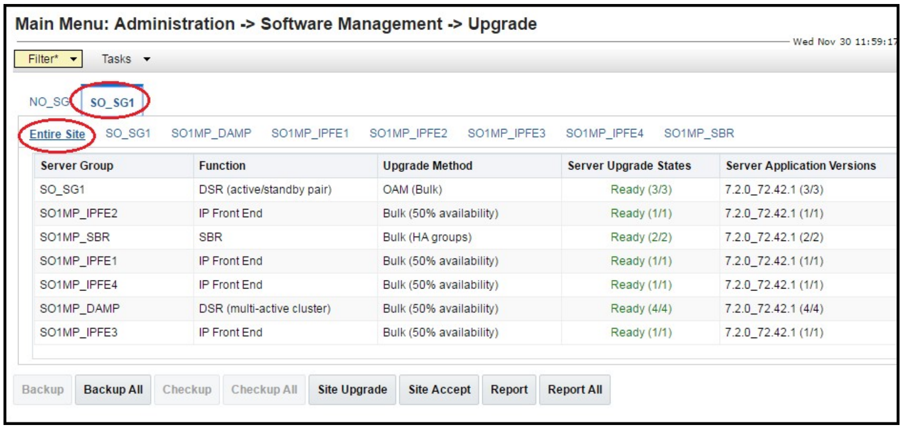
Procedure 32: Automated Site Upgrade

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.</b></td></tr>
<tr><td><b>1</b>
□</td><td>Review site upgrade plan and site readiness</td><td>Review the site upgrade plan created in Sections 3.2 and 3.3. This step verifies that the servers and server groups to be upgraded are in the proper state.

1. Log into the NOAM GUI using the VIP
2. Select <b>Administration > Software Management > Upgrade</b>.
The Upgrade Administration screen is displayed.
3. Select the SOAM tab of the site to be upgraded.
4. Verify the <b>Entire Site</b> 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.


<b>Main Menu: Administration -> Software Management -> Upgrade</b>

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

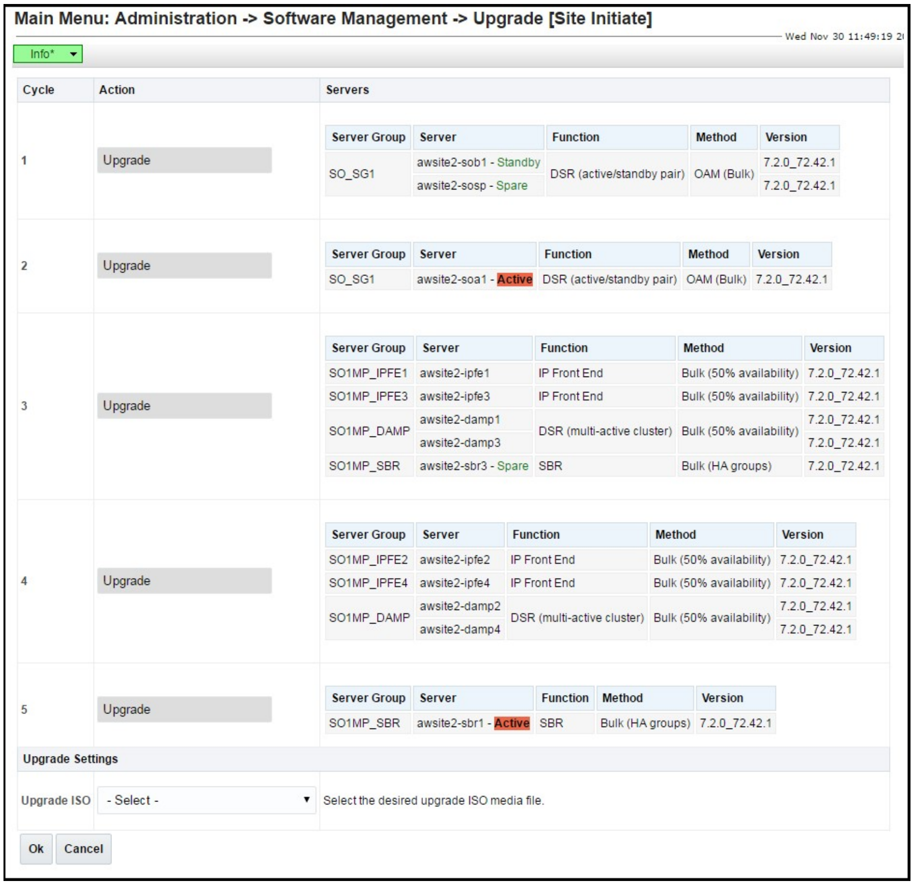
Note: The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including “Accept or Reject”, “Ready”, “Backup Needed”, “Failed”, or “Not Ready”. Only the servers in the “Ready” state or “Failed” state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

Procedure 32: Automated Site Upgrade

2 ☐ **Active NOAM VIP:**

Initiate the site upgrade.

1. Verify that no Server Groups are selected on the upgrade administration screen. The Site Upgrade button is not available if a Server Group is selected.
2. Select the **Site Upgrade** button.
   The Upgrade [Site Initiate] screen is displayed.
3. Review the upgrade plan as presented on the [Site Initiate] screen. This plan represents an approximation of how the servers will be upgraded. Due to the dynamic nature of upgrade, some servers (typically only C-level) may be upgraded in a different cycle than displayed here.



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

Wed Nov 30 11:49:19 2(

Cycle	Action	Server Group	Server	Function	Method	Version
1	Upgrade	SO_SG1	awsite2-sob1 - Standby awsite2-sosp - Spare	DSR (active/standby pair)	OAM (Bulk)	7.2.0_72.42.1 7.2.0_72.42.1
2	Upgrade	SO_SG1	awsite2-soa1 - Active	DSR (active/standby pair)	OAM (Bulk)	7.2.0_72.42.1
3	Upgrade	SO1MP_IPFE1	awsite2-ipfe1	IP Front End	Bulk (50% availability)	7.2.0_72.42.1
		SO1MP_IPFE3	awsite2-ipfe3	IP Front End	Bulk (50% availability)	7.2.0_72.42.1
		SO1MP_DAMP	awsite2-damp1 awsite2-damp3	DSR (multi-active cluster)	Bulk (50% availability)	7.2.0_72.42.1 7.2.0_72.42.1
		SO1MP_SBR	awsite2-sbr3 - Spare	SBR	Bulk (HA groups)	7.2.0_72.42.1
4	Upgrade	SO1MP_IPFE2	awsite2-ipfe2	IP Front End	Bulk (50% availability)	7.2.0_72.42.1
		SO1MP_IPFE4	awsite2-ipfe4	IP Front End	Bulk (50% availability)	7.2.0_72.42.1
		SO1MP_DAMP	awsite2-damp2 awsite2-damp4	DSR (multi-active cluster)	Bulk (50% availability)	7.2.0_72.42.1 7.2.0_72.42.1
5	Upgrade	SO1MP_SBR	awsite2-sbr1 - Active	SBR	Bulk (HA groups)	7.2.0_72.42.1

Upgrade Settings

Upgrade ISO	- Select -	Select the desired upgrade ISO media file.

4. In the **Upgrade Settings** section of the form, use the **Upgrade ISO** picklist, to select the target ISO.
5. Click **Ok** to start the upgrade sequence. Control returns to the Upgrade Administration screen.

Procedure 32: Automated Site Upgrade

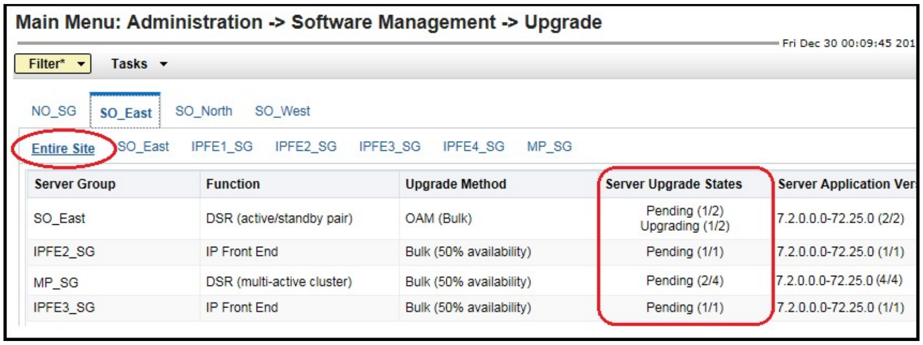
3 □ **Active NOAM VIP:**

View the Upgrade Administration form to monitor upgrade progress.

See step 4 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 will be shown as "FAILED".
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. With the **Entire Site** link selected, a summary of the upgrade status for the selected site is displayed. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. This view can be used to monitor the upgrade status of the overall site.



Main Menu: Administration -> Software Management -> Upgrade

Fri Dec 30 00:09:45 201

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Ver
SO_East	DSR (active/standby pair)	OAM (Bulk)	Pending (1/2) Upgrading (1/2)	7.2.0.0.0-72.25.0 (2/2)
IPFE2_SG	IP Front End	Bulk (50% availability)	Pending (1/1)	7.2.0.0.0-72.25.0 (1/1)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Pending (2/4)	7.2.0.0.0-72.25.0 (4/4)
IPFE3_SG	IP Front End	Bulk (50% availability)	Pending (1/1)	7.2.0.0.0-72.25.0 (1/1)

More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.

During the upgrade, the servers may have a combination of the following expected alarms.
NOTE: Not all servers will 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 to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

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 to contact MOS by referring to Appendix S of this document and provide these files.Refer to Appendix O for failed server recovery procedures.

Procedure 32: Automated Site Upgrade

5 □	Post upgrade verification	**Proceed to Section 5.7 - Site Post-Upgrade Procedures for post upgrade verification procedures.**
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 14 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 14. 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 15 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 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 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 15. 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 16 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. 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 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 16. 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 17 should be used to plan the upgrade of each site. For the server groups that will be upgraded using ASG, the only planning necessary is to record the server group name. ASG will automatically select 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 17. Site Upgrade Planning Sheet.

Iteration 1		Notes
Standby SOAM Hostname Spare SOAM Hostname		If a Spare SOAM exists, the Spare and Standby SOAMs will be upgraded manually. Otherwise, the SOAMs will be upgraded with ASG.
Iteration 2		**Notes**
Active SOAM		The Active SOAM will be upgraded in iteration 2, either manually or by ASG.
Iteration 3		**Notes**
DA-MP Group 1		ASG will automatically select 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 will automatically select the Spare SBR(s) for upgrade
Iteration 4		**Notes**
DA-MP Group 2		ASG will automatically select 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 will automatically select the Standby SBR(s) for upgrade
Iteration 5		**Notes**
Active SBR(s)		ASG will automatically select the Active SBR(s) for upgrade

Table 18 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 18 as a guide for determining the order in which the procedures are to be executed.

NOTE: If the TVOE Hosts are upgraded during the same Maintenance Window as the application upgrade, refer to Table 10 (Section 3.4.6) for additional time estimates associated with the TVOE upgrade.

Table 18. Site Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 24	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 25	0:05-0:10	0:15-0:30	Site Pre-Upgrade Health Check for Release 8.0 and later	None
or Procedure 26	0:10-0:15	0:20-0:25	Site Pre-Upgrade Health Check for Release 7.x/8.0	None
or Procedure 27	0:10-0:20	0:20-0:40	Site Pre-Upgrade Health Check for Release 6.0	None
Procedure 29	0:01-0:05	0:16-0:45	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 33	0:01-0:05	0:17-0:50	SOAM Upgrade Pre-Checks	No Traffic Impact
Iteration 1	0:40-1:00	0:57-1:50	Standby SOAM, Spare SOAM (if equipped)	Refer to Section 5.3 for details
Iteration 2	0:40-1:00	1:37-2:50	Active SOAM	Refer to Section 5.3 for details
Iteration 3	0:40-1:00	2:17-3:50	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Spare SBR(s)	Refer to Section 5.4 for details
Iteration 4	0:40-1:00	2:57-4:50	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s)	Refer to Section 5.5 for details
Iteration 5	0:00-1:00	2:57-5:50	Active SBR(s)	Refer to Section 5.6 for details
Procedure 39	0:02	2:59-5:52	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 40	0:10-0:15	3:09-6:07	Site Post-Upgrade Health Check	None

5.3.1.1 RMS Notes

RMS-based DSRs are deployed in one of two supported configurations: without geographic redundancy, or with geographic redundancy. In both cases, the RMS-based DSR implements just a single Diameter network element.

When an RMS-based DSR has no geographic redundancy, there is just a single RMS geographic site, functioning as a single RMS Diameter site. The upgrade of this DSR deployment should be done in two maintenance windows: one for the NOAMs, and the second for all remaining servers.

When an RMS-based DSR includes geographic redundancy, there are two RMS geographic sites (but still functioning as a single RMS Diameter site). The primary RMS site contains the NOAM Active/Standby pair that manages the network element, while the geo-redundant RMS site contains a Disaster Recovery NOAM pair. Each RMS geographic site includes its own SOAM pair, but only the SOAMs at the primary RMS site are used to manage the signaling network element. The SOAMs at the geo-redundant site are for backup purposes only. The upgrade of this DSR deployment should be done in three maintenance windows: one for all NOAMs; a second for the SOAMs and DA-MPs at the geo-redundant backup RMS site; and a third for the SOAMs and DA-MPs at the primary RMS site.

5.3.1.2 TVOE Upgrade Check

When using the Automated Server Group Upgrade feature, it is not possible to upgrade the TVOE hosts with the application, as the application upgrades are performed continuously to completion. Therefore, all TVOE hosts associated with the server group must be upgraded, if necessary, prior to initiating the server group upgrade sequence. Refer to Section 3.4.6 for TVOE host upgrade procedures. Once the TVOE hosts upgrades are complete, return to this section to continue the site upgrade.

Note: for RMS and VEDSR configurations, the TVOE for the server hosting the PM&C may have already been upgraded.

The TVOE version check is especially applicable to VEDSR systems, wherein all of the DSR applications run as guests of a TVOE host. In particular, consideration must be given to Spare SOAMs and Spare SBRs, which may be located at a different physical location, but will be upgraded with the server group to which the Spare server belongs.

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. TVOE Hosts may be upgraded during this procedure, if the TVOE needs to be upgraded. It assumes that each of the SOAM servers is running on a TVOE Host (i.e. it assumes that there are 2 or 3 TVOE hosts to be upgraded at the site.)

It is highly recommended that TVOE Hosts at a site be upgraded in a Maintenance Window prior to the start of the DSR 8.0 Application upgrade. If the TVOE Hosts are upgraded with the Application, consideration must be given to the risks and consequences of exceeding the Maintenance Window.

During the site upgrade (SOAMs plus all C-level servers), site provisioning is disabled. Provisioning will be 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 19 shows the estimated execution times for the SOAM upgrade. Procedure 34: Automated SOAM Upgrade (Active/Standby) is the recommended procedure for upgrading the SOAMs when there is no Spare SOAM. ASG will automatically upgrade the Standby SOAM, followed by the Active SOAM.

If the site does have a Spare SOAM, Procedure 35: Manual SOAM Upgrade (Active/Standby/Spare) is the recommended procedure. The manual upgrade procedure will upgrade the Standby and Spare SOAMs in parallel, followed by the Active SOAM.

Table 19: SOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		

Iteration 1 & 2 Procedure 34 or Procedure 35	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 24; **[**Procedure 25, Procedure 26, or Procedure 27**]**; Procedure 29

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 33 is required to ensure site provisioning is disabled.

If the site does ***not*** include a Spare SOAM, use the automated SOAM upgrade in Procedure 34.
If the site does include a Spare SOAM, use the manual SOAM upgrade in Procedure 35.

Procedure 33: SOAM Upgrade Pre-Checks

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active SOAM VIP:** Verify Traffic status	View KPIs to verify traffic status. 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > KPIs**. 3. Inspect KPI reports to verify traffic is at the expected condition.
2. □	**Active SOAM VIP:** Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 29. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, continue with the next procedure per Table 18, otherwise, execute: Procedure 29: Disable Site Provisioning
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.3.3.1 Automated SOAM Upgrade (Active/Standby)

Procedure 34 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 35. Upon completion of this procedure, proceed to Section 5.4 Upgrade Iteration 3 Overview.

Procedure 34: Automated SOAM Upgrade (Active/Standby)

STEP #	This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option. If necessary, the TVOE on each server that hosts an SOAM guest is also upgraded. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	Upgrade TVOE Host for Active and/or Standby SOAM servers	If the TVOE Host for the Active or Standby SOAM needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Active and/or Standby SOAM, as necessary. **NOTE: In an RMS-based DSR, the SOAM is a guest on a TVOE Host that has already been upgraded as part of the NOAM upgrade.**
2. □	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 J** — Upgrade Multiple Servers Procedure After successfully completing the procedure in **Appendix J**, return to this point and proceed to Section 5.4 Upgrade Iteration 3 Overview.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 will be inhibited due to the difference in release versions.

5.3.3.2 Manual SOAM Upgrade (Active/Standby/Spare)

Procedure 35 is used to upgrade the SOAM Server Group if the site includes a Spare SOAM. If the SOAM Server Group was upgraded using Procedure 34, do not execute this procedure; proceed to Section 5.4 Upgrade Iteration 3 Overview.

Procedure 35: Manual SOAM Upgrade (Active/Standby/Spare)

STEP #	This procedure upgrades the SOAM(s) in a DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	Upgrade TVOE Host for Active, Standby, and/or Spare SOAM servers	If the TVOE Host for the Active, Standby, or Spare SOAM needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Active, Standby, and/or Spare SOAM, as necessary. **NOTE: In an RMS-based DSR, the SOAM is a guest on a TVOE Host that has already been upgraded as part of the NOAM upgrade.**
2. □	Upgrade Standby and Spare SOAMs	Upgrade the Standby and Spare SOAM servers in parallel using the Upgrade Multiple Servers procedure : **Execute Appendix J** - Upgrade Multiple Servers Procedure After successfully completing the procedure in Appendix J, return to this point and continue with the next step.
3. □	Upgrade Active SOAM	Upgrade the Active SOAM server using Upgrade Single Server procedure : **Execute Appendix G** - Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and proceed to Section 5.4 Upgrade Iteration 3 Overview.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 will be 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 17, iteration 3 consists of upgrading the DA-MPs, SS7-MPs, IPFEs, and Spare SBR(s), if equipped. The C-level components will be upgraded in parallel to maximize Maintenance Window usage.

Table 20 shows the estimated time required to upgrade the C-level servers for iteration 3.

Table 20: Iteration 3 Upgrade Execution Overview.

Procedure	**Elapsed Time (hr:min)**		**Procedure Title**	**Impact**
	This Step	**Cumulative**		
Procedure 36	0:40-1:00	0:40-1:00	Upgrade Iteration 3	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Spare SBR(s) will be offline

CAUTION	**ASG DOES NOT ALLOW THE OPERATOR TO SPECIFY THE UPGRADE ORDER OF THE DA-MP SERVERS. IF A MANUAL UPGRADE WAS RECOMMENDED IN SECTION 3.2, DO NOT USE ASG TO UPGRADE THE DA-MPS IN THIS ITERATION. ALTERNATE UPGRADE PROCEDURES ARE PROVIDED IN Appendix M.4**

5.4.1 Upgrade Iteration 3

Procedure 36 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 17 for the hostnames of the servers to be upgraded in this iteration.

Procedure 36: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.	
1. □	**Active NOAM VIP:** View pre-upgrade status of DA-MPs	Select the DA-MP server group. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 3. Select the SOAM tab of the site being upgraded. 4. Select the DA-MP Server Group link. 5. For the DA-MP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.

Procedure 36: Upgrade Iteration 3

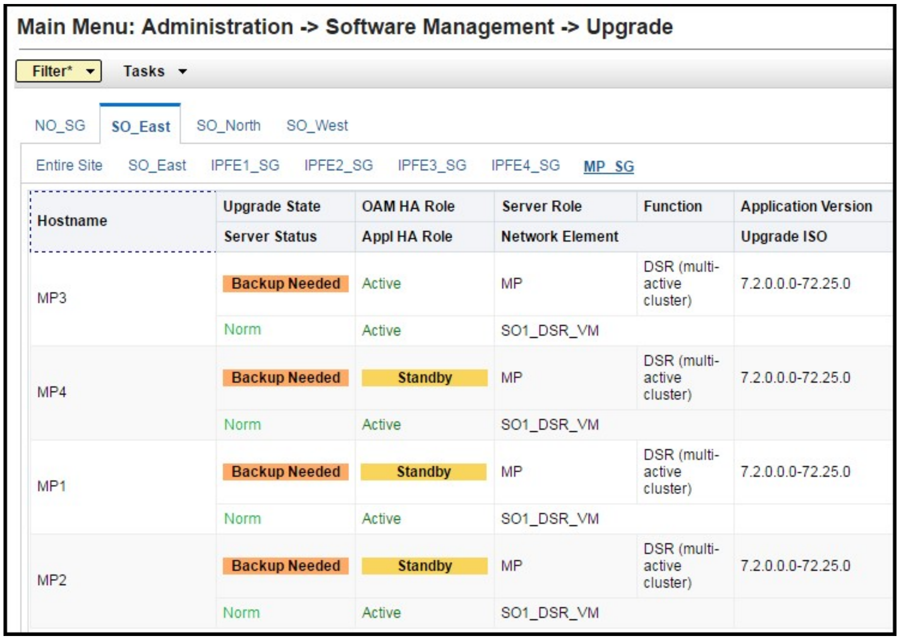
2. □

Active NOAM VIP:

View pre-upgrade status of DA-MPs

View the pre-upgrade status of the DA-MP servers.

1. If the servers are in “**Backup Needed”** state, select the servers and click the “**Backup**” button. The Upgrade State changes to “**Backup in Progress**”. When the backup is complete, the Upgrade State changes to “**Ready**”.
2. Verify the “OAM Max Ha Role” **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)



Main Menu: Administration -> Software Management -> Upgrade

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

Procedure 36: Upgrade Iteration 3

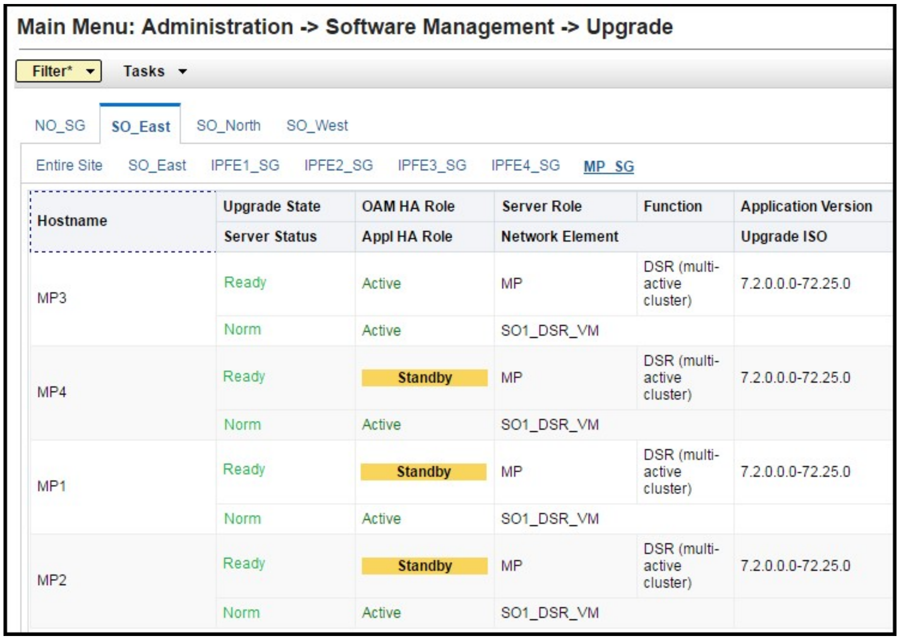
3. □

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 is displayed. Navigate to the DA-MP server group of the site being upgraded.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		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		

Servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 36: Upgrade Iteration 3

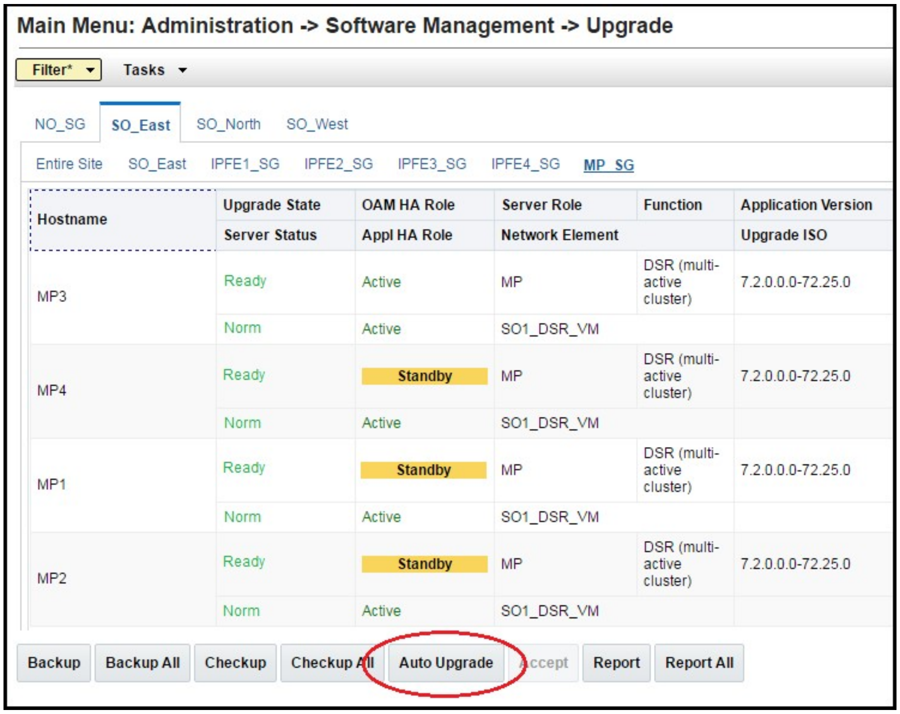
4. □

Active NOAM VIP:

Initiate DA-MP upgrade (part 1)

Select the Automated Server Group Upgrade option

1. To utilize the Automated Server Group upgrade option, verify that no servers in the server group are selected.
2. Click the **Auto Upgrade** button.



Main Menu: Administration -> Software Management -> Upgrade

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

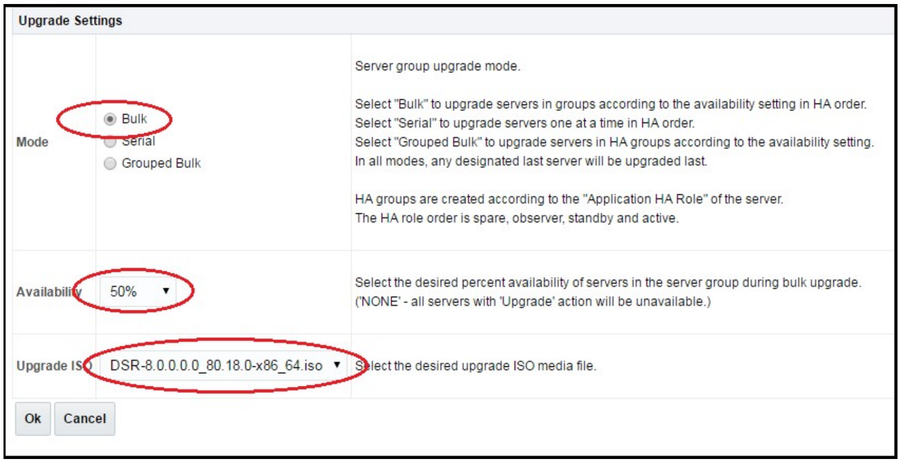
5. □

Active NOAM VIP:

Initiate DA-MP upgrade (part 2)

Start the Automated Server Group Upgrade of the DA-MPs.

1. The **Upgrade Settings** section of the Initiate screen controls the behavior of the server group upgrade. Select **Bulk** Mode.
2. Select **50%** for the **Availability** setting.
3. Select the appropriate ISO from the **Upgrade ISO** pick list.
4. Click the **Ok** button to start the upgrade.



Upgrade Settings

Mode	● Bulk ○ Serial ○ Grouped Bulk	Server group upgrade mode. Select "Bulk" to upgrade servers in groups according to the availability setting in HA order. Select "Serial" to upgrade servers one at a time in HA order. Select "Grouped Bulk" to upgrade servers in HA groups according to the availability setting. In all modes, any designated last server will be upgraded last. HA groups are created according to the "Application HA Role" of the server. The HA role order is spare, observer, standby and active.
Availability	50% ▾	Select the desired percent availability of servers in the server group during bulk upgrade. ('NONE' - all servers with 'Upgrade' action will be unavailable.)
Upgrade ISO	DSR-8.0.0.0.0_80.18.0-x86_64.iso ▾	Select the desired upgrade ISO media file.

Procedure 36: Upgrade Iteration 3

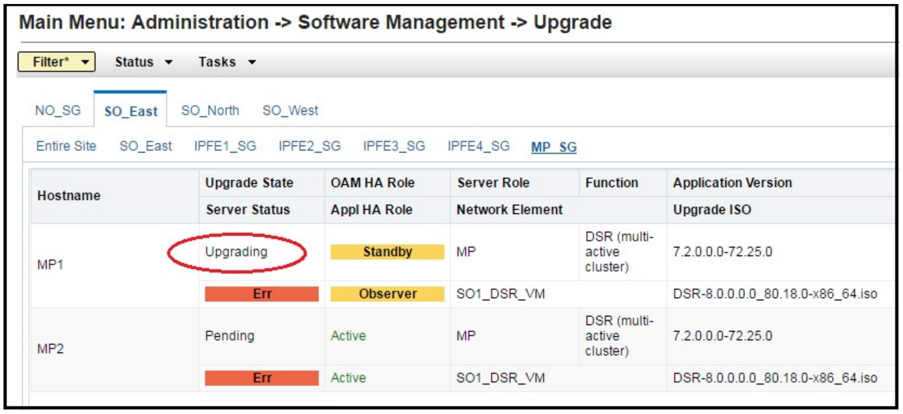
6. □

Active NOAM VIP:

View In-Progress Status (monitor)

View the Upgrade Administration form to monitor upgrade progress.

1. Observe the **Upgrade State** of the DA-MP servers. Upgrade status will be displayed under the **Status Message** column.


Main Menu: Administration -> Software Management -> Upgrade

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 17, identify the SS7-MP server group(s) to upgrade in iteration 3.

8. □

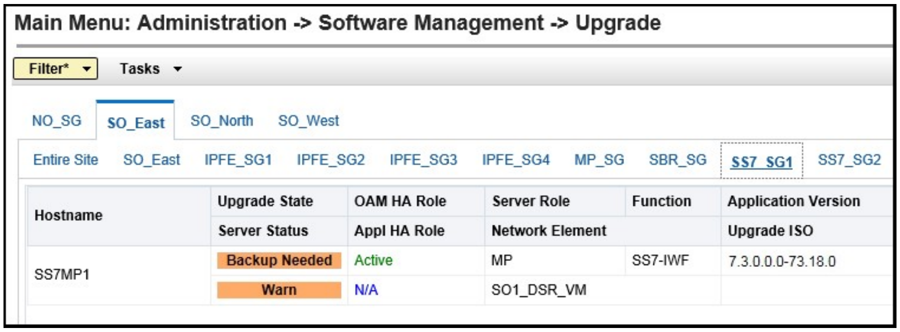
Active NOAM VIP:

View pre-upgrade status of SS7-MPs

View the pre-upgrade status of the SS7-MP servers.

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed
2. Select the SOAM tab of the site being upgraded.
3. Select the link for each SS7-MP Server Group to be upgraded.
4. For the SS7-MP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.

5. If a server is in "**Backup Needed"** state, select the server and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**".
6. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)


Main Menu: Administration -> Software Management -> Upgrade

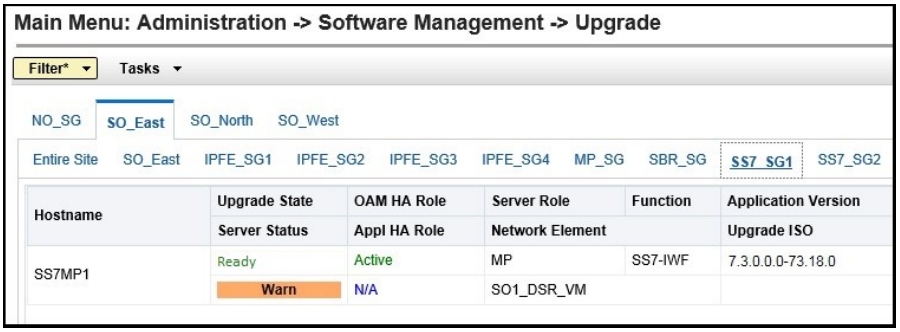
Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SS7MP1	Backup Needed	Active	MP	SS7-IWF	7.3.0.0.0-73.18.0
	Warn	N/A	SO1_DSR_VM		

Procedure 36: Upgrade Iteration 3

<table>
<tr>
<td>9.
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Verify Upgrade Status is “Ready”</td>
<td>
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 is displayed. Navigate to the SS7-MP server group being upgraded.



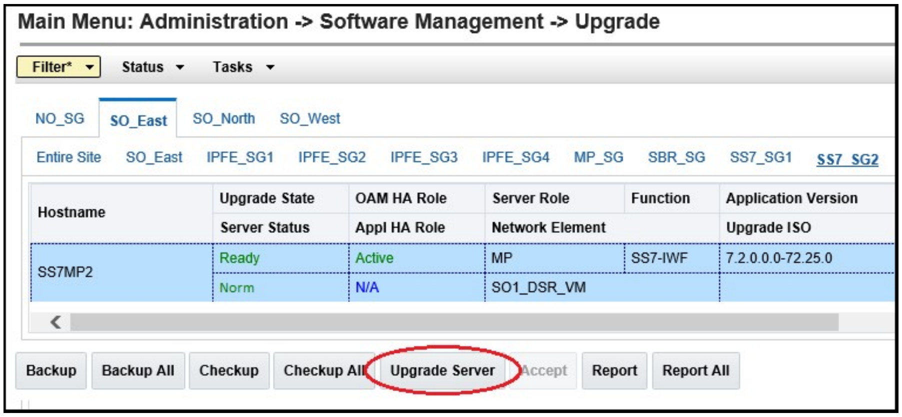
<table>
<tr><th>Hostname</th><th>Upgrade State
Server Status</th><th>OAM HA Role
Appl HA Role</th><th>Server Role
Network Element</th><th>Function</th><th>Application Version
Upgrade ISO</th></tr>
<tr><td>SS7MP1</td><td>Ready
Warn</td><td>Active
N/A</td><td>MP
SO1_DSR_VM</td><td>SS7-IWF</td><td>7.3.0.0.0-73.18.0</td></tr>
</table>

Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms:

Alarm ID = <b>10008 (Provisioning Manually Disabled)</b>
Alarm ID = <b>10073 (Server Group Max Allowed HA Role Warning)</b>
Alarm ID = <b>10075 (The server is no longer providing services because application processes have been manually stopped)</b>
Alarm ID = <b>32515 (Server HA Failover Inhibited)</b>
Alarm ID = <b>31101 (DB Replication to slave DB has failed)</b>
Alarm ID = <b>31106 (DB Merge to Parent Failure)</b>
Alarm ID = <b>31107 (DB Merge From Child Failure)</b>
Alarm ID = <b>31228 (HA Highly available server failed to receive mate heartbeats)</b> or <b>(Lost Communication with Mate Server)</b>
</td>
</tr>
<tr>
<td>10.
□</td>
<td><b><u>Active NOAM VIP:</u></b>

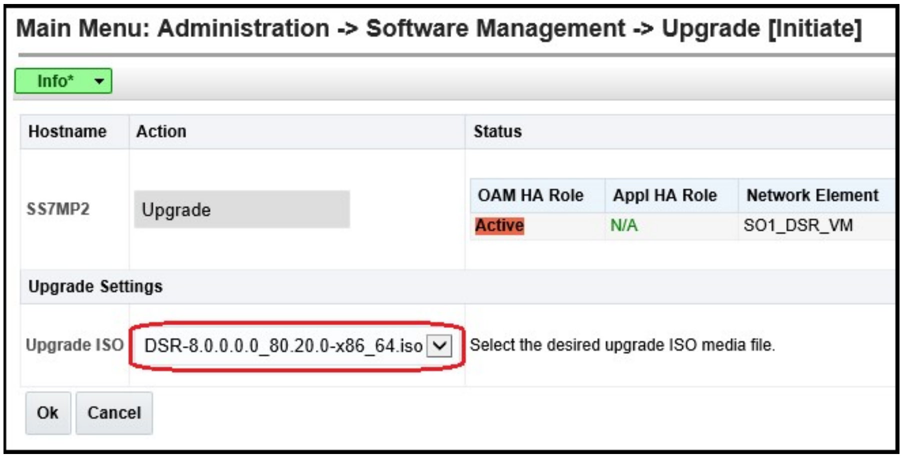
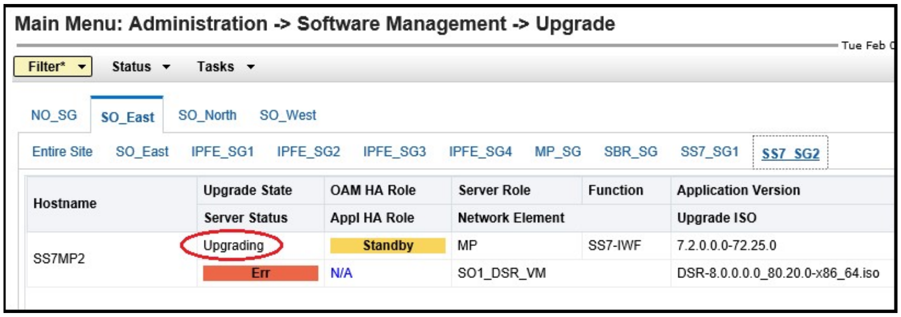
Initiate SS7-MP upgrade (part 1)</td>
<td>
Select the Upgrade Server upgrade method.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the “<b>Upgrade Server”</b> button.



<table>
<tr><th>Hostname</th><th>Upgrade State
Server Status</th><th>OAM HA Role
Appl HA Role</th><th>Server Role
Network Element</th><th>Function</th><th>Application Version
Upgrade ISO</th></tr>
<tr><td>SS7MP2</td><td>Ready
Norm</td><td>Active
N/A</td><td>MP
SO1_DSR_VM</td><td>SS7-IWF</td><td>7.2.0.0.0-72.25.0</td></tr>
</table>
</td>
</tr>
</table>

Procedure 36: Upgrade Iteration 3

<table>
<tr>
<td>11.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Initiate SS7-MP upgrade (part 2)</td>
<td>Select target ISO.
1. On the <b>Upgrade [Initiate]</b> screen, select the target ISO from the Upgrade ISO picklist.
2. Click <b>Ok</b> to initiate the upgrade.

Main Menu: Administration -> Software Management -> Upgrade [Initiate]
<table>
<tr><th>Hostname</th><th>Action</th><th>Status</th></tr>
<tr><td>SS7MP2</td><td>Upgrade</td><td>OAM HA Role: Active
Appl HA Role: N/A
Network Element: SO1_DSR_VM</td></tr>
<tr><td colspan="3">Upgrade Settings</td></tr>
<tr><td>Upgrade ISO</td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td><td>Select the desired upgrade ISO media file.</td></tr>
</table>
</td>
</tr>
<tr>
<td>12.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View In-Progress Status (monitor)</td>
<td>View the Upgrade Administration form to monitor upgrade progress.
1. Observe the <b>Upgrade State</b> of the SS7-MP server. Upgrade status will be displayed under the <b>Status Message</b> column.

Main Menu: Administration -> Software Management -> Upgrade

Tue Feb 0
Filter*
Status
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
<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">SS7MP2</td><td>Upgrading</td><td>Standby</td><td>MP</td><td>SS7-IWF</td><td>7.2.0.0.0-72.25.0</td></tr>
<tr><td>Err</td><td>N/A</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
</table></td>
</tr>
<tr>
<td>13.
□</td>
<td>Repeat for each SS7-MP</td>
<td>Repeat steps 6 through 12 for the next SS7-MP to be upgraded per Table 17.</td>
</tr>
<tr>
<td>14.
□</td>
<td>Continue upgrade iteration 3</td>
<td>While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.</td>
</tr>
<tr>
<td>15.
□</td>
<td>Identify the IPFE Server Group(s) to Upgrade</td>
<td>From the data captured in Table 17, identify the IPFE server group(s) to upgrade in iteration 3.</td>
</tr>
</table>

Procedure 36: Upgrade Iteration 3

16.

□

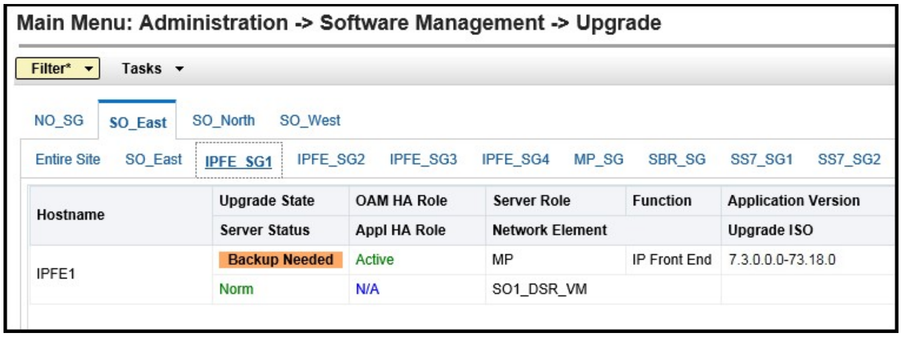
Active NOAM VIP:

View pre-upgrade status of IPFEs

View the pre-upgrade status of the IPFE servers.

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed
2. Select the SOAM tab of the site being upgraded.
3. Select the link for each IPFE Server Group to be upgraded.
4. For the IPFE servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.

5. If a server is in "**Backup Needed"** state, select the server and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**".
6. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
IPFE1	Backup Needed	Active	MP	IP Front End	7.3.0.0.0-73.18.0
	Norm	N/A	SO1_DSR_VM		

17.

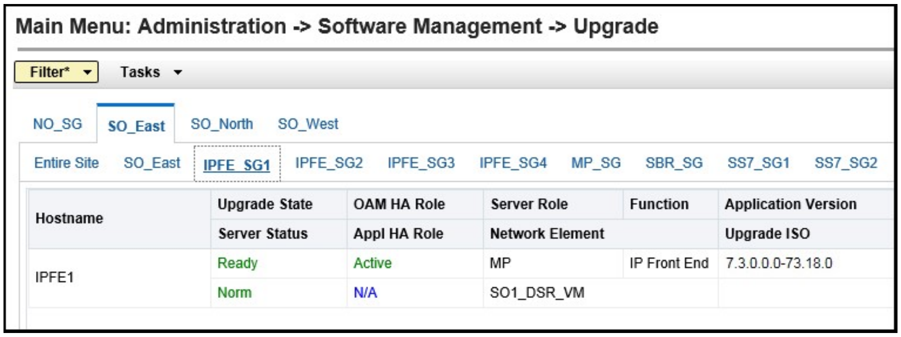
□

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 is displayed. Navigate to the IPFE server group being upgraded.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
IPFE1	Ready	Active	MP	IP Front End	7.3.0.0.0-73.18.0
	Norm	N/A	SO1_DSR_VM		

Servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 36: Upgrade Iteration 3

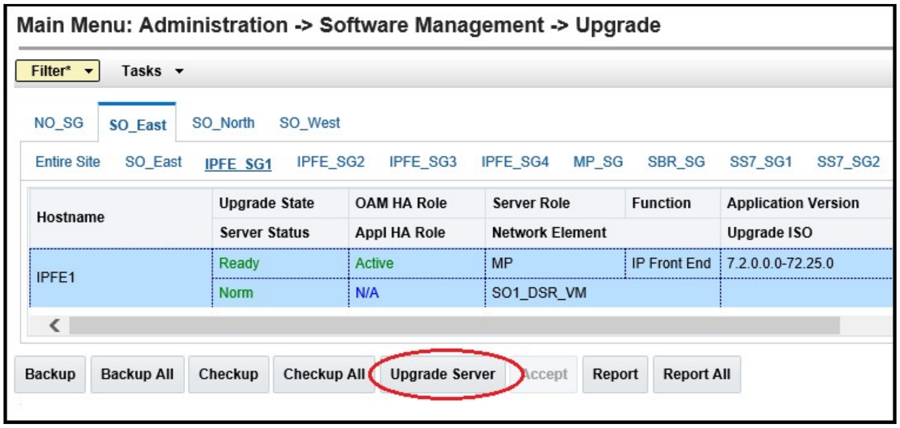
18. □

Active NOAM VIP:

Initiate IPFE upgrade (part 1)

Select the Upgrade Server upgrade method.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the "**Upgrade Server"** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
IPFE1	Ready Norm	Active N/A	MP SO1_DSR_VM	IP Front End	7.2.0.0.0-72.25.0

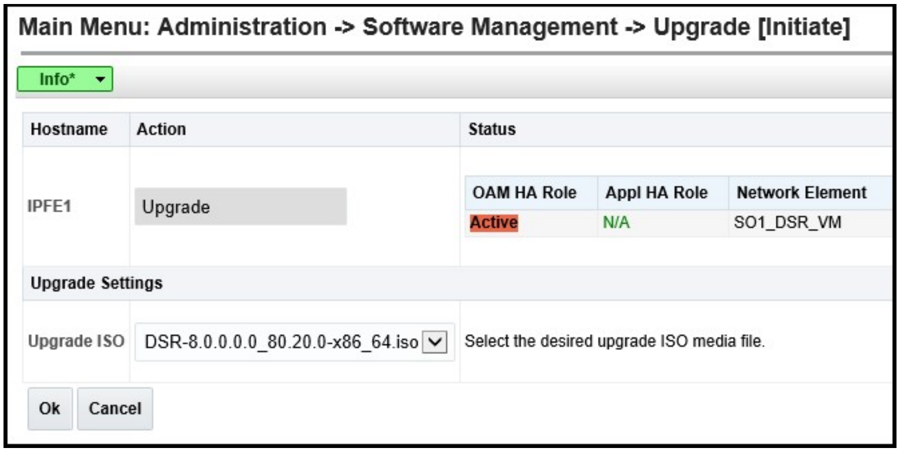
19. □

Active NOAM VIP:

Initiate SS7-MP upgrade (part 2)

Select target ISO.

1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist.
2. Click **Ok** to initiate the upgrade.



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

Hostname	Action	OAM HA Role	Appl HA Role	Network Element
IPFE1	Upgrade	Active	N/A	SO1_DSR_VM

Upgrade Settings

Upgrade ISO: DSR-8.0.0.0.0_80.20.0-x86_64.iso — Select the desired upgrade ISO media file.

Procedure 36: Upgrade Iteration 3

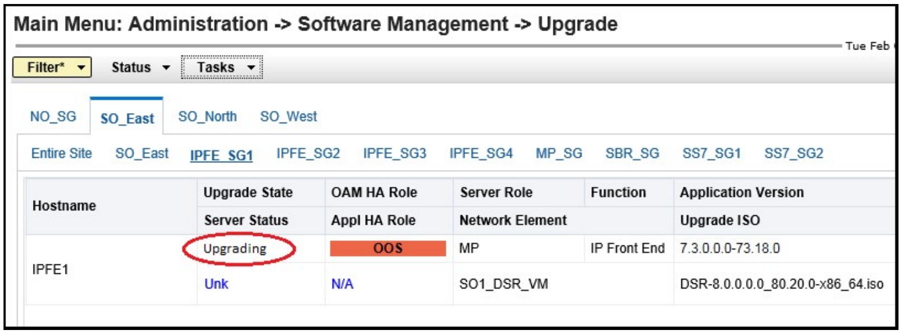
20. □

Active NOAM VIP:

View In-Progress Status (monitor)

View the Upgrade Administration form to monitor upgrade progress.

1. Observe the **Upgrade State** of the IPFE server. Upgrade status will be displayed under the **Status Message** column.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
IPFE1	Upgrading	OOS	MP	IP Front End	7.3.0.0.0-73.18.0
	Unk	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.20.0-x86_64.iso

21. □

Repeat for each IPFE

Repeat steps 15 through 20 for the next IPFE to be upgraded in this iteration per Table 17.

22. □

Identify the SBR Server Group(s) to Upgrade

From the data captured in Table 17, identify the SBR server group(s) to upgrade in iteration 3.

23. □

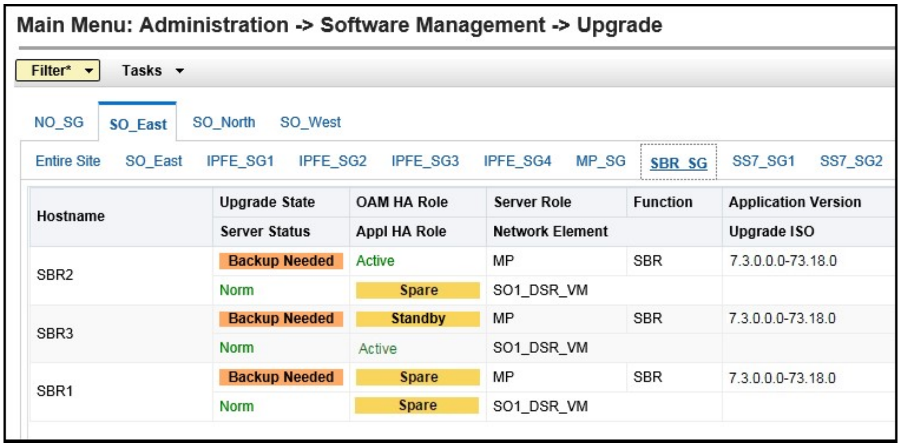
Active NOAM VIP:

View pre-upgrade status of SBRs

View the pre-upgrade status of the SBR servers to be upgraded.

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed.
2. Select the SOAM tab of the site being upgraded.
3. Select the link of the SBR server group to be upgraded.
4. For the SBR servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version

   .
5. If the server is in “**Backup Needed”** state, select the server and click the “**Backup**” button. The Upgrade State changes to “**Backup in Progress**”. When the backup is complete, the Upgrade State changes to “**Ready**”.
6. Verify the “OAM Max Ha Role” **is the expected condition (Spare, Standby or Active)** (this will depend on the server being upgraded)



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SBR2	Backup Needed	Active	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Spare	SO1_DSR_VM		
SBR3	Backup Needed	Standby	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Active	SO1_DSR_VM		
SBR1	Backup Needed	Spare	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Spare	SO1_DSR_VM		

Procedure 36: Upgrade Iteration 3

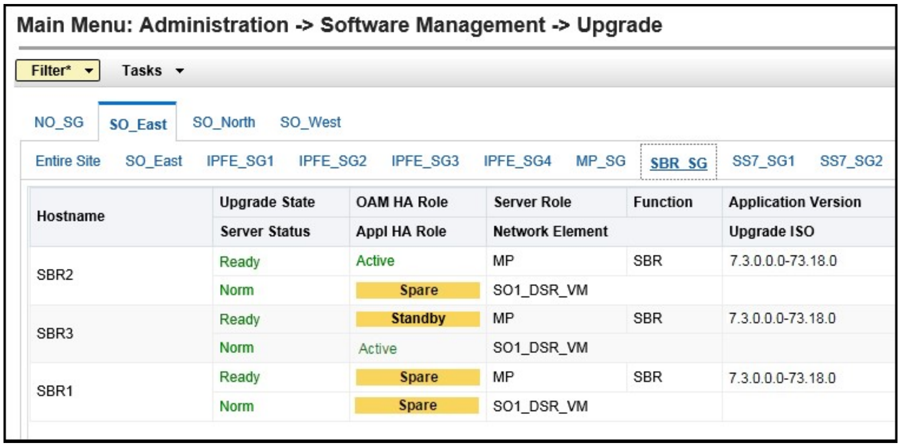
24. □

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 is displayed. Navigate to the SBR server group being upgraded.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SBR2	Ready	Active	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Spare	SO1_DSR_VM		
SBR3	Ready	Standby	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Active	SO1_DSR_VM		
SBR1	Ready	Spare	MP	SBR	7.3.0.0.0-73.18.0
	Norm	Spare	SO1_DSR_VM		

Servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 36: Upgrade Iteration 3

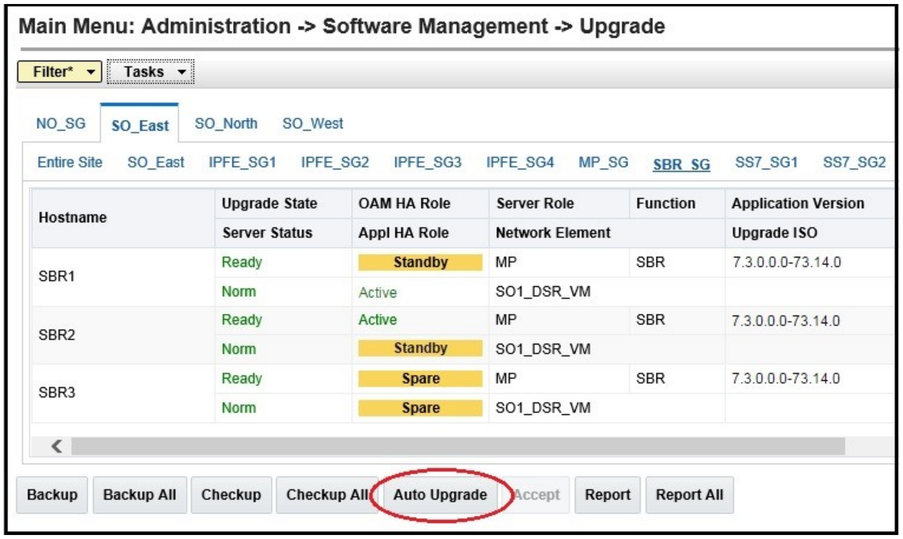
25. □

Active NOAM VIP:

Initiate SBR upgrade (part 1)

Select the Auto Upgrade upgrade method

1. To utilize the Automated Server Group upgrade option, select the SBR server group to be upgraded.
2. Verify that no servers in the server group are selected.
3. Click the **Auto Upgrade** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SBR1	Ready	Standby	MP	SBR	7.3.0.0.0-73.14.0
	Norm	Active	SO1_DSR_VM		
SBR2	Ready	Active	MP	SBR	7.3.0.0.0-73.14.0
	Norm	Standby	SO1_DSR_VM		
SBR3	Ready	Spare	MP	SBR	7.3.0.0.0-73.14.0
	Norm	Spare	SO1_DSR_VM		

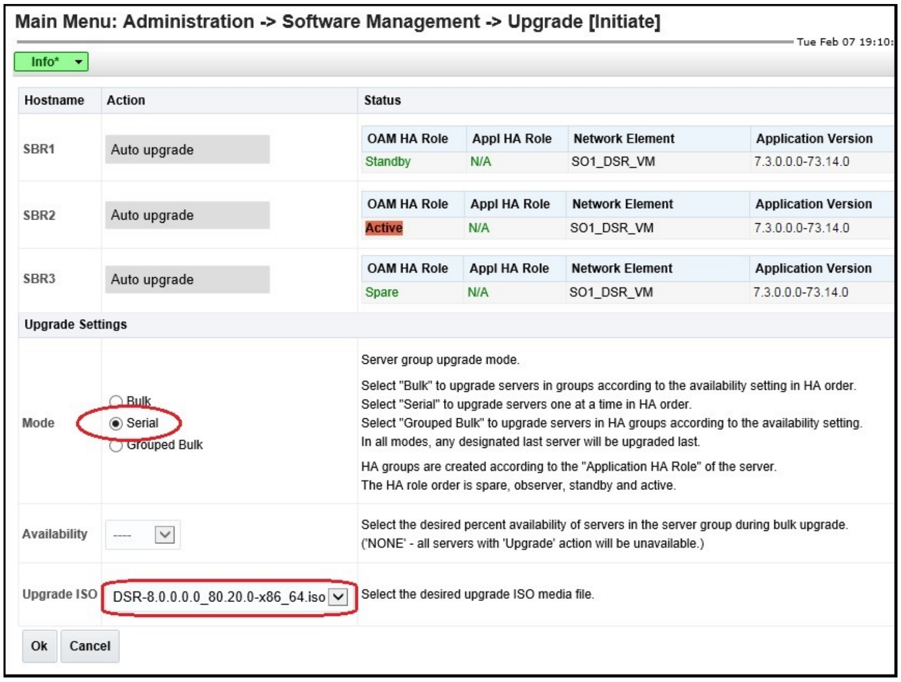
26. □

Active NOAM VIP:

Initiate SBR upgrade (part 2)

Set upgrade options and start the Automated Server Group Upgrade.

1. The Upgrade **Settings** section of the Initiate screen controls the behavior of the automated upgrade. Select **Serial** Mode.
2. Select the appropriate ISO from the **Upgrade ISO** pick list.
3. Click the **Ok** button to start the upgrade.



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

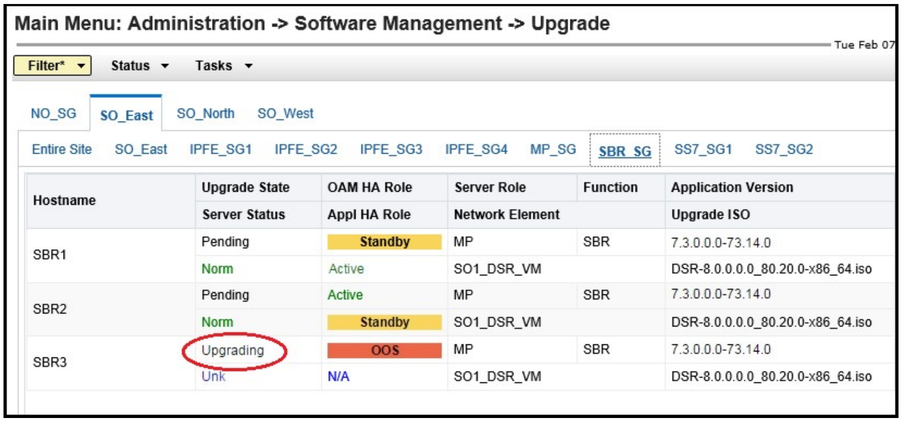
Tue Feb 07 19:10:

Hostname	Action	OAM HA Role	Appl HA Role	Network Element	Application Version
SBR1	Auto upgrade	Standby	N/A	SO1_DSR_VM	7.3.0.0.0-73.14.0
SBR2	Auto upgrade	Active	N/A	SO1_DSR_VM	7.3.0.0.0-73.14.0
SBR3	Auto upgrade	Spare	N/A	SO1_DSR_VM	7.3.0.0.0-73.14.0

Upgrade Settings

Mode	○ Bulk ● Serial ○ Grouped Bulk	Server group upgrade mode. Select "Bulk" to upgrade servers in groups according to the availability setting in HA order. Select "Serial" to upgrade servers one at a time in HA order. Select "Grouped Bulk" to upgrade servers in HA groups according to the availability setting. In all modes, any designated last server will be upgraded last. HA groups are created according to the "Application HA Role" of the server. The HA role order is spare, observer, standby and active.
Availability	----	Select the desired percent availability of servers in the server group during bulk upgrade. ('NONE' - all servers with 'Upgrade' action will be unavailable.)
Upgrade ISO	DSR-8.0.0.0.0_80.20.0-x86_64.iso	Select the desired upgrade ISO media file.

Procedure 36: Upgrade Iteration 3

<table>
<tr>
<td>27.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View In-Progress Status (monitor)</td>
<td>
View the Upgrade Administration form to monitor upgrade progress.
1. Observe the <b>Upgrade State</b> of the SBR Server Group. Upgrade status will be displayed under the <b>Status Message</b> column (not shown).

Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">SBR1</td><td>Pending</td><td>Standby</td><td>MP</td><td>SBR</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>Active</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
<tr><td rowspan="2">SBR2</td><td>Pending</td><td>Active</td><td>MP</td><td>SBR</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>Standby</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
<tr><td rowspan="2">SBR3</td><td>Upgrading</td><td>OOS</td><td>MP</td><td>SBR</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Unk</td><td>N/A</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
</table>
</td>
</tr>
<tr>
<td>28.
□</td>
<td>Repeat for each SBR Server Group</td>
<td>Repeat steps 22 through 27 for the next SBR Server Group to be upgraded per Table 17.</td>
</tr>
</table>

Procedure 36: Upgrade Iteration 3

29. □	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 30 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 will be shown as "FAILED".* *The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Navigate to **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. Select the SOAM tab of the site being upgraded. 3. Sequence through the server group links for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column. During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 Auto Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers will not be updated until resolved. Refer to **APPENDIX R** to resolve this issue. 4. Half of the DA-MP and SBR server groups are upgraded in iteration 3. ASG will automatically sequence to iteration 4 to upgrade the remaining servers. Periodically monitor these servers for failures. 5. For the SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The **Status Message** column will show "Success" after approximately 20 to 50 minutes. Do not proceed to iteration 4 until the SS7-MP and IPFE servers have completed upgrade. **NOTE: Do Not Accept any upgrades at this time.** **If any upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O 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/upgrade.log`
		It is recommended to contact MOS by referring to Appendix S of this document and provide these files.Refer to Appendix O for failed server recovery procedures.

THIS PROCEDURE HAS BEEN COMPLETED.

5.5 Upgrade Iteration 4 Overview

Upgrade iteration 4 continues the upgrade of the site C-level servers. As shown in Table 17, 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 21 shows the estimated time required to upgrade the C-level servers for iteration 4.

Table 21: Iteration 4 Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 37	0:40-1:00		Upgrade Iteration 4	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s) will be offline

5.5.1 Upgrade Iteration 4

Procedure 37 provides the steps to upgrade ½ of the SS7-MPs, and ½ of the IPFEs. The DA-MPs and SBRs will automatically be upgraded by ASG. Refer to Table 17 for the hostnames of the servers to be upgraded in this iteration.

Procedure 37: Upgrade Iteration 4

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	Identify the SS7-MP Server Group(s) to Upgrade	From the data captured in Table 17, identify the SS7-MP server group(s) to upgrade in iteration 4.

Procedure 37: Upgrade Iteration 4

2. □

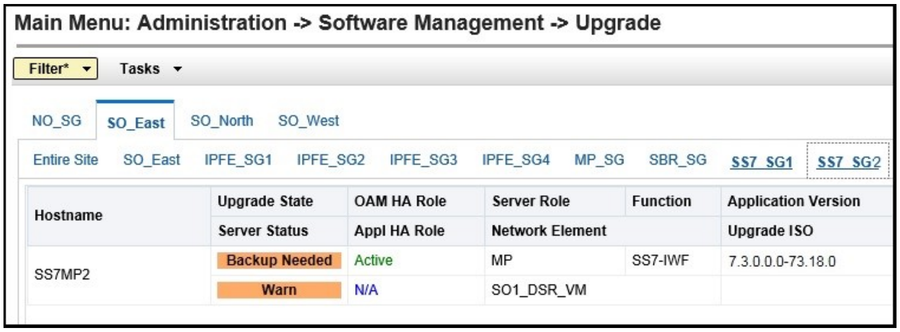
Active NOAM VIP:

View pre-upgrade status of SS7-MPs

View the pre-upgrade status of the SS7-MP servers.

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed
2. Select the SOAM tab of the site being upgraded.
3. Select the link for each SS7-MP server group to be upgraded.
4. For the SS7-MP servers to be upgraded in iteration 4, verify the Application Version value is the expected source software release version.

5. If a server is in "**Backup Needed"** state, select the server and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**".
6. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SS7MP2	Backup Needed	Active	MP	SS7-IWF	7.3.0.0.0-73.18.0
	Warn	N/A	SO1_DSR_VM		

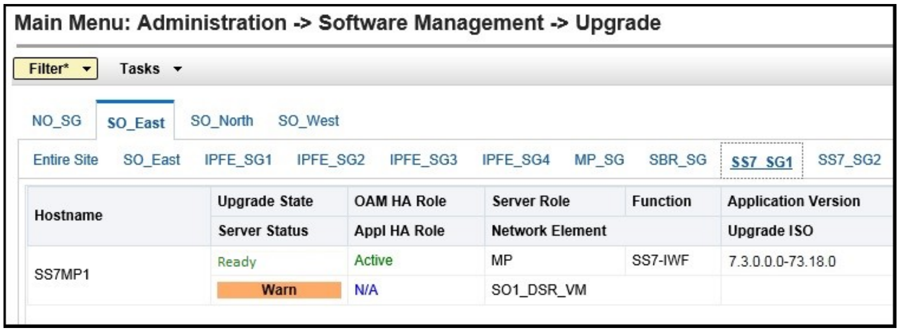
3. □

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 is displayed. Navigate to the SS7-MP server group being upgraded.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SS7MP1	Ready	Active	MP	SS7-IWF	7.3.0.0.0-73.18.0
	Warn	N/A	SO1_DSR_VM		

Servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 37: Upgrade Iteration 4

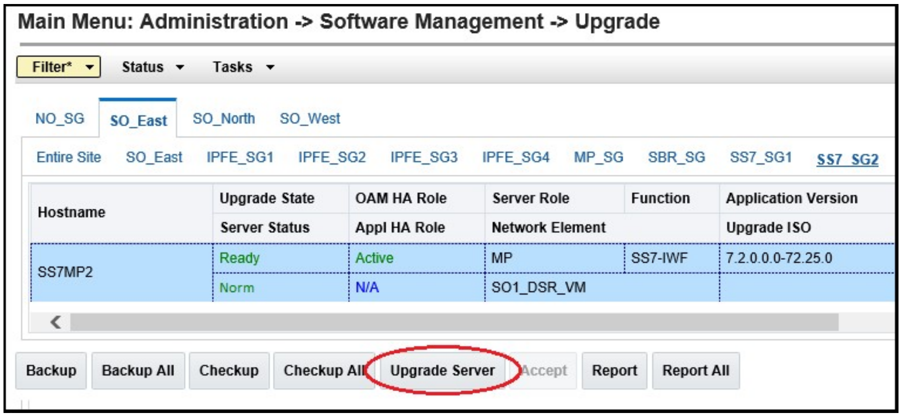
4. □

Active NOAM VIP:

Initiate SS7-MP upgrade (part 1)

Select the Upgrade Server upgrade method.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the "**Upgrade Server"** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SS7MP2	Ready	Active	MP	SS7-IWF	7.2.0.0.0-72.25.0
	Norm	N/A	SO1_DSR_VM		

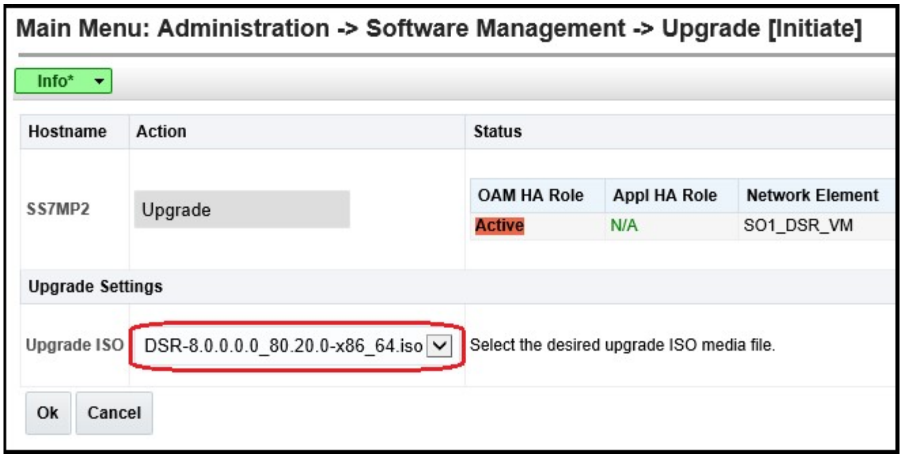
5. □

Active NOAM VIP:

Initiate SS7-MP upgrade (part 2)

Select target ISO.

1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist.
2. Click **Ok** to initiate the upgrade.



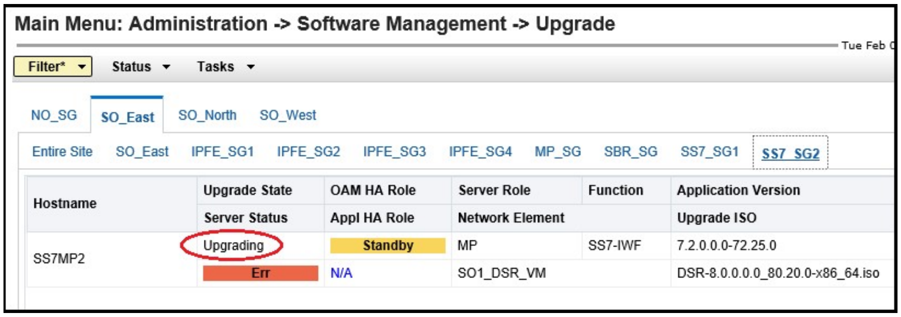
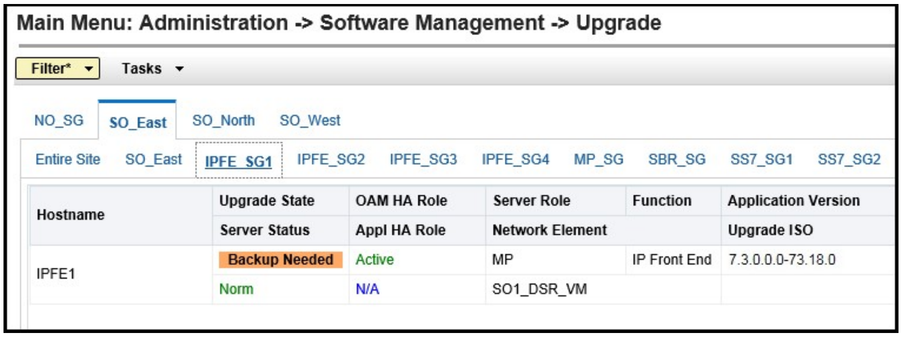
Main Menu: Administration -> Software Management -> Upgrade [Initiate]

Hostname	Action	Status		
		OAM HA Role	Appl HA Role	Network Element
SS7MP2	Upgrade	Active	N/A	SO1_DSR_VM

Upgrade Settings

Upgrade ISO: DSR-8.0.0.0.0_80.20.0-x86_64.iso — Select the desired upgrade ISO media file.

Procedure 37: Upgrade Iteration 4

<table>
<tr>
<td>6.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View In-Progress Status (monitor)</td>
<td>View the Upgrade Administration form to monitor upgrade progress.
1. Observe the <b>Upgrade State</b> of the SS7-MP server. Upgrade status will be displayed under the <b>Status Message</b> column.

Main Menu: Administration -> Software Management -> Upgrade
Tue Feb 0
Filter*
Status
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
<table>
<tr><th>Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th></th><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td>SS7MP2</td><td>Upgrading</td><td>Standby</td><td>MP</td><td>SS7-IWF</td><td>7.2.0.0.0-72.25.0</td></tr>
<tr><td></td><td>Err</td><td>N/A</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
</table>
</td>
</tr>
<tr>
<td>7.
□</td>
<td>Repeat for each SS7-MP</td>
<td>Repeat steps 1 through 6 for the next SS7-MP to be upgraded in this iteration per Table 17.</td>
</tr>
<tr>
<td>8.
□</td>
<td>Continue upgrade iteration 4</td>
<td>While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.</td>
</tr>
<tr>
<td>9.
□</td>
<td>Identify the IPFE Server Group(s) to Upgrade</td>
<td>From the data captured in Table 17, identify the IPFE server group(s) to upgrade in iteration 4.</td>
</tr>
<tr>
<td>10.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View pre-upgrade status of IPFEs</td>
<td>View the pre-upgrade status of the IPFE servers.
1. Navigate to <b>Administration > Software Management > Upgrade</b>
The Upgrade Administration screen is displayed
2. Select the SOAM tab of the site being upgraded.
3. Select the link of each IPFE server group to be upgraded.
4. For the IPFE servers to be upgraded in iteration 4, verify the Application Version value is the expected source software release version.
5. If a server is in “<b>Backup Needed”</b> state, select the server and click the “<b>Backup</b>” button. The Upgrade State changes to “<b>Backup in Progress</b>”. When the backup is complete, the Upgrade State changes to “<b>Ready</b>”.
6. Verify the “OAM Max Ha Role” <b>is the expected condition (either Standby or Active)</b> (this will depend 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
<table>
<tr><th>Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th></th><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td>IPFE1</td><td>Backup Needed</td><td>Active</td><td>MP</td><td>IP Front End</td><td>7.3.0.0.0-73.18.0</td></tr>
<tr><td></td><td>Norm</td><td>N/A</td><td>SO1_DSR_VM</td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

Procedure 37: Upgrade Iteration 4

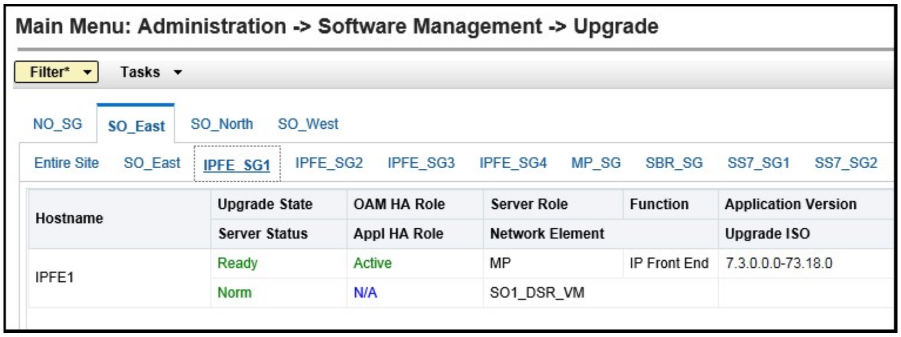
11. □

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 is displayed. Navigate to the IPFE server group being upgraded.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
IPFE1	Ready	Active	MP	IP Front End	7.3.0.0.0-73.18.0
	Norm	N/A	SO1_DSR_VM		

Servers may have a combination of the following expected alarms. NOTE: Not all servers will 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)**

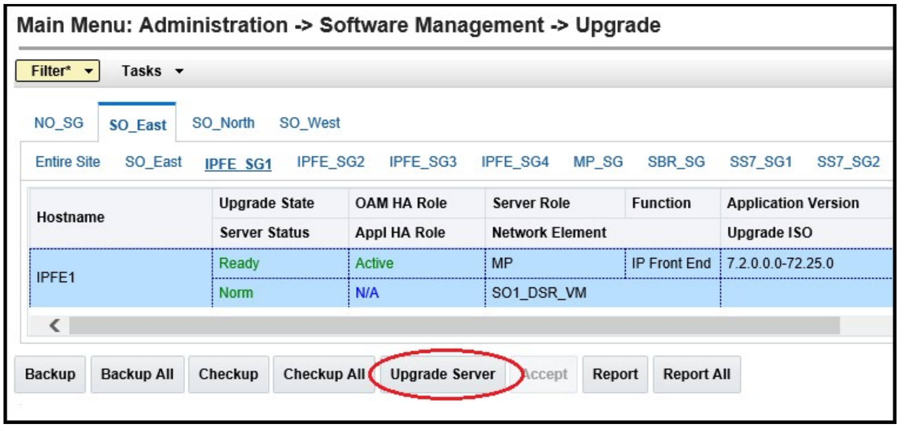
12. □

Active NOAM VIP:

Initiate IPFE upgrade (part 1)

Select the Upgrade Server upgrade method.

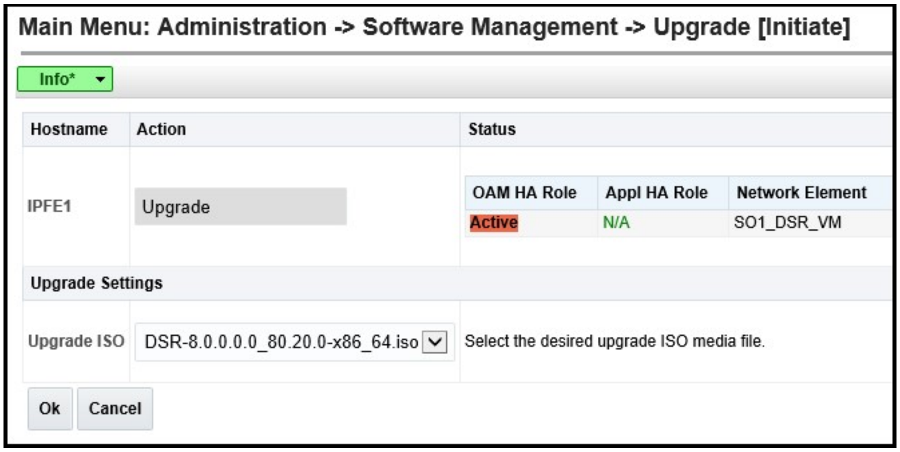
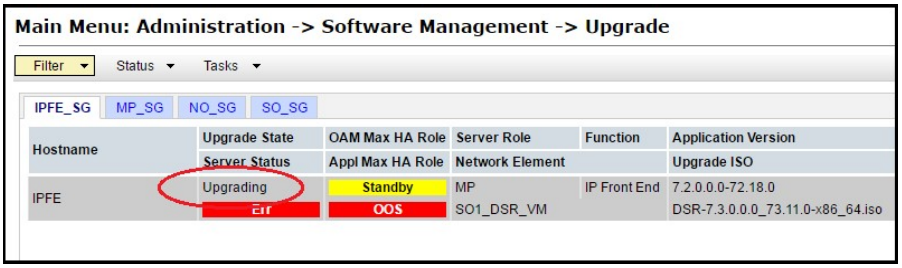
1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the "**Upgrade Server"** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
IPFE1	Ready	Active	MP	IP Front End	7.2.0.0.0-72.25.0
	Norm	N/A	SO1_DSR_VM		

Procedure 37: Upgrade Iteration 4

<table>
<tr>
<td>13.
□</td>
<td><u>Active NOAM VIP:</u>
Initiate SS7-MP upgrade (part 2)</td>
<td>Select target ISO.
1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist.
2. Click **Ok** to initiate the upgrade.

Main Menu: Administration -> Software Management -> Upgrade [Initiate]
Info*
<table>
<tr><td>Hostname</td><td>Action</td><td>Status</td><td></td><td></td></tr>
<tr><td></td><td></td><td>OAM HA Role</td><td>Appl HA Role</td><td>Network Element</td></tr>
<tr><td>IPFE1</td><td>Upgrade</td><td>Active</td><td>N/A</td><td>SO1_DSR_VM</td></tr>
<tr><td>Upgrade Settings</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Upgrade ISO</td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td><td>Select the desired upgrade ISO media file.</td><td></td><td></td></tr>
</table>
Ok Cancel</td>
</tr>
<tr>
<td>14.
□</td>
<td><u>Active NOAM VIP:</u>
View In-Progress Status (monitor)</td>
<td>View the Upgrade Administration form to monitor upgrade progress.
1. Observe the **Upgrade State** of the IPFE server. Upgrade status will be displayed under the **Status Message** column.

Main Menu: Administration -> Software Management -> Upgrade
Filter Status Tasks
IPFE_SG MP_SG NO_SG SO_SG
<table>
<tr><td>Hostname</td><td>Upgrade State</td><td>OAM Max HA Role</td><td>Server Role</td><td>Function</td><td>Application Version</td></tr>
<tr><td></td><td>Server Status</td><td>Appl Max HA Role</td><td>Network Element</td><td></td><td>Upgrade ISO</td></tr>
<tr><td>IPFE</td><td>Upgrading</td><td>Standby</td><td>MP</td><td>IP Front End</td><td>7.2.0.0.0-72.18.0</td></tr>
<tr><td></td><td>Err</td><td>OOS</td><td>SO1_DSR_VM</td><td></td><td>DSR-7.3.0.0.0_73.11.0-x86_64.iso</td></tr>
</table></td>
</tr>
<tr>
<td>15.
□</td>
<td>Repeat for each IPFE</td>
<td>Repeat steps 9 through 14 for the next IPFE to be upgraded per Table 17.</td>
</tr>
</table>

Procedure 37: Upgrade Iteration 4

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 will be shown as "FAILED".* *The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Navigate to **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. Select the SOAM tab of the site being upgraded. 3. Sequence through the server group tabs for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column. During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 Auto Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers will not be updated until resolved. Refer to **APPENDIX R** to resolve this issue. 4. The SBR server groups being upgraded with ASG will upgrade the Standby SBR in iteration 4, and automatically sequence to iteration 5. Periodically monitor these servers for failures, if equipped. 5. For the DA-MP, SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The **Status Message** column will show "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 to consult with MOS on the best course of action. Refer to Appendix O 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`

		THIS PROCEDURE HAS BEEN COMPLETED.

5.6 Upgrade Iteration 5 Overview

Upgrade iteration 5 continues the upgrade of the site C-level servers. As shown in Table 17, iteration 5 consists of upgrading the Active SBR(s).

Table 22 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

Table 22: Iteration 5 Upgrade Execution Overview.

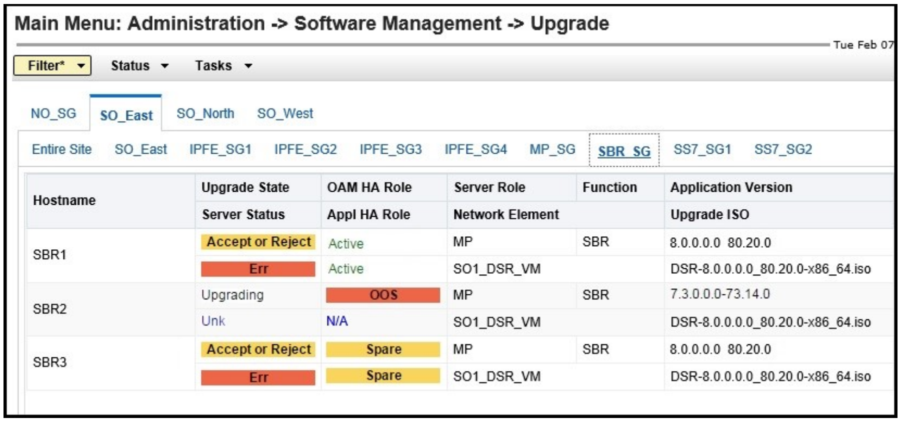
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 38	0:40-1:00		Upgrade Iteration 5	Standby SBR will become Active; previously Active SBR will be offline for upgrade

5.6.1 Upgrade Iteration 5

Procedure 38 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 17 for the hostnames of the servers upgraded in this iteration.

Procedure 38: Upgrade Iteration 5

<table>
<tr>
<td>1.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
<u>Iteration 5</u></td>
<td>At iteration 5, the Active SBR is upgraded, causing the Standby to become Active.



Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th>Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th></th><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td>SBR1</td><td>Accept or Reject</td><td>Active</td><td>MP</td><td>SBR</td><td>8.0.0.0.0 80.20.0</td></tr>
<tr><td></td><td>Err</td><td>Active</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
<tr><td>SBR2</td><td>Upgrading</td><td>OOS</td><td>MP</td><td>SBR</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td></td><td>Unk</td><td>N/A</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
<tr><td>SBR3</td><td>Accept or Reject</td><td>Spare</td><td>MP</td><td>SBR</td><td>8.0.0.0.0 80.20.0</td></tr>
<tr><td></td><td>Err</td><td>Spare</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.20.0-x86_64.iso</td></tr>
</table>
</td>
</tr>
<tr>
<td>2.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View In-Progress Status (monitor)</td>
<td>View the Upgrade Administration form to monitor upgrade progress.

See step 3 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 will be shown as “FAILED”.
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. Navigate to **Administration > Software Management > Upgrade.**
   The Upgrade Administration screen is displayed.
2. Select the SOAM tab of the site being upgraded.
3. Sequence through the server group tabs for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the
</td>
</tr>
</table>

		Status Message column. During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will 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 Auto Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers will not be updated until resolved. Refer to **APPENDIX R** to resolve this issue. 4. Wait for the SBR upgrades to complete. The “Status Message” column will show “Success”. This step will take approximately 20 to 50 minutes.

3.	**Server CLI:**
	If the upgrade of a server fails:
		If any upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O 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/upgrade.log`

THIS PROCEDURE HAS BEEN COMPLETED.

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

- **Procedure 39: Allow Site Provisioning**
- **Procedure 40: 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 53: Accepting Upgrade**

5.7 Site Post-Upgrade Procedures

The post-upgrade procedures consist of procedures that are performed after each site upgrades is complete. The final Health Check of the system collects alarm and status information to verify that 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 WILL BE LOST IF THE UPGRADE IS BACKED OUT**

Procedure 39: Allow Site Provisioning

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active SOAM VIP:** Enable Site Provisioning	Enable site provisioning. 1. Log into the SOAM GUI of the site just upgraded using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. 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. 1. Navigate to **Diameter > Maintenance > Signaling Firewall**. 2. Select the Signaling Node that was just upgraded. 3. Click the **Enable** button. 4. 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.)
	THIS PROCEDURE HAS BEEN COMPLETED.	

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-Upgrade Health Check

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

Procedure 40: Site Post-Upgrade Health Check

STEP #

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.

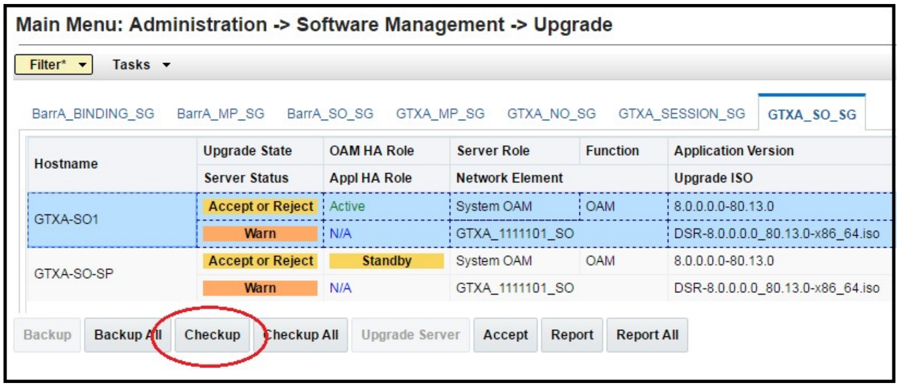
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**.

1 □

Active NOAM VIP:

This procedure will run the automated post-upgrade Health Checks.

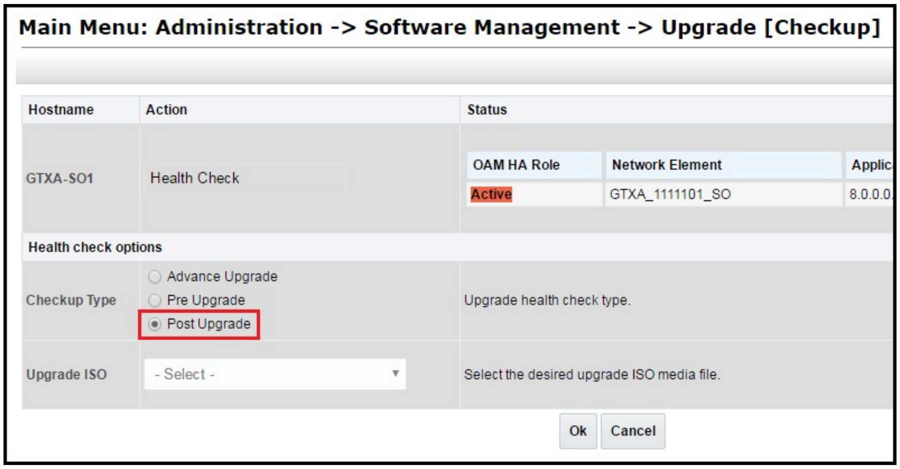
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the SOAM tab of the site being upgraded.
3. Select the SOAM server group link for the site being upgraded.
4. Select the Active SOAM.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
GTXA-SO1	Accept or Reject	Active	System OAM	OAM	8.0.0.0-80.13.0
	Warn	N/A	GTXA_1111101_SO		DSR-8.0.0.0.0_80.13.0-x86_64.iso
GTXA-SO-SP	Accept or Reject	Standby	System OAM	OAM	8.0.0.0-80.13.0
	Warn	N/A	GTXA_1111101_SO		DSR-8.0.0.0.0_80.13.0-x86_64.iso

5. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
6. Under Health check options, select the **Post Upgrade** option.
7. Click **Ok**. Control returns to the Upgrade screen.



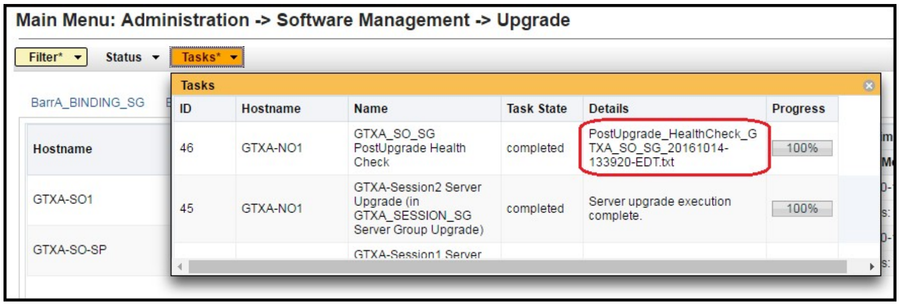
Main Menu: Administration -> Software Management -> Upgrade [Checkup]

Hostname	Action	Status		
		OAM HA Role	Network Element	Applic
GTXA-SO1	Health Check	Active	GTXA_1111101_SO	8.0.0.0

Health check options

Checkup Type	○ Advance Upgrade ○ Pre Upgrade ● Post Upgrade	Upgrade health check type.
Upgrade ISO	- Select -	Select the desired upgrade ISO media file.

Procedure 40: Site Post-Upgrade Health Check

2 □	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results.  Main Menu: Administration -> Software Management -> Upgrade Tasks ID Hostname Name Task State Details Progress 46 GTXA-NO1 GTXA_SO_SG PostUpgrade Health Check completed PostUpgrade_HealthCheck_GTXA_SO_SG_20161014-133920-EDT.txt 100% 45 GTXA-NO1 GTXA-Session2 Server Upgrade (in GTXA_SESSION_SG Server Group Upgrade) completed Server upgrade execution complete. 100% GTXA-Session1 Server Filter* Status Tasks* BarrA_BINDING_SG Hostname GTXA-SO1 GTXA-SO-SP
3 □	**Active NOAM VIP:** Analyze health check results	Analyze 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. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named "UpgradeHealthCheck.log" and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix S. If the health check log contains the message "Unable to execute Health Check on <Active NOAM hostname>", perform health checks in accordance with Procedure 41.
4 □	**Active SOAM VIP:** Export and archive the Diameter configuration data	Export Diameter configuration data 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry named "**ALL**". 3. Verify the requested data is exported using the tasks button at the top of the screen. 4. Browse 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 SOAM to the client machine. 5. Select **Diameter > Maintenance > Applications** 6. Verify Operational Status is '**Available**' for all applications
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.

Procedure 40: Site Post-Upgrade Health Check

6 □	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Verify that 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 3.4.2. If system operation is degraded, it is recommended to contact MOS.
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.7.2.2 Alternate Site 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 40.

Procedure 41: Alternate 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**

Procedure 41: Alternate Site Post-Upgrade Health Check

5.
□
	ACTIVE SOAM CLI:
	Verify SOAM post-Upgrade Status
		Run SOAM post-upgrade health check.
		1. Use an SSH client to connect to the Active SOAM:
		`ssh admusr@<SOAM XMI IP address>`
		`password:    <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter the command:
		`$ upgradeHealthCheck postUpgradeHealthCheckOnSoam`
		This command creates two 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:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears 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 to contact MOS for guidance.
		4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

6. □	**ACTIVE SOAM CLI:** Capture Diameter Maintenance Status	Capture Diameter Maintenance status. 1. Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command will output 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 message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

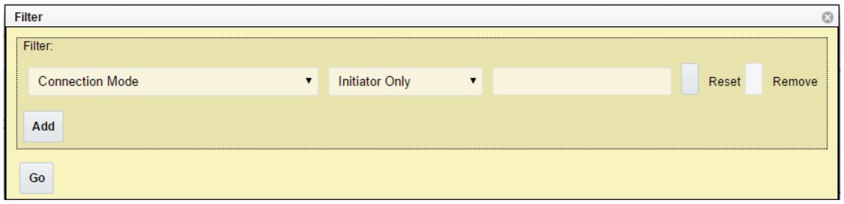
Procedure 41: Alternate Site Post-Upgrade Health Check

7. □	**ACTIVE SOAM CLI:** View DA-MP Status	Capture DA-MP status. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established ____________
8. □	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Verify that the health check status of the upgraded site as collected in this procedure is the same as the pre-upgrade health checks taken in Procedure 2. If system operation is degraded, it is recommended to report it to MOS.
		THIS PROCEDURE HAS BEEN COMPLETED.

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 42: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1 □	**<u>Active SOAM VIP:</u>** 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. 1. Navigate to **Diameter > Maintenance > Signaling Firewall**. 2. Select the Signaling Node that was just upgraded. 3. Click the **Enable** button. 4. 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.)
2 □	**<u>Active SOAM VIP:</u>** Toggle initiator connections **For Source Release 7.0 only**	**This step is required only if the source release is DSR 7.0.** 1. Navigate to **Diameter > Maintenance > Connections**. 2. Use the filter settings shown below to search for 'Initiator Only' connections.  Filter Filter: Connection Mode Initiator Only Reset Remove Add Go 3. If the resulting list is empty, this step is complete. 4. Otherwise, for the connections in the search results: a. Select one or more connections **Note: the following steps will momentarily disrupt traffic flow for the selected connections.** b. Click the **Disable** button c. Click the **Enable** button d. Verify the Admin State changes to **Enabled**.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 23. 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 24. 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 23 and Table 24 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 that all patches are on-hand prior to completing the backout procedures.

Table 23: Emergency Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 43	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 will vary.	None.
Procedure 44	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 45	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 will cause traffic loss.
Procedure 50	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 will cause traffic loss.
Procedure 46	See Note	See Note	Emergency NOAM Backout: NOTE: Execution time of downgrading a single server is approximately equivalent to	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
			execution time to upgrade the server.	traffic loss.
Procedure 52	See Note	See Note	Oracle Server Backout NOTE: Execution time of downgrading the Oracle server is approximately equivalent to execution time to upgrade the server.	None
Procedure 51	0:01-0:05	Varies	Post-Backout Health Check	None

Table 24. Normal Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 43	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 will vary.	None.
Procedure 44	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 47	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 will cause traffic loss.
Procedure 50	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 will cause traffic loss.
Procedure 48	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 will cause traffic loss.
Procedure 52	See Note	See Note	Oracle Server Backout NOTE: Execution time of downgrading the Oracle server is approximately equivalent to execution time to upgrade the server.	None
Procedure 51	0:01-0:05	Varies	Post-Backout Health Check	None

6.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to MOS by referring to Appendix S of this document. Before executing any of these procedures, it is recommended to contact MOS.
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 contact MOS as described in Appendix S.

Warning

Backout procedures WILL cause traffic loss.
NOTE: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 80.y.z release to the previously installed 6.0/7.0.x/7.1.x/7.2/7.3 release). Backout of an initial installation is not supported.

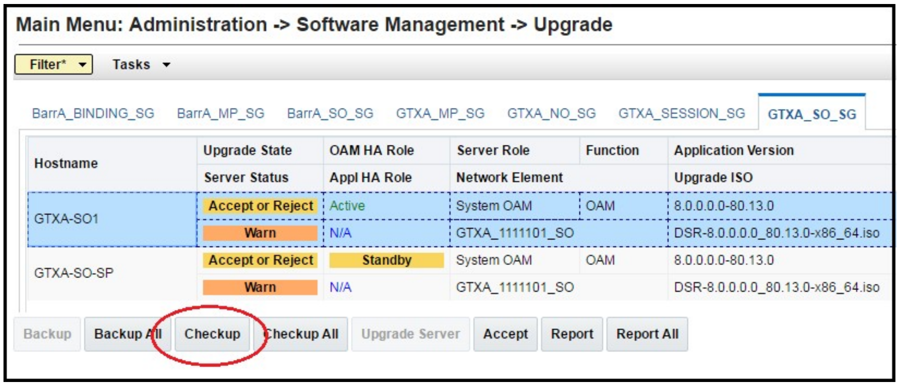
6.2 2Backout Health Check

This section provides the procedure to verify that the DSR is ready for backout. The site post-upgrade Health Check is used to perform the backout Health Check.

Procedure 43: Backout Health Check

<table>
<tr><td>S
T
E
P
#</td><td colspan="2">This procedure performs a Health Check on the site prior to backing out the upgrade.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u></b>.</td></tr>
<tr><td>1
□</td><td><b><u>Active NOAM VIP:</u></b></td><td>
This procedure will run the automated post-upgrade Health Checks for backout.

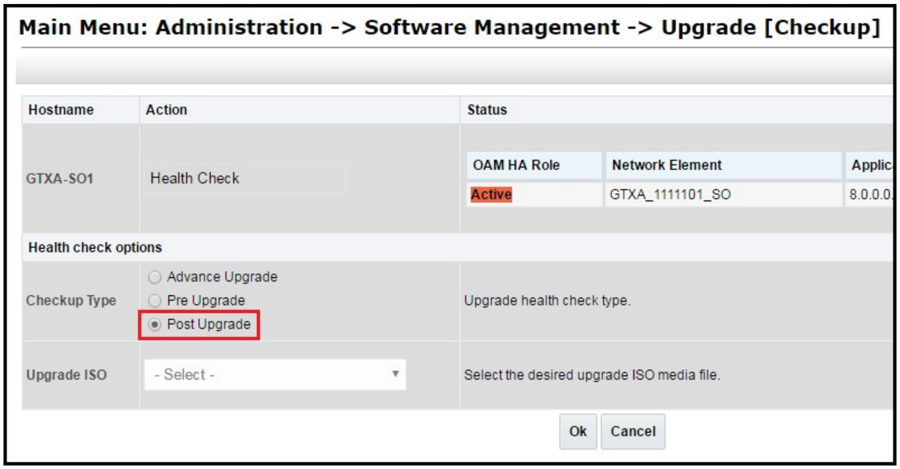
1. Select **Administration > Software Management > Upgrade**.
   The Upgrade screen is displayed.
2. Select the SOAM tab of the site being backed out.
3. Select the SOAM server group link for the site being backed out.
4. Select the Active SOAM.



Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">GTXA-SO1</td><td>Accept or Reject</td><td>Active</td><td>System OAM</td><td>OAM</td><td>8.0.0.0.0-80.13.0</td></tr>
<tr><td>Warn</td><td>N/A</td><td>GTXA_1111101_SO</td><td></td><td>DSR-8.0.0.0.0_80.13.0-x86_64.iso</td></tr>
<tr><td rowspan="2">GTXA-SO-SP</td><td>Accept or Reject</td><td>Standby</td><td>System OAM</td><td>OAM</td><td>8.0.0.0.0-80.13.0</td></tr>
<tr><td>Warn</td><td>N/A</td><td>GTXA_1111101_SO</td><td></td><td>DSR-8.0.0.0.0_80.13.0-x86_64.iso</td></tr>
</table>

5. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
6. Under Health check options, select the **Post Upgrade** option.
7. Click **Ok**. Control returns to the Upgrade screen.

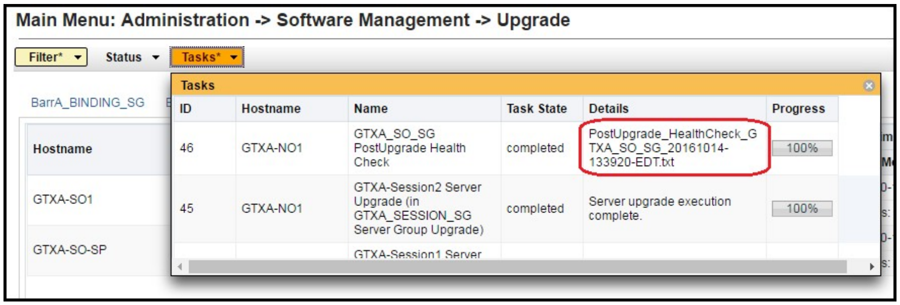


Main Menu: Administration -> Software Management -> Upgrade [Checkup]

<table>
<tr><th>Hostname</th><th>Action</th><th>Status</th></tr>
<tr><td>GTXA-SO1</td><td>Health Check</td><td>OAM HA Role: Active
Network Element: GTXA_1111101_SO
Applic: 8.0.0.0.</td></tr>
<tr><td colspan="3">Health check options</td></tr>
<tr><td>Checkup Type</td><td>○ Advance Upgrade
○ Pre Upgrade
● Post Upgrade</td><td>Upgrade health check type.</td></tr>
<tr><td>Upgrade ISO</td><td>- Select - ▾</td><td>Select the desired upgrade ISO media file.</td></tr>
</table>

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

Procedure 43: Backout Health Check

<table>
<tr>
<td>2
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Monitor health check progress</td>
<td>
Monitor for the completion of the Health Check.
<ol>
<li>Click the <b>Tasks</b> dropdown to display the currently executing tasks. The Health Check task name appears as <b>&lt;SOServerGroup> PostUpgrade Health Check</b>.</li>
<li>Monitor the Health Check task until the Task State is <b>completed</b>. The Details column will display a hyperlink to the Health Check report.</li>
<li>Click the hyperlink to download the Health Check report. Open the report and review the results.</li>
</ol>

Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th>ID</th><th>Hostname</th><th>Name</th><th>Task State</th><th>Details</th><th>Progress</th></tr>
<tr><td>46</td><td>GTXA-NO1</td><td>GTXA_SO_SG PostUpgrade Health Check</td><td>completed</td><td>PostUpgrade_HealthCheck_GTXA_SO_SG_20161014-133920-EDT.txt</td><td>100%</td></tr>
<tr><td>45</td><td>GTXA-NO1</td><td>GTXA-Session2 Server Upgrade (in GTXA_SESSION_SG Server Group Upgrade)</td><td>completed</td><td>Server upgrade execution complete.</td><td>100%</td></tr>
<tr><td></td><td></td><td>GTXA-Session1 Server</td><td></td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>3
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Analyze health check results</td>
<td>
Analyze Health Check results. If the Health Check report status is anything other than “Pass”, the Health Check logs can be analyzed to determine if the backout can proceed.
<ol>
<li>Select <b>Status & Manage &gt; Files</b>.
The Files screen is displayed.</li>
<li>Select the file named “UpgradeHealthCheck.log” and click <b>View</b>.</li>
<li>Locate the log entries for the most recent health check.</li>
<li>Review the log for failures. Analyze the failures and determine if it is safe to continue the backout. If necessary, it is recommended to contact MOS for guidance as described in Appendix S.</li>
</ol>
</td>
</tr>
<tr>
<td>4
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Identify IP addresses of servers to be backed out</td>
<td>
<ol>
<li>Select <b>Administration > Software Management > Upgrade.</b></li>
<li>Select the SOAM tab of the site being backed out.</li>
<li>Select each server group link, making note of the application version of each server.</li>
<li>Based on the “Application Version” column, identify all the hostnames that need to be backed out.</li>
<li>Select <b>Configuration > Servers.</b></li>
<li>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.</li>
</ol>
The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures <b>WILL</b> cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended to contact MOS as stated in the <b>Warning</b> box above.
</td>
</tr>
<tr>
<td>5
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Verify backup archive files</td>
<td>
<ol>
<li>Select <b>Status & Manage &gt; Files</b>.</li>
<li>For each server to be backed out, select the server tab on the Files screen. Verify that 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 will have the format:</li>
</ol>
Backup.<application>.<server>.<b>FullDBParts</b>.<role>.<date_time>.<b>UPG</b>.tar.bz2
Backup. <application>.<server>.<b>FullRunEnv</b>.<role>.<date_time>.<b>UPG</b>.tar.bz2
</td>
</tr>
</table>

Procedure 43: 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.

1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM.

   ```
   ssh admusr@<server IP>
   password: <enter password>
   ```

   (Answer 'yes' if you are prompted to confirm the identity of the server.)

2. 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
   ```

3. 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 23 (Emergency) or Table 24 (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.**

4. Repeat sub-steps 1 thru 3 for all servers to be backed out.

THIS PROCEDURE HAS BEEN COMPLETED.

6.3 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 and sites are backed out. Provisioning will be re-enabled once the NOAM upgrade is complete.

Procedure 44. Disable Global Provisioning

S T E P #	This procedure disables provisioning for the NOAM servers, prior to upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: 1. Log into the Active NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
	THIS PROCEDURE HAS BEEN COMPLETED.	

EMERGENCY SITE BACKOUT

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

6.4 Perform Emergency Backout

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 to contact MOS, as stated in the warning box in Section 6.1, to verify that 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 WILL RESULT IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR. TRAFFIC BEING PROCESSED BY THE MATE DSR IS NOT AFFECTED.**

Procedure 45: Emergency Site Backout

STEP #	This procedure is used to backout 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, SBRs, and even TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>**	
1. □	**<u>Active NOAM VIP:</u>** Identify all servers that require Backout	Identify all servers that require Backout (within a Site): 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. 3. Select the SOAM tab of the site being backed out. 4. Select each server group link, making note of the application version of the servers. 5. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 6. Make note of these servers. They have been identified for backout. 7. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.

Procedure 45: Emergency Site Backout

2. □	**Active SOAM VIP:** Disable Site Provisioning for the site to be backed out.	Disable Site Provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning.** A yellow information box will be displayed at the top of the view screen which 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 WILL RESULT 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.
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 NOAM VIP:** Prep for TVOE backout TVOE, if upgraded previously	**If the SOAM is a guest under the same host as a NOAM, do not backout the TVOE at this time. Proceed to step 10.** **Otherwise, if the SOAM is a guest of the TVOE software, determine if TVOE backout is required. Unless a TVOE issue is the cause of the backout, it is an option to leave the TVOE upgrade in place to save time. TVOE is backward compatible with all source releases and may remain upgraded. This is a customer decision.** **If backout is not required, proceed to step 10.** **Execute the following steps to backout the SOAM TVOE server upgraded previously.** Disable all applications running on the TVOE server. 1. Log into the NOAM GUI using VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Stop** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the ‘Appl State’ for all selected servers changes to ‘**Disabled**’.

Procedure 45: Emergency Site Backout

7.
□
	TVOE CLI:
	Backout TVOE
		Backout the TVOE upgrade.
		1. Login to the TVOE host
		`ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. List the guests running on the current TVOE host by using following command :
		`$ sudo virsh list`
		NOTE: the output of above command will list all guests running on the TVOE host.
		3. Execute the following command for each guest listed:
		`$ sudo virsh shutdown <guestname>`
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE servers on which SOAM(s) are hosted are successfully backed out.
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		`$ sudo virsh list`
		5. Backout TVOE on the blade according to reference [3].

8.
□
	TVOE CLI:
	Start TVOE guests
		Restart the TVOE guests.
		1. Login to the TVOE host:
		`ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. Execute the following command to start the TVOE guest shutdown in step 7 above (if not already started).
		`$ sudo virsh start <guestname>`
		3. Periodically execute the following command until the command displays all the VM guests running.
		`$ sudo virsh list`

9. □	**Active NOAM VIP:** Enable applications	Enable all applications running on the backed out TVOE server. 1. Log into the NOAM VIP GUI 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Restart** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the ‘Appl State’ for all selected servers is changed to ‘**Enabled**’. Repeat steps 6 thru 8 for another TVOE server hosting a SOAM (as applicable).

Procedure 45: Emergency Site Backout

10. □	<u>**Active SOAM VIP:**</u> Enable Site Provisioning	Enable Site provisioning. 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Site Provisioning.**
		THIS PROCEDURE HAS BEEN COMPLETED.

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

6.4.2 Emergency NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 46: Emergency NOAM Backout

STEP #	This procedure is used to perform an emergency backout of the DSR application software from the NOAM servers. This includes the DSR NOAMs, DR NOAMs, and TVOE hosts. 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE 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.
5. □	**Active NOAM VIP:** Disable applications	**If the NOAM is a guest of the TVOE software, determine if TVOE backout is required. Unless a TVOE issue is the cause of the backout, it is an option to leave the TVOE upgrade in place to save time. TVOE is backward compatible with all source releases and may remain upgraded. This is a customer decision.** **If a TVOE backout is not required, proceed to step 9.** Execute the following steps for each TVOE server upgraded previously. Disable all applications running on the TVOE server. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Stop** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all selected servers changes to '**Disabled**'.

Procedure 46: Emergency NOAM Backout

6.
□
	TVOE CLI:
	Backout TVOE if upgraded previously
		Backout TVOE. This step is executed only if TVOE was upgraded as part of the DSR upgrade.
		1. Login to the TVOE host:
		`$ ssh admusr@<TVOE IP>`
		`password: <enter password>`
		2. List the guests running on the current TVOE host:
		`$ sudo virsh list`
		The output of this command will list all guests running on the TVOE host.
		3. Execute the following command for each guest listed :
		`$ sudo virsh shutdown <guestname>`
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE servers on which NOAM(s) are hosted are successfully backed out.
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		`$ sudo virsh list`
		5. Backout TVOE on the blade according to reference [3].

7.
□
	TVOE CLI:
	Start TVOE guests
		Restart the TVOE guests.
		1. Login to the TVOE host:
		`$ ssh admusr@<TVOE IP>`
		`password: <enter password>`
		2. Execute the following command to start the TVOE guests shutdown in step 6 (if not already started).
		`$ sudo virsh start <guestname>`
		3. Periodically execute the following command until the command displays all the VM guests running.
		`$ sudo virsh list`

8. □	**Active NOAM VIP:** Enable applications	Enable all applications running on the backed out TVOE server. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Restart** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all selected servers is changed to '**Enabled**'. Repeat steps 5 thru 7 for another TVOE server hosting a NOAM (as applicable).

Procedure 46: Emergency NOAM Backout

9. □	**Active NOAM VIP:** Enable Global Provisioning	Enable global provisioning and configuration updates on the entire network 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.

10.
□
	Active NOAM VIP:
	Remove 'Ready' state for any backed out server
		Remove 'Ready' state
		1. Select **Status & Manage > Servers**.
		The Server Status screen is displayed.
		2. If any backed-out server Application Status is '**Disabled**', then select the server row and press the **Restart** button.
		3. Select **Administration >Software Management >Upgrade**
		The Upgrade Administration screen is displayed.
		4. If any backed-out server shows an Upgrade State of "**Ready**" or "**Success**", then select that server and press the **Complete Upgrade** button. Otherwise, skip this step.
		The Upgrade [Make Ready] screen will appear.
		5. Click **OK**. This will now remove 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 appear 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.
		6. Verify the Application Version value for servers has been downgraded to the original release version.

		THIS PROCEDURE HAS BEEN COMPLETED.

NORMAL SITE BACKOUT

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

6.5 Perform Normal Backout

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 to contact MOS, as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

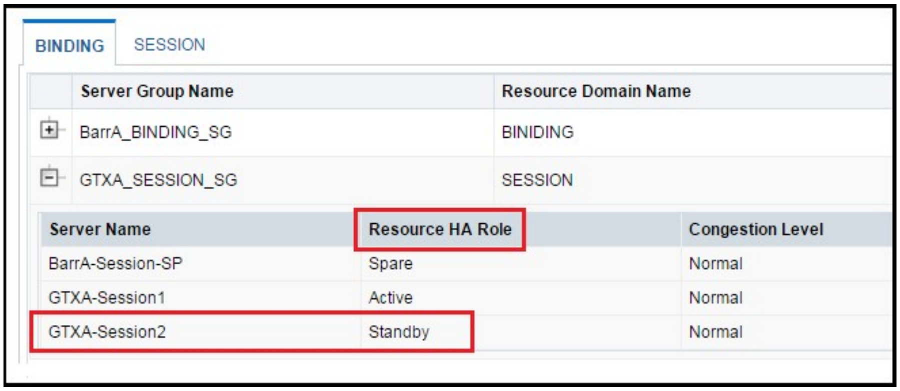
6.5.1 Normal Site Backout

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

Procedure 47: Normal Site Backout

S T E P #	This procedure is used to backout 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, SBRs, and even TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>**	
1. □	**<u>Active NOAM VIP:</u>** Identify all servers that require Backout	Identify all servers that require Backout (within a Site): 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management > Upgrade.** The Upgrade Administration screen is displayed. 3. Select the SOAM tab of the site being backed out. 4. Select each server group link, making note of the application version of each server. 5. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 6. Make note of these servers. They have been identified for Backout. 7. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. □	**<u>Active SOAM VIP:</u>** Disable Site Provisioning for the site to be backed out	Disable Site Provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning.** A yellow information box should also be displayed at the top of the view screen which 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)**

Procedure 47: 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 5 and step 6 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 6. 1. Navigate to **Main Menu > SBR > Maintenance > SBR Status.** Open the tab of the server group being upgraded. 2. Do not proceed to step 6 until the **Resource HA Role** for the Standby server has a status of **Standby**. 

	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

Procedure 47: Normal Site Backout

5. □	**Active NOAM VIP:** Verify bulk download is complete	Verify that bulk download is complete between the Active SBR in the server group to the Standby and Spare SBRs. 1. Navigate to **Main Menu > Alarm & Event > View History** 2. 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. 3. 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	Backout 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 47: Normal Site Backout

10. □	**Active NOAM VIP:** Disable applications	**If the SOAM is a guest under the same host as a NOAM, do not backout the TVOE at this time. Proceed to step 14.** **Otherwise, if the SOAM is a guest of the TVOE software, determine if TVOE backout is required. Unless a TVOE issue is the cause of the backout, it is an option to leave the TVOE upgrade in place to save time. TVOE is backward compatible with all source releases and may remain upgraded. This is a customer decision.** **If a TVOE backout is not required, proceed to step 14.** **Execute the following steps for a TVOE server previously upgraded.** Disable all applications running on the TVOE server. 1. Login to the NOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Stop** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all selected servers changes to **'Disabled'**.

11.
□
	TVOE CLI:
	Backout TVOE if upgraded previously
		Backout TVOE. This step is executed only if TVOE was upgraded as part of the DSR upgrade.
		1. Login to the TVOE host:
		`$ ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. List the guests running on the TVOE host:
		`$ sudo virsh list`
		The output of the command will list all guests running on the TVOE host.
		3. Execute the following command for each guest listed :
		`$ sudo virsh shutdown <guestname>`
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE servers on which SOAM(s) are hosted are successfully backed out.
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		`$ sudo virsh list`
		5. Backout TVOE on the blade according to reference [3].

Procedure 47: Normal Site Backout

12.
□
	TVOE CLI:
	Start TVOE guests
		Restart the TVOE guests.
		1. Login to the TVOE host:
		`ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. Execute the following command to start the TVOE guest shutdown in step 11 (if not already started).
		`$ sudo virsh start <guestname>`
		3. Periodically execute the following command until the command displays all the VM guests running.
		`$ sudo virsh list`

13. □	**Active NOAM VIP:** Enable applications	Enable all applications running on the backed out TVOE server. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Restart** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all selected servers is changed to **'Enabled'**. Repeat steps 10 thru 13 for another TVOE server hosting a SOAM (as applicable).
14. □	**Active SOAM VIP:** Enable Site Provisioning	Enable Site provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Site Provisioning**
		THIS PROCEDURE HAS BEEN COMPLETED.

NOTE: If another site is to be backed out, follow all procedures in Table 24 in another maintenance window.

6.5.2 Normal NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 48: Normal NOAM Backout

S T E P #	This procedure is used to perform a normal backout of the DSR application software from the NOAM servers. This includes the DSR NOAMs, DR NOAMs, and TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>**	
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 Active NOAM server: Execute Section 6.6 Backout Single Server.
5. □	**<u>Active NOAM VIP:</u>** Disable applications	**If the NOAM is a guest of the TVOE software, determine if TVOE backout is required. Unless a TVOE issue is the cause of the backout, it is an option to leave the TVOE upgrade in place to save time. TVOE is backward compatible with all source releases and may remain upgraded. This is a customer decision.** **If a TVOE backout is not required, proceed to step 9.** Execute the following steps for a TVOE server upgraded previously. Disable all applications running on the TVOE server. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Stop** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all selected servers changes to **'Disabled'**.

Procedure 48: Normal NOAM Backout

6.
□
	TVOE CLI:
	Backout TVOE if upgraded previously
		Backout TVOE. This step is executed only if the TVOE was upgraded as part of the DSR upgrade.
		1. Login to the TVOE host:
		`ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. List the guests running on the TVOE:
		`$ sudo virsh list`
		The output of the command will list all guests running on the TVOE host.
		3. Execute the following command for each guest listed :
		`$ sudo virsh shutdown <guestname>`
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE servers on which NOAM(s) are hosted are successfully backed out.
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		`$ sudo virsh list`
		5. Backout TVOE on the blade according to reference [3].

7.
□
	TVOE CLI:
	Start TVOE guests
		Restart the TVOE guests.
		1. Log into the TVOE host:
		`ssh admusr@<TVOE IP>`
		`password:  <enter password>`
		2. Execute the following command to start the TVOE guests shutdown in step 6 (if not already started).
		`$ sudo virsh start <guestname>`
		3. Periodically execute the following command until the command displays all the VM guests running.
		`$ sudo virsh list`

8. □	**Active NOAM VIP:** Enable applications	Enable all applications running on the backed out TVOE server: 1. Log into the NOAM VIP GUI 2. Select **Status & Manage > Server**. The Server Status screen is displayed 3. Select all applications running on the current TVOE server. 4. Click the **Restart** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the ‘Appl State’ for all selected servers is changed to **‘Enabled’**. Repeat steps 5 thru 8 for another TVOE server hosting an NOAM (as applicable).

Procedure 48: Normal NOAM Backout

9. □	**Active NOAM VIP:** Enable Global Provisioning	Enable global provisioning and configuration updates on the entire network 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.

THIS PROCEDURE HAS BEEN COMPLETED.

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 49: Backout Single Server

S T E P #	This procedure will backout the upgrade of DSR 8.0 application software. Any server requiring backout can be included: NOAMs, SOAMs, DA-MPs, SS7-MPs, IPFEs, SBRs, and even TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE 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. 1. Select **Administration > Software Management > Upgrade**. The Upgrade Administration screen is displayed. 2. Select the SOAM tab of the site being backed out. 3. 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: 4. Select **Status & Manage > HA.** The HA status screen displays. 5. Click the **Edit** button. 6. 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, selecting OK will initiate an HA switchover, causing the GUI session to log out.** 7. Click the **Ok** button. *** Critical *** Do NOT omit this step 8. **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 9. The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. 10. Select **Status & Manage > Server.** The server status screen is displayed. 11. Select the server to be backed out and click **Stop**. Click **Ok** to confirm the operation, then verify the Appl State changes to **Disabled**. 12. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 13. Select the SOAM tab of the site being backed out. 14. Select the link 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 49: Backout Single Server

2 □ **Server CLI:** SSH to server

Use an SSH client to connect to the server (e.g. ssh, putty):

```
ssh admusr@<server address>
password:  <enter password>
```

NOTE: If direct access to the IMI is not available, or if TVOE is installed on a blade, 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.

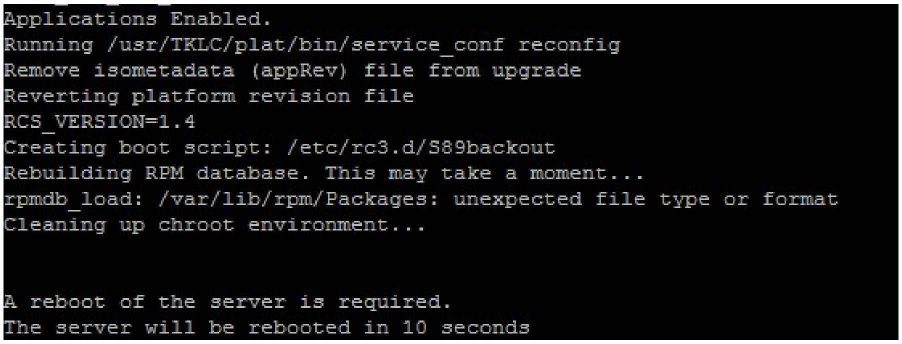
```
[admusr@SO2 ~]# ha.mystate
           resourceId  role       node        subResources      lastUpdate
        DbReplication  Stby   B2435.024                  0 0127:113603.435
                  VIP  Stby   B2435.024                  0 0127:113603.438
         SbrBBaseRepl   OOS   B2435.024                  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
```

```
$ sudo /var/TKLC/backout/reject
```

NOTE: If backout prompts to continue, answer "**y**".

(The reject command will create a no-hang-up shell session, so that the command will continue 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
```

4 □ Backout proceeds

Many informational messages are output to the terminal screen as the backout proceeds.

Finally, after backout is complete, the server will automatically reboot.

5 □ **Server CLI:** SSH to server

Use an SSH client to connect to the server (e.g. ssh, putty):

```
ssh admusr@<server address>
password:  <enter password>
```

Procedure 49: Backout Single Server

6
□
	<u>**Server CLI:**</u>
	Restore the full DB run environment
		1. 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 will not be 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 will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		If the restore was successful, the following will be displayed:
		`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 to consult with MOS by referring to Appendix S of this document for further instructions.

Procedure 49: Backout Single Server

7 □

Server CLI:

Verify the backout

1. Examine the output of the following commands to determine if any errors were reported:

```
$ sudo verifyUpgrade
```

Note: The verifyUpgrade command will detected 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 will show 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 will search the upgrade log and report all errors found.

2. If the backout was successful (no errors or failures reported), then proceed to step 8.

3. 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'
```

4. 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.

5. If the backout failed due to errors found in the upgrade log, it is recommended to contact MOS by referring to Appendix S of this document for further instructions.

Procedure 49: Backout Single Server

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

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 10.
		Verify OAM services have restarted.
		1. Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		`login as:  admusr`
		`password:  <enter password>`
		3. Execute the following command to verify the httpd service is running.
		`$ sudo service httpd status`
		4. 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 to contact MOS by referring to Appendix S of this document for further instructions.

10 □	**Active NOAM VIP:** Verify server states	Verify server state. 1. Select **Administration > Software Management > Upgrade** to observe the server upgrade status. 2. Select the SOAM tab of the site being backed out. 3. 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:** 4. 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:** 5. If the server status is **Ready**, proceed to step 12; otherwise proceed to step 14.

Procedure 49: Backout Single Server

<table>
<tr>
<td>11
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Correct Upgrade State on backed out server

<b>For Active NOAM on release 7.1.x and later</b></td>
<td>Modify the backed out server to transition the Upgrade State to <b>Ready</b>.

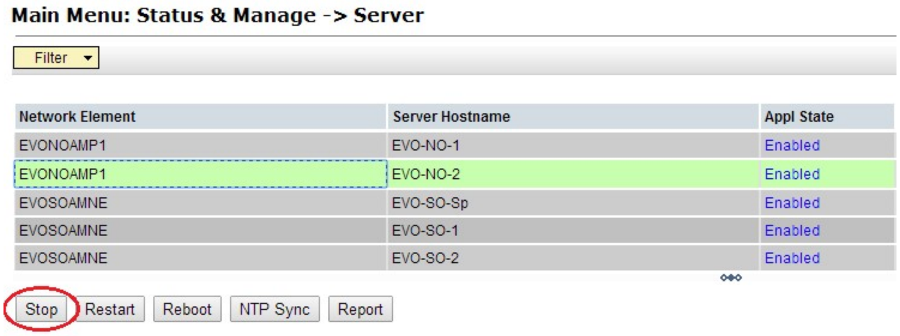
1. Select <b>Status & Manage &gt; HA</b>
The HA status screen is displayed.
2. Click the <b>Edit</b> button.
3. Select the backed out server and choose a Max Allowed HA Role value of <b>Active</b> (unless it is a Query server, in which case the value should remain set to <b>Observer</b>).
4. Click the <b>Ok</b> button.
5. The HA status screen is displayed. Verify the Max Allowed HA Role is set to the desired value for the server.
6. Select <b>Status & Manage > Server.</b>
The Server status screen is displayed.
7. Select the server being backed out and click <b>Restart</b>. Click <b>Ok</b> to confirm the operation. Verify the Appl State updates to <b>Enabled</b>.
8. Select <b>Administration > Software Management > Upgrade</b>;
The Upgrade Status screen is displayed.
9. Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now <b>Ready</b>. (It might take a couple minutes for the grid to update.)

<b>Proceed to step 14 to complete this procedure.</b></td>
</tr>
<tr>
<td>12
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Stop the Application

<b>For Active NOAM on release 6.0 or 7.0.x only</b></td>
<td>To transition to the Not Ready state, stop the Application.

1. Log into the NOAM GUI using the VIP.
2. Select <b>Status & Manage > Server.</b>
The Server Status screen is displayed.
3. If the server just backed-out shows an “<b>Appl State”</b> of <b>“Enabled”</b>, then select the server row and press the <b>Stop</b> button.


Main Menu: Status & Manage -&gt; Server

<table>
<tr><th>Network Element</th><th>Server Hostname</th><th>Appl State</th></tr>
<tr><td>EVONOAMP1</td><td>EVO-NO-1</td><td>Enabled</td></tr>
<tr><td>EVONOAMP1</td><td>EVO-NO-2</td><td>Enabled</td></tr>
<tr><td>EVOSOAMNE</td><td>EVO-SO-Sp</td><td>Enabled</td></tr>
<tr><td>EVOSOAMNE</td><td>EVO-SO-1</td><td>Enabled</td></tr>
<tr><td>EVOSOAMNE</td><td>EVO-SO-2</td><td>Enabled</td></tr>
</table>
</td>
</tr>
</table>

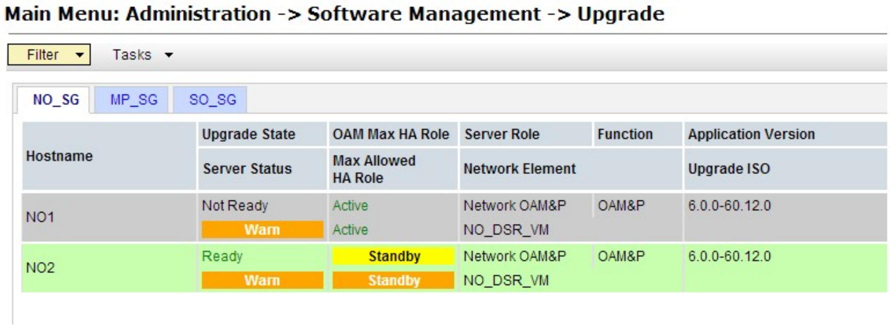
Procedure 49: Backout Single Server

<table>
<tr>
<td>13
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Correct Upgrade State on backed out server

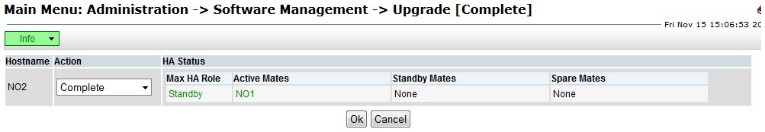
<b>For Active NOAM on release 6.0 or 7.0.x only</b></td>
<td>
Change the upgrade state for the backed out server.

1. Select <b>Administration > Software Management > Upgrade.</b>
The Upgrade Administration screen is displayed.
2. Select the SOAM tab of the site being backed out.
3. Select the link of the server group containing the server being backed out.
4. If the server just backed-out shows an Upgrade State of “<b>Ready</b>” or “<b>Success</b>”, then select the backed-out server and press <b>Complete.</b>
<b>Otherwise, skip to step 14.</b>


<b>Main Menu: Administration -> Software Management -> Upgrade</b>

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM Max HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Max Allowed HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">NO1</td><td>Not Ready</td><td>Active</td><td>Network OAM&amp;P</td><td>OAM&amp;P</td><td>6.0.0-60.12.0</td></tr>
<tr><td>Warn</td><td>Active</td><td>NO_DSR_VM</td><td></td><td></td></tr>
<tr><td rowspan="2">NO2</td><td>Ready</td><td>Standby</td><td>Network OAM&amp;P</td><td>OAM&amp;P</td><td>6.0.0-60.12.0</td></tr>
<tr><td>Warn</td><td>Standby</td><td>NO_DSR_VM</td><td></td><td></td></tr>
</table>

5. The <b>Upgrade</b> [<b>Complete]</b> screen will appear. Leave the Action set to the default value of <b>Complete</b>.
6. Click <b>OK.</b> This will update the Max Allowed HA Role of the backed-out server to Active, which will cause the server’s Upgrade State to move to <b>Not Ready</b>.


<b>Main Menu: Administration -> Software Management -> Upgrade [Complete]</b>
Fri Nov 15 15:06:53 20

<table>
<tr><th>Hostname</th><th>Action</th><th colspan="4">HA Status</th></tr>
<tr><td></td><td></td><th>Max HA Role</th><th>Active Mates</th><th>Standby Mates</th><th>Spare Mates</th></tr>
<tr><td>NO2</td><td>Complete</td><td>Standby</td><td>NO1</td><td>None</td><td>None</td></tr>
</table>

The following SOAP error may appear in the GUI banner:
<code><b>SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]</b></code>
It is safe to ignore this error message.
</td>
</tr>
<tr>
<td>14
□</td>
<td><b><u>Active NOAM VIP:</u></b>

Verify application version</td>
<td>
Verify the application version is correct for the backed out server.

1. Select <b>Administration > Software Management > Upgrade</b>
The Upgrade screen is displayed
2. Select the SOAM tab of the site being backed out.
3. Select the link of the server group containing the server that was backed out.
<b>4.</b> Verify the <b>Application Version</b> value for this server has been downgraded to the original release version.
</td>
</tr>
<tr>
<td>15
□</td>
<td>Procedure Complete</td>
<td>The single server backout is now complete.

Return to the overall DSR backout procedure step that directed the execution of this procedure.</td>
</tr>
<tr>
<td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td>
</tr>
</table>

6.7 Backout Multiple Servers

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

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 50: Backout Multiple Servers

STEP #	This procedure will backout the upgrade of DSR 8.0 application software for multiple servers. Any server requiring backout can be included. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>**	
1 □	**<u>Active NOAM VIP:</u>** Prepare the server for backout.	Perform the following steps to prepare the server for backout. 1. Select **Administration > Software Management > Upgrade**. The Upgrade Administration screen is displayed. 2. Select the SOAM tab of the site being backed out. 3. Select the link of the server group containing the server to be backed out. Verify the Upgrade State is '**Accept or Reject**'. Make the server '**Backout Ready'** as follows: 4. Select **Status & Manage > HA.** The HA status screen displays. 5. Click the **Edit** button. 6. 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, selecting OK will initiate an HA switchover, causing the GUI session to log out.** 7. Click the **Ok** button. *** Critical *** Do NOT omit this step 8. **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 9. The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. 10. Select **Status & Manage > Server.** The server status screen is displayed. 11. Select the server to be backed out and click **Stop**. Click **Ok** to confirm the operation, then verify the Appl State updates to **Disabled**. 12. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 13. Select the SOAM tab of the site being backed out. 14. Select the link 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 50: Backout Multiple Servers

2 □ **Server CLI:**

Login to the server(s)

Use an SSH client to connect to the server (e.g. ssh, putty):

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

1. Execute following command to find the server role :

```
$ ha.mystate
```

In the example output below, the HA state is Standby.

```
[admusr@SO2 ~]$ ha.mystate
      resourceId       role       node  DC   subResources          lastUpdate
-----------------------------------------------------------------------------
   DbReplication    Act/Stb  B1102.216                0     1121:162812.328
             VIP    Act/Stb  B1102.216                0     1121:162812.569
  CacdProcessRes    Act/OOS  B1102.216                0     1121:162810.062
   CAPM_HELP_Proc   Act/Stb  B1102.216                0     1121:162823.833
     DSROAM_Proc    Act/Stb  B1102.216                0     1121:162823.873
  CAPM_PSFS_Proc    Act/Stb  B1102.216                0     1121:162823.788
```

If the state of the server is Active, then return to step 1 above.

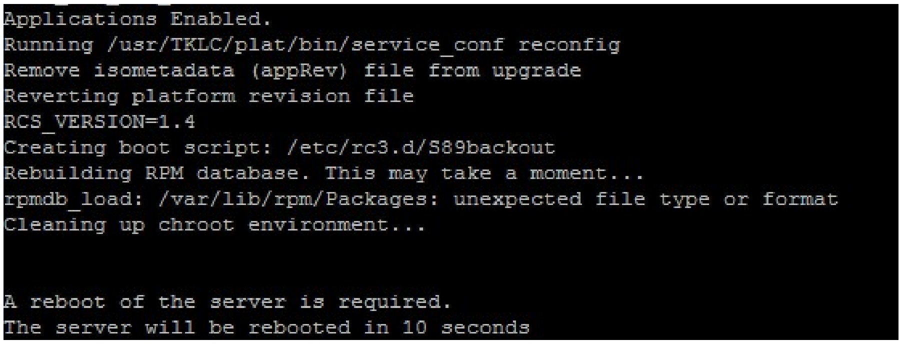
2. Execute the **reject** command to initate the backout:

```
$ sudo /var/TKLC/backout/reject
```

NOTE: If backout prompts to continue, answer "**y**".

(The reject command will create a no-hang-up shell session, so that the command will continue 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
```

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 will automatically reboot.

5 □ Repeat for each server to be backed out.

Repeat steps 1 through 4 for each server to be backed out.

Procedure 50: Backout Multiple Servers

6
□
	Server CLI:
	Login to the server
		Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh admusr@<server address>`
		`password:  <enter password>`

7
□
	Server CLI:
	Restore the full DB run environment
		1. Execute the backout_restore utility to restore the full database run environment:
		`$ sudo /var/tmp/backout_restore`
		If prompted to proceed, answer "**y**".
		NOTE: In some incremental upgrade scenarios, the backout_restore file will not be 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 will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		If the restore was successful, the following will be displayed:
		`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 to consult with MOS by referring to Appendix S of this document for further instructions.

Procedure 50: Backout Multiple Servers

8 □

Server CLI:

Verify the backout

1. Examine the output of the following commands to determine if any errors were reported:

   ```
   $ sudo verifyUpgrade
   ```

   Note: The verifyUpgrade command will detected 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 will show 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 will search the upgrade log and report all errors found.

2. If the backout was successful (no errors or failures reported), then proceed to step 9.

3. 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'
   ```

4. 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.

5. If the backout failed due to errors found in the upgrade log, it is recommended to contact MOS by referring to Appendix S of this document for further instructions.

Procedure 50: Backout Multiple Servers

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

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:
		1. Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		`login as:  admusr`
		`password:  <enter password>`
		3. Verify the httpd service is running.
		`$ sudo service httpd status`
		4. 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 to contact MOS by referring to Appendix S 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. 1. Select **Administration > Software Management > Upgrade** to observe the server upgrade status. 2. If the server status is **Not Ready**, continue to step 13; otherwise proceed to step 14.

Procedure 50: 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**. 1. Select **Status & Manage > HA** The HA status screen is displayed. 2. Click the **Edit** button. 3. 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**). 4. Click the **Ok** button. 5. The HA status screen is displayed. Verify the Max Allowed HA Role is set to the desired value for the server. 6. Select **Status & Manage > Server.** The Server status screen is displayed. 7. Select the server being backed out and click **Restart**. Click **Ok** to confirm the operation. Verify the Appl State updates to **Enabled**. 8. Select **Administration > Software Management > Upgrade**; The Upgrade Status screen is displayed. 9. 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.)
14 □	**Active NOAM VIP:** Verify application version	Verify the application version of the backed out server. 1. Select **Administration > Software Management > Upgrade** The Upgrade screen is displayed 2. Select the SOAM tab of the site being backed out. 3. Select the link of the Server Group containing the server that was backed out. **4.** Verify the **Application Version** value for this server has been downgraded to the original release version.
15 □	Procedure Complete	**The multiple server backout is now complete.** **Return to the overall DSR backout procedure step that directed the execution of this procedure.**
		THIS PROCEDURE HAS BEEN COMPLETED.

6.8 Post-Backout Health Check

This procedure is used to determine the health and status of the DSR network and servers following the backout of the entire system.

Procedure 51: Post-Backout Health Check

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active NOAM VIP:** Verify Server Status is Normal	Verify Server Status is Normal 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 4. Do not proceed with the upgrade if any server status is not **Norm**. 5. 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: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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 backout the Oracle Server if backing out to release 7.1 or later.

Procedure 52: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	

1
□
	Oracle Server CLI
	Login to the server
		Use an SSH client to connect to the Oracle server (e.g. ssh, putty):
		`ssh admusr@<server address>`
		`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`

THIS PROCEDURE HAS BEEN COMPLETED.		

6.9.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [12].

7 APPENDIXES

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 provided 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) will be displayed 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 will not be allowed to backout 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 CUSTOMER SHOULD BE ADVISED THAT ONCE UPGRADE HAS BEEN ACCEPTED, IT WILL NOT BE POSSIBLE TO BACKOUT TO THE PREVIOUS RELEASE**

Procedure 53: Accepting 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>**.	
1. □	It is recommended that this procedure be performed two weeks after the upgrade.	Verify that the upgraded system has been stable for two weeks or more. **NOTE: It will not be possible to backout after this is procedure is executed.**
2. □	**<u>Active NOAM VIP:</u>** Execute this step if accepting a NOAM server. Log all current alarms present at the NOAM.	Log all alarms before accepting the NOAM upgrade. 1. Log into the NOAM GUI. 2. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 3. Click the **Report** button to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers will 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.

1. Log into the SOAM GUI.
2. Select **Alarms & Events > View Active.**
   The Alarms & Events > View Active screen is displayed.
3. Click the **Report** button to generate an Alarms report.
4. Save the report and/or print the report. Keep these copies for future reference.

All other upgraded servers will have the following expected alarm:
Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

4. □

Active NOAM VIP:

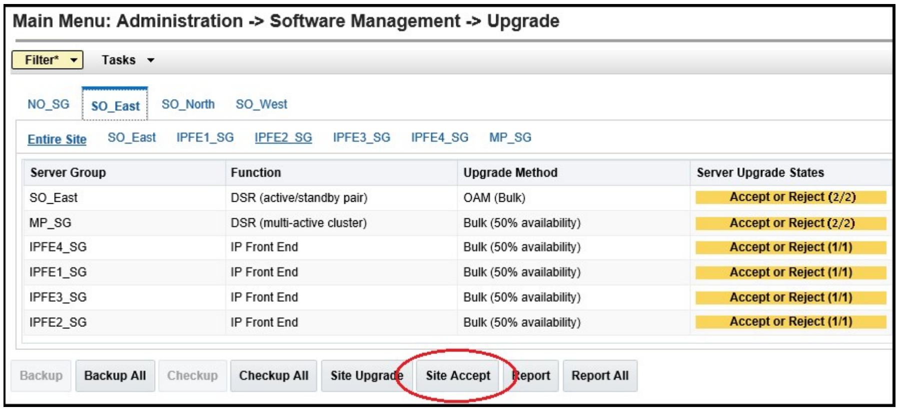
Accept upgrade for multiple servers

Accept the upgrade of multiple servers.

1. Log into the NOAM GUI using the VIP.
2. Select **Administration >Software Management >Upgrade.**
   The Upgrade Administration screen is displayed.
3. Select the SOAM tab of the site being upgraded.

   Note: The **Site Accept** button 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 use the **Accept** button to accept the upgrade of only the servers in the selected server group.

4. Click the **Site Accept** button



Main Menu: Administration -> Software Management -> Upgrade

Server Group	Function	Upgrade Method	Server Upgrade States
SO_East	DSR (active/standby pair)	OAM (Bulk)	Accept or Reject (2/2)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Accept or Reject (2/2)
IPFE4_SG	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)
IPFE1_SG	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)
IPFE3_SG	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)
IPFE2_SG	IP Front End	Bulk (50% availability)	Accept or Reject (1/1)

5. A confirmation dialog will warn that once accepted, the server will not be able to revert back to the previous image state.
6. Click **Ok.**
   The Upgrade Administration screen re-displays.
7. Select **Alarms & Events > View Active**.
   The Alarms & Events > View Active screen displays.

   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**".

THIS PROCEDURE HAS BEEN COMPLETED.

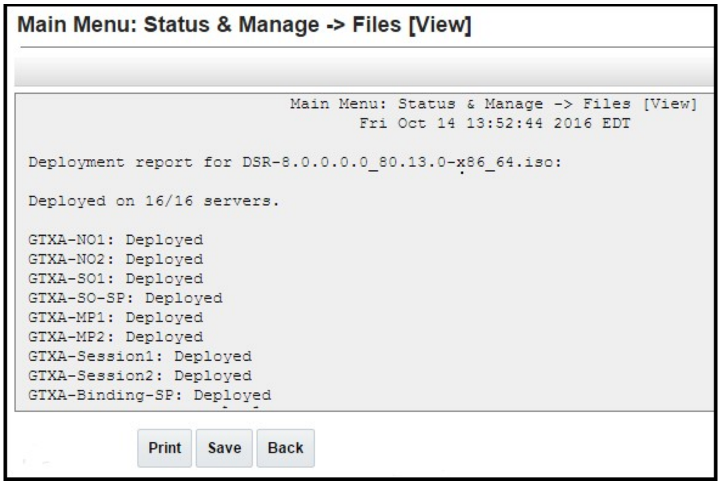
Appendix A.2 Undeploy ISO

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 54: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1. □	**<u>Active NOAM VIP:</u>** View files	View the files in the File Management Area on the Active NOAM. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Files.** The Files screen is displayed.
2. □	**<u>Active NOAM VIP:</u>** Start ISO undeploy	Start the ISO undeploy sequence. 1. Select an ISO that is stored in the isos directory of the File Management Area. The ISO filename will have the format: `isos/DSR-8.0.0.0.0_80.12.0-x86_64.iso` 2. Click the **Undeploy ISO** button. 3. Click **OK** in the confirmation dialog box to start the undeploy sequence. After clicking Ok the **Status & Manage > Files** screen will refresh.

3.
□
	<u>Active NOAM VIP:</u>
	Monitor progress
		Monitor the ISO undeploy progress.
		1. Select the ISO being deployed in step 2.
		2. Click the **View ISO Deployment Report** button.
		3. If some servers show the ISO as "Deployed", click the **Back** button on the **Files [View]** page
		4. Periodically repeat sub-steps 1 thru 3 until all servers indicate "Not Deployed".
		
		Main Menu: Status & Manage -> Files [View]
		`Main Menu: Status & Manage -> Files [View]`
		`Fri Oct 14 13:52:44 2016 EDT`
		`Deployment report for DSR-8.0.0.0.0_80.13.0-x86_64.iso:`
		`Deployed on 16/16 servers.`
		`GTXA-NO1: Deployed`
		`GTXA-NO2: Deployed`
		`GTXA-SO1: Deployed`
		`GTXA-SO-SP: Deployed`
		`GTXA-MP1: Deployed`
		`GTXA-MP2: Deployed`
		`GTXA-Session1: Deployed`
		`GTXA-Session2: Deployed`
		`GTXA-Binding-SP: Deployed`

4. □	**<u>Active NOAM VIP:</u>** Repeat as necessary	1. 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 Post Upgrade Procedures

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

Procedure 55: PCA Post Upgrade Procedure

STEP #

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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**

1. □

Active NOAM CLI:

Reset COMCOL compatibility flag

This step is required only if the source release is pre-8.0.

1. 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.

2. 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 ===
```

3. 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 56 must be executed on PCA systems after the upgrade to DSR 8.0 is accepted. Do not run this procedure until *after* Procedure 53 has been completed. This procedure executes the PCA top level activation script to remedy a potential PCA activation issue from earlier releases.

Procedure 56: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	

1.
□
	<u>Active NOAM CLI:</u>
	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@<server address>`
		`password:  <enter password>`

2.
□
	<u>Active NOAM CLI</u>
	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. □	**<u>Active NOAM CLI</u>** Clear cache	Execute the following command to reset the initialization caches: `clearCache`
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix B INCREASE MAX 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 57: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**

1 □

Active NOAM CLI:

Currently open file count

Determine the number of files currently open.

1. 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.

2. 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
```

3. 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):

____

4. 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
```

5. 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 57: Increase Max Number of Open Files

<table>
<tr><td>2
□</td><td><b><u>Active NOAM CLI:</u></b>

Max number of open files</td><td>Display the maximum number of open files for idbsvc.

1. Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command below.<pre>$ sudo cat /proc/XXXX/limits | grep -i open
Max open files   32768   32768   files</pre>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): _________________

Display the maximum number of open files for tpdProvd.

2. Use the highlighted value from step 1, sub-step 4 for tpdProvd in place of XXXX in the cat command below.<pre>$ sudo cat /proc/XXXX/limits | grep -i open
Max open files   1024   4096   files</pre>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): _________________</td></tr>
<tr><td>3
□</td><td><b>Check if current number of open files (used by idbsvc) is in safe limit</b>

🛑</td><td><b>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.</b>

<b>Then further steps are not required to be executed on this NOAM Server.</b>

<b>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.</b>

Repeat this procedure and below steps (if required) for other NOAM Server.</td></tr>
<tr><td>4
□</td><td><b>Check if max number of open files for tpdProvd is already set</b>

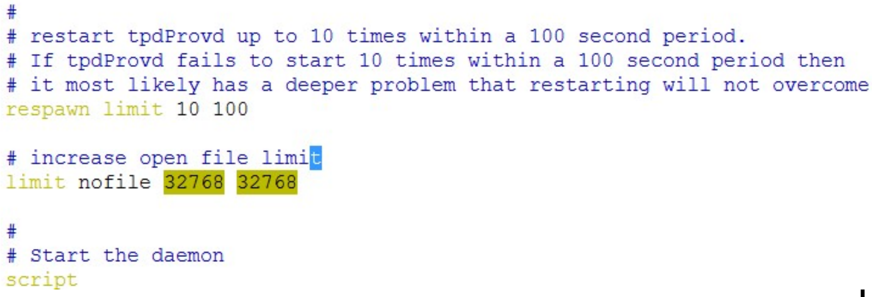
🛑</td><td><b>If the maximum number of open files value (step 2, sub-step 2 - Soft Limit) for tpdProvd is already set to 32768, this procedure is complete.</b>

<b>Then further steps are not required to be executed on this NOAM Server.</b>

<b>If maximum value is not already set, then go to Step 5 below.</b>

Repeat this procedure and below steps (if required) for other NOAM Server.</td></tr>
</table>

Procedure 57: Increase Max Number of Open Files

5
□
	Active NOAM CLI:
	Increase max number of open files
		Increase max number of open files.
		1. Using a text editor with sudo, edit the file `/etc/init/tpdProvd.conf` to add the following two lines:
		`# increase open file limit`
		`limit nofile 32768 32768`
		Just prior to the comment line in the file `/etc/init/tpdProvd.conf` 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`
		2. Save the file and close the editor.
		Caution: - Don't edit any other line in this file. You can take backup of the file if required.

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

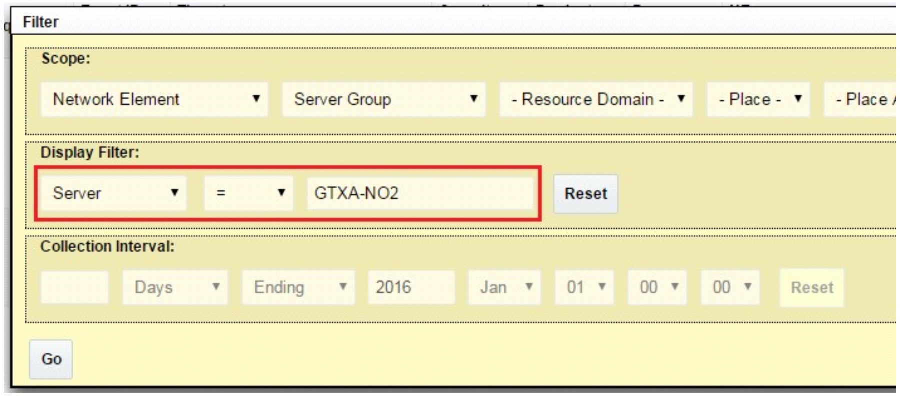
7
□
	Active NOAM CLI:
	Recheck open file max limit
		Check the max file limit is set for tpdProvd.
		1. Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in blue in the sample output below:
		`$ps -ef | grep -i tpdProvd`
		`tpdProvd 347635       1  0 06:09 ?        00:00:11`
		`/usr/TKLC/plat/bin/tpdProvd`
		2. Use the highlighted value from sub-step 1 just above in place of XXXX in the cat command below.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files        32768           32768          files`
		3. 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 to contact MOS per Appendix S.

THIS PROCEDURE HAS BEEN COMPLETED.

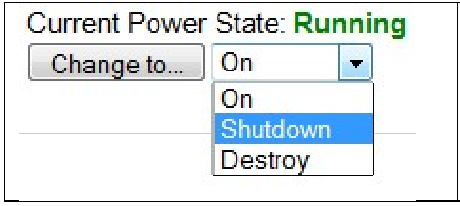
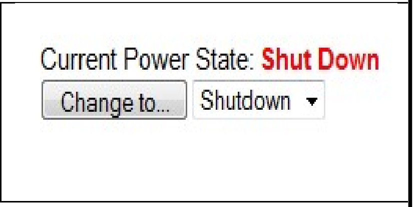
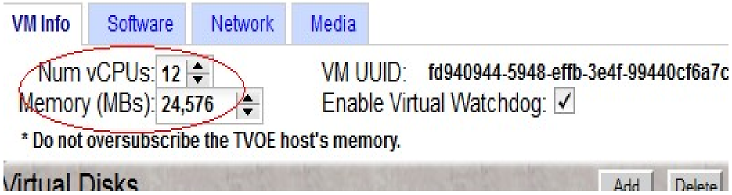
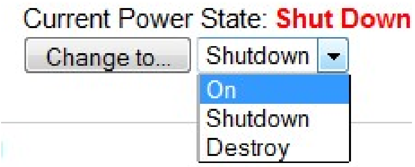
Appendix C UPDATE NOAM GUEST VM CONFIGURATION

This procedure updates the VM configuration for NOAM guests hosted on an RMS. The new configuration increases the number of virtual CPUs and RAM available to the NOAMs to improve performance in high load conditions. This procedure should be executed only when the NOAM is virtualized on an RMS with no B-level or C-level servers.

Procedure 58: Update NOAM Guest VM Configuration

S T E P #	This procedure modifies the VM configuration for the NOAM guest. This procedure applies only to NOAMs hosted on an RMS. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**.	
1. □	**Active NOAM VIP:** Log all current alarms for the Standby NOAM	When the NOAM Guest VM is shutdown prior to updating the configuration, a number of alarms will be generated by the event. Thus it is necessary to note any existing alarms for the server prior to the shutdown. 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Select the **Filter** dropdown menu. Select "Server = <StbyNOAM>" for the **Display Filter**, where <StbyNOAM> is the hostname of the Standby NOAM. 3. Click **Go** to filter the alarms on the specified criteria. 4. Make note of all alarms that are displayed as a result of the applied filter. These should be the only alarms displayed once the VM is restarted. Filter Scope: Network Element, Server Group, - Resource Domain -, - Place -, - Place Display Filter: Server = GTXA-NO2 Collection Interval: Days, Ending, 2016, Jan, 01, 00, 00

Procedure 58: Update NOAM Guest VM Configuration

2. □	**PM&C GUI:** Edit the NOAM guest VM configuration	Edit NOAM Guest VM configuration 1. Log into the PM&C GUI by navigating to http://<pmac_management_ip> 2. Select **Main Menu > VM Management.** 3. Select the TVOE Host that is hosting the NOAM VM to be upgraded. 4. Select the NOAM VM to edit. 5. Change the power state of the guest VM from Running to Shutdown and click the "**Change to…**" button. Confirm the pop-up and wait for the power state to change to Shutdown. This may take a few moments as this executes a graceful shutdown of the NOAM guest.  Current Power State: Running  Current Power State: Shut Down 6. Click the **Edit** button near the bottom of the window. 7. Change the following guest configuration values from the current value to the values presented in bold: • Num vCPUs: **12** • Memory (MBs): **24,576**  VM Info Software Network Media Num vCPUs: 12 Memory (MBs): 24,576 VM UUID: fd940944-5948-effb-3e4f-99440cf6a7c Enable Virtual Watchdog: ✓ * Do not oversubscribe the TVOE host's memory. Virtual Disks Add Delete **No other configuration values should be changed.** 8. Select **Save**. The GUI may gray out for a moment while the changes are committed.
3. □	**PM&C GUI:** Modify the guest power state.	Change the guest power state. 1. Change the guest VM power state from **Shutdown** to **On** and click the "**Change to…**" button. This will restart the VM.  Current Power State: Shut Down

Procedure 58: Update NOAM Guest VM Configuration

4. □	**Active NOAM VIP:** Monitor current alarms for the Standby NOAM	Monitor the alarms for the Standby NOAM until the alarm count is down to those that existed prior to the VM shutdown, as recorded in Step 1. 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Select the **Filter** dropdown menu. Select “Server = <StbyNOAM>” for the **Display Filter**, where <StbyNOAM> is the hostname of the Standby NOAM. 3. Click **Go** to filter the alarms on the specified criteria. 4. Monitor Standby NOAM alarms.
THIS PROCEDURE HAS BEEN COMPLETED.		

Appendix D PCRF POOLING MIGRATION CHECK

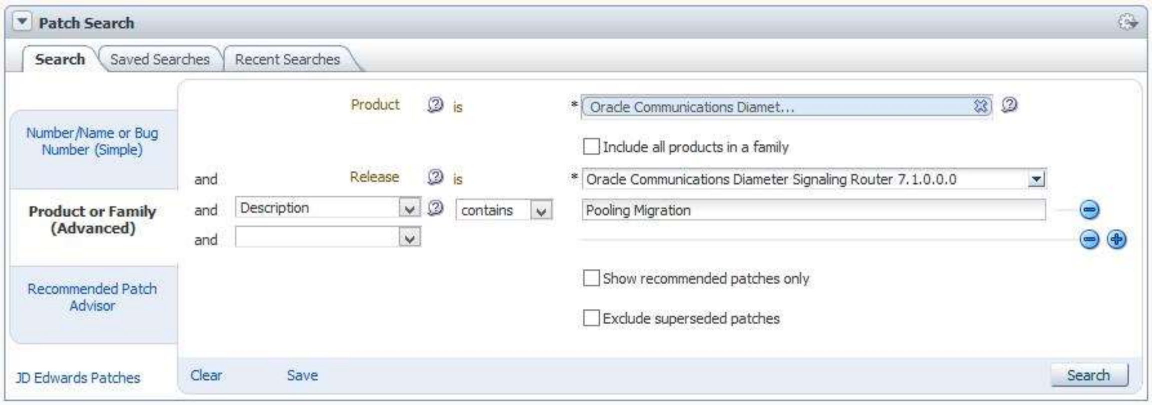
If the PCA application or the PDRA application has been activated in the source release, a check of the PCRF Pooling Migration is **REQUIRED** prior to the start of a major upgrade to DSR 8.0.

The PCRF Pooling Migration check is NOT required for a DSR 8.0 incremental upgrade.
The PCRF Pooling Migration check is NOT required for a DSR 7.1, 7.2, or 7.3 to 8.0 upgrade.

Follow the steps in Procedure 59 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 is complete and the tool indicates that upgrade is allowed.

Procedure 59: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**.	
1. □	Download PCRF Pooling Migration Tool	Download the PCRF Pooling Migration Tool from MOS. The tool is used to determine the status of the PCRF pooling migration. 1. Navigate to the MOS site at https://support.oracle.com/ and sign in. 2. Select the **Patches & Updates** tab 3. In the Patch Search window, select the **Product or Family (Advanced)** tab on left. 4. Use the following search criteria to locate and download the migration tool (as shown in the figure below): • Product is: Oracle Communications Diameter Signaling Router (DSR) • Release is: 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 contains**: Pooling Migration  Patch Search Search Saved Searches Recent Searches Number/Name or Bug Number (Simple) Product or Family (Advanced) Recommended Patch Advisor JD Edwards Patches □ Include all products in a family □ Show recommended patches only □ Exclude superseded patches Clear Save Search Product is * Oracle Communications Diamet... and Release is * Oracle Communications Diameter Signaling Router 7.1.0.0.0 and Description contains Pooling Migration and
2. □	Copy the PCRF Pooling Migration Tool	Copy the PCRF Pooling Migration Tool to the Active NOAM. `scp -p <patchfilename> admusr@<Active_NOAM>`

3.
□
	Active NOAM CLI:
	SSH to the Active NOAM
		Using a SSH tool, login to the Active NOAM server.
		`ssh admusr@<NOAM_VIP>`
		`password:  <enter password>`

Procedure 59: PCRF Pooling Migration Check

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 =============`

8. □	**Active NOAM CLI:** Verify that 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 will inform the user if the PCRF Pooling Migration has completed. If PCRF Pooling Migration is complete, the command will print the following output: "`Upgrade is allowed.`" If PCRF Pooling Migration is **NOT** complete, the command will print the following output: "`Upgrade is not allowed.`"

Procedure 59: PCRF Pooling Migration Check

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 will output 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.`

		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix E DETERMINE IF TVOE UPGRADE IS REQUIRED

When upgrading a server that exists as a virtual guest on a TVOE Host, it is first necessary to determine whether the TVOE Host (i.e. the “bare-metal”) server must be upgraded to a newer release of TVOE.

NOAM and SOAM servers are often implemented as TVOE guests in C-class deployments, so the TVOE upgrade check is necessary. DA-MPs are not implemented as TVOE guests in C-class deployments, so the TVOE upgrade check is not necessary when upgrading C-class DA-MPs.

When DSR is deployed in the VEDSR configuration, or on Rack Mounted Servers (RMSs), all servers are virtual guests, and the TVOE upgrade check is always required. However, DA-MPs are often deployed as guests on the same TVOE Host as the OAM server(s), and so by the time the DA-MP servers are being upgraded, TVOE has already been upgraded and there is no need to do so again.

Procedure 60: Determine if TVOE Upgrade is Required

S T E P #	This procedure checks if TVOE upgrade is required. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>.**	

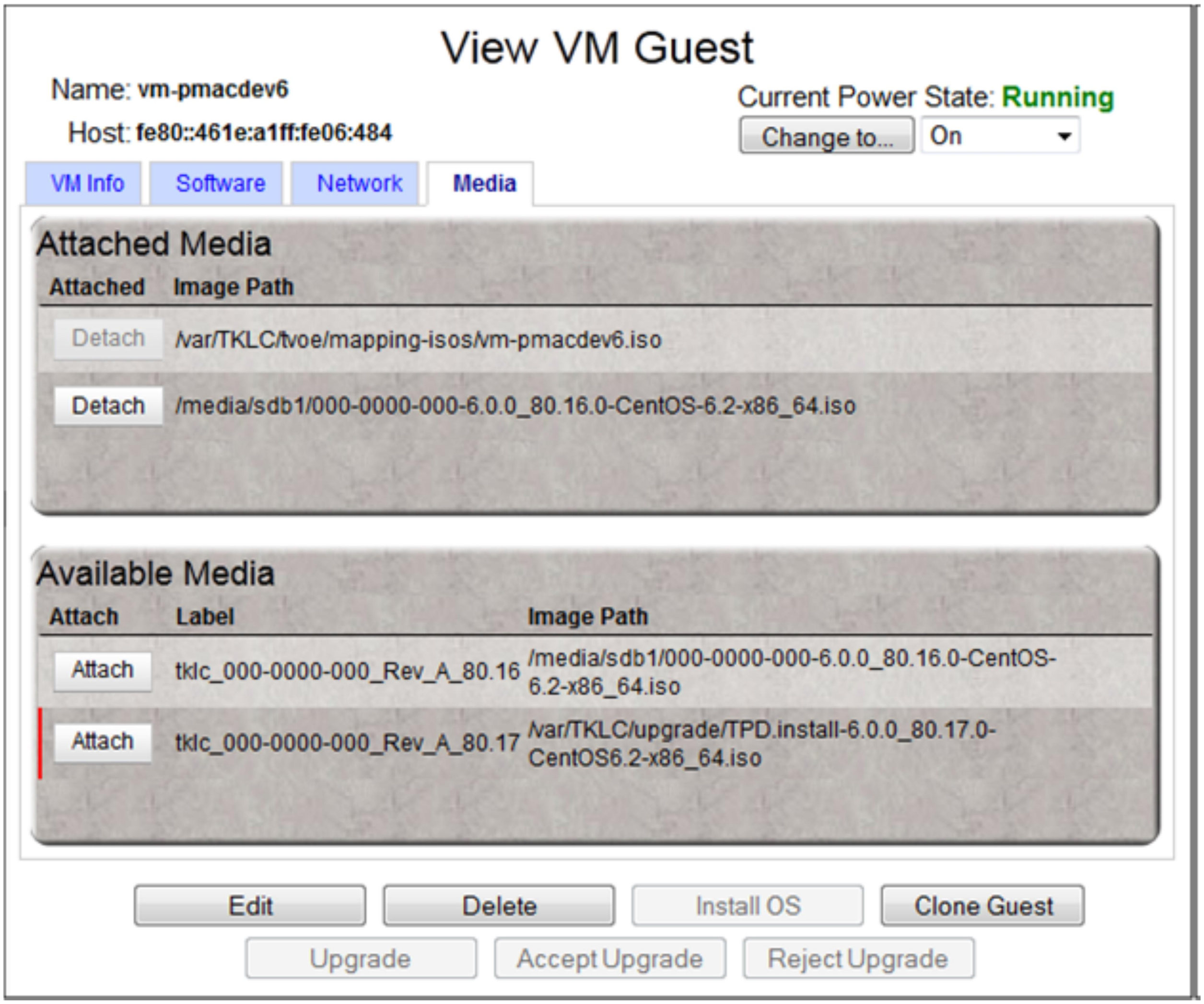
4.
□
	<u>TVOE CLI:</u>
	Determine the version of TVOE already running on the bare-metal server that hosts the virtual guest currently being upgraded
		1. Log into the host server on which TVOE is installed.
		2. Execute the following command to get the current TVOE installed version :
		`# appRev`
		`        Install Time: Thu Aug 14 08:17:52 2014`
		`        Product Name: TVOE`
		`     Product Release: 2.7.0_84.17.0`
		`     Part Number ISO: 872-2290-104`
		`     Part Number USB: 872-2290-104`
		` Base Distro Product: TPD`
		` Base Distro Release: 7.0.0_70.6.0`
		`     Base Distro ISO: TPD.install-6.7.0_84.17.0-CentOS6.2-x86_64.iso`
		`                  OS: CentOS 6.2`

5. □	Check the TVOE release version required for target DSR release	It is recommended to contact MOS by referring to Appendix S of this document to determine the appropriate release version.
6. □	If the release in step 1 is less than what is required in step 2 then upgrade of TVOE is required	The procedure to upgrade TVOE on the host server is in Appendix J.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix F ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY

If the ISO image is delivered on optical media, or USB device, continue with step 1 of this Appendix; otherwise, if the ISO image was delivered to the PM&C using sftp, continue with step 5.

1. In the PM&C GUI, navigate to **Main Menu > VM Management.** In the "**VM Entities**" list, select the PM&C Guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.
2. Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



View VM Guest

Name: vm-pmacdev6

Host: fe80::461e:a1ff:fe06:484

Current Power State: Running

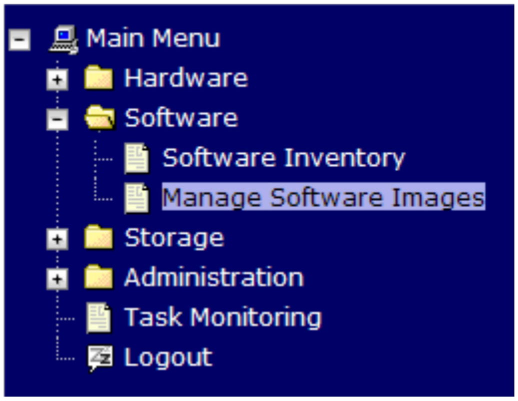
Attached Media

Attached	Image Path
Detach	/var/TKLC/tvoe/mapping-isos/vm-pmacdev6.iso
Detach	/media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso

Available Media

Attach	Label	Image Path
Attach	tklc_000-0000-000_Rev_A_80.16	/media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso
Attach	tklc_000-0000-000_Rev_A_80.17	/var/TKLC/upgrade/TPD.install-6.0.0_80.17.0-CentOS6.2-x86_64.iso

3. **PM&C GUI:** Navigate to **Manage Software Images**
   Navigate to **Main Menu ➤ Software ➤ Manage Software Images**



4. **PM&C GUI:** Add image
   Press the **Add Image** button.

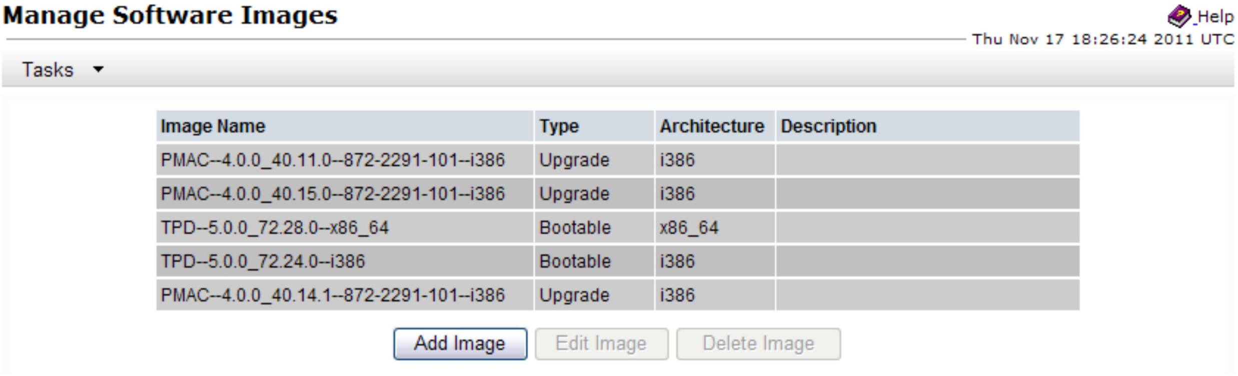
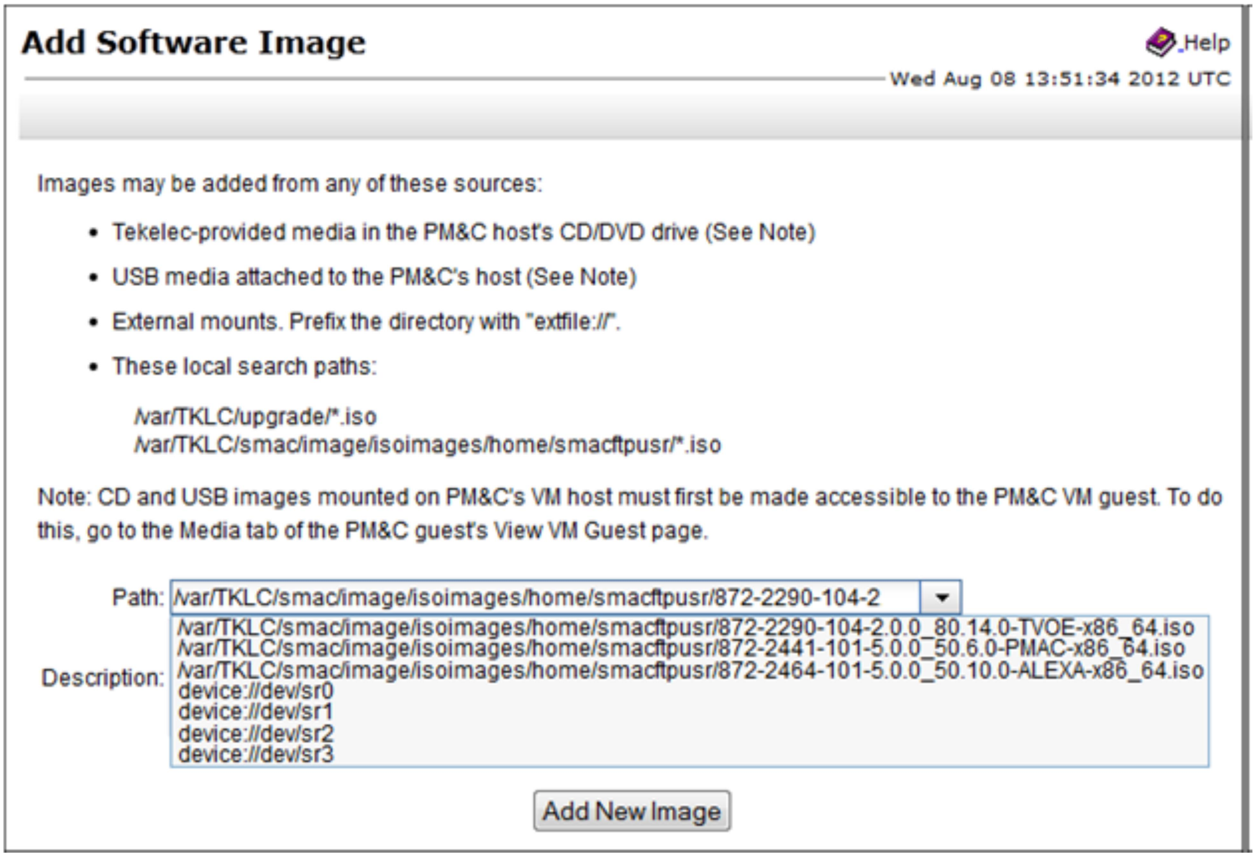


Image Name	Type	Architecture	Description
PMAC--4.0.0_40.11.0--872-2291-101--i386	Upgrade	i386	
PMAC--4.0.0_40.15.0--872-2291-101--i386	Upgrade	i386	
TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	
TPD--5.0.0_72.24.0--i386	Bootable	i386	
PMAC--4.0.0_40.14.1--872-2291-101--i386	Upgrade	i386	

5. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:
   - If the image was transferred to PM&C via sftp, it will appear in the list as a local file `"/var/TKLC/..."`.
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device (`"device://..."`). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the ISO image of interest is normally present on the second device, `"device://dev/sr1"`. If one or more CD or USB-based images were already present on the Management Server before this procedure was started, choose a correspondingly higher device number.

   Enter an appropriate image description and press the **Add New Image** button.



Add Software Image

Wed Aug 08 13:51:34 2012 UTC

Images may be added from any of these sources:

- Tekelec-provided media in the PM&C host's CD/DVD drive (See Note)
- USB media attached to the PM&C's host (See Note)
- External mounts. Prefix the directory with "extfile://".
- These local search paths:

  /var/TKLC/upgrade/*.iso
  /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso

Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM&C VM guest. To do this, go to the Media tab of the PM&C guest's View VM Guest page.

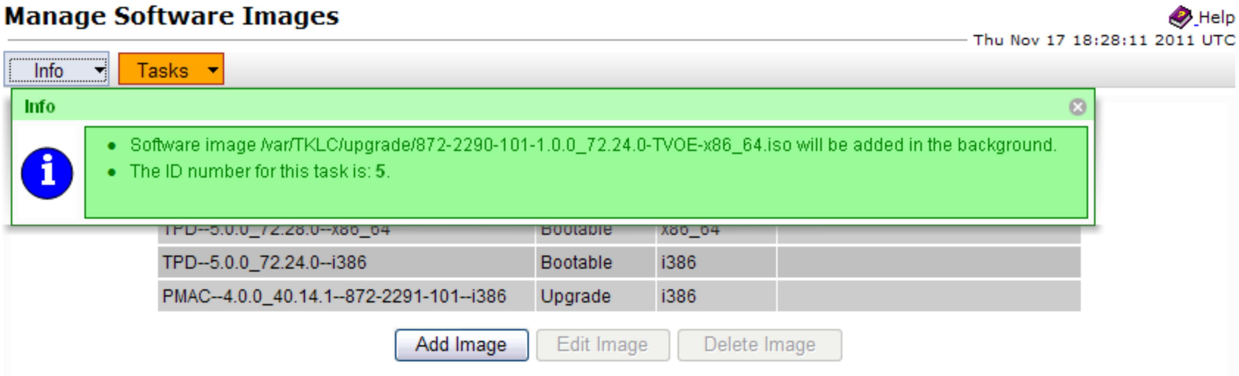
Path: /var/TKLC/smac/image/isoimages/home/smacftpusr/872-2290-104-2

Description:

/var/TKLC/smac/image/isoimages/home/smacftpusr/872-2290-104-2.0.0_80.14.0-TVOE-x86_64.iso
/var/TKLC/smac/image/isoimages/home/smacftpusr/872-2441-101-5.0.0_50.6.0-PMAC-x86_64.iso
/var/TKLC/smac/image/isoimages/home/smacftpusr/872-2464-101-5.0.0_50.10.0-ALEXA-x86_64.iso
device://dev/sr0
device://dev/sr1
device://dev/sr2
device://dev/sr3

6. **PM&C GUI** Monitor the Add Image status

The Manage Software Images page is then redisplayed with a new background task entry in the table at the bottom of the page:



Manage Software Images

Thu Nov 17 18:28:11 2011 UTC

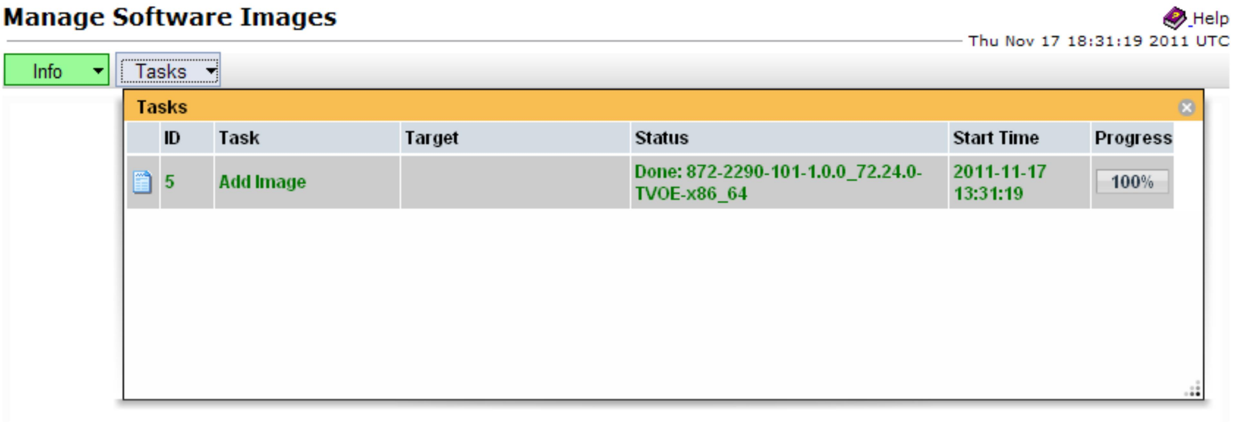
Info

- Software image /var/TKLC/upgrade/872-2290-101-1.0.0_72.24.0-TVOE-x86_64.iso will be added in the background.
- The ID number for this task is: 5.

TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	
TPD--5.0.0_72.24.0--i386	Bootable	i386	
PMAC--4.0.0_40.14.1--872-2291-101--i386	Upgrade	i386	

7. **PM&C GUI** Wait until the Add Image task finishes

When the task is complete, its text changes to green and its Progress column indicates "100%". Check that the correct image name appears in the Status column:



ID	Task	Target	Status	Start Time	Progress
5	Add Image		Done: 872-2290-101-1.0.0_72.24.0-TVOE-x86_64	2011-11-17 13:31:19	100%

8. **PM&C GUI:** Detach the image from the PM&C guest

If the image was supplied on CD or USB, return to the PM&C Guest's "**Media**" tab used in Step 2, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use.

Remove the CD or USB device from the Management Server.

Appendix G 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 G to mark up, or keep another form of written record of the steps performed.

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

<table>
<tr>
<td><b>S
T
E
P
#</b></td>
<td colspan="2">This procedure executes the Upgrade Single Server – Upgrade Administration steps for an Active NOAM on Release 8.0.

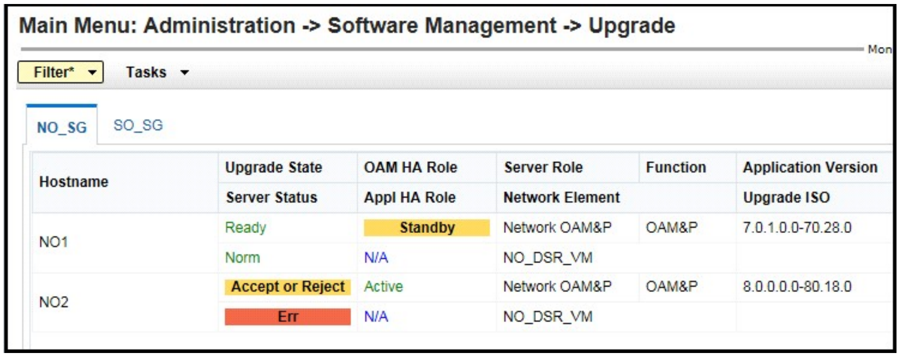
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.</b></td>
</tr>
<tr>
<td><b>1</b>

□</td>
<td><b><u>Active NOAM VIP:</u></b>

View the pre-upgrade status of Servers</td>
<td>View the pre-upgrade status

1. Log into the NOAM GUI using the VIP
2. Select <b>Administration > Software Management > Upgrade</b>
The Upgrade Administration screen is displayed.
3. Select the Network Element of the server to be upgraded (NOAM or Site).


<b>Main Menu: Administration -> Software Management -> Upgrade</b>

<table>
<tr><th>Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th></th><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td>NO1</td><td>Ready</td><td>Standby</td><td>Network OAM&amp;P</td><td>OAM&amp;P</td><td>7.0.1.0.0-70.28.0</td></tr>
<tr><td></td><td>Norm</td><td>N/A</td><td>NO_DSR_VM</td><td></td><td></td></tr>
<tr><td>NO2</td><td>Accept or Reject</td><td>Active</td><td>Network OAM&amp;P</td><td>OAM&amp;P</td><td>8.0.0.0.0-80.18.0</td></tr>
<tr><td></td><td>Err</td><td>N/A</td><td>NO_DSR_VM</td><td></td><td></td></tr>
</table>

The Active NOAM server may have some or all of the following expected alarms:
Alarm ID = <b>10008 (Provisioning Manually Disabled)</b>
Alarm ID = <b>32532 (Server Upgrade Pending Accept/Reject)</b></td>
</tr>
</table>

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

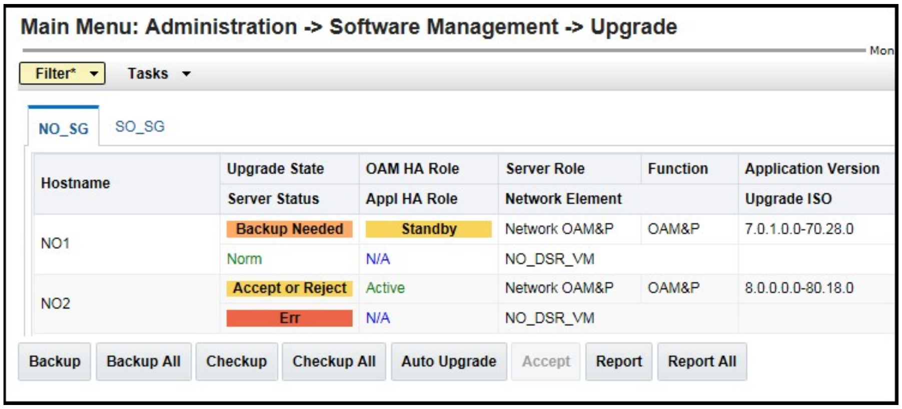
2 □

Active NOAM VIP:

Verify status of Server to be upgraded

For the server to be upgraded:

1. Identify the server to be upgraded (NOAM, SOAM, MP, etc) ______________________________(record hostname)
2. Verify the Application Version value is the expected source software release version.
3. If the server is in the "**Backup Needed"** state, select the server and click the **Backup** button. On the **Upgrade [Backup]** screen, click **Ok**. The Upgrade State changes to "**Backup in Progress**".
4. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)


Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Backup Needed	Standby	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0
	Norm	N/A	NO_DSR_VM		
NO2	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	N/A	NO_DSR_VM		

When the backup is complete, verify the server state changes to "**Ready**".

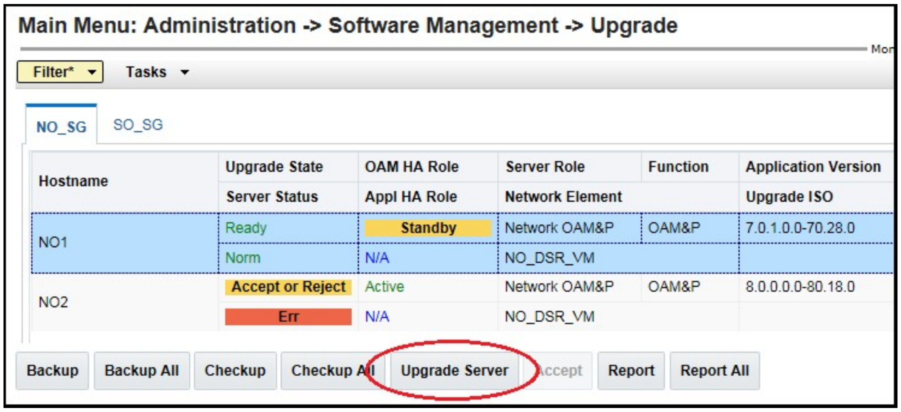
3 □

Active NOAM VIP:

Initiate Upgrade

Initiate the server upgrade.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the **Upgrade Server** button.
   The Initiate Upgrade form will be displayed


Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Ready	Standby	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0
	Norm	N/A	NO_DSR_VM		
NO2	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	N/A	NO_DSR_VM		

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

4 □

Active NOAM VIP:

Select upgrade ISO

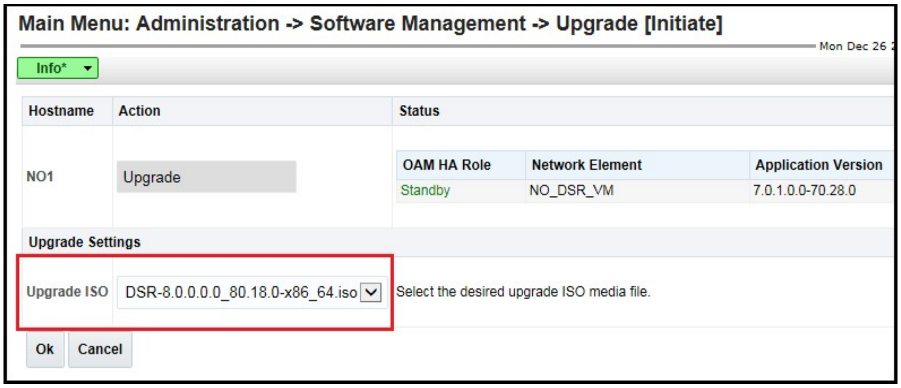
Initiate the server upgrade.

1. In the **Upgrade Settings** – **Upgrade ISO** pick list, select the ISO to use in the server upgrade,

   Note: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing 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 will display “Active” with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the Make Ready action WILL cause an HA switchover.

2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen.



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

Hostname	Action	Status		
		OAM HA Role	Network Element	Application Version
NO1	Upgrade	Standby	NO_DSR_VM	7.0.1.0.0-70.28.0

Upgrade Settings

Upgrade ISO: DSR-8.0.0.0.0_80.18.0-x86_64.iso — Select the desired upgrade ISO media file.

*** Critical *** Do NOT omit this step

3. **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

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

5 □

Active NOAM VIP:

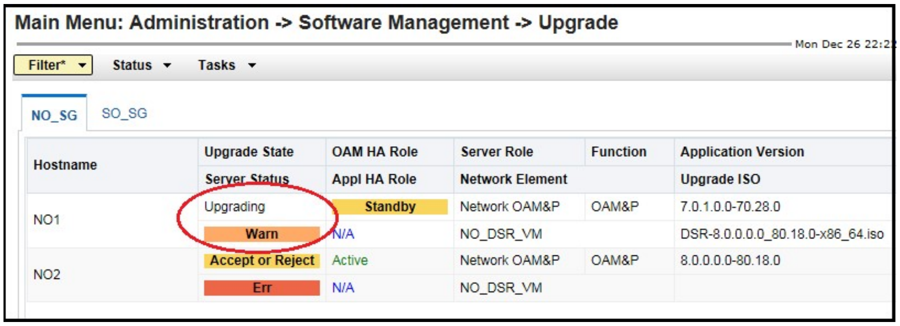
View In-Progress Status

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 will be shown as “FAILED”.
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. 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 is displayed in the Server Upgrade States column.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO1	Upgrading	Standby	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0
	Warn	N/A	NO_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso
NO2	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	N/A	NO_DSR_VM		

Servers may have a combination of the following expected alarms.
Note: Not all servers will 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**

2. Wait for the upgrade to complete. The “Status Message” column will show “Success”. This step will take approximately 20 to 50 minutes.

If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

6 □

Server CLI:

Optional : View In-Progress Status from command line of server

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
```

This command will display the upgrade log entries as the events occur. Once the upgrade is complete, the server will re-boot. It will then take a couple of minutes for the DSR Application processes to start up.

This command will show 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 to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

7 □

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/upgrade.log

It is recommended to contact MOS by referring to Appendix S of this document and provide these files.Refer to Appendix O for failed server recovery procedures.

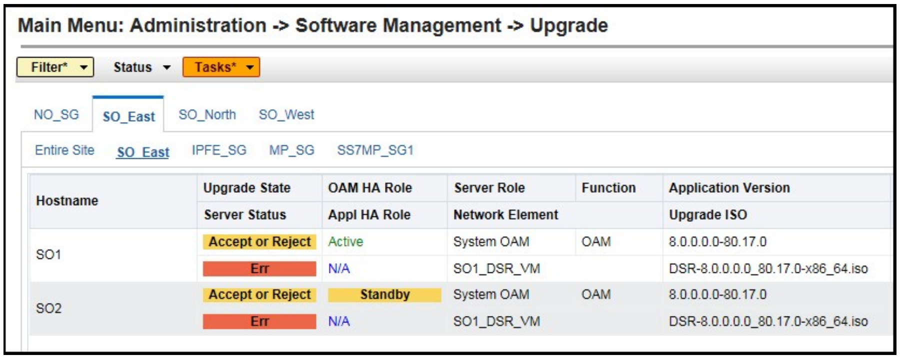
8 □

Active NOAM VIP:

Verify post upgrade status

Verify post upgrade status

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed.
2. Select the tab of the NOAM or site being upgraded.
3. Verify the Application Version value for this server has been updated to the target software release version.
4. Verify the Upgrade State of the upgraded server is "**Accept or Reject**".



Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
SO1	Accept or Reject	Active	System OAM	OAM	8.0.0.0.0-80.17.0
	Err	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.17.0-x86_64.iso
SO2	Accept or Reject	Standby	System OAM	OAM	8.0.0.0.0-80.17.0
	Err	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.17.0-x86_64.iso

Procedure 61: Upgrade Single Server – Upgrade Administration - DSR 8.x

9 □	**Active NOAM/SOAM VIP:** Verify the server was successfully upgraded	View the Post-Upgrade Status of the server: 1. Navigate to **Alarm & Events > View Active**. The active alarms screen is displayed. 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 will have 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 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 Appendix G.

Appendix H UPGRADE SINGLE SERVER – PRE DSR 8.X

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 is used to upgrade the Standby NOAM only. The remaining servers will be upgraded using Procedure 61.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

S T E P #

This procedure executes the Upgrade Single Server – Upgrade Administration steps.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**

1 □

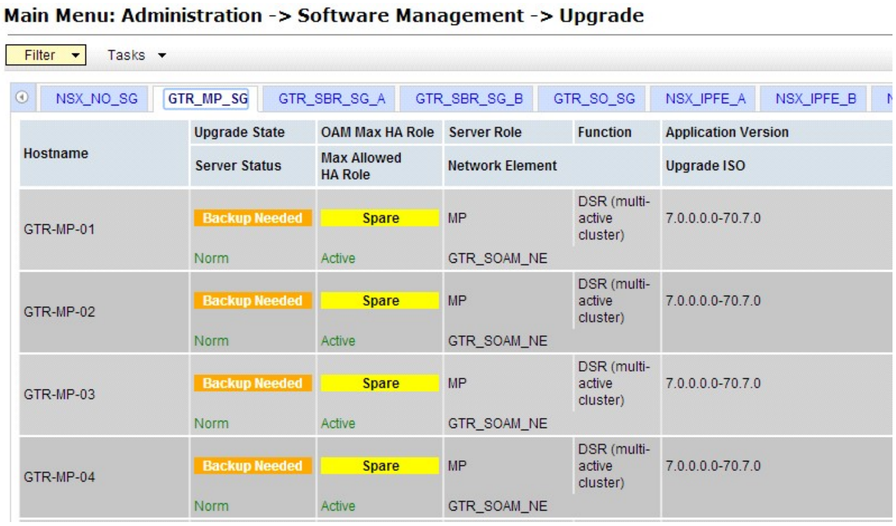
Active NOAM VIP:

View the pre-upgrade status of Servers

View the pre-upgrade status

1. Log into the NOAM GUI using the VIP
2. Select **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed (example below):

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

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO
GTR-MP-01	Backup Needed	Spare	MP	DSR (multi-active cluster)	7.0.0.0-70.7.0
	Norm	Active	GTR_SOAM_NE		
GTR-MP-02	Backup Needed	Spare	MP	DSR (multi-active cluster)	7.0.0.0-70.7.0
	Norm	Active	GTR_SOAM_NE		
GTR-MP-03	Backup Needed	Spare	MP	DSR (multi-active cluster)	7.0.0.0-70.7.0
	Norm	Active	GTR_SOAM_NE		
GTR-MP-04	Backup Needed	Spare	MP	DSR (multi-active cluster)	7.0.0.0-70.7.0
	Norm	Active	GTR_SOAM_NE		

2 □

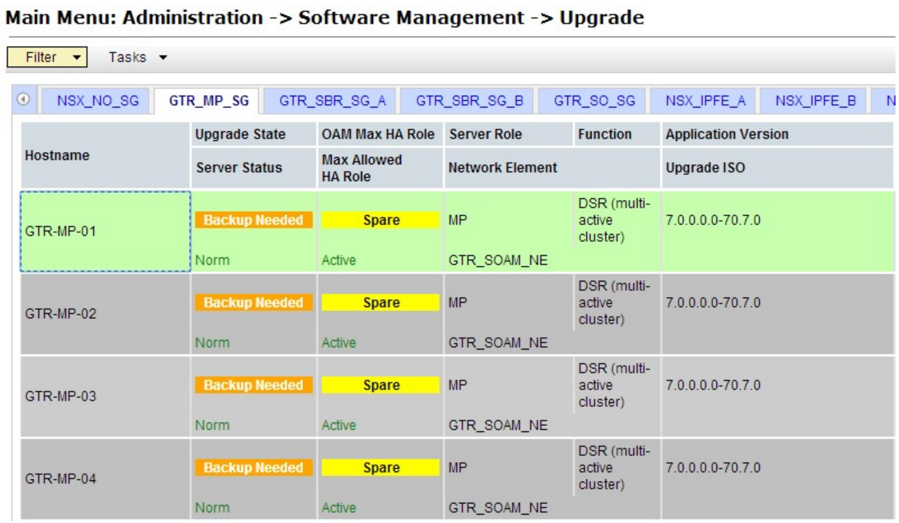
Active NOAM VIP:

Verify status of Server to be upgraded

For the server to be upgraded:

1. Identify the server (NOAM, SOAM, MP, etc) _________________________(record name)
2. Verify the Application Version value is the expected source software release version.
3. From the **Administration > Software Management > Upgrade** screen, select the Server Group of the server to be upgraded.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x



Main Menu: Administration -> Software Management -> Upgrade

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)	7.0.0.0-70.7.0
GTR-MP-02	Backup Needed Norm	Spare Active	MP GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0-70.7.0
GTR-MP-03	Backup Needed Norm	Spare Active	MP GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0-70.7.0
GTR-MP-04	Backup Needed Norm	Spare Active	MP GTR_SOAM_NE	DSR (multi-active cluster)	7.0.0.0-70.7.0

4. If the server is in the “**Backup Needed”** state, select the server and click the “**Backup**” button. On the **Upgrade [Backup]** screen, click ‘**Ok**’. The Upgrade State changes to “**Backup in Progress**”.
5. Verify the “OAM Max Ha Role” **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)

For Active NOAM on release 6.0 and 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 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

3 □

Active NOAM VIP:

Prepare Upgrade (step 1)

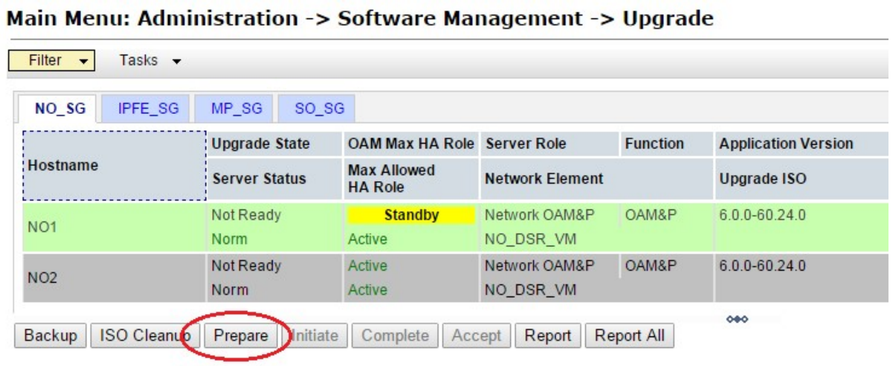
For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Prepare the server for upgrade.

1. On the Upgrade form, make the server 'Upgrade Ready', by selecting the server to be upgraded, and selecting the **Prepare** button.

(In this example, an NOAM with name "NO2" will be made ready for Upgrade)



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO
NO1	Not Ready	Standby	Network OAM&P	OAM&P	6.0.0-60.24.0
	Norm	Active	NO_DSR_VM		
NO2	Not Ready	Active	Network OAM&P	OAM&P	6.0.0-60.24.0
	Norm	Active	NO_DSR_VM		

4 □

Active NOAM VIP:

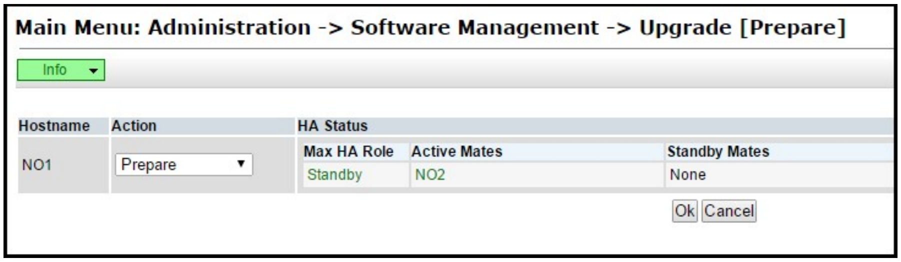
Prepare Upgrade (step 2)

For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Prepare the server for upgrade.

The **Upgrade [Prepare]** form is displayed.



Main Menu: Administration -> Software Management -> Upgrade [Prepare]

Hostname	Action	HA Status		
		Max HA Role	Active Mates	Standby Mates
NO1	Prepare ▼	Standby	NO2	None

For the Max Ha Role:

1. Verify the selected server status **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)

2. If the state of the server to be upgraded is as expected, select **Ok.**

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

5 □

Active NOAM VIP:

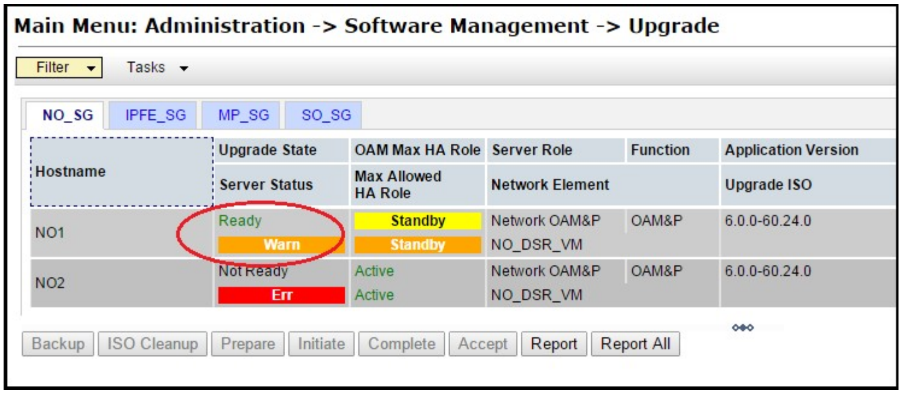
Verify upgrade status is "Ready

For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Verify the server upgrade status is ready.

Upon preparing the selected server, the Upgrade Administration form will refresh, and the server to be upgraded will show Upgrade State = **Ready** (This may take a minute)



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Max Allowed HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Ready Warn	Standby Standby	Network OAM&P NO_DSR_VM	OAM&P	6.0.0-60.24.0
NO2	Not Ready Err	Active Active	Network OAM&P NO_DSR_VM	OAM&P	6.0.0-60.24.0

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 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

6 □

Active NOAM VIP:

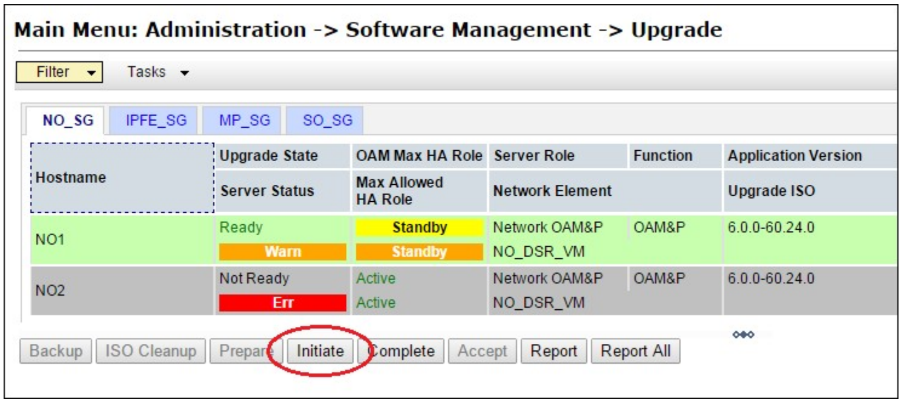
Initiate Upgrade (part 1)

For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Initiate the upgrade on the server.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the "**Initiate"** button



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Max Allowed HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Ready Warn	Standby Standby	Network OAM&P NO_DSR_VM	OAM&P	6.0.0-60.24.0
NO2	Not Ready Err	Active Active	Network OAM&P NO_DSR_VM	OAM&P	6.0.0-60.24.0

7 □

Active NOAM VIP:

Initiate Upgrade (part 2)

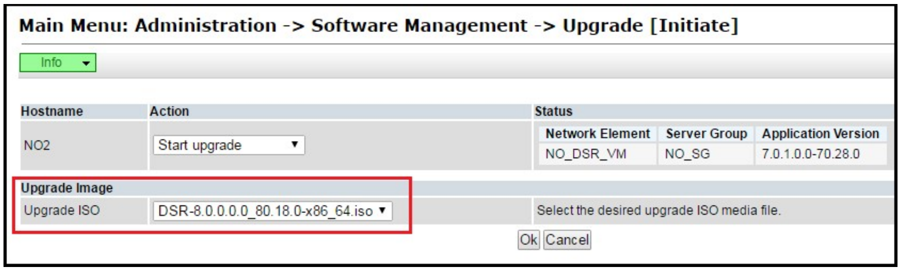
For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Initiate the upgrade on the server.

The Initiate Upgrade form will be displayed:
Administration > Software Management > Upgrade [Initiate]

1. In the **Upgrade Image – Upgrade ISO** pick list, select the ISO to use in the server upgrade,
2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen.



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

Hostname	Action	Status		
		Network Element	Server Group	Application Version
NO2	Start upgrade	NO_DSR_VM	NO_SG	7.0.1.0.0-70.28.0
Upgrade Image				
Upgrade ISO	DSR-8.0.0.0.0_80.18.0-x86_64.iso	Select the desired upgrade ISO media file.		

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

8

□

Active NOAM VIP:

View In-Progress Status (monitor)

For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

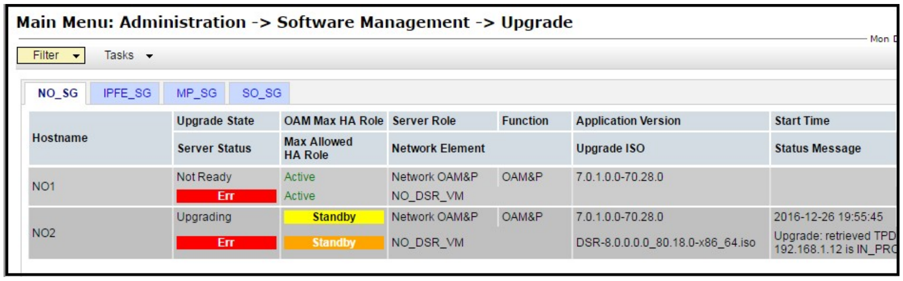
View the Upgrade Administration form to monitor upgrade progress.

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 will be shown as “FAILED”.
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. Observe the **Upgrade State** of the server of interest. Upgrade status will be displayed under the **Status Message** column.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version	Start Time
	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO	Status Message
NO1	Not Ready	Active	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0	
	Err	Active	NO_DSR_VM			
NO2	Upgrading	Standby	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0	2016-12-26 19:55:45
	Err	Standby	NO_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso	Upgrade: retrieved TPD 192.168.1.12 is IN_PRC

Servers may have a combination of the following expected alarms.
Note: Not all servers will 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**

2. Wait for the upgrade to complete. The “Status Message” column will show “Success”. This step will take approximately 20 to 50 minutes.

If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

9 ☐

Active NOAM VIP:

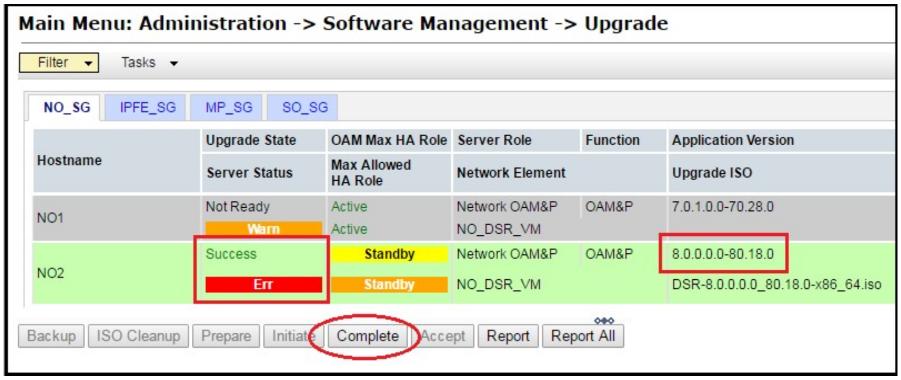
Take the upgraded server out of the upgrade ***SUCCESS*** state (part 1)

For Active NOAM on release 6.0 or 7.0.x only

This step is for an Active NOAM on release 6.0 or 7.0.x only.

Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type.

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed.
2. Verify the **Application Version** value for this server has been updated to the target software release version.
3. Verify the **Upgrade State** of the server that was upgraded is **Success**.
4. Select the server that was upgraded
5. Click the **Complete** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO
NO1	Not Ready	Active	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0
	Warn	Active	NO_DSR_VM		
NO2	Success	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	Standby	NO_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso

10 ☐

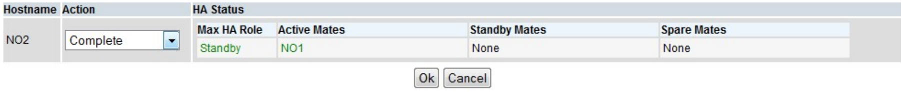
Active NOAM VIP:

Take the upgraded server out of the upgrade ***SUCCESS*** state (part 2)

For Active NOAM on release 6.0 or 7.0.x only

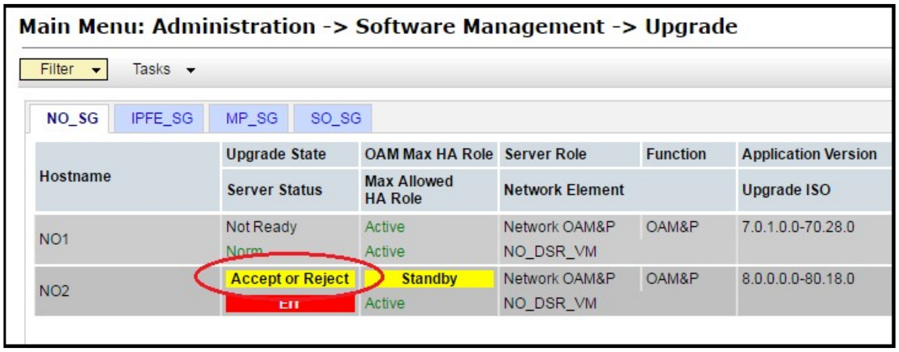
This step is for an Active NOAM on release 6.0 or 7.0.x only.

The **Upgrade[Complete]** screen is displayed



Hostname	Action	HA Status			
		Max HA Role	Active Mates	Standby Mates	Spare Mates
NO2	Complete	Standby	NO1	None	None

1. Click **OK**. This completes the upgrade action on the server.
   The Upgrade Administration screen is displayed.
2. 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**.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version
	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO
NO1	Not Ready	Active	Network OAM&P	OAM&P	7.0.1.0.0-70.28.0
	Norm	Active	NO_DSR_VM		
NO2	Accept or Reject	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	Active	NO_DSR_VM		

Proceed to step 18 to complete this procedure.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

11 □

Active NOAM VIP:

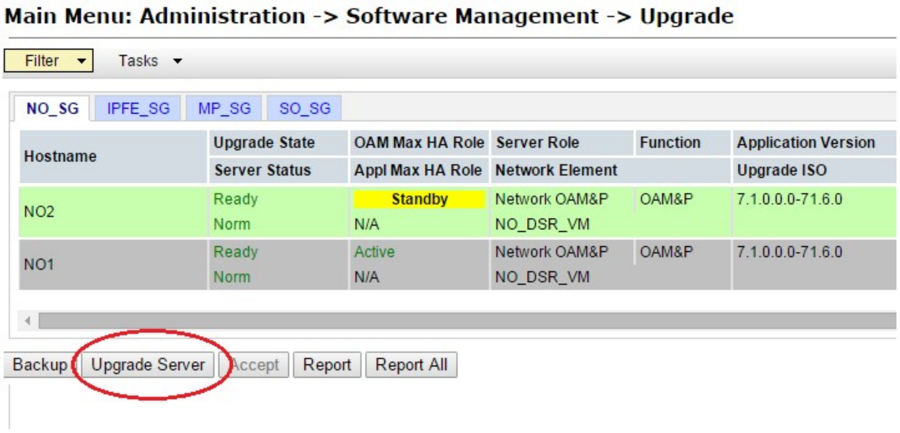
Initiate Upgrade (part 1)

For Active NOAM on release 7.1.x and later

This step is for an Active NOAM on release 7.1.x or later.

Initiate the server upgrade.

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Click the “**Upgrade Server”** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO2	Ready Norm	Standby N/A	Network OAM&P NO_DSR_VM	OAM&P	7.1.0.0.0-71.6.0
NO1	Ready Norm	Active N/A	Network OAM&P NO_DSR_VM	OAM&P	7.1.0.0.0-71.6.0

The Initiate Upgrade form will be displayed:

Administration > Software Management > Upgrade [Initiate]

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

12 □

Active NOAM VIP:

Initiate 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.

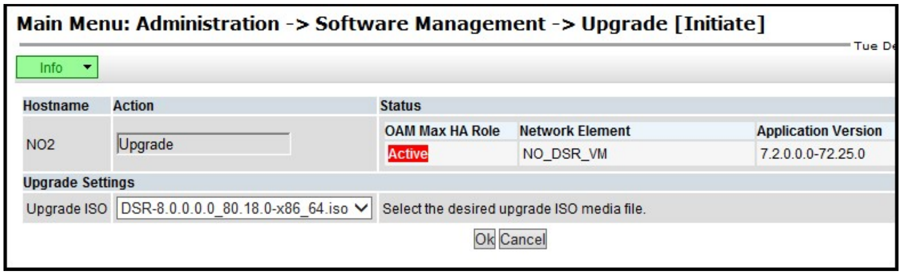
Initiate the server upgrade.

1. In the **Upgrade Settings – Upgrade ISO** pick list, select the ISO to use in the server upgrade,

   Note: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing 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 will display “Active” with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the action WILL cause an HA switchover.

2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen.



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

Hostname	Action	Status		
		OAM Max HA Role	Network Element	Application Version
NO2	Upgrade	Active	NO_DSR_VM	7.2.0.0.0-72.25.0

Upgrade Settings

Upgrade ISO	DSR-8.0.0.0.0_80.18.0-x86_64.iso	Select the desired upgrade ISO media file.

*** Critical *** Do NOT omit this step

3. **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 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

4. If the server being upgraded is not the Active NOAM, continue with step 13 to monitor upgrade status.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

13 □

Active NOAM VIP:

View In-Progress Status (monitor)

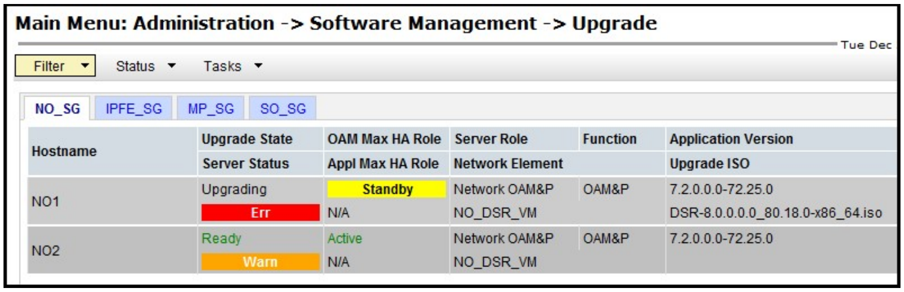
View the Upgrade Administration form to monitor upgrade progress.

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 will be shown as "FAILED".
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. Observe the **Upgrade State** of the server of interest. Upgrade status will be displayed under the **Status Message** column.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO1	Upgrading Err	Standby N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.25.0 DSR-8.0.0.0.0_80.18.0-x86_64.iso
NO2	Ready Warn	Active N/A	Network OAM&P NO_DSR_VM	OAM&P	7.2.0.0.0-72.25.0

Servers may have a combination of the following expected alarms.
Note: Not all servers will 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**

2. Wait for the upgrade to complete. The "Status Message" column will show "Success". This step will take approximately 20 to 50 minutes.

If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

3. Proceed to step 17 to continue the upgrade.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

14 □

Active NOAM VIP:

View In-Progress Status

For Active NOAM on DSR 8.0 only

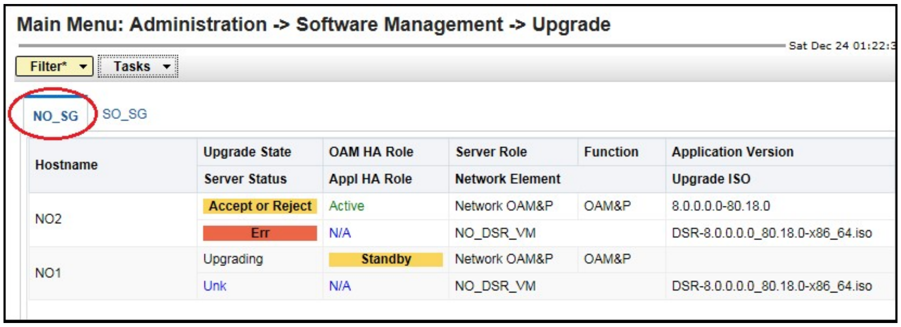
This step is for monitoring upgrade status of the formerly Active NOAM after a role change. The NOAM that was Active when the upgrade was initiated is now the Standby NOAM. Monitoring from this point on is from the new Active NOAM on DSR 8.0.

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 will be shown as “FAILED”.
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. The upgrade status of the Standby NOAM can be observed on the Upgrade Administration screen by selecting the NOAM server group tab.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
NO2	Accept or Reject	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.0
	Err	N/A	NO_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso
NO1	Upgrading	Standby	Network OAM&P	OAM&P	
	Unk	N/A	NO_DSR_VM		DSR-8.0.0.0.0_80.18.0-x86_64.iso

2. Wait for the upgrade to complete. The **Upgrade State** column will show “Success”. This step will take approximately 20 to 50 minutes.

If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

3. Proceed to step 18 to continue the upgrade.

15 □

Server CLI:

Optional : View In-Progress Status from command line of server

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 will re-boot, and then it will take a couple of minutes for the DSR Application processes to start up.

This command will show 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 to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

Procedure 62: Upgrade Single Server – Upgrade Administration - pre DSR 8.x

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/upgrade.log
```

It is recommended to contact MOS by referring to Appendix S of this document and provide these files.Refer to Appendix O for failed server recovery procedures.

17 □

Active NOAM VIP:

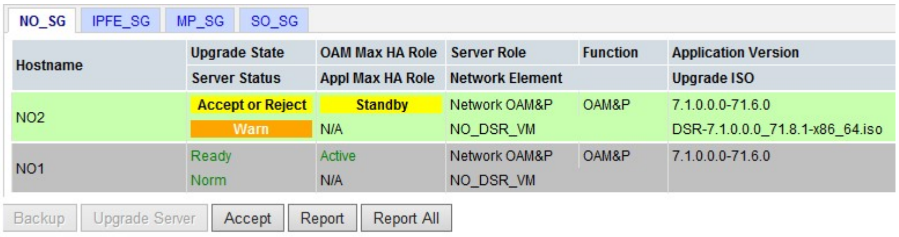
Verify post upgrade status

Verify post upgrade status

1. Navigate to **Administration > Software Management > Upgrade**
   The Upgrade Administration screen is displayed.
2. Verify the Application Version value for this server has been updated to the target software release version.

If the Active NOAM is on release 6.0 or 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**.



Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
NO2	Accept or Reject Warn	Standby N/A	Network OAM&P NO_DSR_VM	OAM&P	7.1.0.0.0-71.6.0 DSR-7.1.0.0.0_71.8.1-x86_64.iso
NO1	Ready Norm	Active N/A	Network OAM&P NO_DSR_VM	OAM&P	7.1.0.0.0-71.6.0

18 □

Active NOAM/SOAM VIP:

Verify the server was successfully upgraded

View the Post-Upgrade Status of the server:

1. Navigate to Alarm & Events > View Active.
   The active alarms screen is displayed.

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 will have 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 Appendix H.

Appendix I UPGRADE FIRMWARE

This section is not applicable to Software Centric installations/upgrades.

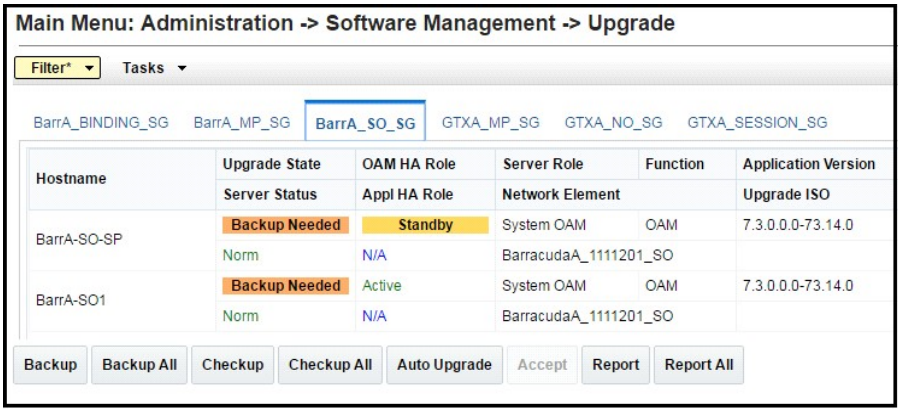
Firmware upgrade procedures are not included in this document. It is recommended to contact MOS by referring to Appendix S of this document for the latest information on firmware upgrades.

Appendix J UPGRADE MULTIPLE SERVERS – UPGRADE ADMINISTRATION

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

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

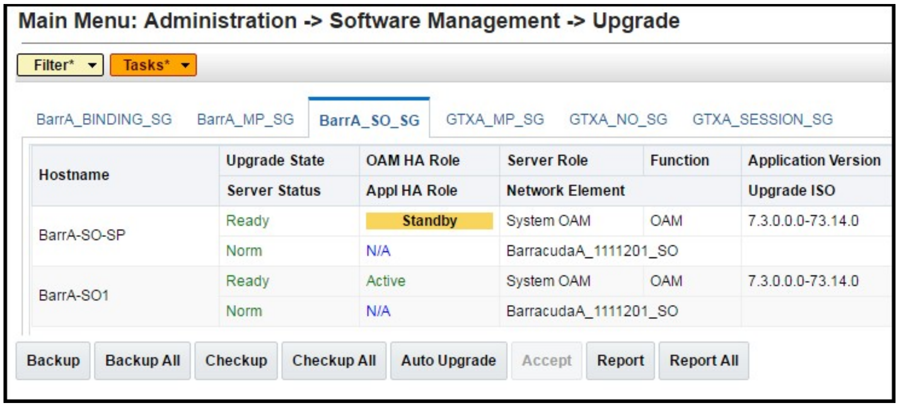
Procedure 63: Upgrade Multiple Servers - Upgrade Administration

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">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.
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.</b></td></tr>
<tr><td><b>1.</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
View pre-upgrade status</td><td>View the pre-upgrade status of the servers.
1.
Active NOAM server may have some or all of the following expected alarms:
Alarm ID = <b>10008 (Provisioning Manually Disabled)</b>
Alarm ID = <b>32532 (Server Upgrade Pending Accept/Reject)</b></td></tr>
<tr><td><b>2.</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
Verify status of Servers to be upgraded</td><td>For the servers to be upgraded:
1. Identify the MP servers to be upgraded in parallel ___________________________ (record names)
2. Verify the Application Version value is the expected source software release version for each MP server to be upgraded.
3. From the <b>Administration > Software Management > Upgrade</b> screen, select the Server Group of the server to be upgraded.

Main Menu: Administration -> Software Management -> Upgrade

Filter*
Tasks
BarrA_BINDING_SG
BarrA_MP_SG
BarrA_SO_SG
GTXA_MP_SG
GTXA_NO_SG
GTXA_SESSION_SG
<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">BarrA-SO-SP</td><td>Backup Needed</td><td>Standby</td><td>System OAM</td><td>OAM</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>N/A</td><td>BarracudaA_1111201_SO</td><td></td><td></td></tr>
<tr><td rowspan="2">BarrA-SO1</td><td>Backup Needed</td><td>Active</td><td>System OAM</td><td>OAM</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>N/A</td><td>BarracudaA_1111201_SO</td><td></td><td></td></tr>
</table>
Backup
Backup All
Checkup
Checkup All
Auto Upgrade
Accept
Report
Report All

4. If the server is in “<b>Backup Needed”</b> state, select the server and click the “<b>Backup</b>” button. The Upgrade State changes to “<b>Backup in Progress</b>”. When the backup is complete, the Upgrade State changes to “<b>Ready</b>”.
5. Verify the “OAM Max Ha Role” <b>is the expected condition (either Standby or Active)</b> (this will depend on the server being upgraded)</td></tr>
</table>

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

<table>
<tr>
<td>3.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Verify Upgrade Status is “Ready”</td>
<td>
<p>The Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the server being upgraded, new alarms may occur.</p>
<p>The Upgrade Administration screen is displayed:</p>

<p>Main Menu: Administration -&gt; Software Management -&gt; Upgrade</p>

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th colspan="2">Network Element</th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">BarrA-SO-SP</td><td>Ready</td><td>Standby</td><td>System OAM</td><td>OAM</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>N/A</td><td colspan="2">BarracudaA_1111201_SO</td><td></td></tr>
<tr><td rowspan="2">BarrA-SO1</td><td>Ready</td><td>Active</td><td>System OAM</td><td>OAM</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>N/A</td><td colspan="2">BarracudaA_1111201_SO</td><td></td></tr>
</table>
<p>Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms:</p>
<p>Alarm ID = <b>10008 (Provisioning Manually Disabled)</b>
Alarm ID = <b>10073 (Server Group Max Allowed HA Role Warning)</b>
Alarm ID = <b>10075 (The server is no longer providing services because application processes have been manually stopped)</b>
Alarm ID = <b>32515 (Server HA Failover Inhibited)</b>
Alarm ID = <b>31101 (DB Replication to slave DB has failed)</b>
Alarm ID = <b>31106 (DB Merge to Parent Failure)</b>
Alarm ID = <b>31107 (DB Merge From Child Failure)</b>
Alarm ID = <b>31228 (HA Highly available server failed to receive mate heartbeats)</b> or <b>(Lost Communication with Mate Server)</b></p>
</td>
</tr>
<tr>
<td></td>
<td>Determine upgrade method – manual or automatic</td>
<td><b>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.</b></td>
</tr>
</table>

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

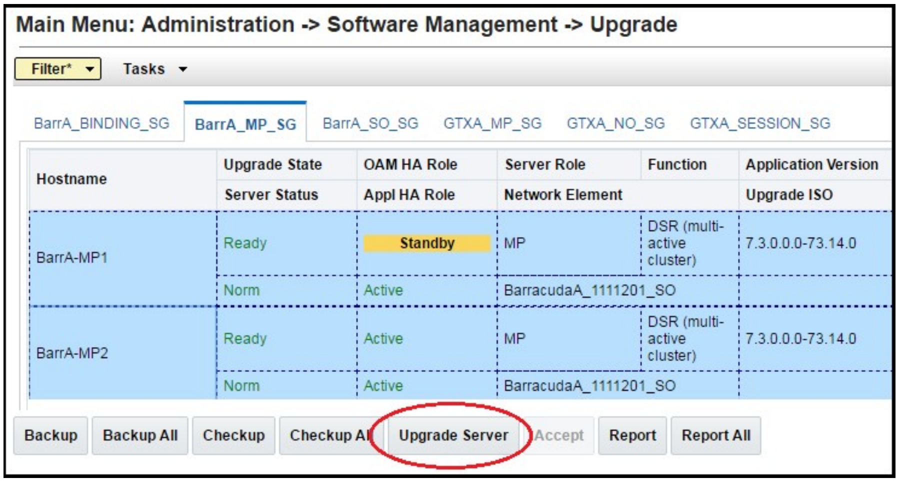
4. □

Active NOAM VIP:

Initiate upgrade (initiate) (part 1)

Initiate the upgrade.

1. From the Upgrade Administration screen, select the servers to be upgraded.
2. Click the "**Upgrade Server"** button.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
BarrA-MP1	Ready	Standby	MP	DSR (multi-active cluster)	7.3.0.0.0-73.14.0
	Norm	Active	BarracudaA_1111201_SO		
BarrA-MP2	Ready	Active	MP	DSR (multi-active cluster)	7.3.0.0.0-73.14.0
	Norm	Active	BarracudaA_1111201_SO		

The Initiate Upgrade form will be displayed:
Administration > Software Management > Upgrade [Initiate]

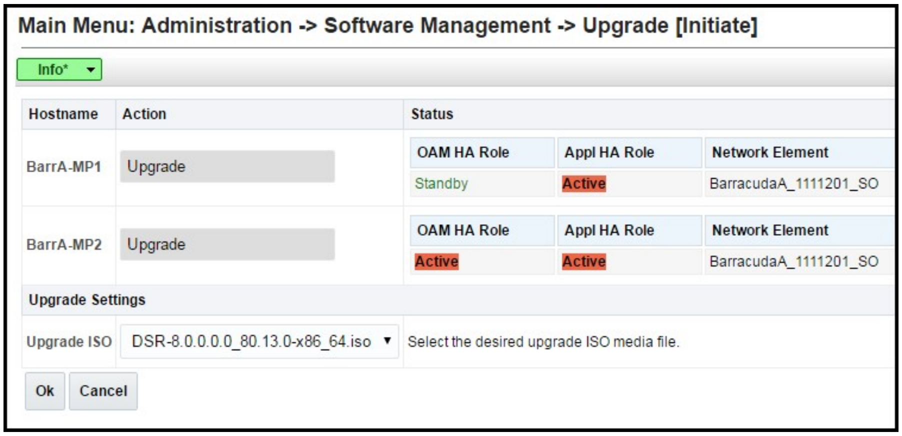
5. □

Active NOAM VIP:

Initiate Upgrade (part 2) – Select ISO form

Start the upgrade.

1. In the **Upgrade Settings – Upgrade ISO** pick list, select the ISO to use in the server upgrade,
2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen.



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

Hostname	Action	Status: OAM HA Role	Status: Appl HA Role	Status: Network Element
BarrA-MP1	Upgrade	Standby	Active	BarracudaA_1111201_SO
BarrA-MP2	Upgrade	Active	Active	BarracudaA_1111201_SO

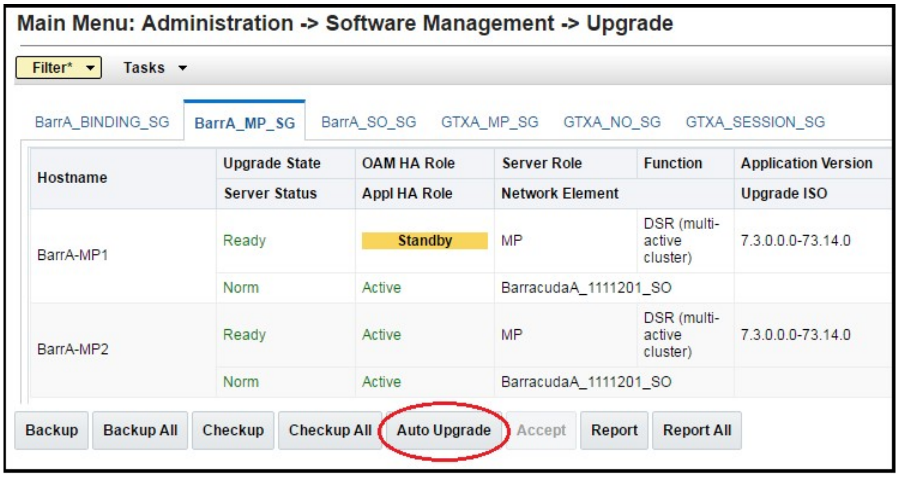
Upgrade Settings

Upgrade ISO	DSR-8.0.0.0.0_80.13.0-x86_64.iso ▾	Select the desired upgrade ISO media file.

Proceed to step 8 to complete this procedure.

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

<table>
<tr>
<td>6.
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Initiate (part 1) - <b>Automated Server Group Upgrade</b></td>
<td>
Initiate the Automated Server Group Upgrade option
<ol>
<li>To utilize the Automated Server Group upgrade option, verify that no servers in the server group are selected.



Main Menu: Administration -> Software Management -> Upgrade

<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">BarrA-MP1</td><td>Ready</td><td>Standby</td><td>MP</td><td>DSR (multi-active cluster)</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>Active</td><td>BarracudaA_1111201_SO</td><td></td><td></td></tr>
<tr><td rowspan="2">BarrA-MP2</td><td>Ready</td><td>Active</td><td>MP</td><td>DSR (multi-active cluster)</td><td>7.3.0.0.0-73.14.0</td></tr>
<tr><td>Norm</td><td>Active</td><td>BarracudaA_1111201_SO</td><td></td><td></td></tr>
</table>

</li>
<li>Click the <b>Auto Upgrade</b> button.
The Upgrade [Initiate] screen is displayed.</li>
</ol>
</td>
</tr>
</table>

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

7. □

Active NOAM VIP:

Initiate (part 2) - **Automated Server Group Upgrade**

Start the Automated Server Group Upgrade.

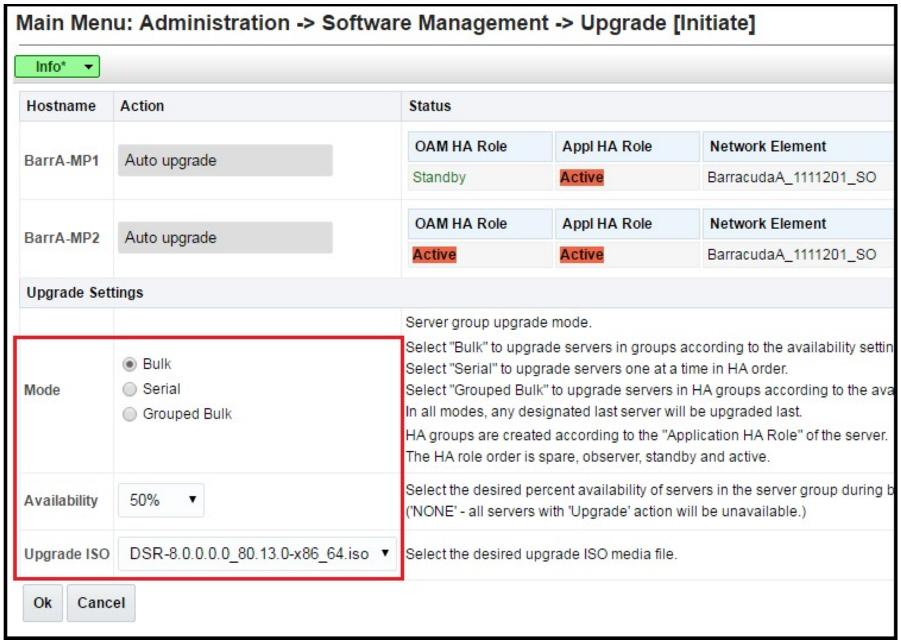
Note: The settings to be used in this step are specified in the calling procedure.

1. 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 will remain in service while servers in the server group are upgraded. For example, a setting of 50% will ensure 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 will upgrade each server in the server group one at a time, and can be used on any server group type.

2. Select the appropriate ISO from the **Upgrade ISO** pick list.
3. Click the **Ok** button to start the upgrade.



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

Hostname	Action	Status		
		OAM HA Role	Appl HA Role	Network Element
BarrA-MP1	Auto upgrade	Standby	Active	BarracudaA_1111201_SO
		OAM HA Role	Appl HA Role	Network Element
BarrA-MP2	Auto upgrade	Active	Active	BarracudaA_1111201_SO

Upgrade Settings

Mode	● Bulk ○ Serial ○ Grouped Bulk	Server group upgrade mode. Select "Bulk" to upgrade servers in groups according to the availability settin Select "Serial" to upgrade servers one at a time in HA order. Select "Grouped Bulk" to upgrade servers in HA groups according to the ava In all modes, any designated last server will be upgraded last. HA groups are created according to the "Application HA Role" of the server. The HA role order is spare, observer, standby and active.
Availability	50% ▾	Select the desired percent availability of servers in the server group during b ('NONE' - all servers with 'Upgrade' action will be unavailable.)
Upgrade ISO	DSR-8.0.0.0.0_80.13.0-x86_64.iso ▾	Select the desired upgrade ISO media file.

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

8.

□

Active NOAM VIP:

View In-Progress Status (monitor)

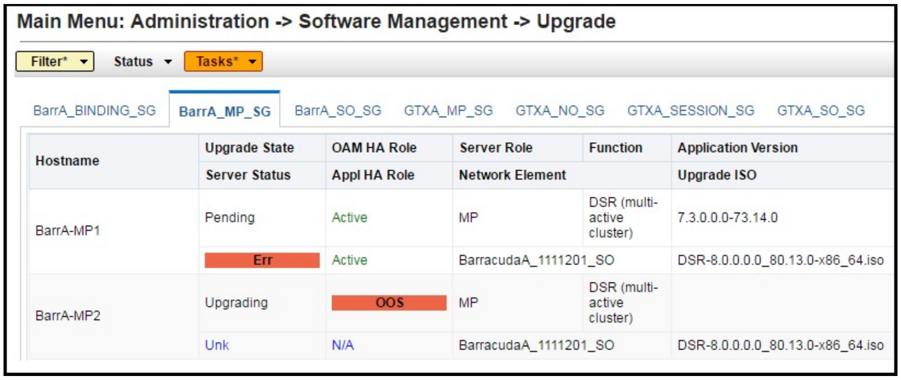
View the Upgrade Administration form to monitor upgrade progress.

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 will be shown as “FAILED”.
The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.

1. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column.



Main Menu: Administration -> Software Management -> Upgrade

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
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 will 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)**

2. Wait for the upgrades to complete. The “Status Message” column will show “Success”. This step will take approximately 20 to 50 minutes.

When an upgraded SOAM becomes active on Release 8.x, alarm 25607 is raised to alert the operator to enable the new Signaling Firewall feature. This alarm will be active until the firewall is enabled in Procedure 39.

Alarm ID = **25607 (DSR Signaling Firewall is administratively Disabled)**

If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

Procedure 63: Upgrade Multiple Servers - Upgrade Administration

9.
□
	Server CLI:
	Optional : View in-progress status from command line
		Optional method to view upgrade progress from a command line:
		
		To view the detailed progress of the upgrade –
		Access the server command line (via ssh or Console), and:
		`$ tail -f  /var/TKLC/log/upgrade/upgrade.log`
		
		Once a server is upgraded, it will re-boot, and then it will take a couple of minutes for the DSR application processes to start up.
		
		This command will show 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 to consult with MOS on the best course of action. Refer to Appendix O for failed server recovery procedures.

10.
□
	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 to contact MOS by referring to Appendix S of this document and provide these files. Refer to Appendix O for failed server recovery procedures.

11. □	**Active NOAM VIP:** Verify post upgrade status	Verify post-upgrade status 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed. 2. Verify the Application Version value for the servers has been updated to the target software release version. 3. Verify the Status Message indicates success. 4. Verify the Upgrade State of the upgraded servers is Accept or Reject.
12. □	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.
13. □	Procedure Complete.	The multiple servers upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix J.

THIS PROCEDURE HAS BEEN COMPLETED

Appendix K TVOE PLATFORM

This Appendix provides procedures for gracefully shutting down TVOE guests and for upgrading TVOE on a host server that supports one or more DSR virtual guests.

If upgrading a DSR server that is deployed as a virtual guest of the TVOE host software, then TVOE itself may have to be upgraded first. Refer to Appendix E to determine if a TVOE upgrade is required.

If the server being upgraded is not virtualized, then this Appendix does not apply.

Appendix K.1 TVOE Upgrade

This procedure is used to upgrade the TVOE host of DSR VM guests. The guests of the host must be shutdown prior to executing this procedure.

CAUTION	**CAUTION: UPGRADE OF THE TVOE HOST CREATES A SNAPSHOT OF THE LOGICAL VOLUMES (LV) PRESENT ON THE DISK. THIS SNAPSHOT IS REQUIRED IN CASE OF "BACKOUT" TO THE PREVIOUS RELEASE.**

CAUTION	**CAUTION: UPGRADING THE TVOE SHUTS DOWN ALL GUESTS OPERATING IN THE TVOE ENVIRONMENT. ADVANCE PLANNING IS REQUIRED TO ENSURE TRAFFIC PROCESSING IS NOT ADVERSELY AFFECTED.**

Be aware that snapshot corruption can occur if large scale changes (such as the deletion or addition of an ISO image) are made on the TVOE host prior to the Upgrade Accept.

Procedure 64: Upgrade TVOE Platform

STEP #	This procedure upgrades TVOE. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1 □	Upgrade TVOE	Upgrade TVOE using the "PM&C Aided TVOE Upgrade Procedure" from Reference [3]. [If the "PM&C Aided TVOE Upgrade" procedure is not possible, it is also possible to upgrade TVOE using the alternate procedure provided in Reference [3].] Note: when Reference [3] direct the shutdown of the guest VMs, return to this document and execute **Error! Reference source not found.**, then return to Reference [3]. **NOTE: If the Active NOAM is hosted on the TVOE server which is being upgraded, VIP may be lost until TVOE is successfully upgraded.**

<table>
<tr>
<td>2
□</td>
<td>

<u>**TVOE Host CLI**</u>

Set the tuned profile

For VEDSR only

</td>
<td>

This step is applicable to the VEDSR configuration only. For all other configurations, continue to step 3.

If the TVOE being upgraded hosts a VEDSR component, set the tuned profile on the upgraded TVOE Host

1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the TVOE Host

```
ssh admusr@<TVOE host>
password:  <enter password>
```

(Answer ‘yes’ if you are prompted to confirm the identity of the server.)

2. Check the currently active tuned profile with the `tuned-adm` command. If the active profile is `tvoe_profile`, proceed to the next step. Otherwise, continue with this step to set the tuned profile.

```
$ sudo tuned-adm active
Current active profile: tvoe_profile
Service tuned: enabled, running
Service ktune: enabled, running
```

3. Enter the following command to set the tuned profile:

```
$ sudo tuned-adm profile tvoe_profile
```

```
[Sample output]
Calling '/etc/ktune.d/tunedadm.sh stop':  [  OK  ]
Reverting to cfq elevator: dm-0 dm-1 dm-10 dm-11 dm-12 dm-
1[  OK  ]dm-15 dm-16 dm-17 dm-18 dm-19 dm-2 dm-20 dm-21
dm-22 dm-23 dm-24 dm-25 dm-26 dm-27 dm-28 dm-29 dm-3 dm-30
dm-4 dm-5 dm-6 dm-7 dm-8 dm-9 sda sdb
Stopping tuned:   [  OK  ]
Switching to profile 'tvoe_profile'
Applying deadline elevator: dm-0 dm-1 dm-10 dm-11 dm-12
dm-[  OK  ] dm-15 dm-16 dm-17 dm-18 dm-19 dm-2 dm-20 dm-21
dm-22 dm-23 dm-24 dm-25 dm-26 dm-27 dm-28 dm-29 dm-3 dm-30
dm-4 dm-5 dm-6 dm-7 dm-8 dm-9 sda sdb
Applying ktune sysctl settings:
/etc/ktune.d/tunedadm.conf: [  OK  ]
Calling '/etc/ktune.d/tunedadm.sh start': [  OK  ]
Applying sysctl settings from /etc/sysctl.conf
Starting tuned:    [  OK  ]
```

4. Verify the `tvoe_profile` is active

```
$ sudo tuned-adm active
Current active profile: tvoe_profile
Service tuned: enabled, running
Service ktune: enabled, running
```

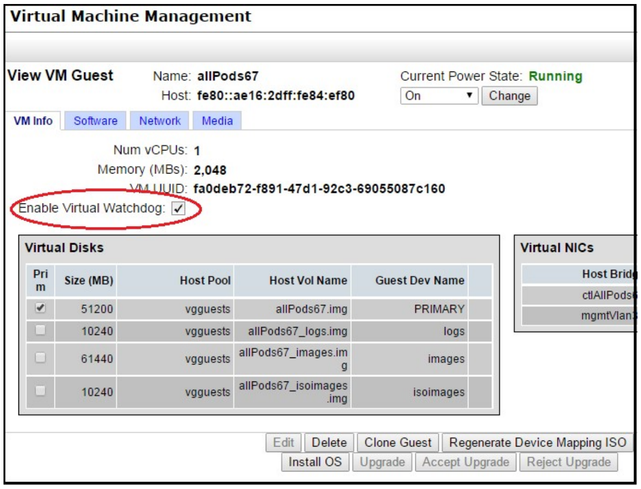
</td>
</tr>
<tr>
<td>3
□</td>
<td>After completed …</td>
<td>

After the TVOE upgrade is completed on the Host Server, the Application(s) may not be started automatically.

Proceed with the next step to restore service.

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

4 □	**PM&C GUI:** Restart guest VMs	Restart the guest VMs following the TVOE upgrade. 1. Log into the PM&C GUI by navigating to http://<pmac_management_ip> 2. Select **Main Menu > VM Management.** The VM Management screen is displayed. 3. Display the TVOE guest VMs by expanding the TVOE host that is to be upgraded. 4. Select a guest VM of the TVOE to be upgraded. 5. If the 'Enable Virtual Watchdog' checkbox is not checked, a. Click the **Edit** button, b. Check the **Enable Virtual Watchdog** checkbox. c. Click 'Save'.



Virtual Machine Management

View VM Guest

Name: allPods67

Host: fe80::ae16:2dff:fe84:ef80

Current Power State: Running

On ▾ Change

Num vCPUs: 1

Memory (MBs): 2,048

VM UUID: fa0deb72-f891-47d1-92c3-69055087c160

Enable Virtual Watchdog: ☑

Virtual Disks

Prim	Size (MB)	Host Pool	Host Vol Name	Guest Dev Name
☑	51200	vgguests	allPods67.img	PRIMARY
□	10240	vgguests	allPods67_logs.img	logs
□	61440	vgguests	allPods67_images.img	images
□	10240	vgguests	allPods67_isoimages.img	isoimages

Virtual NICs

Host Brid
ctlAllPods6
mgmtVlan3

1. Change the power state of the guest VM from **Shutdown** to **On** and click the **'Change'** button. Confirm the pop-up and wait for the power state to change to **Running**. This may take a few moments as guest VM reboots.

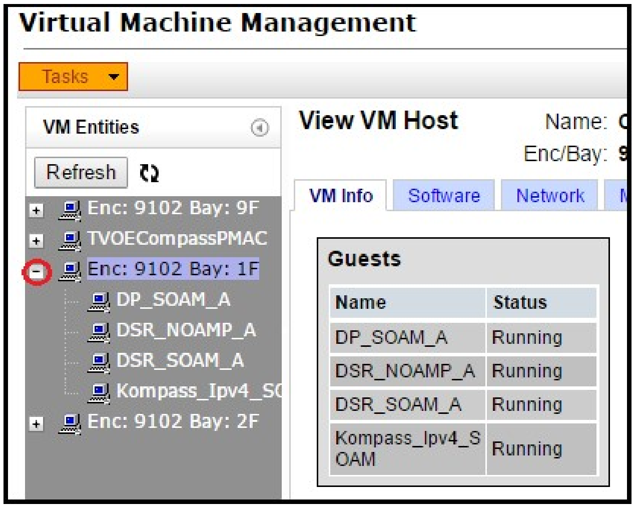
5 □	**Active DSR NOAM VIP:** Enable DSR applications	Enable the DSR applications running on upgraded TVOE 1. Log into the DSR NOAM GUI using the VIP 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Select all the applications running on upgraded TVOE, excluding the server which is in upgrade 'Ready' state. The Upgrade State can be verified from the Administration > Upgrade screen. 4. Click the '**Restart**' button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the '**Appl State**' for all the selected servers is changed to '**Enabled**'.
6 □	**Active SDS NOAM VIP:** Enable SDS applications	Enable the SDS applications running on upgraded TVOE. 1. Log into the SDS NOAM GUI using the VIP 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Select all the applications running on upgraded TVOE, excluding the server which is in upgrade 'Ready' state. The Upgrade State can be verified from the Administration > Upgrade screen. 4. Click the '**Restart**' button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the '**Appl State**' for all the selected servers is changed to '**Enabled**'.

THIS PROCEDURE HAS BEEN COMPLETED.

Appendix K.2 TVOE Guest Shutdown

This procedure gracefully shuts down the guest VMs of a TVOE host. This procedure is required to be performed prior to upgrading the host TVOE.

Procedure 65: Shutdown TVOE Guests

S T E P #	This procedure upgrades TVOE. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1 □	**<u>PM&C GUI:</u>** Display TVOE guest VMs	Display guest VMs of the TVOE to be upgraded. 1. Log into the PM&C GUI by navigating to http://<pmac_management_ip> 2. Select **Main Menu > VM Management.** The VM Management screen is displayed. 3. Display the TVOE guest VMs by expanding the TVOE host to be upgraded.  Virtual Machine Management Tasks VM Entities Refresh Enc: 9102 Bay: 9F TVOECompassPMAC Enc: 9102 Bay: 1F DP_SOAM_A DSR_NOAMP_A DSR_SOAM_A Kompass_Ipv4_SC Enc: 9102 Bay: 2F View VM Host Name: C Enc/Bay: 9 VM Info Software Network M Guests Name Status DP_SOAM_A Running DSR_NOAMP_A Running DSR_SOAM_A Running Kompass_Ipv4_SOAM Running
2 □	**<u>Active DSR NOAM VIP:</u>** Disable DSR applications	If any DSR applications are guest VMs of the TVOE to be upgraded (as shown in step 1), disable all applications running on the current TVOE. 1. Log into the DSR NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Select the virtual servers that are running on the TVOE environment to be upgraded, as identified in step 1. 4. Click the '**Stop**' button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. Verify that the 'Appl State' for all the selected servers is changed to '**Disabled**'.

Procedure 65: Shutdown TVOE Guests

3 □

Active SDS NOAM VIP:

Disable SDS applications

For VEDSR only

This step is applicable to the VEDSR configuration only.

If any SDS applications are guest VMs of the TVOE to be upgraded (as shown in step 1), coordinate with the SDS team to shutdown the SDS applications.

1. Log into the SDS NOAM GUI using the VIP.
2. Select **Status & Manage > Server.**
   The Server Status screen is displayed
3. Select the virtual servers that are running on the TVOE environment to be upgraded, as identified in step 1.
4. Click the ‘**Stop**’ button.
5. Confirm the operation by clicking **Ok** in the popup dialog box.
6. Verify that the ‘Appl State’ for all the selected servers is changed to ‘**Disabled**’.

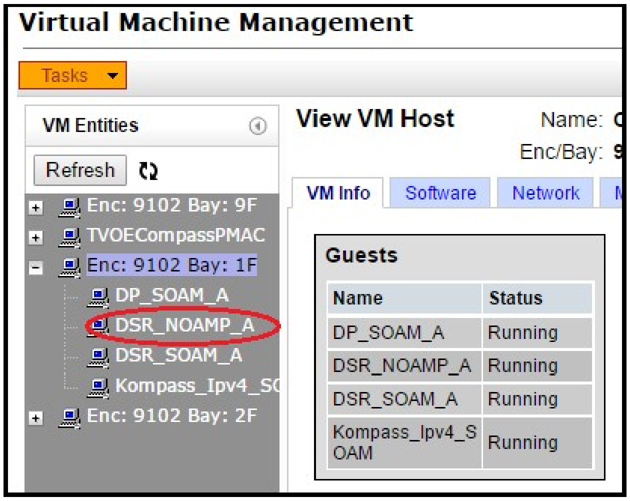
4 □

PM&C GUI:

Shutdown guest VMs

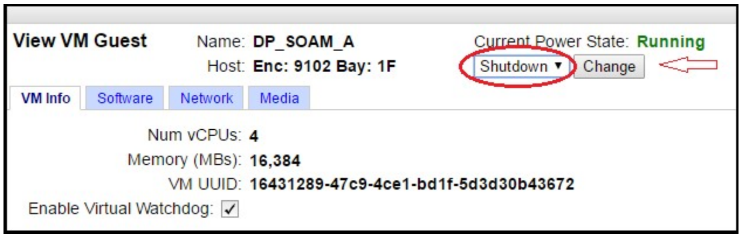
Shutdown TVOE guest VMs.

1. On the PM&C Virtual Machine Management screen, select a guest VM of the TVOE to be upgraded.



Name	Status
DP_SOAM_A	Running
DSR_NOAMP_A	Running
DSR_SOAM_A	Running
Kompass_Ipv4_SOAM	Running

2. Change the power state of the guest VM from **Running** to **Shutdown** and click the **’Change’** button. Confirm the pop-up and wait for the power state to change to Shutdown. This may take a few moments as this executes a graceful shutdown of the guest VM.



Name: **DP_SOAM_A**
Host: **Enc: 9102 Bay: 1F**
Current Power State: **Running**

Num vCPUs: **4**
Memory (MBs): **16,384**
VM UUID: **16431289-47c9-4ce1-bd1f-5d3d30b43672**
Enable Virtual Watchdog: ☑

3. Verify the **Current Power State** changes to **‘Shut Down’**.

4. Repeat sub-steps 1 thru 3 for each guest VM shown in step 1.

THIS PROCEDURE HAS BEEN COMPLETED.

Appendix L 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 will automatically restore the configuration data from the Oracle database.

Table 25 shows the elapsed time estimates for IDIH upgrade.

Table 25. IDIH Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 66	1:15-1:45	1:15-1:45	Oracle Guest Upgrade	None
Procedure 67	0:30-0:45	1:45-2:30	Non-VEDSR Mediation and Application Guest	None
Procedure 68	0:30-0:45	1:45-2:30	VEDSR Mediation and Application Guest Upgrade	None

Appendix L.1 Oracle Guest Upgrade

The Oracle Guest is upgraded first.

Note: When attempting to repeat an upgrade following a backout, it is not necessary to upgrade the Oracle Guest if the source release is 7.1 or later. The Oracle Guest is backed out only if the source release is 7.0 or earlier.

Procedure 66: 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.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**

1 □

IDIH CLI

Perform a system health check on the Oracle guest

Perform a system health check.

1. Login in to the Oracle guest as the admusr user.

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

2. 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
```

Procedure 66: Oracle Guest Upgrade

		`:`
		`:`
		`13:25:02: All tests passed!`
		`13:25:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 0`
		
		`If the output indicates the following error, ignore the error and continue the upgrade. This error indicates that the target release and the running release are the same.`
		
		`00:47:29: Checking runlevel`
		`00:47:29: >>> Error: Runlevel value "3 4" is different from "N 4"`
		
		If the output indicates any other failure failure, do not proceed with the upgrade. It is recommended to contact MOS for guidance.

2 □	**IDIH CLI** Shutdown Mediation and Application guests	Shutdown the Mediation and Application guests. 1. Shutdown the Mediation guest by logging in as admusr and running. `$ sudo init 0` 2. Shutdown the Application guest by logging in as admusr and running. `$ 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 □	**PM&C GUI** Start the upgrade of the Oracle guest via the PM&C GUI.	Initate the Oracle Guest upgrade 1. Navigate to the PM&C **VM Management** menu. 2. Select the Oracle guest, and click the **Upgrade** button. 3. On the **Select Image** screen, select the target image from the list of available images. 4. Click the **Start Software Upgrade** button to initate the upgrade.
4 □	**PM&C GUI** Using the PM&C GUI, monitor the upgrade until it finishes.	Navigate to the **Task Monitoring** menu and wait until the upgrade task finishes. When it finishes, the status will be either **Success** or **Failed**. If the upgrade fails, do not proceed with the upgrade. It is recommended to contact MOS for guidance.

5
□
	IDIH CLI
	Perform a system health check on the Oracle guest
		Wait a few minute 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)`

THIS PROCEDURE HAS BEEN COMPLETED

Appendix L.2 Upgrade the Mediation and Application Guests

The Mediation and Application Guest upgrade is similar to the installation procedure. The procedure varies slightly for VEDSR systems so a separate procedure is provided for that configuration.
For non-VEDSR systems, execute Procedure 67 to upgrade the Mediation and Application guests.

Procedure 68 is used to upgrade the Mediation and Application guests for VEDSR systems.

Appendix L.2.1 Non-VEDSR Mediation and Application Guest Upgrade

This procedure updates the Mediation and Application guests in a non-VEDSR system.

Procedure 67: Non-VEDSR Mediation and Application Guest Upgrade

STEP #	This procedure performs the IDIH Mediation and Application server upgrade for a non-VEDSR system. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**	

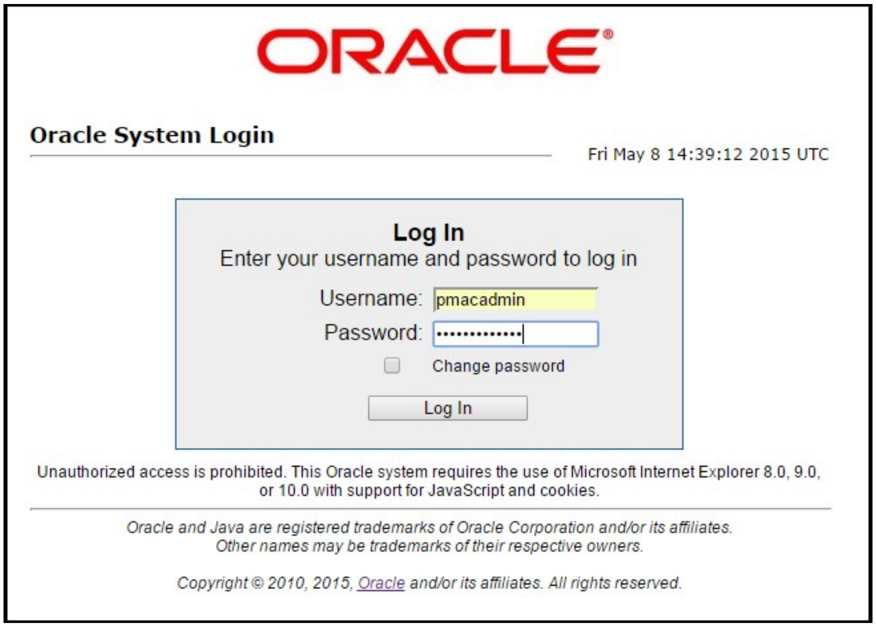
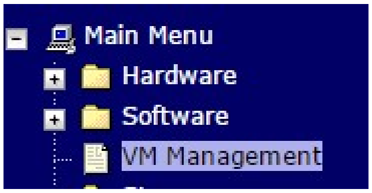
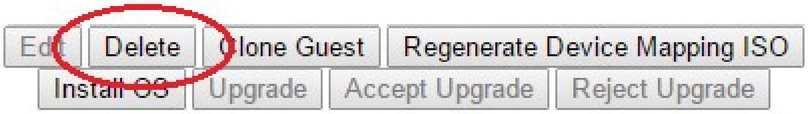
1
□
	PM&C CLI:
	Login to the PM&C server
		Login in to the PM&C server as the admusr user.
		`ssh <PM&C IP address>`
		`login as:    admusr`
		`password:    <enter password>`

2 □	**PM&C CLI:** Save existing fdc.cfg file	If an fdc.cfg file exists in `/var/TKLC/smac/guest-dropin`, rename the file to ‘`fdc.cfg-old`’. The contents of the file will be referenced in step 4 below.
3 □	**PM&C CLI:** Copy the fdc.cfg file to the guest	Copy the fdc.cfg file to the pmac guest-dropin directory using the command: `> sudo cp /usr/TKLC/smac/html/TPD/mediation-*/fdc.cfg /var/TKLC/smac/guest-dropin`
4 □	**PM&C CLI:** Configure the fdc.cfg file	Edit the fdc.cfg file for the Mediation and Application guest installation. See Appendix Q for a breakdown of the fdc.cfg file parameters. Update the software versions, hostnames, bond interfaces, network addresses, and network vlan information for the Mediation and Application guests being installed. The old fdc.cfg file saved in step 2 can be used as a reference for obtaining the hostnames, bond interfaces, network addresses, and network vlan information. Do not copy the software versions from the old fdc.cfg file.

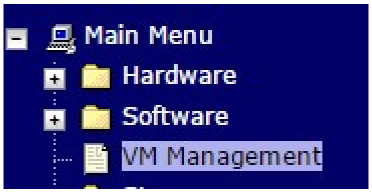
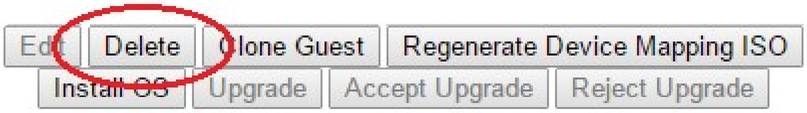
5
□
	PM&C CLI:
	Run the FDC creation script
		Run the FDC creation script using the config file created in step 4.
		`$ cd /var/TKLC/smac/guest-dropin`
		`$ /usr/TKLC/smac/html/TPD/mediation- x.x.x.x.x_x.x.x -x86_64/fdc.sh  fdc.cfg`
		Note: Rename the fdc.cfg file as desired. Also note that two files are generated by the fdc shell script. One is for the Installation procedure and the other file is used for the upgrade procedure. The upgrade FDC is named upgrade.

6 □	**PM&C CLI:** Reset the guest creation timeout	Enter the following command to reset the guest creation timeout value. `$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=3000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"';`

Procedure 67: Non-VEDSR Mediation and Application Guest Upgrade

S T E P #	This procedure performs the IDIH Mediation and Application server upgrade for a non-VEDSR system. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**	
7 □	**PM&C GUI** Login to PM&C	1. Using a web browser, navigate to: `<pmac ip address>` 2. Login as **pmacadmin** user  Oracle System Login Fri May 8 14:39:12 2015 UTC Log In Enter your username and password to log in Username: pmacadmin Password: ••••••••••••• ☐ Change password Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.*
8 □	**PM&C GUI** Remove existing Application Server	1. Navigate to **Main Menu > VM Management**  2. Select the Application guest 3. Click the Delete button  Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade Accept Upgrade Reject Upgrade

Procedure 67: Non-VEDSR Mediation and Application Guest Upgrade

STEP #	This procedure performs the IDIH Mediation and Application server upgrade for a non-VEDSR system. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>**	
9 □	**<u>PM&C GUI</u>** Remove existing Mediation Server	1. Navigate to **Main Menu > VM Management**  2. Select the Mediation guest 3. Click the Delete button  Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade Accept Upgrade Reject Upgrade

10
□
	<u>PM&C CLI</u>
	Establish SSH session and login
		Use an SSH client to connect to the PM&C:
		`ssh <PM&C IP address>`
		`login as:     admusr`
		`password:     <enter password>`

11 □	**<u>PM&C CLI</u>** Reinstall the Mediation and Application servers	**CAUTION** **The "upgrade" config file must be used in the following command, or the database will be destroyed, and all database data will be lost.** Execute the following command, using the upgrade file: `sudo fdconfig config --file=hostname-upgrade_xx-xx-xx.xml`
12 □	**<u>PM&C GUI</u>** Monitor installation	From the PM&C GUI, monitor the IDIH installation on the Task Monitoring page until the installation is complete.
13 □	Reconfiguration	Reconfigure the system NOTE: If upgrading from 6.0 to 7.1 and later, all application server and mediation server configuration will be lost. Follow the site configuration steps to re-configure the system.
	THIS PROCEDURE HAS BEEN COMPLETED	

Appendix L.2.2 VEDSR Mediation and Application Guest Upgrade

This procedure updates the Mediation and Application guests in a VEDSR system. In order to upgrade the guests, the installation fdconfig file is copied and modified before the fdconfig utility is run to recreate the guests.

Procedure 68: VEDSR Mediation and Application Guest Upgrade

S T E P #

This procedure performs the IDIH Mediation and Application server upgrade for a VEDSR system.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE**

1 □

TVOE host CLI

Establish SSH session and login

Use an SSH client to connect to the TVOE host:

```
ssh <TVOE host IP address>
login as:     admusr
password:     <enter password>
```

2 □

TVOE Host:

Note the CPU Pinning allocations

Execute the following commands to allocate CPU sets for EACH (including the PMAC(s)) VM configured:

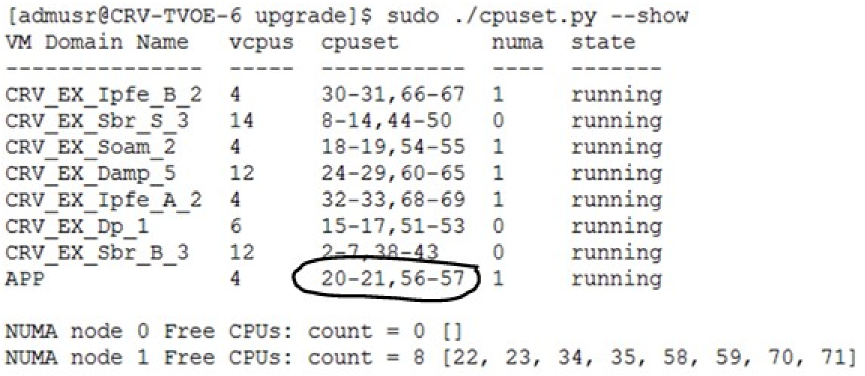
```
$ cd /var/TKLC/upgrade
```

Print the current CPU pinning allocations:

```
$ sudo ./cpuset.py -show
```

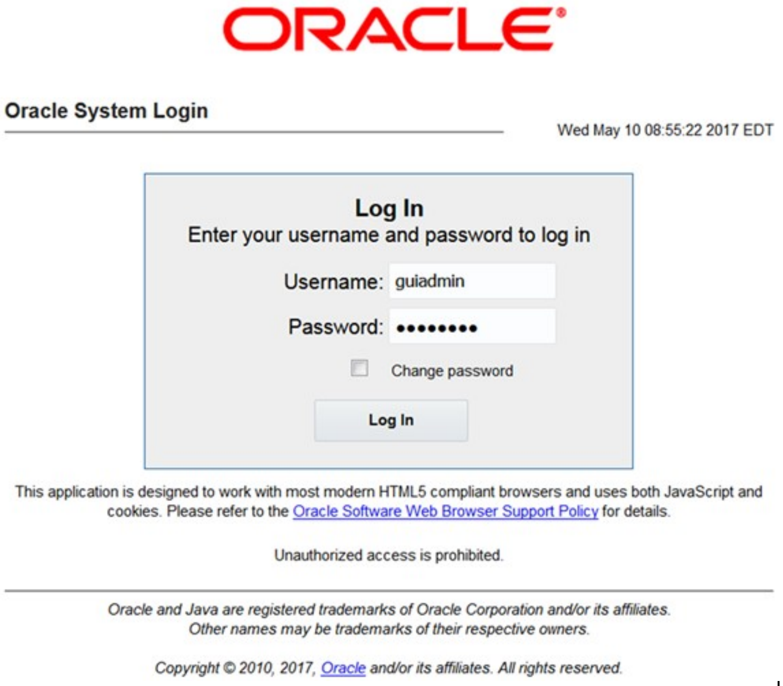
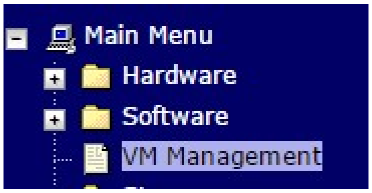
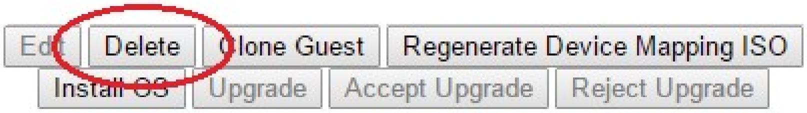
Note down the mapping of cpuset values to Mediation and Application VMs.

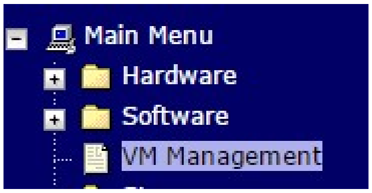
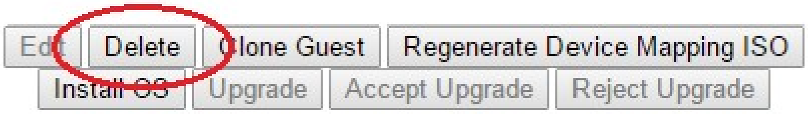
For Example:-



```
[admusr@CRV-TVOE-6 upgrade]$ sudo ./cpuset.py --show
VM Domain Name   vcpus  cpuset       numa  state
---------------  -----  -----------  ----  -------
CRV_EX_Ipfe_B_2  4      30-31,66-67  1     running
CRV_EX_Sbr_S_3   14     8-14,44-50   0     running
CRV_EX_Soam_2    4      18-19,54-55  1     running
CRV_EX_Damp_5    12     24-29,60-65  1     running
CRV_EX_Ipfe_A_2  4      32-33,68-69  1     running
CRV_EX_Dp_1      6      15-17,51-53  0     running
CRV_EX_Sbr_B_3   12     2-7,38-43    0     running
APP              4      20-21,56-57  1     running

NUMA node 0 Free CPUs: count = 0 []
NUMA node 1 Free CPUs: count = 8 [22, 23, 34, 35, 58, 59, 70, 71]
```

3 □	**PM&C GUI** Login to PM&C	1. Using a web browser, navigate to: `<pmac ip address>` 2. Login as **guiadmin** user  ORACLE Oracle System Login Wed May 10 08:55:22 2017 EDT Log In Enter your username and password to log in Username: guiadmin Password: •••••••• □ Change password Log In This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.*
4 □	**PM&C GUI** Remove existing Application Server	1. Navigate to **Main Menu > VM Management**  2. Select the Application guest 3. Click the Delete button  Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade Accept Upgrade Reject Upgrade

5 ☐	**PM&C GUI** Remove existing Mediation Server	1. Navigate to **Main Menu > VM Management**  2. Select the Mediation guest 3. Click the Delete button  Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade Accept Upgrade Reject Upgrade

6
☐
	PM&C CLI
	Establish SSH session and login
		Use an SSH client to connect to the PM&C:
		`ssh <PM&C IP address>`
		`login as:     admusr`
		`password:     <enter password>`

7
☐
	PM&C CLI
	Create upgrade fdconfig file
		An upgrade configuration file is created by copying the installation config file, and modifying the copy to support upgrade.
		1. Navigate to `/var/TKLC/smac/guest-dropin`
		`$ cd /var/TKLC/smac/guest-dropin`
		2. Copy the installation config file to an upgrade config file.
		`$ sudo cp <hostname>_xx-xx-xx.xml <hostname>-upgrade_xx-xx-xx.xml`
		where `<hostname>_xx-xx-xx.xml` is the config file used during installation.
		Note: it is recommended to name the upgrade config file using the pattern specified above.
		If the upgrade Config file was created from the installation Config file above, proceed to step 7; otherwise, **if the installation config file does not exist in `/var/TKLC/smac/guest-dropin`, perform step 6 to create the upgrade file from a template.**

8 ☐	**PM&C CLI:** Create upgrade fdconfig file from a template	Create an upgrade configuration file from a template. 1. Copy the installation config template to an upgrade config file. `$ sudo cp /usr/TKLC/smac/html/TPD/mediation-x.x.x.0.0_x.x.x-x86_64/vedsr_idih_upgrade.xml.template ./<hostname>-upgrade_dd-mm-yy.xml` 2. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests to be upgraded. Refer to Appendix Q for a breakdown of the config file parameters.
9 ☐	**PM&C CLI:** Reset the guest creation timeout	Enter the following command to reset the guest creation timeout value. `$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=3000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"';`

10 □

PM&C CLI

Modify the upgrade config file

The Oracle guest stanza must be removed from the newly created upgrade config file. Failure to do so will cause the Oracle guest server to be re-installed.

1. Edit the upgrade config file and locate the Oracle guest stanza. The sections to be removed are highlighted in the config file excerpt shown below:

```
  <!--REMOVE_FOR_DR_START  (DO NOT remove this line! )-->
           <!--Oracle Guest Configuration-->
           <tvoeguest id="ORA">
                   <infrastructure>PMAC</infrastructure>
                   <tvoehost>mgmtsrvrtvoe</tvoehost>
                   <!--Oracle Guest Profile: Update if hardware is
Gen6 default is Gen8-->
                   <!--profile>ORA_GEN6</profile-->
                   <profile>ORA_GEN8</profile>

                •

                •
                       <postdeploy>
                           <scriptfile id="oraHealthcheck">
                           <filename>/usr/bin/sudo</filename>
                           <arguments>/usr/TKLC/xIH/plat/bin/ana...
                           </scriptfile>
                           </postdeploy>
                   </scripts>
           </tvoeguest>
   <!--REMOVE_FOR_DR_END (DO NOT remove this line! )-->
```

2. In the `<infrastructures>` section of the upgrade config file, update the “**tpd**”, “**ora**”, “**med**”, and “**app**” release numbers to reflect the target release.

   Config file excerpt. Update the highlighted values.

```
    <image id="tvoe">
        <name>TVOE-3.0.2.0.0_86.28.0-x86_64</name>
    </image>
```

11 □

PM&C CLI

Reinstall the Mediation and Application servers

CAUTION

The “upgrade” config file must be used in the following command, or the database will be destroyed, and all database data will be lost.

Execute the following command, using the upgrade file:

```
    sudo fdconfig config --file=hostname-upgrade_xx-xx-
    xx.xml
```

12 □

PM&C GUI

Monitor installation

From the PM&C GUI, monitor the IDIH installation on the Task Monitoring page until the installation is complete.

13 □

TVOE Host:

Execute the CPU Pinning script

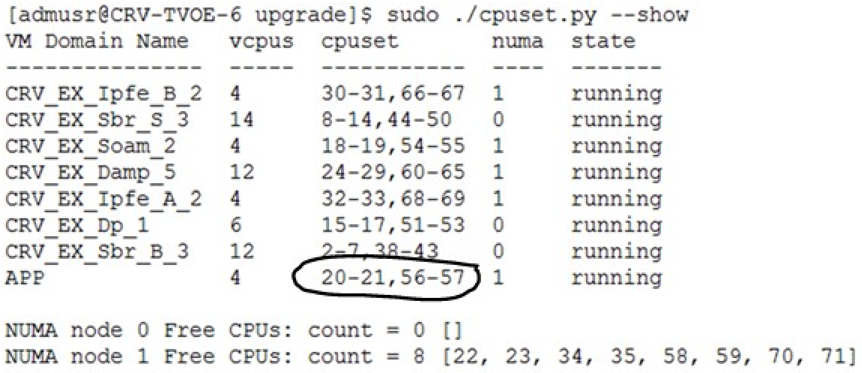
Establish an SSH session to the TVOE Host, login as admusr.

Print the current CPU pinning allocations:

```
$ cd /var/TKLC/upgrade
```

```
$ sudo ./cpuset.py --show
```

For Example:-



```
[admusr@CRV-TVOE-6 upgrade]$ sudo ./cpuset.py --show
VM Domain Name   vcpus  cpuset       numa  state
---------------  -----  -----------  ----  -------
CRV_EX_Ipfe_B_2  4      30-31,66-67  1     running
CRV_EX_Sbr_S_3   14     8-14,44-50   0     running
CRV_EX_Soam_2    4      18-19,54-55  1     running
CRV_EX_Damp_5    12     24-29,60-65  1     running
CRV_EX_Ipfe_A_2  4      32-33,68-69  1     running
CRV_EX_Dp_1      6      15-17,51-53  0     running
CRV_EX_Sbr_B_3   12     2-7,38-43    0     running
APP              4      20-21,56-57  1     running

NUMA node 0 Free CPUs: count = 0 []
NUMA node 1 Free CPUs: count = 8 [22, 23, 34, 35, 58, 59, 70, 71]
```

If we **DO NOT** see “None” for either cpuset or numa (or both), we first clear the pinning for those VMs using following command:

```
[admusr@CRV-TVOE-6 upgrade ~]$ sudo ./cpuset.py --clear=APP
Successful. Domain APP must be restarted for changes to take
affect
```

Have the mapping of the VMs to cpuset ready which was determined from **step 2** above.

Execute the following to allocate CPU pinning on EACH VM according to the mapping:

```
$ sudo ./cpuset.py --set=<VM Name> --cpuset=<cpuset>

Example:-

[admusr@CRV-TVOE-6 upgrade ~]$ sudo ./cpuset.py --set=APP –
cpuset=20-21,56-57
Successful. Domain APP must be restarted for changes to take
affect
```

Note: Execute the CPU pinning script for both the application and mediation server VMs.

14 □

TVOE Host:

Restart the VMs or TVOE host

Restart the VMs for which the pinning has been assigned or modified using below command:

```
[admusr@CRV-TVOE-6 ~]$ sudo virsh shutdown <VM Name>
[admusr@CRV-TVOE-6 ~]$ sudo virsh start <VM Name>
```

Alternately, we can restart the entire TVOE sever using below command:

```
$ sudo init 6
```

15 □

TVOE Host:

Verify CPU Pinning

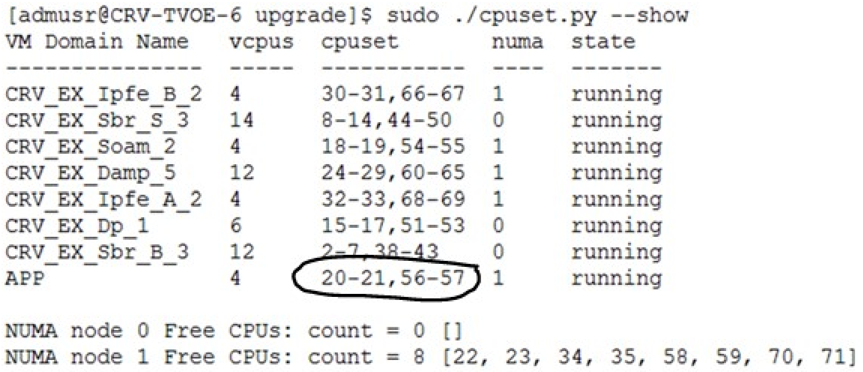
Once the TVOE host is restarted, establish an SSH session to the TVOE Host, login as ***admusr***.

Verify the CPU pinning is allocated as set in **step 11** by executing the following commands:

```
$ cd /var/TKLC/upgrade
```

Print the newly allocated CPU pinning allocations and cross check with the mapping:

For Example:-



```
[admusr@CRV-TVOE-6 upgrade]$ sudo ./cpuset.py --show
VM Domain Name    vcpus  cpuset        numa  state
---------------   -----  -----------   ----  -------
CRV_EX_Ipfe_B_2   4      30-31,66-67   1     running
CRV_EX_Sbr_S_3    14     8-14,44-50    0     running
CRV_EX_Soam_2     4      18-19,54-55   1     running
CRV_EX_Damp_5     12     24-29,60-65   1     running
CRV_EX_Ipfe_A_2   4      32-33,68-69   1     running
CRV_EX_Dp_1       6      15-17,51-53   0     running
CRV_EX_Sbr_B_3    12     2-7,38-43     0     running
APP               4      20-21,56-57   1     running

NUMA node 0 Free CPUs: count = 0 []
NUMA node 1 Free CPUs: count = 8 [22, 23, 34, 35, 58, 59, 70, 71]
```

16 □

Repeat for Each TVOE HOST

Repeat this procedure for each TVOE host.

THIS PROCEDURE HAS BEEN COMPLETED

Appendix M 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 MOS or by other procedures within this document.

Appendix M.1 Alternate Pre-Upgrade Backup

This procedure is an alternative to the normal pre-upgrade backup provided in Procedure 24. It is recommended that this procedure be executed only under the direction of MOS.

Procedure 69: Alternate Pre-Upgrade Backup

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE 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>`
2. □	**Active SOAM CLI:** Start a screen session.	Enter the following commands: **`# screen`** (The screen tool will create a no-hang-up shell session, so that the command will continue 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 will remotely access each specified server, and run 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 will result 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 will be 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 will indicate successful completion:

Procedure 69: Alternate Pre-Upgrade Backup

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>**	

		`Script Completed. Status:`
		`HOSTNAME                         | STATUS`
		`--------------------------------------------`
		`HPC3blade02                      | PASS`
		`HPC3blade01                      | PASS`
		`HPC3blade03                      | PASS`
		`HPC3blade04                      | PASS`
		(Errors will also report back to the command line.)
		NOTE: There is no progress indication for this command; only the final report when it completes.

4.
□
	<u>Active SOAM CLI:</u>
	Exit the screen session.
		`# exit`
		`[screen is terminating]`
		NOTE: "screen -ls" is used to show active screen sessions on a server, and "screen -dr" is used to re-enter a disconnected screen session.

5.
□
	ALTERNATIVE METHOD (Optional)
	<u>Server CLI:</u>
	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 will indicate 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.
□
	<u>Active NOAM VIP:</u>
	Verify that backup files are present on each server.
		1. Log into the Active NOAM GUI using the VIP.
		2. Select **Status & Manage > Files**
		The **Files** menu is displayed
		3. Click on each server tab, in turn
		4. For each server, verify that 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.

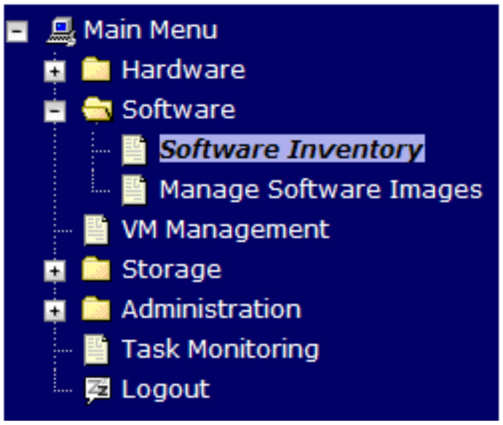
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix M.2 Server Upgrade Using PM&C

This appendix provides the procedure for upgrading the Standby NOAM and DR-NOAM using the PM&C interface. This upgrade method is an alternative to using the NOAM Upgrade GUI, and is used only when the NOAM Upgrade GUI refresh is sluggish due to the large number of C-level servers.

NOTE: Before executing this procedure, download the target release ISO to the PM&C image repository in accordance with Appendix F.

Procedure 70: Alternate Server Upgrade using PM&C

STEP #	This procedure performs an upgrade of one or more servers using the PM&C interface instead of the more typical NOAM Upgrade GUI. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 □	**PM&C GUI:** Login	1. If needed, open a web browser and enter: `http://<pmac_management_ip>` 2. Login as the pmacadmin user.
2 □	**PM&C GUI:** Navigate to Software Inventory	1. Navigate to **Main Menu > Software > Software Inventory**.  Main Menu Hardware Software Software Inventory Manage Software Images VM Management Storage Administration Task Monitoring Logout

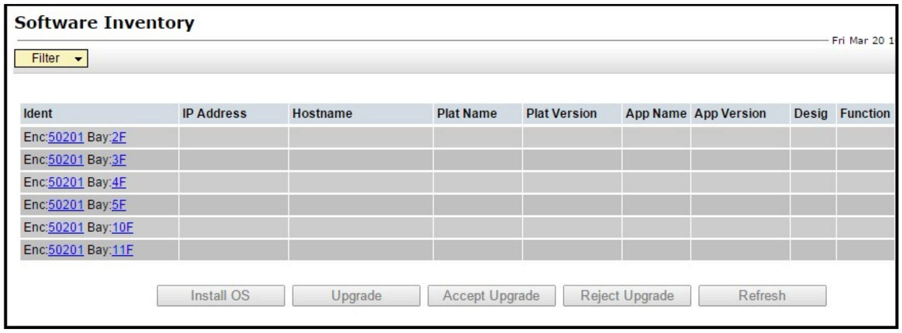
Procedure 70: Alternate Server Upgrade using PM&C

3 □

PM&C GUI:

Select server to be upgraded

1. Select the server(s) to be upgraded. If upgrading more than one server at a time, select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in green.



Software Inventory

Fri Mar 20 1

Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Desig	Function
Enc:50201 Bay:2F								
Enc:50201 Bay:3F								
Enc:50201 Bay:4F								
Enc:50201 Bay:5F								
Enc:50201 Bay:10F								
Enc:50201 Bay:11F								

2. Press the **Upgrade** button.

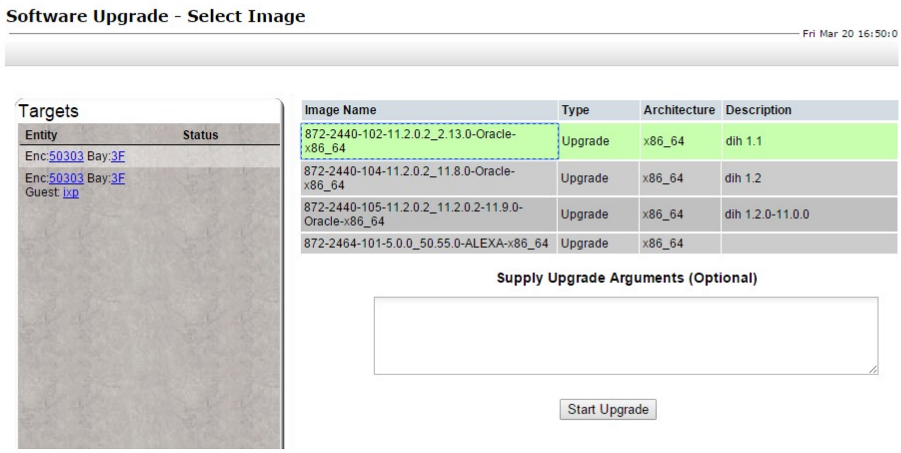
NOTE: Until the target servers are fully discovered by PM&C, the user will be unable to start an upgrade on the servers. A server that has not yet been discovered is represented by an empty row on the Software Inventory page (no IP address, hostname, plat name, plat version, etc. is displayed).

4 □

PM&C GUI:

Select the target release ISO

1. The left side of the screen displays the servers to be upgraded. From the list of upgrade images on the right side of the screen, select the image to install on the selected servers.



Software Upgrade - Select Image

Fri Mar 20 16:50:0

Targets

Entity	Status
Enc:50303 Bay:3F	
Enc:50303 Bay:3F Guest: ixp	

Image Name	Type	Architecture	Description
872-2440-102-11.2.0.2_2.13.0-Oracle-x86_64	Upgrade	x86_64	dih 1.1
872-2440-104-11.2.0.2_11.8.0-Oracle-x86_64	Upgrade	x86_64	dih 1.2
872-2440-105-11.2.0.2_11.2.0.2-11.9.0-Oracle-x86_64	Upgrade	x86_64	dih 1.2.0-11.0.0
872-2464-101-5.0.0_50.55.0-ALEXA-x86_64	Upgrade	x86_64	

Supply Upgrade Arguments (Optional)

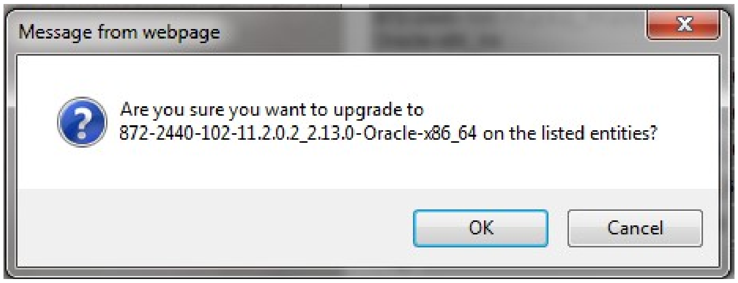
2. Press the **Start Upgrade** button.

5 □

PM&C GUI:

Start the upgrade

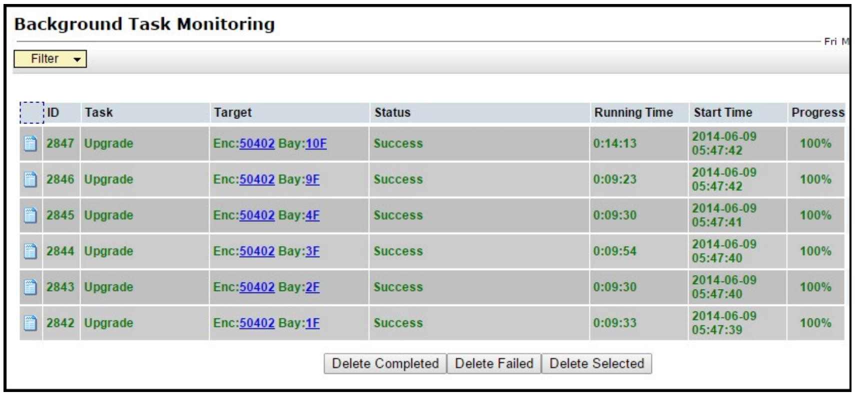
Press the **OK** button to proceed with the upgrade.



Message from webpage

Are you sure you want to upgrade to 872-2440-102-11.2.0.2_2.13.0-Oracle-x86_64 on the listed entities?

Procedure 70: Alternate Server Upgrade using PM&C

<table>
<tr><td>6
□</td><td><b><u>PM&C GUI:</u></b>
Monitor the upgrade</td><td>Navigate to <b>Main Menu > Task Monitoring</b> to monitor the progress of the Upgrade background task. A separate task will appear for each server being upgraded.


Fri M
Filter
Delete Completed
Delete Failed
Delete Selected

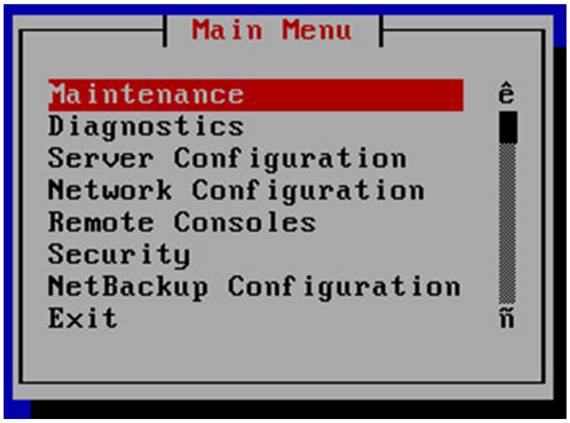
Background Task Monitoring
<table>
<tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td>2847</td><td>Upgrade</td><td>Enc:50402 Bay:10F</td><td>Success</td><td>0:14:13</td><td>2014-06-09 05:47:42</td><td>100%</td></tr>
<tr><td>2846</td><td>Upgrade</td><td>Enc:50402 Bay:9F</td><td>Success</td><td>0:09:23</td><td>2014-06-09 05:47:42</td><td>100%</td></tr>
<tr><td>2845</td><td>Upgrade</td><td>Enc:50402 Bay:4F</td><td>Success</td><td>0:09:30</td><td>2014-06-09 05:47:41</td><td>100%</td></tr>
<tr><td>2844</td><td>Upgrade</td><td>Enc:50402 Bay:3F</td><td>Success</td><td>0:09:54</td><td>2014-06-09 05:47:40</td><td>100%</td></tr>
<tr><td>2843</td><td>Upgrade</td><td>Enc:50402 Bay:2F</td><td>Success</td><td>0:09:30</td><td>2014-06-09 05:47:40</td><td>100%</td></tr>
<tr><td>2842</td><td>Upgrade</td><td>Enc:50402 Bay:1F</td><td>Success</td><td>0:09:33</td><td>2014-06-09 05:47:39</td><td>100%</td></tr>
</table>

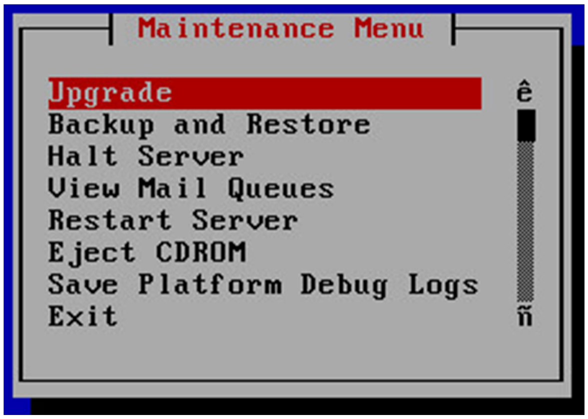
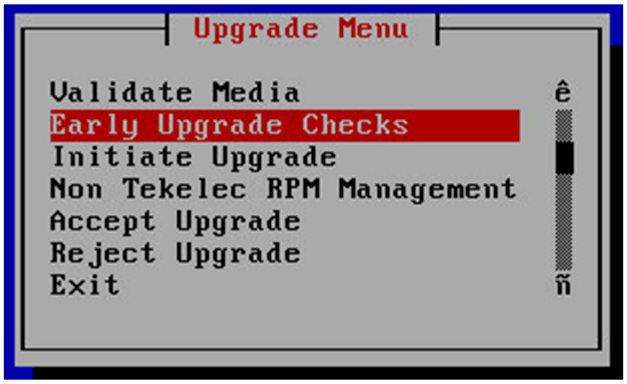
When the task is complete and successful, the text will change to green and the Progress column will indicate "100%".</td></tr>
<tr><td>7
□</td><td>Procedure Complete</td><td>The alternate server upgrade procedure is now complete.
Return to the overall DSR upgrade procedure step that directed the execution of Appendix K.2.</td></tr>
<tr><td colspan="3"><i>THIS PROCEDURE HAS BEEN COMPLETED.</i></td></tr>
</table>

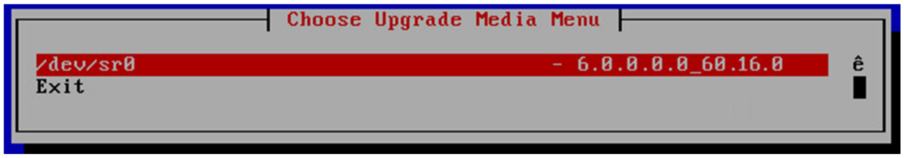
Appendix M.3 Server Upgrade using platcfg

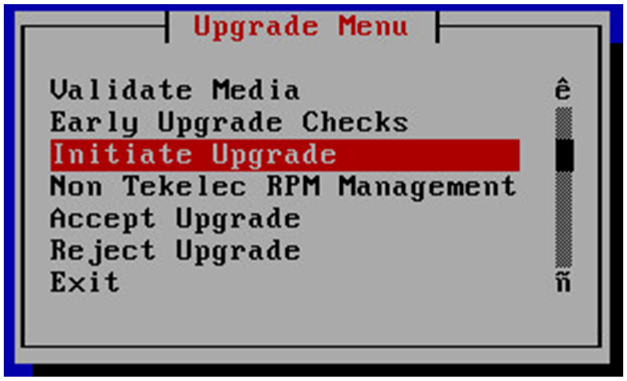
The procedure provided in this appendix enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of MOS.

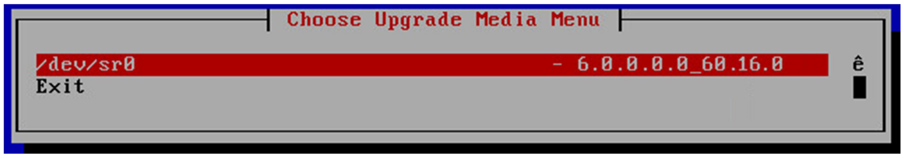
Procedure 71: Server Upgrade using platcfg

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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1 □	**Server CLI:** Login to the server to be upgraded	Log into the server console 1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the server to be upgraded: `ssh admusr@<server_ip>` (Answer 'yes' if prompted to confirm the identity of the server.)
2 □	**Server CLI:** Enter the platcfg menu	Switch to the platcfg user to start the configuration menu. `$ sudo su - platcfg` From the Main Menu, select **`Maintenance`**  Main Menu Maintenance Diagnostics Server Configuration Network Configuration Remote Consoles Security NetBackup Configuration Exit

3 □	**Server CLI:** Select Upgrade	From the Maintenance Menu, select **`Upgrade`**  Maintenance Menu Upgrade Backup and Restore Halt Server View Mail Queues Restart Server Eject CDROM Save Platform Debug Logs Exit
4 □	**Server CLI:** Select Early Upgrade Checks	From the Upgrade Menu, select **`Early Upgrade Checks`**  Upgrade Menu Validate Media Early Upgrade Checks Initiate Upgrade Non Tekelec RPM Management Accept Upgrade Reject Upgrade Exit

5
□
	Server CLI:
	Select the Upgrade Media
		1. From the Choose Upgrade Media Menu, select the desired target media. This will initiate the early upgrade checks in the console window.
		 Choose Upgrade Media Menu
		/dev/sr0 - 6.0.0.0.0_60.16.0
		Exit
		Informational messages will be displayed as the checks progress. At the end of a successful test, a message similar to the following will appear:
		`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!`
		2. Verify early upgrade checks pass. In case of errors, it is recommended to contact MOS.
		3. Press 'q' to exit the screen session and return to the platcfg menu.
		4. From the Choose Upgrade Media Menu, select **`Exit.`**

6 □	**Server CLI:** Initiate the upgrade	From the Upgrade Menu, select `Initiate Upgrade`.  Upgrade Menu Validate Media Early Upgrade Checks Initiate Upgrade Non Tekelec RPM Management Accept Upgrade Reject Upgrade Exit

7
□
	Server CLI:
	Select the Upgrade Media
		The screen will display a message that it is searching for upgrade media. Once the upgrade media is found, an Upgrade Media selection menu will be displayed similar to the example shown below.
		From the Choose Upgrade Media Menu, select the desired target media. This will initiate the server upgrade.
		 Choose Upgrade Media Menu
		/dev/sr0 - 6.0.0.0.0_60.16.0
		Exit
		Many informational messages will come across the terminal screen as the upgrade proceeds.
		Finally, after upgrade is complete, the server will reboot.
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

8 □	**Server CLI:** 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 prompted to confirm the identity of the server.)

9
□
	Server CLI:
	Check for upgrade errors
		Examine the upgrade logs in the directory /var/TKLC/log/upgrade and verify that 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/upgrade.log`
		It is recommended to contact MOS by referring to Appendix S of this document and provide these files.

10
□
	Server CLI:
	Verify the upgrade
		Check the upgrade log for the upgrade complete message
		`grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		Verify that the message "**UPGRADE IS COMPLETE**" is displayed. If not, it is recommended to contact MOS.
		`[admusr@NO2 ~]$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		`1407786220::  UPGRADE IS COMPLETE`

THIS PROCEDURE HAS BEEN COMPLETED.		

Appendix M.4 Manual DA-MP (N+0) Upgrade Procedure

Procedure 72 is used to manually upgrade a multi-active DA-MP Server Group. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 72 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 72 must be executed four distinct times.

Procedure 72: Manual DA-MP (N+0) Upgrade Procedure

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	Identify all the DA-MPs to be upgraded together	From the data captured in Table 5, 1. 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 J : Upgrade Multiple Servers** After successfully completing the procedure in Appendix J, return to this point and continue with the next step.
1. □	Repeat for all servers identified in Step 1 of this procedure.	Repeat step 2 of this procedure for the remaining DA-MP servers.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix M.5 Manual DA-MP (1+1) Upgrade Procedure

Procedure 73 is used to manually upgrade an Active/Standby DA-MP Server Group. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 73: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	Upgrade the standby DA-MP server	Upgrade the Standby DA-MP server using the Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure - DSR 8.x After successfully completing the procedure in **Appendix G**, 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 Appendix G** -- Single Server Upgrade Procedure - DSR 8.x
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix M.6 ASG SBR Upgrade Procedure

Procedure 74 is used to upgrade the SBR server group using Auto Server Group upgrade. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Procedure 74: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	Identify the SBR Server Group(s) to Upgrade	1. 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 will be located at different sites.** 1. 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 J** — Upgrade Multiple Servers Procedure
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.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix M.7 Manual SBR Upgrade Procedure

Procedure 75 is used to upgrade the SBR Server Group manually. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Note: Before upgrading the Active SBR, it is imperative that the database audit of the Spare and Standby servers complete successfully. Failure to comply could result in a loss of session data.

Procedure 75: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. □	**Active NOAM VIP:** Identify the SBR Server Group(s) to Upgrade	Identify the Active, Standby, and Spare SBR servers.

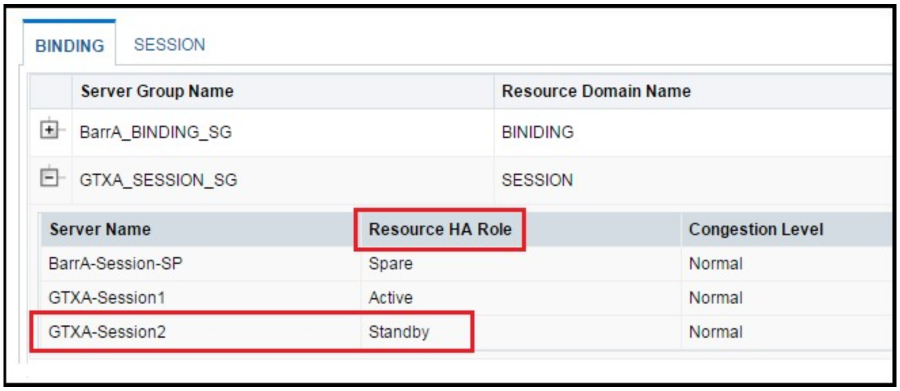
Identify the Active, Standby, and Spare SBR servers.

2. 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.

3. Log into the NOAM GUI using the VIP.

4. 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



	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 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).

Procedure 75: Manual SBR Upgrade Procedure

2. □	**Active NOAM VIP:** Upgrade Spare SBR Server identified in step 1 of this procedure.	**NOTE: The Spare SBRs of this server group will be located at different sites.** 1. Upgrade the Spare SBR server using the Upgrade Single Server procedure : **Execute Appendix G**—Upgrade Single Server Procedure After successfully completing the procedure in Appendix G, return to this point to monitor server status. **From the Active NOAM GUI:** 2. Navigate to **Main Menu > Policy and Charging > Maintenance > SBR Status**. Open the tab of the server group being upgraded. NOTE: After executing Appendix G, the Spare SBR will temporarily disappear from the SBR Status screen. When the server comes back online, it will reappear on the screen with a status of “Out of Service”. 3. Monitor the **Resource HA Role** status of the Spare server. Wait for the status to transition from “Out of Service” to “Spare”. 4. 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 the Upgrade Single Server procedure : **Execute Appendix G -** Upgrade Single Server Procedure After successfully completing the procedure in **Appendix G**, 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**
4. □	**Active NOAM VIP:** Verify Standby SBR server status	1. Navigate to **Main Menu > Policy and Charging >Maintenance > SBR Status.** Open the tab of the server group being upgraded. NOTE: After executing Appendix G, the Standby SBR will temporarily disappear from the SBR Status screen, and the Spare server will assume the Standby role. When the upgraded server comes back online, it will reappear on the screen with a status of “Out of Service”. 2. 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**”.

Procedure 75: Manual SBR Upgrade Procedure

5. □	<u>**Active NOAM VIP:**</u> Verify bulk download completes	Verify that the bulk download from the Active SBR to the Standby and Spare SBRs completes. 1. Navigate to **Main Menu > Alarm & Event > View History** 2. 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. 3. 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 G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, 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.
		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix N EXPIRED PASSWORD WORKAROUND PROCEDURE

This appendix provides the procedures to handle password expiration during upgrade. Procedure 76 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 77 after the site is upgraded. Failure to remove the workaround will inhibit password aging on the server.

Appendix N.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 will expire at that site. It is expected that the workaround will be removed once the site is upgraded.

Procedure 76: Expired Password Workaround Procedure

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.**	

1
□
	<u>Active SOAM CLI:</u>
	SSH to Active SOAM server
		Disable password aging.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		(Answer 'yes' if prompted to confirm the identity of the server.)
		2. Create a text file with the following content (exactly as formatted):
		`[production]`
		`aw.policy.pwchange.isExpired =`
		`aw.policy.db.checkPw =`
		`[development : production]`
		`[test : development]`
		3. Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		4. Change the file permissions:
		`sudo chmod 644 pw.ini`
		5. Execute the following command:
		`clearCache`
		NOTE: For each server on which this workaround is enacted, the old "expired" 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	Repeat step 1 for the Standby SOAM

Procedure 76: Expired Password Workaround Procedure

□	SOAM	
3 □	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix N.2 Enable Password Aging

This procedure removes the password expiration workaround that is enabled by Procedure 76.

Procedure 77: Expired Password Workaround Removal Procedure

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1
□
	Active SOAM CLI:
	SSH to Active SOAM server
		Re-enable password aging.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		(Answer 'yes' if prompted to confirm the identity of the server.)
		2. Delete the pw.ini file:
		`$ sudo rm /var/TKLC/appworks/ini/pw.ini`
		3. Execute the following command:
		`$ sudo clearCache`
		4. Repeat sub-steps 1 through 3 for the Standby SOAM

2 □	Repeat for all non-upgraded sites	Repeat steps 1 for all non-upgraded sites.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix N.3 Password Reset

Procedure 78 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 78: 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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1
□
	Active NOAM CLI:
	SSH to Active NOAM server
		Rest the password.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM:
		`ssh admusr@<NOAM_VIP>`
		(Answer 'yes' if prompted to confirm the identity of the server.)
		2. Execute the reset command:
		`$ sudo /usr/TKLC/appworks/sbin/resetPassword guiadmin`
		3. At the prompt "`Enter new Password for guiadmin: `", enter a new password.
		4. Attempt to login to the NOAM GUI using the new password. If the login is not successful, it is recommended to contact MOS for guidance.

		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix O NETWORK IDIH COMPATIBILITY PROCEDURES

The procedures in this appendix are used to provide IDIH compatibility when upgrading to Release 8.0. Procedure 79 is performed on a Release 8.0 IDIH to make the trace data viewable on prior release IDIH systems, as described in Section 1.7.5. 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 80 must be executed on every IDIH on which Procedure 79 was previously performed.

Procedure 79: Enable IDIH 8.0 Compatibility

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1 □	**Appserver CLI:** Login to the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to login to the appserver: `ssh admusr@<server_ip>` (Answer 'yes' if prompted 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 enable`
4 □	Repeat as needed	Repeat this procedure on each IDIH 8.0 appserver as needed.

Procedure 80: Disable IDIH 8.0 Compatibility

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1 □	**Appserver CLI:** Login to the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to login to the appserver: `ssh admusr@<server_ip>` (Answer 'yes' if prompted to confirm the identity of the server.)

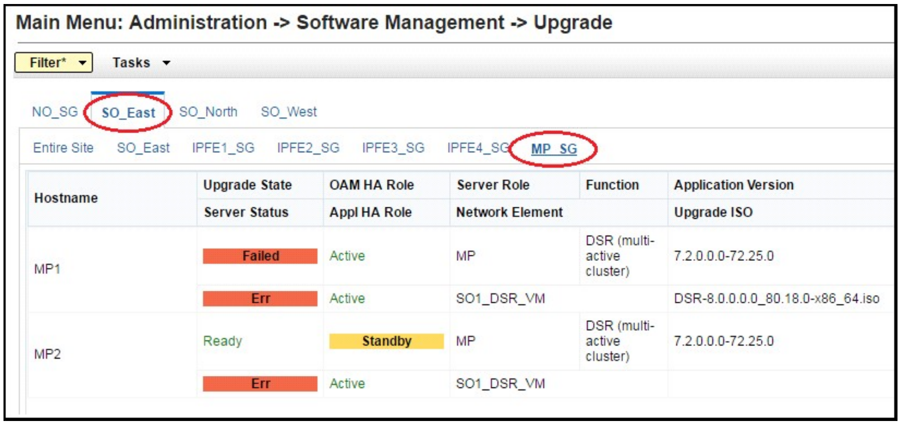
Procedure 80: Disable IDIH 8.0 Compatibility

2 ☐	**<u>Appserver CLI:</u>** Change user	Change to the system user tekelec: `sudo su - tekelec`
3 ☐	**<u>Appserver CLI:</u>** 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 P 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 to contact MOS for guidance while executing this procedure.

Procedure 81: Recovering from a Failed Upgrade

<table>
<tr><td><b>STEP #</b></td><td colspan="2">This procedure provides the basic steps for returning a server to a normal state after an upgrade failure. Note that the server will be 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.
SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED <b>TO CONTACT <u>MOS AND</u> ASK FOR <u>UPGRADE ASSISTANCE</u>.</b></td></tr>
<tr><td><b>1</b>
□</td><td><b><u>Active NOAM VIP:</u></b>
Select affected server group</td><td>From the Upgrade screen, select the server group containing the failed server.


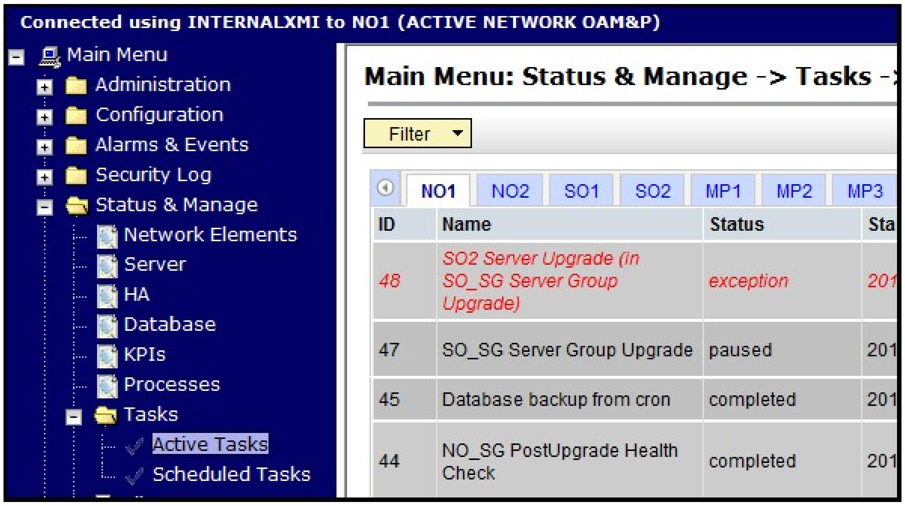
<table>
<tr><th rowspan="2">Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr>
<tr><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr>
<tr><td rowspan="2">MP1</td><td>Failed</td><td>Active</td><td>MP</td><td>DSR (multi-active cluster)</td><td>7.2.0.0.0-72.25.0</td></tr>
<tr><td>Err</td><td>Active</td><td>SO1_DSR_VM</td><td></td><td>DSR-8.0.0.0.0_80.18.0-x86_64.iso</td></tr>
<tr><td rowspan="2">MP2</td><td>Ready</td><td>Standby</td><td>MP</td><td>DSR (multi-active cluster)</td><td>7.2.0.0.0-72.25.0</td></tr>
<tr><td>Err</td><td>Active</td><td>SO1_DSR_VM</td><td></td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td>• <b>If the failed server was upgraded manually, or by using the Auto Site Upgrade feature, then skip to step 7 of this procedure</b>
• <b>If the failed server was upgraded using the Automated Server Group Upgrade option, then continue with step 2 of this procedure.</b></td></tr>
</table>

Procedure 81: Recovering from a Failed Upgrade

<table>
<tr>
<td>2
□</td>
<td><b><u>Active NOAM VIP:</u></b>
View Active Tasks</td>
<td>

Navigate to the Active Tasks screen to view the tasks.

1. Navigate to **Status & Manage > Tasks > Active Tasks**
   The Active Tasks screen is displayed.



Connected using INTERNALXMI to NO1 (ACTIVE NETWORK OAM&P)

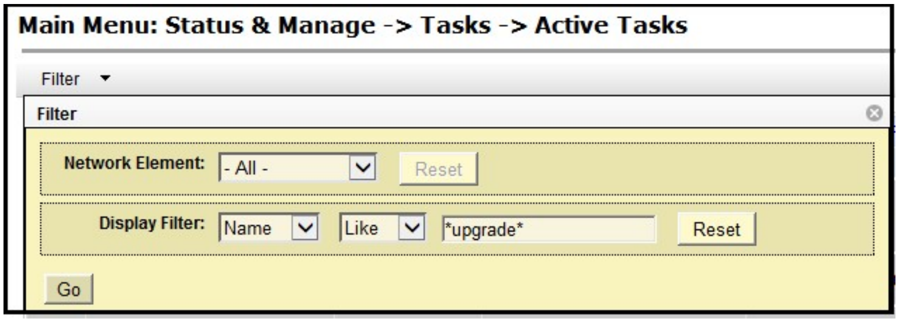
Main Menu: Status & Manage -> Tasks -

<table>
<tr><th>ID</th><th>Name</th><th>Status</th><th>Sta</th></tr>
<tr><td>48</td><td>SO2 Server Upgrade (in SO_SG Server Group Upgrade)</td><td>exception</td><td>201</td></tr>
<tr><td>47</td><td>SO_SG Server Group Upgrade</td><td>paused</td><td>201</td></tr>
<tr><td>45</td><td>Database backup from cron</td><td>completed</td><td>201</td></tr>
<tr><td>44</td><td>NO_SG PostUpgrade Health Check</td><td>completed</td><td>201</td></tr>
</table>

</td>
</tr>
<tr>
<td>3
□</td>
<td><b><u>Active NOAM VIP:</u></b>
Search for upgrade task</td>
<td>

Use the filter to locate the server group upgrade task.

1. Click the Filter dropdown and enter the following filter values:
   a. Network Element: **All**
   b. Display Filter: **Name Like *upgrade***
2. Click the **Go** button.



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

Filter

Network Element: - All -

Display Filter: Name Like *upgrade*

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

Procedure 81: Recovering from a Failed Upgrade

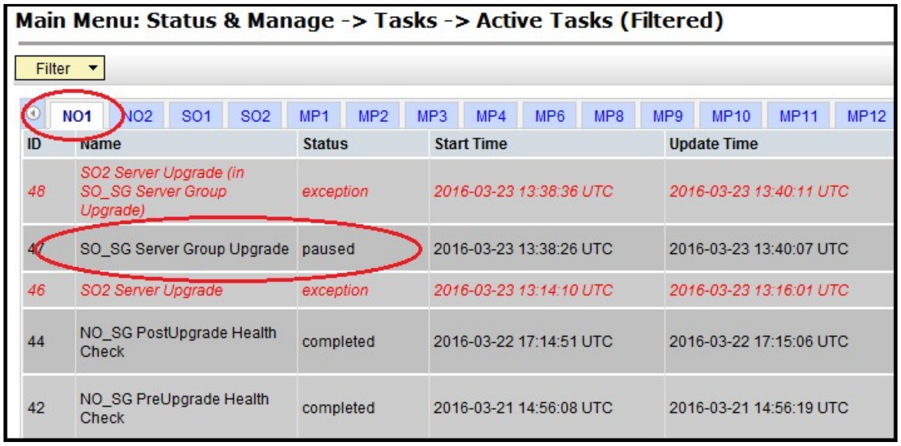
4 □

Active NOAM VIP:

Identify the upgrade task

In the search results list, locate the **Server Group Upgrade** task.

1. If not already selected, select the tab displaying the hostname of the Active NOAM server.
2. Locate the task for the **Server Group Upgrade**. It will show a status of “paused”.



Main Menu: Status & Manage -> Tasks -> Active Tasks (Filtered)

ID	Name	Status	Start Time	Update Time
48	SO2 Server Upgrade (in SO_SG Server Group Upgrade)	exception	2016-03-23 13:38:36 UTC	2016-03-23 13:40:11 UTC
47	SO_SG Server Group Upgrade	paused	2016-03-23 13:38:26 UTC	2016-03-23 13:40:07 UTC
46	SO2 Server Upgrade	exception	2016-03-23 13:14:10 UTC	2016-03-23 13:16:01 UTC
44	NO_SG PostUpgrade Health Check	completed	2016-03-22 17:14:51 UTC	2016-03-22 17:15:06 UTC
42	NO_SG PreUpgrade Health Check	completed	2016-03-21 14:56:08 UTC	2016-03-21 14:56:19 UTC

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 hitting cancel button 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).
We need to make sure that we are not cancelling any task which has some servers still in running state.

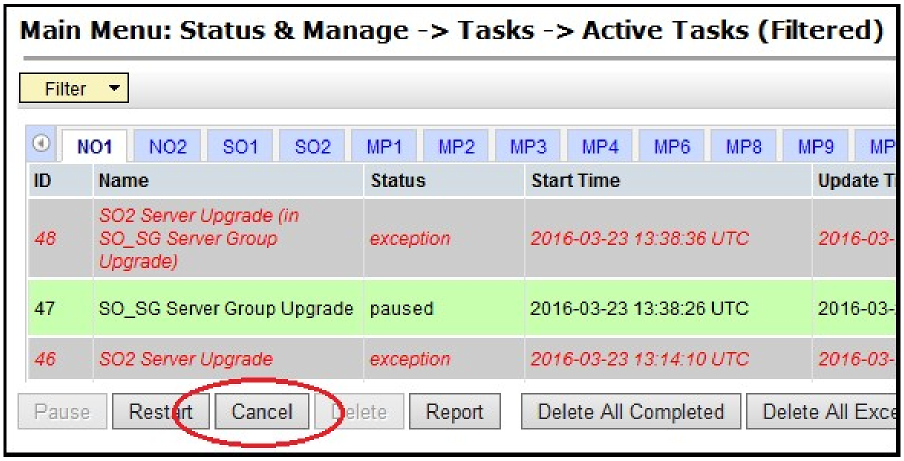
5 □

Active NOAM VIP:

Cancel the upgrade task

Cancel the **Server Group Upgrade** task.

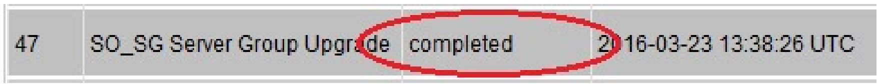
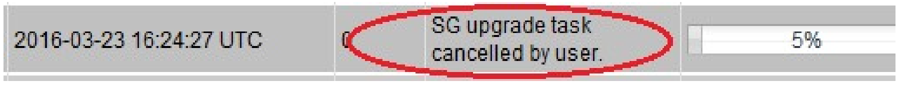
1. Click the Server Group Upgrade task to select it. It will become highlighted on the screen.
2. Click the **Cancel** button to cancel the task.
3. Click **OK** on the confirmation dialog box to confirm the cancellation.



Main Menu: Status & Manage -> Tasks -> Active Tasks (Filtered)

ID	Name	Status	Start Time	Update T
48	SO2 Server Upgrade (in SO_SG Server Group Upgrade)	exception	2016-03-23 13:38:36 UTC	2016-03-
47	SO_SG Server Group Upgrade	paused	2016-03-23 13:38:26 UTC	2016-03-
46	SO2 Server Upgrade	exception	2016-03-23 13:14:10 UTC	2016-03-

Procedure 81: Recovering from a Failed Upgrade

6 □	**Active NOAM VIP:** Verify task cancellation	Verify the Server Group Upgrade task is canceled. 1. On the Active Tasks screen, verify the task that was canceled in step 5 shows a status of "**completed**".  47 SO_SG Server Group Upgrade completed 2016-03-23 13:38:26 UTC  2016-03-23 16:24:27 UTC 0 SG upgrade task cancelled by user. 5%

7
□
	Failed server CLI:
	Inspect upgrade log
		Login to the failed server to inspect the upgrade log for the cause of the failure.
		1. 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.
		2. View or edit the upgrade log at `/var/TKLC/log/upgrade/upgrade.log` for clues to the cause of the upgrade failure.
		3. 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`

		• Although outside of the scope of this document, the user is expected to use standard troubleshooting techniques to clear the alarm condition from the failed server. • If troubleshooting assistance is needed, it is recommended to contact MOS as described in Appendix S - Accessing Oracle Customer Support Site. • **DO NOT PROCEED TO STEP 2 OF THIS PROCEDURE UNTIL THE ALARM CONDITION HAS BEEN CLEARED!**

8
□
	Failed Server CLI:
	Verify Platform alarms are cleared
		Verify all Platform alarms have been cleared from the failed server.
		1. Use the alarmMgr utility to verify that all Platform alarms have been cleared from the system.
		`$ sudo alarmMgr --alarmstatus`
		Example output:
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		` 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`
		***** user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm *****
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		`[admusr@SO2 ~]$`

Procedure 81: Recovering from a Failed Upgrade

9 □	**Active NOAM VIP:** Re-execute the server upgrade	Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the "**Upgrade Server**" option. **Note: Once a server has failed while using the Automated Server Group Upgrade option, the "Auto Upgrade" option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the "Upgrade Server" option.**

Appendix Q FAST DEPLOYMENT CONFIGURATION FILE DESCRIPTION

An XML configuration file is the primary source of automated deployment and configuration information for the feature. The configuration defines one or more infrastructures that represent a set of hardware, software and TVOE hosts associated with a PM&C. The file also defines one or more application servers that are to be deployed to a specified infrastructure.

The sections to be modified are identified below with a brief description

Note: Any sub-element that is not described should not be modified.

More information on the FDC Fast deployment configuration file can be found in [11].

Software Element

The optional software `element` contains one or more image elements representing deployable ISO images. Each image element has a required id attribute used to uniquely reference that image in the configuration file. The only element that should be modified is the name.

`Name` defines the ISO version of TVOE, Application, Mediation, Oracle or TPD image. Verify that the versions match the version of software that to be installed. If they do not match, modify the configuration file as needed.

Enclosure Element

The enclosure element specifies the enclosure for a set of blade servers.

`cabhwid` refers to the cabinet identification used at each site.

`encid` refers to the enclosure identification used at each site.

`oa1` refers to the IP Address for the first OA within an enclosure.

`oa2` refers to the IP Address for the second OA within an enclosure.

Blade Element

The `blade` element specifies the blade within an enclosure, on which an IDIH system will be installed.

Use the `enchwid` that has been specified within the PM&C to be IPM'd.

`bay` is the bay location of the blade to be IPM'd.

`type` is the hardware type, e.g., Gen 6 or Gen 8 blade.

RMS Element

The `rms` element specifies a rack-mount server in the infrastructure, and provisions it in PM&C if not already present. The `rmsOOBIP`, `rmsname,` and `cabhwid` elements should be modified.

The `rmsOOBIP` sub-element is the only required sub-element, and it specifies the IP address of the RMS iLO.

The `rmsname` sub-element specifies the name of the RMS when provisioned in PM&C. The `cabhwid` sub-element specifies the ID of the cabinet.

TVOE Software Element

The TVOE software stanza should not be added to an IDIH system where the IDIH guest is co-located with a PM&C guest.

Note: Do not IPM the TVOE host when the IDIH guest and PM&C guest are on the same TVOE host.

TVOE Serverinfo Element

A serverinfo element specifies configuration information for TVOE hosts, guests, and native application servers. The only subelements that should be changed are the TVOE hostname and TVOE ntpserver ipaddress.

The hostname subelement sets the hostname for the TVOE host.

The ntpservers subelement sets NTP servers for the system. It may contain up to five ntpserver subelements. Each ntpserver element contains name and ipaddress subelements which are the host name and IP address of the NTP servers.

TVOE tpdinterface Sub-Element

The tpdinterface subelement specifies the TVOE interface configuration. The only subelements that should be modified are the device, type, vlandata and vlandid elements.

device contains the name of the TVOE interface device.

type can be either Vlan or Bonding .

vlandata contains a vlanid sub-element with the ID of the vlan.

TVOE tpdbridge Sub-Element

Each tpdbridge subelement specifies the TVOE bridge configuration. The subelements that should be modified are interfaces, address, and netmask.

interfaces defines the interfaces in the TVOE host bridge.

address defines the IP address of the TVOE host bridge.

netmask defines the network mask for the TVOE host bridge.

TVOE tpdroute Sub-Element

This tpdroute subelement specifies the TVOE route configuration. The only subelement that should be modified is the gateway.

gateway specifies the gateway for the XMI route used by the TVOE host.

Oracle Guest Scripts Element Network

The scripts element defines files that will be executed as part of the IPM process. Currently, network configuration of the TVOE guest is not directly supported by the Fast Deployment. Instead, the netAdm script is called with arguments. The only arguments that should be modified are the address, netmask, and gateway.

address defines the IP XMI address of the Oracle guest.

netmask defines the Oracle guest XMI netmask.

gateway defines the XMI default route used by the Oracle guest.

Mediation Guest Scripts Element Network

The scripts element defines files that will be executed as part of the IPM process. Currently, network configuration of the TVOE guest is not directly supported by the Fast Deployment. Instead, the netAdm script is called with arguments. The only arguments that should be modified are the address, netmask, and gateway.

address defines the IP XMI and IMI address of the Mediation guest.

netmask defines the Mediation guest XMI and IMI netmask.

`gateway` defines the XMI default route used by the mediation guest.

Application Guest Scripts Element Network

The `scripts` element defines files that will be executed as part of the IPM process. Currently, network configuration of the TVOE guest is not directly supported by the Fast Deployment. Instead, the `netAdm` script is called with arguments. The only arguments that should be modified are the `address`, `netmask,` and `gateway`.

`address` defines the IP XMI address of the Application guest.

`netmask` defines the Application guest XMI netmask.

`gateway` defines the XMI default route used by the Application guest.

Appendix Q.1 Sample FDC Configuration File

```
<fdc>
    <infrastructures>
    <infrastructure name="PMAC">
        <!--Software Elements-->
        <software>
            <image id="tvoe">
                <name>872-2525-101-2.5.0_82.12.1-TVOE-x86_64</name>
            </image>
            <image id="app">
                <name>872-2427-102-7.0.0_7.0.0-apps-x86_64</name>
            </image>
            <image id="med">
                <name>872-2427-101-7.0.0_7.0.0-mediation-x86_64</name>
            </image>
            <image id="ora">
                <name>872-2440-104-7.0.0_7.0.0-oracle-x86_64</name>
            </image>
            <image id="tpd">
                <name>TPD.install-7.5.0_82.15.0-CentOS6.4-x86_64</name>
            </image>
        </software>

        <hardware>
            <cabinet id="cab1">
                <cabid>1</cabid>
            </cabinet>

            <!--Enclosure Element: Update cabhwid, endid and oa ip's-->
            <enclosure id="enc1">
                <cabhwid>cab1</cabhwid>
                <encid>1401</encid>
                <oa1>10.240.71.197</oa1>
                <oa2>10.240.71.198</oa2>
            </enclosure>

            <!--Blade Element: Update enchwid, bay and type-->
            <blade id="blade7">
                <enchwid>enc1</enchwid>
                <bay>7F</bay>
                <type>ProLiant BL460c G6</type>
            </blade>

            <!--Rack Mount Server Element: update rmsOOBIP with ILO IP-->
            <rms id="mgmtsrvr">
                <rmsOOBIP>10.250.36.27</rmsOOBIP>
                <rmsname>d-ray</rmsname>
                <cabhwid>cab1</cabhwid>
                <rmsuser>root</rmsuser>
                <rmspassword>TklcRoot</rmspassword>
                <type>ProLiant DL380 G8</type>
            </rms>
        </hardware>

        <tvoehost id="mgmtsrvrtvoe">
            <!--TVOE Hardware Element: Update the name of the tvoe device-->
            <!--In this example we are configuring a rms server-->
            <hardware>
                <rmshwid>mgmtsrvr</rmshwid>
                <!--bladehwid>blade7</bladehwid-->
            </hardware>

            <!--TVOE Software Element-->
            <!--Do Not Use this element when the PM&C host co-exist with IDIH-->
            <software>
                <baseimage>tvoe</baseimage>
            </software-->

            <serverinfo>
                <!--tvoe hostname: Update hostname-->
                <hostname>d-ray</hostname>
                <!--tvoe ntpservers: Update ip address-->
                <ntpservers>
                    <ntpserver>
                        <name>ntpserver1</name>
                        <ipaddress>10.250.32.10</ipaddress>
                    </ntpserver>
                </ntpservers>
            </serverinfo>

            <tpdnetworking>
                <tpdinterfaces>
                    <!--tvoe xmi interface: Update device and vlanid-->
                    <tpdinterface id="xmi">
                        <device>bond0.3</device>
                        <type>Vlan</type>
                        <vlandata>
                            <vlanid>3</vlanid>
                        </vlandata>
                        <onboot>yes</onboot>
                        <bootproto>none</bootproto>
                    </tpdinterface>

                    <!--Tvoe imi interface: Update device and vlanid-->
                    <tpdinterface id="imi">
                        <device>bond0.4</device>
                        <type>Vlan</type>
                        <vlandata>
                            <vlanid>4</vlanid>
                        </vlandata>
                        <onboot>yes</onboot>
                        <bootproto>none</bootproto>
                    </tpdinterface>
                </tpdinterfaces>

                <tpdbridges>
                    <!--Tvoe xmi bridge: Update interfaces, ipaddress and netmask-->
                    <tpdbridge id="xmibr">
                        <name>xmi</name>
                        <!--Make sure this value matches the imi tpdinterface-->
                        <interfaces>bond0.3</interfaces>
                        <bootproto>none</bootproto>
                        <address>10.240.51.39</address>
                        <netmask>255.255.255.0</netmask>
                        <onboot>yes</onboot>
                    </tpdbridge>

                    <!--Tvoe imi bridge: Update interfaces, ipaddress and netmask-->
                    <tpdbridge id="imibr">
                        <name>imi</name>
                        <!--Make sure this value matches the imi tpdinterface-->
                        <interfaces>bond0.4</interfaces>
                        <bootproto>none</bootproto>
                        <onboot>yes</onboot>
                    </tpdbridge>
                    <tpdbridge id="intbr">
                        <name>int</name>
                        <bootproto>none</bootproto>
                        <onboot>yes</onboot>
                    </tpdbridge>
                </tpdbridges>

                <tpdroutes>
                    <!--Tvoe default gateway address: Update gateway-->
                    <tpdroute id="default">
                        <type>default</type>
                        <device>xmi</device>
                        <gateway>10.240.30.3</gateway>
                    </tpdroute>
                </tpdroutes>
            </tpdnetworking>

            <scripts>
                <predeploy>
                    <!--configExt configures external disk-->
                    <scriptfile id="configExt">
                        <image>med</image>
                        <imagefile>external.pl</imagefile>
                        <filename>/root/external.pl</filename>
                    </scriptfile>
                </predeploy>
            </scripts>
        </tvoehost>
    </infrastructure>
    </infrastructures>

    <servers>
        <!--Oracle Guest Configuration-->
        <tvoeguest id="Oracle">
            <infrastructure>PMAC</infrastructure>
            <tvoehost>mgmtsrvrtvoe</tvoehost>

            <!--Oracle Guest Profile: Update if hardware is Gen6 default is Gen8-->
            <!--profile>ORA_GEN6</profile-->
            <profile>ORA_GEN8</profile>
            <name>oracle</name>
            <software>
                <baseimage>tpd</baseimage>
                <appimage>ora</appimage>
            </software>
            <serverinfo>

                <!--Oracle guest hostname-->
                <hostname>mamie</hostname>
            </serverinfo>

            <scripts>
                <presrvapp>
                    <scriptfile id="oracleInt">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>set --device=int --address=10.254.254.2 --netmask=255.255.255.224
                            --onboot=yes --bootproto=none</arguments>
                    </scriptfile>

                    <!--Oracle Guest xmi network: Update address and netmask-->
                    <scriptfile id="oracleXmi">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>set --device=xmi --address=10.250.51.184 --netmask=255.255.255.0
                            --onboot=yes --bootproto=none</arguments>
                    </scriptfile>

                    <!--Oracle Guest xmi default route: Update gateway-->
                    <scriptfile id="oracleRoute">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                    </scriptfile>
                </presrvapp>
                <postsrvapp>
                    <!--Oracle Post Server Application Configuration Script-->
                    <scriptfile id="oracleConfig">
                        <filename>/opt/xIH/oracle/configureOracle.sh</filename>
                        <timeout>2700</timeout>
                    </scriptfile>
                </postsrvapp>
            </scripts>
        </tvoeguest>

        <!--Mediation Guest Configuration-->
        <tvoeguest id="Mediation">
            <infrastructure>PMAC</infrastructure>
            <tvoehost>mgmtsrvrtvoe</tvoehost>

            <!--Mediation Guest Profile: Update if hardware is Gen6 default is Gen8-->
            <!--profile>MED_GEN6</profile-->
            <profile>MED_GEN8</profile>
            <name>mediation</name>
            <software>
                <baseimage>tpd</baseimage>
                <appimage>med</appimage>
            </software>

            <!--Mediation guest hostname-->
            <serverinfo>
                <hostname>poney</hostname>
            </serverinfo>
            <scripts>
                <presrvapp>
                    <scriptfile id="medInt">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>set --device=int --address=10.254.254.3 --netmask=255.255.255.224
                            --onboot=yes --bootproto=none</arguments>
                    </scriptfile>

                    <!--Mediation Guest xmi network: Update address and netmask-->
                    <scriptfile id="medXmi">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                            <arguments>set --device=xmi --address=10.250.51.185 --netmask=255.255.255.0
                                --onboot=yes --bootproto=none</arguments>
                    </scriptfile>
```

```
                    <!--Mediation Guest xmi default route: Update gateway-->
                    <scriptfile id="medRoute">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                    </scriptfile>

                    <!--Mediation Guest imi network: Update address and netmask-->
                    <scriptfile id="medImi">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>set --device=imi --address=192.168.10.55 --netmask=255.255.255.0
                            --onboot=yes --bootproto=none</arguments>
                    </scriptfile>
                </presrvapp>

                <!--Mediation Post Deploy Database Configuration Script-->
                <postdeploy>
                    <scriptfile id="medConfig">
                        <filename>/opt/xIH/mediation/xdrDbInstall/install.sh</filename>
                    </scriptfile>
                </postdeploy>
            </scripts>
        </tvoeguest>

        <!--Application Guest Configuration-->
        <tvoeguest id="Application">
            <infrastructure>PMAC</infrastructure>
            <tvoehost>mgmtsrvrtvoe</tvoehost>

            <!--Application Guest Profile: Update if hardware is Gen6 default is Gen8-->
            <!--profile>APP_GEN6</profile-->
            <profile>APP_GEN8</profile>
            <profile>application</profile>
            <name>application</name>
            <software>
                <baseimage>tpd</baseimage>
                <appimage>app</appimage>
            </software>

            <!--Application guest hostname: Update hostname-->
            <serverinfo>
                <hostname>jesco</hostname>
            </serverinfo>
            <scripts>
                <presrvapp>
                    <scriptfile id="appInt">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>set --device=int --address=10.254.254.4 --netmask=255.255.255.224
                            --onboot=yes --bootproto=none</arguments>
                    </scriptfile>

                    <!--Application Guest xmi network: Update address and netmask-->
                    <scriptfile id="appXmi">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                            <arguments>set --device=xmi --address=10.250.51.186 --netmask=255.255.255.0
                                --onboot=yes --bootproto=none</arguments>
                    </scriptfile>

                    <!--Application Guest xmi default route: Update gateway-->
                    <scriptfile id="appRoute">
                        <filename>/usr/TKLC/plat/bin/netAdm</filename>
                        <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                    </scriptfile>
                </presrvapp>
                <postdeploy>

                    <!--Sleep allows time for mediation scripts completion-->
                    <scriptfile id="appSleep">
                        <filename>/bin/sleep</filename>
                        <arguments>60</arguments>
                    </scriptfile>

                    <!--Application Post Deploy Configuration Script-->
                    <scriptfile id="appConfig">
                        <filename>/opt/xIH/apps/install.sh</filename>
                        <timeout>3000</timeout>
                    </scriptfile>
                </postdeploy>
            </scripts>
        </tvoeguest>
    </servers>
</fdc>
```

Appendix R 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 Auto Site Upgrade (ASU) or during an event that resets multiple servers in parallel. The DB on the child servers will not be updated until resolved.

Procedure 82 must be performed on the server(s) with the above alarms.

Procedure 82: Restart the inetrep process on the affected server(s).

STEP #	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. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR <u>UPGRADE ASSISTANCE</u>.**	
1 □	**<u>Server CLI:</u>** Login to the server	Use the SSH command (on UNIX systems – or putty if running on windows) to login to the server on which the DB replication failure alarm is seen: `ssh admusr@<server_ip>` (Answer 'yes' if prompted to confirm the identity of the server.)
2 □	**<u>Server CLI:</u>** 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 □	**<u>Server CLI:</u>** 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 S ACCESSING ORACLE CUSTOMER SUPPORT SITE

My Oracle Support

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

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

1. For the first set of menu options, select 2, "New Service Request". You will hear another set of menu options.
2. In this set of menu options, select 3, "Hardware, Networking and Solaris Operating System Support". A third set of menu options begins.
3. In the third set of options, select 2, "Non-technical issue". Then you will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center

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

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "**Network Session Delivery and Control Infrastructure**" or "**Platforms**."
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.