Oracle® Communications Diameter Signaling Router

DSR Software Upgrade Guide

Release 7.0

E54117, Revision 04

August 2015

ORACLE®

Oracle® Communications Diameter Signaling Router, DSR Software Upgrade Guide, Release 7.0

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

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

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

TABLE OF CONTENTS

LIST OF FIGURES

List of Tables

List of Procedures

This page intentionally left blank.

1 INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform a major upgrade from DSR 5.x and 6.x to 7.0, or an incremental upgrade from an earlier DSR 7.0 release to a DSR 70.xx.0 or later release. The upgrade of both HP C-Class blades and RMS HP 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.

The DSR 7.0 Software Release includes all Oracle CGBU Platform Distribution (TPD) software. Any upgrade of TPD required to bring the DSR to release 7.0 occurs automatically as part of the DSR 7.0 software upgrade. The execution of this procedure assumes that the DSR 7.0 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.

!! WARNING!! **THIS PROCEDURE DOES NOT SUPPORT AN UPGRADE OF THE 2-TIER CONFIGURATION. 2-TIER CONFIGURATIONS MUST BE MIGRATED TO 3-TIER BEFORE EXECUTING THIS PROCEDURE.**

1.1.1 What is Not Covered by this Document

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

- Distribution of DSR 7.0 software loads. It is recommended to contact MOS for the software loads as described in Appendix M
- Initial installation of DSR software. Refer to [5] and [6], [7] and [8], or [9] and [10]
- IDIH upgrade. Refer to [12]
- Firmware upgrade. Refer to [1] (HP) or [2] (Netra)
- PM&C upgrade. Refer to [4]
- 2-tier to 3-tier migration. Refer to [11]
- SDS upgrade. Refer to [13]

1.2 References

[1] *HP Solutions Firmware Upgrade Pack Release Notes, 795-0000-0xx,*v2.1.1 (or latest 2.1 version)
[2] *Oracle Firmware Upgrade Pack Upgrade Guide, E54963-01, Oracle*
[3] *TVOE 2.7 Upgrade Document. 909-2296-001. Oracle*
[4] *PM&C 5.7 Incremental Upgrade Guide, E54387-01, Oracle*
[5] *DSR 5.0 Installation Part 1/2. 909-2282-001, Oracle*
[6] *DSR 5.0 Installation Part 2/2. 909-2278-001, Oracle*
[7] *DSR 6.0 Installation Part 1/2, E54118-01, Oracle*
[8] *DSR 5.x/6.0 Installation Part 2/2, E52510-01, Oracle*
[9] *DSR 6.x/7.0 Base Hardware and Software Installation Part 1/2, E57789-01, Oracle*
[10] *DSR 7.0 Installation and Configuration Part 2/2, E58954-01, Oracle*
[11] *2-tier to 3-tier migration WI006897, Oracle*
[12] *IDIH upgrade document. E56571-01, Oracle*
[13] *SDS Upgrade document. UG006386.docx, Oracle*
[14] *Maintenance Window Analysis Tool SS006061.xlsx, Oracle*
[15] *DSR 6.0 to 7.0 Migration – IPFE Aspects, WI007086, Oracle*
[16] *IPFE Feature Activation and Configuration, WI006931, Oracle*

1.3 Acronyms

Table 1: Acronyms

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
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
PM&C	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 5.x to DSR 7.0.
Incremental Upgrade	An upgrade within a given DSR release e.g. 7.0.x to 7.0.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Single Server Upgrade	The process of converting a DSR 5.x/6.0 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 7.0 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.
Source release	Software release to upgrade from.
Primary NOAM Network Element	The network element that contains the Active and Standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. 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. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, 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.
Site	Physical location where one or more network elements reside. For a 2-tier DSR, the site is defined by the NOAM. For a 3-tier DSR, the site is defined by the SOAM.
Target release	Software release to upgrade to.
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 a server. The state is defined by the following attributes: • Server is Forced Standby • Server is Application Disabled (signaling servers will not process any traffic)
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) an NOAM HA pair; 2) an 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.

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.

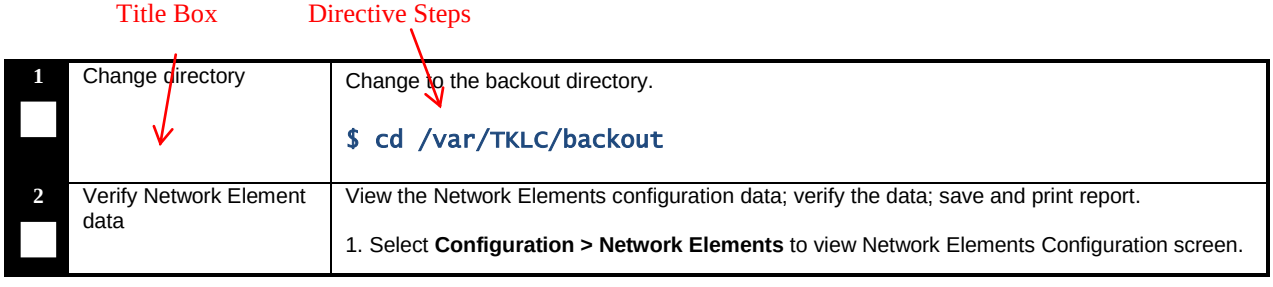
3) If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact MOS for assistance, as described in Appendix M, before attempting to continue.

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



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's 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.

2 GENERAL DESCRIPTION

This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 5.x or 6.x to target release 7.0. An incremental upgrade advances the DSR from an earlier DSR 7.0 source release to a more recent 7.0 target release.

Note that for any incremental upgrade, the source and target releases must have the same value of "x". For example, advancing a DSR from 7.x.0-70.1.0 to 7.x.0-70.2.0 is an incremental upgrade. But advancing a DSR running a 5.0 release to a 7.0 target release constitutes a major upgrade.

2.1 Supported Upgrade Paths

The supported paths to upgrade to a DSR 7.0 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.

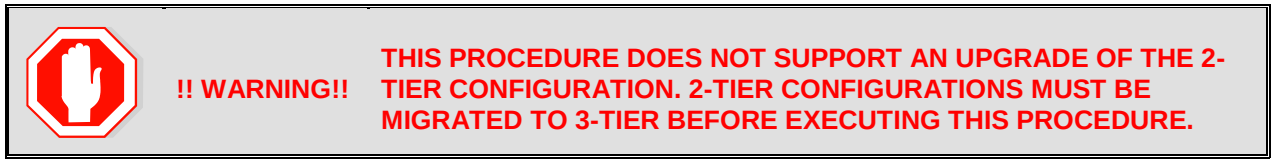
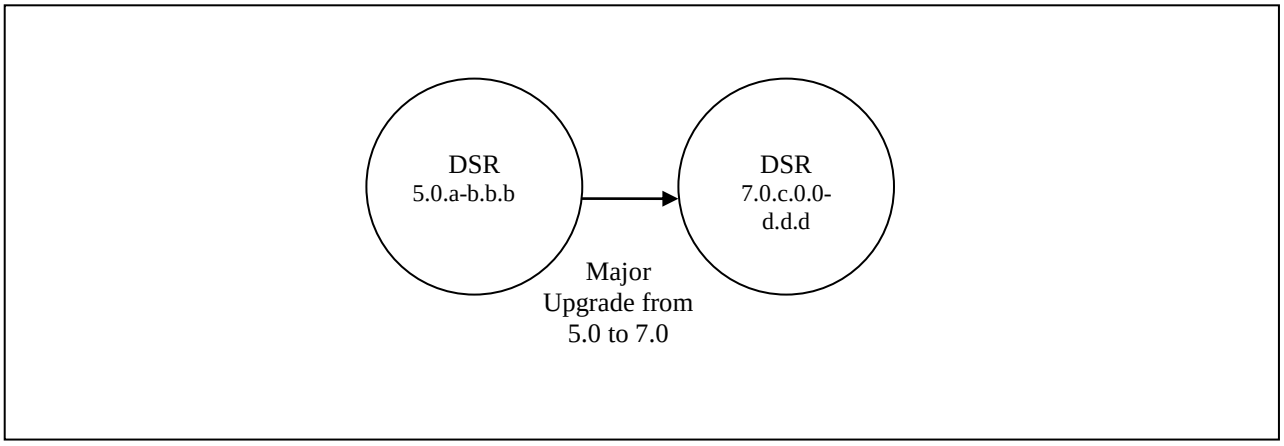
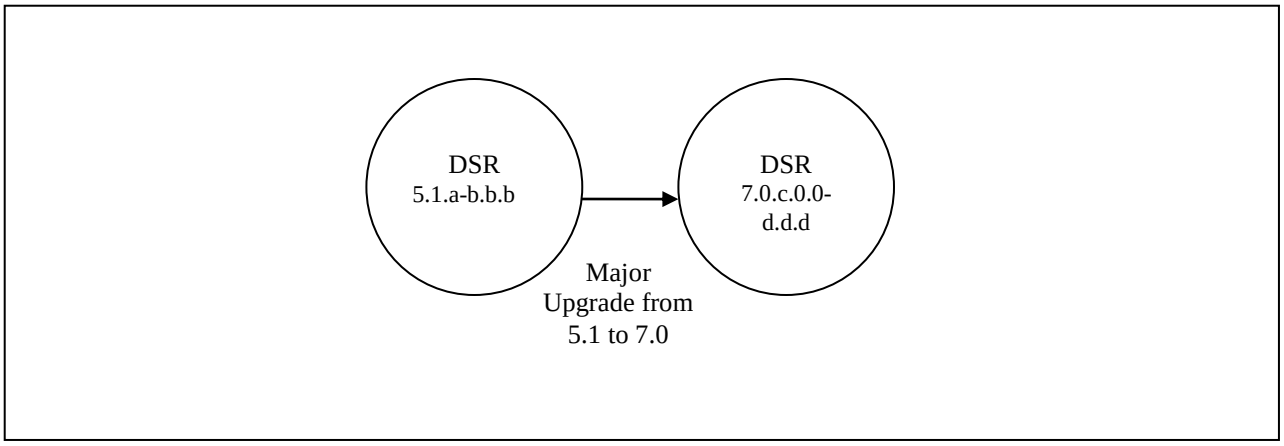
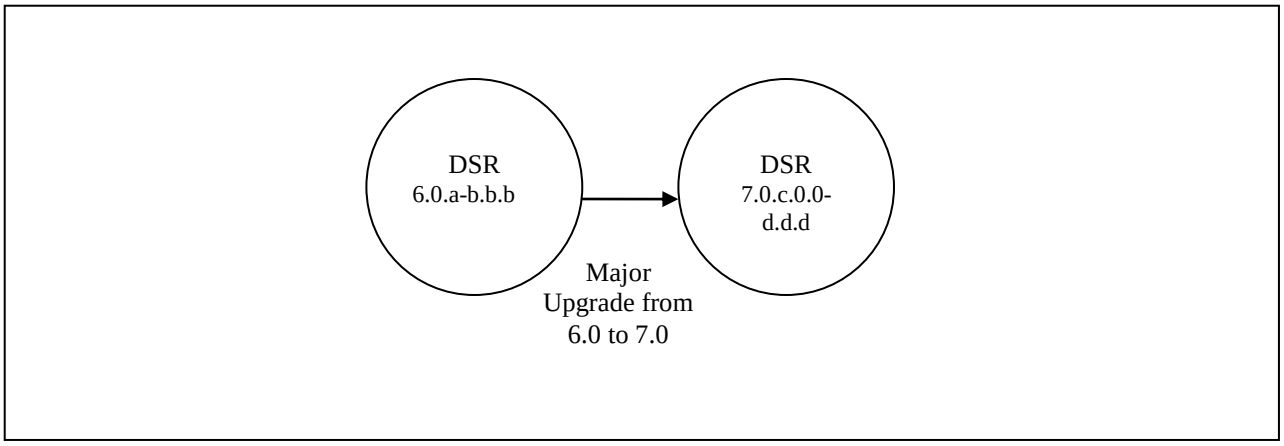
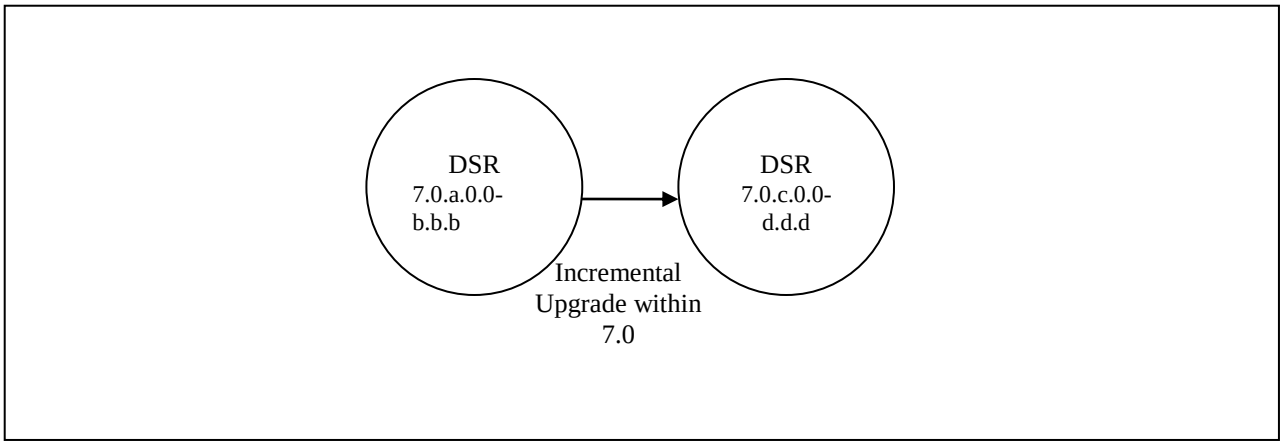


Figure 2. Supported Upgrade Paths









2.2 Active/Standby (1+1) vs Multi-Active (N+0) DA-MPs

The Site upgrade procedures are different for the two DA-MP Redundancy Models:

- Active/Standby DA-MP pair - two servers only
- Multi-Active DA-MPs - up to 16 DA-MPs, and typically including IPFE servers that need to be upgraded

For this reason, separate procedures are provided for these two cases.

2.3 Geo-diverse 3-Tier 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. The PCA upgrade procedure in this document is specific to a configuration that includes Geo-Diversity (Section 5.5).

2.4 Firmware Updates

Firmware upgrades are not in the scope of this document, but may be required before upgrading DSR. It is assumed that these are done when needed by the hardware, and there is typically not a dependency between Firmware version and the DSR 7.0 release. See Release Notes for any dependencies.

2.5 PMAC (Management Server) Upgrades

Each site may have a PMAC (Management Server) that provides support for maintenance activities at the site. There is a separate procedure for PMAC upgrade, including TVOE. PMAC must be upgraded before the other servers at the site are upgraded.

2.6 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:

- PMAC
- 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 PMAC, and the PMAC application, must be upgraded before other TVOE host upgrades, since PMAC is used to perform the TVOE upgrades.

There are three supported strategies for TVOE upgrade (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 SOAM applications. These applications will also be affected.

The procedure for Upgrading TVOE environments in advance of the application upgrades (Option A) is documented in Section 3.3.7.

2.7 SDS Upgrade

If the DSR deployment includes SDS, it is recommended to upgrade SDS NOAMs before the DSR NOAMs and SDS SOAMs before DSR SOAMs.

2.8 Traffic Management during Upgrade

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

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

2.9 RMS Deployments

All Deployments with RMS are 3-Tier. In these smaller deployments, the Message Processing (DA-MP, SS7-MP and IPFE) servers are also virtualized (deployed on a TVOE HOST) to reduce the number of servers required.

The following commercial deployment types are supported:

- 2 RMS servers, one site, no IDIH
- 3 RMS servers, one site, with one server reserved for IDIH (and IDIH storage)
- 4 RMS servers, 2 sites with 2 servers per site, no IDIH
- 6 RMS servers, 2 sites with 3 servers per site, 1 server at each site reserved for IDIH (and IDIH storage)

When an RMS-based DSR is without 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 all 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, MPs (DA-MP and IPFE) at the primary RMS site.

3 UPGRADE PLANNING AND PRE-UPGRADE PROCEDURES

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

There are overview tables throughout this section that help plan the upgrade and estimate how long it 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.

****** PDRA WARNING *******

PDRA upgrade from 5.x to 7.0 is NOT supported. All 5.x PDRA Systems must upgrade to 6.x, and then upgrade to 7.0. Failure to comply will result in the failure of all Session SBR Server Groups. This will cause nearly 100% call failure.

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 5.x/6.x/7.0 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 3]**.
- 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 Application ISO Image File / Media

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

The DSR 7.0 ISO image file name will be in the following format:

```
DSR-7.0.0.0.0_70.13.0-x86_64.iso
```

NOTE: Prior to the execution of this upgrade procedure it is assumed that the DSR 7.0 ISO image file has already been delivered to the customer's premises. The ISO image file must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image file. If the user performing the upgrade is at a remote location, it is assumed the ISO file is already available before starting the upgrade procedure.

3.1.2 Logins, Passwords and Server IP Addresses

Table 3 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 3 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 3: 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)	
	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	

[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.

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	

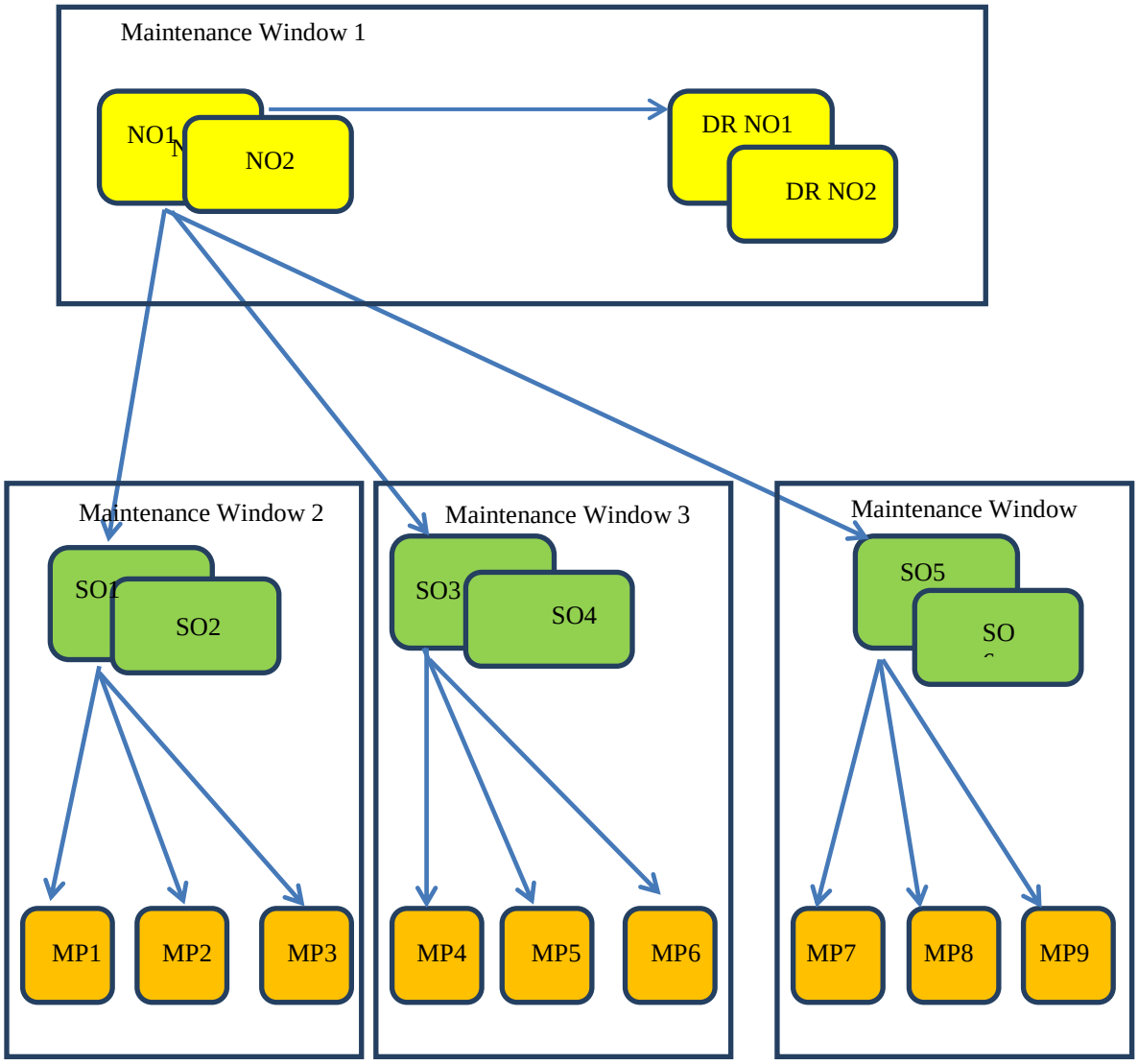
Item	Description	Recorded Value
iLO/LOM	NOAM 1 iLO/LOM IP Address	
	NOAM 2 iLO/LOM IP Address	
	SOAM 1 iLO/LOM IP Address	
	SOAM 2 iLO/LOM IP Address	
	MP 1 iLO/LOM IP Address	
	MP 2 iLO/LOM IP Address	
	……..	
	MP (n) iLO/LOM IP Address	
	IPFE MP iLO/LOM IP Address (optional)	
	IPFE MP iLO/LOM IP Address (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 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 3. Upgrade Maintenance Windows for 3-Tier Upgrade



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

3.2.1 Maintenance Window for PMAC and TVOE Upgrades (optional)

This document includes steps to upgrade PMAC and TVOE as an integrated activity with the upgrades of the DSR application. However, it is an **option** to perform these upgrades as separately planned and executed activities.

- PMAC Upgrade procedure is provided in reference [4] and in
- TVOE Host environment upgrade procedures are included in Appendix H *(Upgrade TVOE platform)* and Reference [3].

PMAC and TVOE upgrades are backwards compatible to prior releases of DSR.

These upgrades may be done a site-at-a-time.

3.2.2 Calculating Maintenance Windows Required

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see ref [14]).

This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. The spreadsheet also specifies, in detail, which servers need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in Reference [14]. Please see the instructions tab of the spreadsheet for more information and details.

3.2.3 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded, and possibly also the PMAC, and the TVOE environments supporting these servers. *(Note that PMAC and/or TVOE environments may be upgraded before Maintenance Window 1, as a preferred option.)*

Maintenance Window 1 ***(NOAM Sites)*** **Date: _____** **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. **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.*	☐ * 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)*: _____

3.2.4 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:** _____ **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. **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.*	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)*

3.3 Prerequisite Procedures

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

Table 4: 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	0:50-3:15	1:00-3:45	Data Collection - Verification of Global and Site Configuration Data	None
Procedure 3	0:10-2:00	1:10-5:45	Full Backup of DB Run Environment at Each Server	None
Procedure 4	0:05-0:15*	1:15-6:00	ISO Administration	None

* 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.

3.3.1 Hardware Upgrade Preparation

There is no hardware preparation necessary when upgrading to DSR release 7.0.

3.3.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the DSR 7.0 release to understand the functional differences and possible traffic impacts of the upgrade.

3.3.3 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 Section 3.2 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 M for these instructions. Note that obtaining a new online support account can take up to 48 hours.
	THIS PROCEDURE HAS BEEN COMPLETED.	

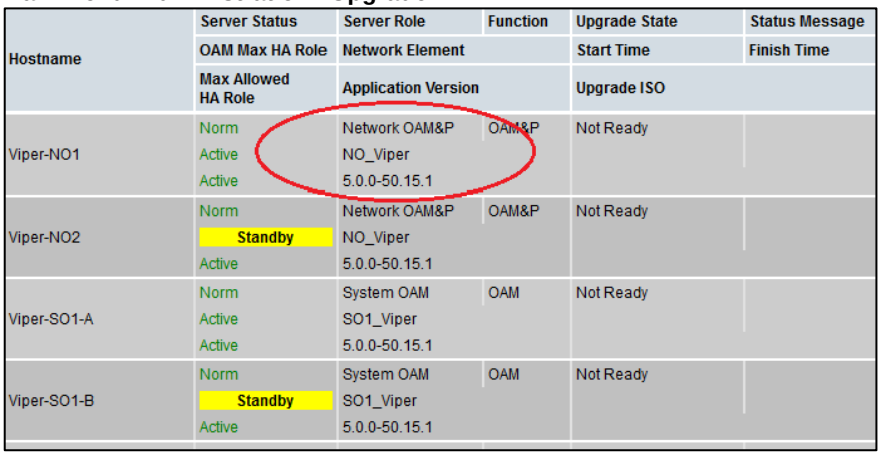
3.3.4 Data Collection - Verification of Global and Site Configuration Data

This procedure is part of Software Upgrade Preparation and is used to collect data required for network analysis and Disaster Recovery. Data is collected from both the Active NOAM and various other servers at each site (TVOE, PM&C, etc).

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

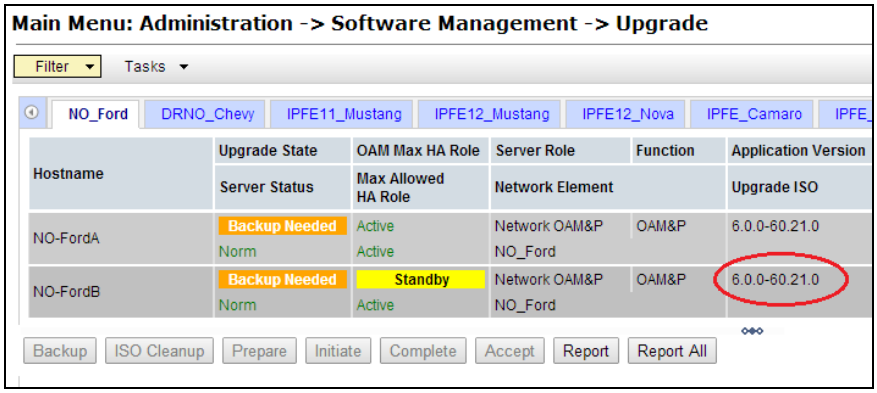
S T E P #	This procedure performs a backup of the Global and Site Provisioning Data Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active NOAM VIP:** Verify 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.
2. ☐	**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.
3. ☐	**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.
4. ☐	**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.
5. ☐	**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.
6. ☐	**Active NOAM VIP:** Verify Server Status is Normal - NOAM	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.

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

7. ☐	**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.
8. ☐	**Active NOAM VIP:** View Communication Agent status for all connections.	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.
9. ☐	**Active NOAM VIP:** View SBR status (if equipped)	**If the source release is 5.x/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 source release is 7.0:** 1. Select **Policy and Charging > Maintenance > SBR Status:** The SBR Status screen is displayed. 2. Select the 1st tab. 3. Expand each Server Group. 4. Verify Congestion Level is 'Normal' for all servers. 5. Repeat sub-steps 2 - 4 for each additional tab that appears on the **Policy and Charging > Maintenance > SBR Status** screen.
10. ☐	**Active NOAM VIP:** **1)** Navigate to the Upgrade **Administration** screen (see right panel for additional information). **2)** Verify that the Upgrade path to the target release is supported as documented in **Section 2.1** *(Supported Upgrade Paths).*	**Upgrade screen in DSR 5.0, and DSR 5.1 releases up to 5.1.0-51.12.2** **Main Menu: Administration >Upgrade** 

Hostname	Server Status	Server Role	Function	Upgrade State	Status Message
	OAM Max HA Role	Network Element		Start Time	Finish Time
	Max Allowed HA Role	Application Version		Upgrade ISO	
Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready	
Viper-NO2	Norm Standby Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready	
Viper-SO1-A	Norm Active Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready	
Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready	

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

11. ☐	**NOTE:** *The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release.*	**Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later** Select the NOAM Server Group and verify the Application Version 

12. ☐	**Active NOAM VIP:**
	
	Check if the setup has customer supplied Apache certificate installed and protected with a passphrase.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM
		
		If the source release is 5.x:
		`ssh root@<NOAM_VIP>`
		
		If the source release is 6.x/7.0:
		`ssh admusr@<NOAM_VIP>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. cd to `/etc/httpd/conf.d` and open the file named `ssl.conf`.
		
		3. Locate the line beginning with the phrase "`SSLCertificateFile`"
		
		4. The path that follows "SSLCertificateFile" is the location of the Apache certificate. If the path is `/usr/TKLC/appworks/etc/ssl/server.crt`,
		then the certificate is supplied by Oracle and no further action is required. Continue with the next procedure.
		
		5. If the path is anything other than `/usr/TKLC/appworks/etc/ssl/server.crt`, then a customer-supplied Apache certificate is likely installed. Rename the certificate, but note the original certificate pathname for use in **Procedure 12** and **Procedure 36**.

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

13. ☐	Verify uptime for each server in the topology.	1. Use the SSH command (on UNIX systems - or putty if running on windows) to login to each physical server in the topology using the server XMI IP Address.
		
		NOTE: ***The user is only required to login to the TVOE host for any OAM server (A / B level) but must log into all C level servers directly (MP, IPFE, etc.).***
		
		If the source release is 5.x:
		`ssh root@<target_server_XMI_IP>`
		
		If the source release is 6.x/7.0:
		`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`
		`[admusr@ipfe-freeport-a1 ~]$`
		
		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".***

14. ☐	Check if a new Firmware Release may be required for the system.	It is recommended to contact MOS by referring to Appendix M of this document 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.
15. ☐	Check the existing PM&C version and identify if PM&C upgrade is required. **NOTE_1:** *If required, PM&C upgrade should be performed as a prerequisite to DSR upgrade.*	Identify any PM&C servers requiring upgrade. 1. Determine the PM&C version installed by logging into PM&C GUI. 2. For upgrade to DSR 7.0, the minimum PM&C required is **5.7**. If the PM&C version is below 5.7, identify the required PM&C upgrade document [4] and plan for additional Maintenance Windows to execute PM&C upgrades. **NOTE_2:** *This step applies to all servers that have a PM&C guest (VM) installed.*

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

<table>
<tr>
<td>16. ☐</td>
<td>Check the TVOE Host server software version</td>
<td>
1. Find the target DSR release from Table 3.

2. It is recommended to contact MOS by referring to Appendix M of this document 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.

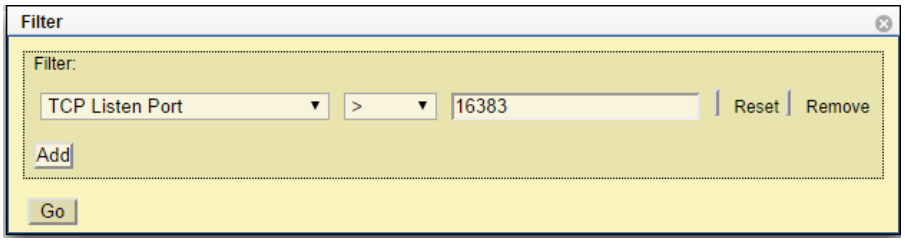
<pre># appRev
        Install Time: Thu Nov 6 14:31:08 2014
        Product Name: TVOE
     Product Release: 2.7.0.0.0_84.20.0
 Base Distro Product: TPD
 Base Distro Release: 6.7.0.0.1_84.20.0
     Base Distro ISO: TPD.install-6.7.0.0.1_84.20.0-
OracleLinux6.5-x86_64.iso
                  OS: OracleLinux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

IMPORTANT: If TVOE Hosts are not on the correct release, refer to Section 3.2.1 to plan for TVOE Host upgrades.

NOTE: This step applies to all RMS & Blade servers that have TVOE installed.
</td>
</tr>
<tr>
<td>17. ☐</td>
<td><u>Active SOAM VIP:</u>

Verify Local Node port ranges</td>
<td>
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.



5. Repeat steps 3 and 4 for the following filter values:

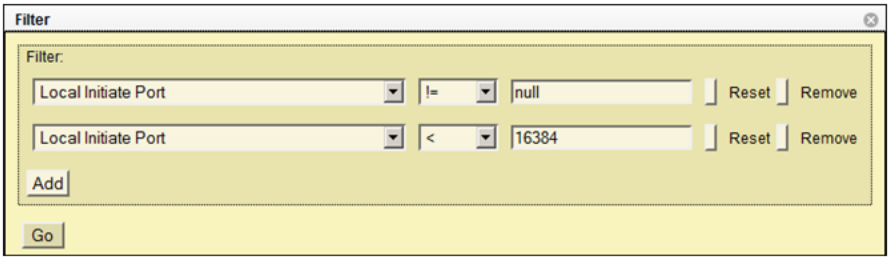
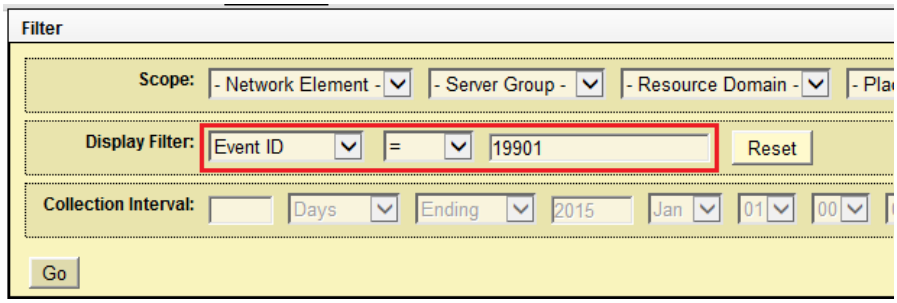
“TCP Listen Port < 1024”
“SCTP Listen Port > 16383”
“SCTP Listen Port < 1024”

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

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

NOTE: Only the customer may modify the port configurations. The customer should refer to Reference [15] for further instruction.
</td>
</tr>
</table>

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

18. ☐	**Active SOAM VIP:** Verify Initiator connection port ranges	Verify the Initiator connection port numbers are within the allowed range. **From Active SOAM GUI:** 1. Navigate to **Diameter > Configuration > Connections**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  4. Repeat 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 his current port configuration is not within recommended best practices.** **NOTE:** *Only the customer may modify the port configurations. The customer should refer to Reference [15] for further instruction.*
19. ☐	Active NOAM VIP Alarm Check	Check for the presence of alarm 19901 – CFG-DB Validation Error. **From the Active NOAM GUI:** 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  4. If the filter returns no results, the database is consistent; **proceed to step 22.** Otherwise, continue with step 20.

20. ☐	Active SOAM CLI
	
	Log into the Active SOAM
		Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active SOAM:
		
		If the source release is 5.x:
		`ssh root@<SOAM_VIP>`
		
		If the source release is 6.x/7.0:
		`ssh admusr@<SOAM_VIP>`

Procedure 2: Data Collection - Verification of Global and Site Configuration Data

21. ☐	Active SOAM CLI
	
	Database consistency check
		Check the transport connections tables.
		
		1. 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`
		
		2. If the entry counts match, **proceed to step 22**.
		
		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.

22. ☐	**Active SOAM VIP:** Verify the port configuration for the next SOAM site.	Repeat **Steps 17 thru 21** for each SOAM site in the topology.
23. ☐	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 [16] to correct the configuration.
24. ☐	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 Steps 1 through 6. 2. It is recommended to plan for any MP upgrades by consulting with MOS 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.

3.3.5 Full Backup of DB Run Environment at Each Server

This procedure is part of software upgrade preparation and is 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.

!! WARNING!!	IF BACKOUT IS NEEDED, ANY CONFIGURATION CHANGES MADE AFTER THE DB IS BACKED UP AT EACH SERVER WILL BE LOST

Procedure 3: Full Backup of DB Run Environment at Each Server

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 VIP:**
	Log into the Active NOAM
		Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM:
		If the source release is 5.x:
		`ssh root@<NOAM_VIP>`
		If the source release is 6.x/7.0:
		`ssh admusr@<NOAM_VIP>`

2. ☐	**Active NOAM VIP:** 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 VIP:**
	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.

Procedure 3: Full Backup of DB Run Environment at Each Server

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**	
4. ☐	**Active NOAM VIP:** 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 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:
		
		`# /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 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`

	THIS PROCEDURE HAS BEEN COMPLETED.	

3.3.6 ISO Administration

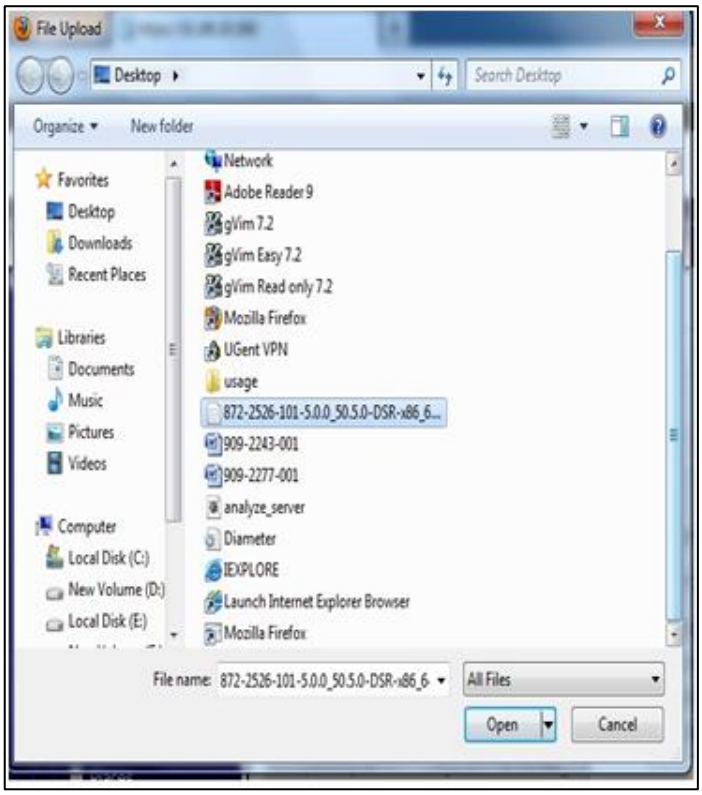
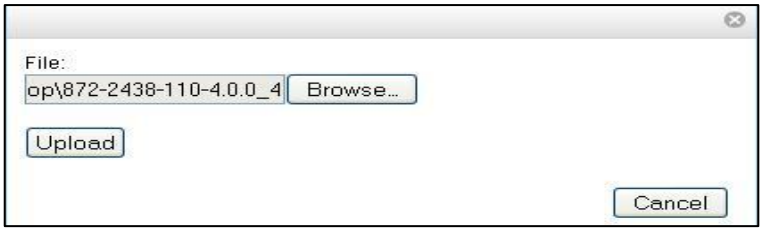
This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

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 4: ISO Administration

S T E P #	This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active NOAM VIP:** Upload ISO to Active NOAM server	There are two methods to upload the application ISO to the Active NOAM based on the type of the media: Execute either: **Option 1** (Use NOAM GUI Upload function for ISO file transfer over the network) Proceed to step 2. **OR** **Option 2** (Local site media ISO transfer, using PM&C). Proceed to step 6.
2. ☐	**Active NOAM VIP:** Option 1 - Transfer via NOAM GUI	**OPTION 1:** 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 **Status & Manage > Files** The Files menu is displayed 3. Click the Active NOAM server in the network. 4. All files stored in the file management storage area of this server display on the screen. 5. 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 **ACTIVE** in the session banner. 6. Click the **Upload** button. The Browse window will open: 

Procedure 4: ISO Administration

3. ☐	**Active NOAM VIP:** Option 1 (cont)	1. **Browse** to select the file to upload. 2. The Choose File window displays, allowing selection of the file to upload.  3. Select the target release ISO image file and click **Open**. 4. The selected file and its path display on the screen.  5. Click **Upload.**

Procedure 4: ISO Administration

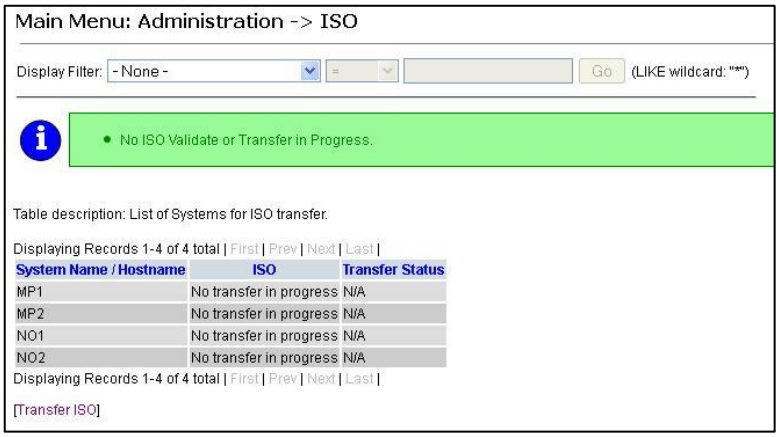
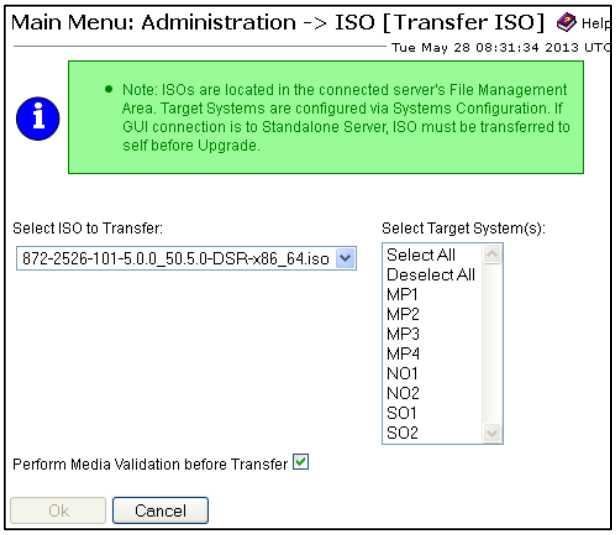
4. ☐	**Active NOAM VIP:**
	Option 1 (cont)
		1. The ISO file begins uploading to the file management storage area.
		2. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This will usually take between 2 to 10 minutes, but more if the network upload speed is slow.
		3. To back up the ISO file to the PMAC, SSH from the Active NOAM and execute the following command. Refer to [4] for creating space on PM&C if desired space is not available on 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 3.*

5. ☐	**Active NOAM VIP:**
	Option 1 (cont) - Copy ISO to the Standby NOAM
		Copy the ISO file to the Standby NOAM
		
		1. Copy the ISO file to the Standby NOAM using the following command from the Active NOAM.
		
		If the source release is 5.x:
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename>`
		`root@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		If the source release is 6.x/7.0:
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename>`
		`admusr@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		2. Execute Steps 3 to 7 of Appendix E to add the ISO image to the PM&C repository.
		
		Proceed to step 8

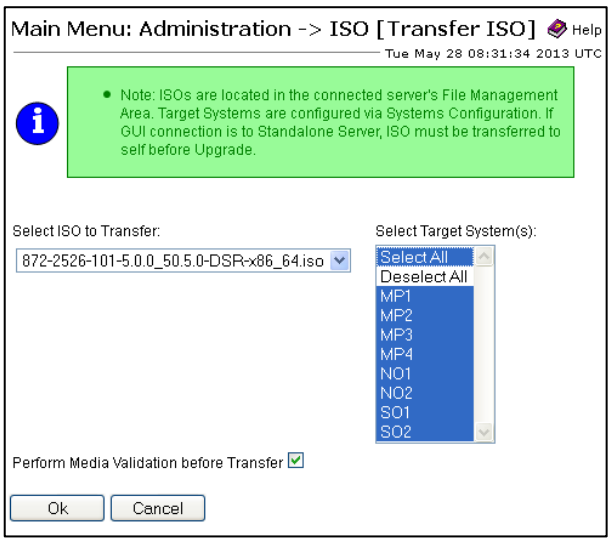
6. ☐	**PM&C Guest:**
	Option 2 - Transfer via PM&C
		OPTION 2 (Local site media ISO transfer, using PM&C):
		
		Using a Media containing the application (recommended for slow network connections between the client computer and the DSR frame
		1. Execute Appendix E to load the ISO onto the PM&C server at the site.
		2. SSH into the PM&C server and SCP the ISO to the Active NOAM using the following commands:
		
		For PM&C 5.0 and DSR 5.x:
		`scp -p /var/TKLC/smac/image/repository/`
		`<DSR_ISO_Filename>`
		`root@<Active_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		For PM&C 5.7 and DSR 6.x/7.0:
		`scp -p /var/TKLC/smac/image/repository/`
		`<DSR_ISO_Filename>`
		`admusr@<Active_NOAM_IP>:/var/TKLC/db/filemgmt`

Procedure 4: ISO Administration

7. ☐	**Active NOAM VIP:**
	Option 2 (cont) - Copy ISO to Standby NOAM
		1. Log into the Active NOAM and execute the following command :
		`chmod 644 /var/TKLC/db/filemgmt/<DSR_ISO_Filename>`
		2. Copy the ISO file to the Standby NOAM using the following command:
		If the source release is 5.x:
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename> root@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`
		If the source release is 6.x/7.0:
		`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.	Transfer the target release ISO image file from the Active NOAM to all other DSR servers. 1. From the Active NOAM GUI, navigate to **Administration >Software Management > ISO Deployment**  2. Click on "**Transfer ISO"** 

Procedure 4: ISO Administration

9. ☐	**Active NOAM VIP:** Continue with the steps shown to the right.	1. Under the "**Select ISO to Transfer:**" drop down menu select the DSR 7.0 ISO. Under the "**Select Target System(s):**" select "**Select All**". 2. Select the checkbox next to "**Perform Media Validation before Transfer**".  3. Click **Ok** 4. 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. 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.

3.3.7 Upgrade TVOE Hosts at a Site (prior to DSR Application Upgrade MW)

This procedure applies if the TVOE Hosts at a site will be upgraded BEFORE the start of the DSR 7.0 upgrade of the NOAMs and other servers. Performing the TVOE upgrade BEFORE reduces the time required for DSR Application Upgrade procedures during the maintenance window.

NOTE: *If the TVOE Hosts will be upgraded in the same Maintenance Windows as the DSR servers, then this procedure does not apply.*

PRECONDITION: *The PMAC Application at each site (and the TVOE Host running the PMAC Virtual server, must be upgraded before performing TVOE Host OS Upgrade for servers that are managed by this PMAC.*

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

Table 5: TVOE Upgrade Execution Overview

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 5	60 min per TVOE Host*	1:00-16:00	Upgrade TVOE Hosts at a Site (prior to DSR Application Upgrade MW)	DSR servers running as virtual guests on the TVOE host will be stopped and unable to perform their DSR 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 5: Upgrade TVOE Hosts at a Site (prior to DSR Application Upgrade MW)

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**.	
	Start of maintenance window	
1. ☐	Record site	Record Site to be upgraded _____
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 PMAC, "Software Inventory" form, will typically list the TVOE Hosts at a site, and their versions.*

Procedure 5: Upgrade TVOE Hosts at a Site (prior to DSR Application Upgrade MW)

3. ☐	Determine if there are SDS Applications on the TVOE Hosts	Log into the TVOE Hosts and execute:
		`# virsh list –all`
		or
		`$ 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.

4. ☐	Upgrade the TVOE hosting a DSR server	Upgrade the TVOE Host of the first server. **Execute Appendix H** **NOTE: This step may cause a failover of the DSR or other active applications on the TVOE.**
5. ☐	Repeat for other TVOE Hosts at a Site	Repeat step 4 for each TVOE Hosts at the site requiring upgrade.
End of maintenance window		

3.4 Software Upgrade Execution Overview

It is recommended to contact MOS as described in Appendix M *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 **Procedure 2**. 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? _____

3.4.1 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 **Section 6** are performed in a separate Maintenance Window to finalize the upgrade. **Procedure 45** "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 (which will also disable provisioning at the SOAM 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 6: NOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 6	0:10-0:30	0:10-0:30	NOAM Pre-Upgrade Checks	None
Procedure 7	0:10-0:30	0:20-1:00	NOAM Health Check and Pre-Upgrade Backup	None
Procedure 8	0:01-0:05	0:21-1:05	Disable Global Provisioning (NOAM Only)	Global and Site Provisioning Disabled
Procedure 9* or Procedure 10*	1:40-2:00	2:01-3:05	NOAM Upgrade or Alternate NOAM Upgrade	No Traffic Impact
Procedure 11	0:01-0:05	2:02-3:10	PCA (formerly PDRA) Topology Hiding Configuration	No Traffic Impact
Procedure 12	0:05-0:15	2:07-3:25	Verify Post Upgrade Status (NOAM)	None

* **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 7.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 7.0 Application upgrade, then see **[Table 5]** for additional time estimates associated with TVOE upgrade.*

4.1 NOAM Pre-Upgrade Checks

This procedure is used to verify that the NOAM NE is ready for upgrade. This procedure must be executed on the Active NOAM.

Procedure 6: NOAM Pre-Upgrade Checks

S T E P #	This procedure performs a Health Check. 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 H for the steps to verify the TVOE Host revision level. (This can also be done from the PMAC 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? _____
2. ☐	Verify ISO for Upgrade has been deployed	Verify the DSR ISO file has been transferred to all servers: Example: **Main Menu: Administration -> ISO** Help Wed Sep 25 17:39:13 2013 UTC Display Filter: - None - = Go (LIKE wildcard: "*") • Transfer ISO Complete. ISO: 872-2526-101-5.0.0_50.12.0-DSR-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 | [Transfer ISO] If not, complete **Section 3.3.6, ISO Administration.** .

System Name / Hostname	ISO	Transfer Status
MP1	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
MP2	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
MP3	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
T2-NO-228-A	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
T2-NO-228-B	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
ipfe1	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
ipfe2	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete

Procedure 6: NOAM Pre-Upgrade Checks

3. ☐	**Active NOAM VIP:**
	Verify that backups are created for all servers
		Verify that a recent COMCOL Environment backup (`backupAllHosts`) 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`
		
		4. Repeat sub-steps 1 through 4 for each site.
		
		See **Section 3.3.5** to perform (or repeat) a full Backup, if needed.

		THIS PROCEDURE HAS BEEN COMPLETED.

4.1.1 NOAM Health Check and Pre-Upgrade Backup

This procedure is used to determine the health and status of the network and servers. 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 7: NOAM Health Check and Pre-Upgrade Backup

S T E P #	This procedure performs a Health Check. 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. ☐	Collect pre-upgrade status depending on the source release	If the source release is 70.20 or later, proceed to step 14. Otherwise, continue with step 2.
2.	**Active NOAM VIP:** Verify Server Status is Normal - NOAM	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. 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 7: NOAM Health Check and Pre-Upgrade Backup

3. ☐	**Active NOAM VIP:** Log all current alarms at NOAM	Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 1. Click the **Report** button to generate an Alarms report. 2. Save the report and/or print the report. Keep these copies for future reference.
4. ☐	**Active NOAM VIP:** View Communication Agent 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.
5. ☐	**Active NOAM VIP:** View SBR status (if equipped)	**If the source release is 5.x/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 source release is 7.0:** 1. Select **Policy and Charging > Maintenance > SBR Status**; The SBR Status screen is displayed. 2. Expand each Server Group. Verify Congestion Level is 'Normal' for all servers.
6. ☐	**Active NOAM VIP:** Export and archive the Diameter configuration data	**If the source release is 5.x:** 1. Select **Main Menu > Diameter Configuration > Export** **If the source release is 6.0 / 7.0:** 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.
7. ☐	**Active NOAM VIP:** Export and archive Configuration Places data	1. Select **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 NOAM VIP:** Backup all global configuration databases for NOAM **IMPORTANT: Required for Disaster Recovery**	1. Select **Status & Manage > Database** to return to the Database Status screen. 2. Click to highlight the **Active NOAM** server; click **Backup.** The Backup and Archive screen is displayed. **(NOTE: the Backup button will only be enabled when the Active server is selected.)** 3. Select the **Configuration** checkbox**.** 4. Enter **Comments** (optional) 5. 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.
9. ☐	**Active NOAM VIP:** Save database backups for NOAM **IMPORTANT: Required for Disaster Recovery**	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**.
10. ☐	**Active SOAM VIP:** Log all current alarms at SOAM	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.

Procedure 7: NOAM Health Check and Pre-Upgrade Backup

11. ☐	**Active SOAM VIP:** 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**
12. ☐	**Active SOAM VIP:** Verify PCA status (if equipped)	1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is 'Available' for all applications
13. ☐	Repeat **Steps 10 - 12** for each SOAM site in the topology.	
	THIS PROCEDURE HAS BEEN COMPLETED.	

14. ☐	**Active NOAM CLI:**
	Verify NOAM pre-Upgrade Status (source release 70.20 and later only)
		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 3.
		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: A report will not be generated if there is no data for a particular entity. The message "No data for report generation" will be recorded in the log.
		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.
		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 7: NOAM Health Check and Pre-Upgrade Backup

15. ☐	**Active SOAM CLI:**
	
	Log SOAM Alarm Status (source release 70.20 and later only)
		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 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck alarmStatusOnSoam`
		
		This command creates a file in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		3. Keep this report for future reference. This report will be compared to alarm and status reports after the upgrade is complete.

16. ☐	**Active SOAM CLI:** View DA-MP Status (source release 70.20 and later only)	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
17. ☐	**Active SOAM CLI:** Verify PCA status (if equipped) (source release 70.20 and later only)	1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. 2. Verify Operational Status is '**Available**' for all applications
18. ☐	• Repeat **Steps 15 - 17** for each SOAM site in the topology.	
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.2 Disable Global Provisioning (NOAM Only)

The following procedure disables provisioning on the NOAM and all Network Element SOAMs. 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 8: Disable Global Provisioning (NOAM Only)

S T E P #	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)**
2. ☐	**Active SOAM VIP:** Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the Active 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.** Repeat sub-steps 1 through 5 for all sites present in the setup.
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 (required) if they were not upgraded previously as recommended in **Section 3.3.7** - *Upgrade TVOE Hosts at a Site (prior to DSR Application Upgrade MW).*

Procedure 9: NOAM Upgrade

S T E P #	This procedure upgrades the TVOE of NOAM servers and upgrades NOAM servers of the setup. 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. ☐	RMS Check	If the NOAM is a guest on an RMS server, perform Appendix C to update the NOAM guest VM configuration. **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. ☐	Upgrade Standby DSR NOAM and DR NOAM servers	NOTE: Before proceeding with this step, execute Appendix H to upgrade the TVOE Hosts if the Standby DR NOAM and/or Standby DSR NOAM are hosted on TVOE blades. 1. Upgrade the Standby DSR NOAM server and Standby DR NOAM(s) (if equipped) in parallel using Upgrade Single Server procedure: **Execute Appendix F** -- Single Server Upgrade Procedure 2. After successfully completing the procedure in Appendix F, 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 = **32532 (Server Upgrade Pending Accept/Reject)** 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)** Alarm ID = **31233 (HA Path Down)** **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action.**
3. ☐	Upgrade Active NOAM and DR NOAM servers	NOTE: Before proceeding with this step, execute Appendix H to upgrade the TVOE Hosts if the Active DR NOAM (mate) and/or Active DSR NOAM (mate) are hosted on TVOE blades. **NOTE: If logged out of the NOAM VIP, login again.** Upgrade the Active NOAM server (the mate) and Active DR NOAM (if equipped) using the Upgrade Single Server procedure: **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step. **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action.**
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.3.1 Alternate NOAM Upgrade

This procedure can be used to upgrade the Standby NOAM for DSRs with a large number of C-level servers. This procedure should only be used when there is a significant delay in the Upgrade GUI screen refresh. This alternate procedure upgrades the Standby NOAM using the PM&C interface rather than the NOAM Upgrade GUI. Subsequent server upgrades should be performed using the normal (NOAM) upgrade GUI.

NOTE: This procedure is applicable when upgrading from a DSR release prior to 5.1.0-51.13.0. Builds later than 51.13.0 feature the Server Group tabs on the Upgrade GUI to alleviate refresh delays.

Procedure 10: Alternate NOAM Upgrade

S T E P #	This procedure upgrades the standby NOAM server using the PM&C interface. 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 ISO to PM&C image repository	If the target ISO is not already present in the PM&C image repository, download the image using Appendix E, Adding ISO Images to PM&C Image Repository
2. ☐	RMS Check	If the NOAM is a guest on an RMS server, perform Appendix C to update the NOAM guest VM configuration. 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.
3. ☐	Upgrade Standby DSR NOAM server	**NOTE:** Before proceeding with this step, execute Appendix H to upgrade the TVOE Hosts if the Standby DR NOAM and/or Standby DSR NOAM are hosted on TVOE blades. Upgrade the Standby DSR NOAM server and Standby DSR DR NOAM(s) (if equipped) in parallel using the PM&C Application Upgrade procedure in reference [4]. After successfully completing the procedure in [4], return to this point and continue with the next step. The NOAM GUI will show the new DSR 7.0 release.
4. ☐	Upgrade Active NOAM server	**NOTE:** Before proceeding with this step, execute Appendix H to upgrade the TVOE Hosts if the Active DR NOAM (mate) and/or Active DSR NOAM (mate) are hosted on TVOE blades. **NOTE: If logged out of the NOAM VIP, log into the NOAM VIP again.** Upgrade the Active NOAM server (the mate) and Active DR NOAM (if equipped) using the Upgrade Single Server procedure: **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
	THIS PROCEDURE HAS BEEN COMPLETED.	

4.3.2 PCA (formerly PDRA) Topology Hiding Configuration

In DSR 7.0, the Policy and Charging Topology Hiding configuration has 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 to DSR 7.0.

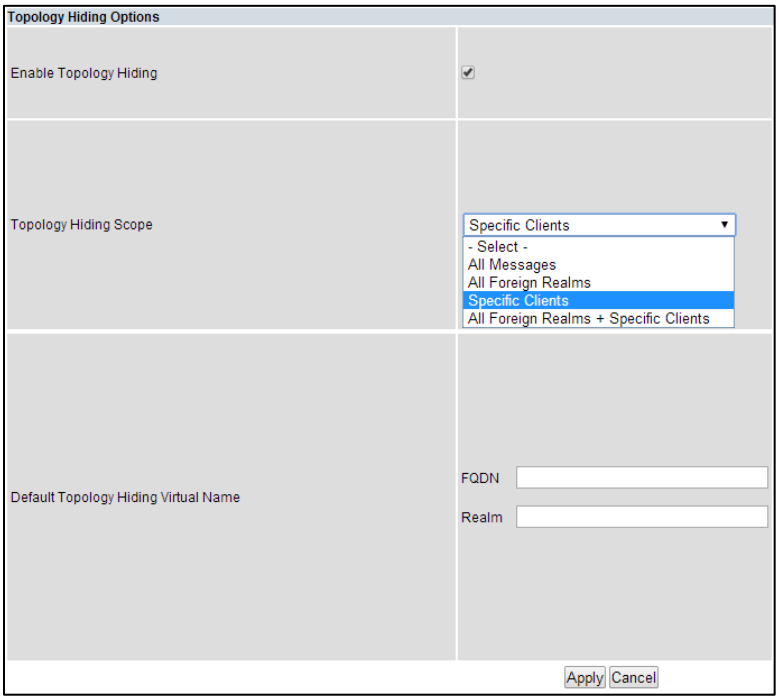
NOTE: The network-wide Topology Hiding settings at the NOAM will apply to each site as it is upgraded. Please note that this may result in a behavior change if the pre-upgrade site settings differ from the network-wide settings.

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

Procedure 11: PCA (formerly PDRA) Topology Hiding Configuration

S T E P #	This procedure sets the network-wide Topology Hiding configuration. This procedure applies only to systems with the Policy and Charging feature enabled. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Enable Global Provisioning	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 11: PCA (formerly PDRA) Topology Hiding Configuration

2. ☐	**Active NOAM VIP:** Configure Topology Hiding settings	1. Navigate to **Policy and Charging > Configuration > Policy DRA > Network-Wide Options**. 2. In the Topology Hiding Options section, select the **Enable Topology Hiding** 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 **Apply**. 
3. ☐	**Active NOAM VIP:** Disable global provisioning and configuration.	1. Select **Status & Manage > Database.** The Database Status screen is displayed 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. 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.

4.4 Verify Post Upgrade Status (NOAM)

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

Procedure 12: Verify Post Upgrade Status (NOAM)

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. ☐	Collect upgrade status depending on the target release	If the source release is 70.20 or later, proceed to step 11. Otherwise, continue with step 2.

2. ☐	**NOAM CLI:**
	Verify Upgrade Status
		1. Execute the following commands on the Active NOAM, Standby NOAM, Active DR NOAM, and Standby DR NOAM servers :
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		`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 3.
		`$ sudo verifyUpgrade`
		3. Examine the output of the above command to determine if any errors were reported. In case of errors it is recommended to contact MOS before proceeding.
		`$ alarmMgr --alarmstatus`
		The following alarm output should be seen, indicating that the upgrade completed.
		`SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33|tpdServerUpgradePendingAccept|1.3.6.1.4.1.323.5.3.18.3.1.3.33`
		[Alarm ID 32532 will be cleared after the upgrade is accepted.]
		It is recommended to contact MOS if the above output is not generated.

3. ☐	**NOAM CLI:** 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.
4. ☐	**Active NOAM VIP:** Log all current 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. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)** All other upgraded servers will have the following expected alarm: Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

Procedure 12: Verify Post Upgrade Status (NOAM)

5. ☐	**Active NOAM VIP:** View Communication Agent 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.
6. ☐	**Active NOAM VIP:** View SBR status (if equipped)	1. Select **Policy and Charging > Maintenance > SBR Status;** The SBR Status screen is displayed. 2. Expand each Server Group. Verify **Congestion Level** is 'Normal' for all servers.
7.	**Active SOAM VIP:** Verify SOAM Alarm status	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. The Active SOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
8.	**Active SOAM VIP:** 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. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count.
9.	**Active SOAM VIP:** Verify PCA status (if equipped)	1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications
10.	**Active SOAM VIP:** Verify Traffic status	1. Select **Status & Manage > KPIs** 2. Inspect KPI reports to verify traffic is at the expected condition.
	PROCEED TO STEP 17	

11.	**ACTIVE NOAM CLI:**
	Verify NOAM Upgrade Status
	(source release 70.20 and later only)
		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 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck verifyUpgradeStatusOnNoam`
		
		This command will analyze the upgrade log for errors and check the alarm status. Any errors found in the upgrade log will be output to the screen. Likewise, any alarms detected by alarmMgr will be output to the screen.
		
		3. Analyze the command output to determine if any unexpected alarms exist in the system. The following alarm output should be seen, indicating that the upgrade completed.
		
		`SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33|tpdServerUpgradePendingAccept|1.3.6.1.4.1.323.5.3.18.3.1.3.33`
		
		[Alarm ID 32532 will be cleared after the upgrade is accepted.]
		
		It is recommended to contact MOS if the above output is not generated.

Procedure 12: Verify Post Upgrade Status (NOAM)

12.	**ACTIVE NOAM CLI:**
	
	Verify Upgrade Health Check
	(source release 70.20 and later only)
		1. Enter the command:
		
		`$ upgradeHealthCheck postUpgradeHealthCheck`
		
		This command will create 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`
		
		2. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact MOS for guidance.
		
		3. Compare the post-upgrade reports with the pre-upgrade reports to verify that the upgrade did not adversely impact system operations.

13.	**ACTIVE SOAM CLI:**
	
	Log SOAM Alarm Status
	(source release 70.20 and later only)
		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 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck alarmStatusOnSoam`
		
		This command creates a file in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		3. Compare the post-upgrade alarm report with the pre-upgrade alarm report to verify that the upgrade did not adversely impact system operations.

14.	**ACTIVE SOAM CLI:** View DA-MP Status	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____ 4. Compare the post-upgrade number of connections with the pre-upgrade number recorded in **Procedure 7**. Verify that any discrepancy in the number of connections is accountable.

Procedure 12: Verify Post Upgrade Status (NOAM)

15.	**ACTIVE NOAM CLI:** Verify PCA status (if equipped)	1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. 2. Verify Operational Status is 'Available' for all applications

16.	**ACTIVE SOAM CLI:**
	
	Verify traffic status
		1. Enter the command:
		
		`$ upgradeHealthCheck trafficStatusOnSoam`
		
		This command will create a file in `/var/TKLC/db/filemgmt/UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_KPIReport_<date-time>.xml`
		
		2. Inspect the KPI report to verify traffic is at the expected condition.

17. ☐	**Active NOAM VIP:**
	
	Update Appworks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NOAM server
		Note 1: This step is only applicable if the setup includes IPFE servers. This step will handle the possible audit discrepancies which may occur after upgrading the IPFE servers. This step prepares the Active NOAM to handle any such discrepancies.
		
		Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute the ipfeNetUpdate.sh script on the IPFE servers after the upgrade. AppWorks performs an audit on the configured IPFE Ethernet devices and will update them with the locally stored information in case of any discrepancies.
		
		Note 3: The steps below will update the locally stored information with the performance optimization parameters. This script checks the Ethernet devices on the servers functioning as IPFE and updates the locally store information for those devices
		
		Log into Active NOAM console and execute the following command:
		
		`$ /usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh`
		
		Output similar to the following may be produced by the command:
		
		`eth0 on IPFE => '--set-ring eth0 rx 4078; --offload eth0 gro off gso off'`
		`eth1 on IPFE => '--set-ring eth1 rx 4078; --offload eth1 gro off gso off'`
		
		NOTE: This command may execute with no output if no changes are required (no devices were found to update).

		THIS PROCEDURE HAS BEEN COMPLETED.

4.5 Allow Provisioning *(post NOAM Upgrade)*

The following procedure enables Global Provisioning, as well as Site Provisioning for all Network Elements.

CAUTION

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

Procedure 13: Allow Provisioning *(post NOAM Upgrade)*

S T E P #		
	This procedure enables provisioning for the NOAM (and DR-NOAM) servers, and all site 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 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.**
2. ☐	**Active SOAM VIP:** Enable Site Provisioning	Enable Site provisioning for all the sites present in the setup : 1. Log into the Active 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**. Repeat sub-steps 1 through 5 for all sites present in the setup.
3. ☐	**Active NOAM VIP:** Add new Network Element (if required).	**Skip this step if the addition of a new Network Element is not 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 5.x Installation Procedures ([5], [6]), the DSR 6.x Installation Procedures ([7], [8]) or the DSR 7.0 Installation Procedures ([9], [10]) 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.	

4.6 Network Device Check *(post NOAM Upgrade)*

This procedure verifies, and corrects if necessary, the configuration status of the signaling network interfaces. Network devices that were provisioned via the command line will have a configuration status of "Discovered", as opposed to a status of "Deployed" for devices that are configured via the GUI. Any network devices that will be used for the External Signaling Interface (XSI) must be manually transitioned to the Deployed state using this procedure.

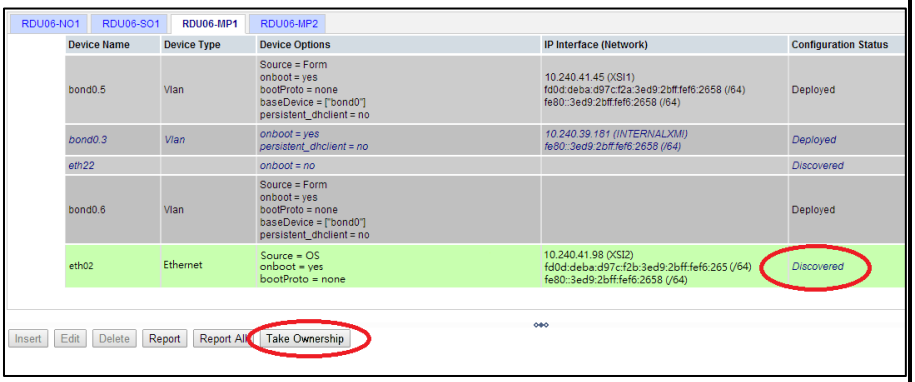
NOTE: For additional information on identifying and configuring External Signaling Interfaces, refer to [6] or [8] as appropriate.

NOTE: This procedure is applicable to upgrades from 5.0 only. This procedure is not necessary for upgrades from 5.1, 6.x, or 7.0.

Table 7: Network Device Check Execution Overview

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 14	0:15 to 0:30	0:15 to 0:30	Network Device Check	Failure to complete this procedure may result in traffic loss.

Procedure 14: Network Device Check

S T E P #	This procedure verifies/corrects the configuration status for the signaling network interfaces. 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 Network Device status	Log into the NOAM GUI and verify the Network Device status: 1. Navigate to **Main Menu > Configuration > Network** 2. Note the Network Name of all External Signaling Interfaces (XSI) 3. Navigate to **Configuration > Network > Devices.** The Network Devices form is displayed. 4. Select an MP or IPFE Server Group tab. (Network devices installed on the server are displayed). 5. For each device that is being used as an unbonded External Signaling Interface (XSI), note the **Configuration Status** column. If the status is ***Discovered***, select the device and click the **Take Ownership** button (refer to [6] or [8] for additional information).  6. Verify the device status changes to **Configured.** NOTE: The status will transition to **Deployed** after all C-level servers that use the interface have been upgraded. Repeat sub-steps 5 through 7 for each MP and IPFE Server Group.
	THIS PROCEDURE HAS BEEN COMPLETED.	

5 SOAM UPGRADE EXECUTION

SOAM UPGRADE: Pre-Upgrade Activities (All Configurations)

Use this section to execute pre-upgrade backups, pre-checks and to disable Site Provisioning for all SOAM configurations.

This section contains the procedures for Pre-Upgrade backups, Pre-Checks and the disabling of Site Provisioning which apply to all DSR 7.0 Upgrade configurations.

5.1 Select SOAM Site Upgrade Path

This section provides the detailed procedure steps of the site upgrade execution. These procedures are executed inside a maintenance window.

Use the answers to the following questions to select the required upgrade procedure from **Table 8**. The right-most column indicates the section of this document that applies.

Is the DA-MP redundancy (1+1) or (N+0)? _____

Are there PCA or SBR servers to upgrade? _____

*It is recommended that the specific upgrade sections be identified **before the Maintenance window**, and sections that will not be used are "grayed out" to avoid any confusion during the MW activity.*

Record Upgrade type selected from Table 8: _____

Table 8: Upgrade Path Reference

Type	Supported Configurations	Upgrade Path	Section Reference
All	Pre-Upgrade backups, Pre-Checks and disable Site Provisioning (All SOAM Sites)	All	Section 5.2
1	DSR 7.0 upgrade for (1+1 / RMS 1+1) configuration (major or incremental)	SOAM Upgrade (1+1 / RMS 1+1)	Section 5.3
2	DSR 7.0 upgrade for (N+0 / RMS N+0) configuration (major or incremental)	SOAM Upgrade (N+0 / RMS N+0)	Section 5.4
5	PCA DSR 7.0 upgrade (major or incremental)	PCA Upgrade	Section 5.5

5.1.1 SOAM Pre-Upgrade Activities Overview (All Configurations)

This section contains the steps required to perform pre-upgrade activities (major or incremental) for all DSR SOAM sites.

Table 9: SOAM Pre-Upgrade Activities Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 15	0:10-0:20	0:10-0:20	SOAM Pre-Upgrade Backups (All Configurations)	None
Procedure 16	0:20-0:25	0:20-0:35	SOAM Pre-Upgrade Health Check (All Configurations)	None
Procedure 17	1:40-2:00	2:00-2:35	Disable Site Provisioning (All SOAM Configurations)	Site Provisioning Disabled, No Traffic Impact

5.2 SOAM Pre-Upgrade Activities

5.2.1 SOAM Pre-Upgrade Backups (All Configurations)

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 15: SOAM Pre-Upgrade Backups (All Configurations)

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**	
1. ☐	**Active SOAM VIP:** Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	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, and then click **Backup.** The Backup and Archive screen is displayed. **(NOTE: the Backup button will only be enabled when the Active server is selected.)** 4. Selected the **Configuration** checkbox. 5. Enter **Comments** (optional). 6. 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**	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**.

3. ☐	**Active SOAM VIP:**
	SSH to the Active SOAM
		Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active SOAM:
		
		If the source release is 5.x:
		`ssh root@<SOAM_VIP>`
		
		If the source release is 6.x/7.0:
		`ssh admusr@<SOAM_VIP>`

4. ☐	**Active SOAM VIP:**
	If logged in as "admusr" use "sudo" to become the "root" user.
		If logged in as "admusr", become the "root user:
		
		`$ sudo su -`
		`#`

Procedure 15: SOAM Pre-Upgrade Backups (All Configurations)

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**	
5. ☐	**Active SOAM VIP:** 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.)

6. ☐	**Active SOAM VIP:**
	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.]
		If the source release is 5.0.x:
		The following option allows the user to select either a single hostname or multiple hostnames associated with a given SOAM site to be upgraded:
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1,hostname2…hostnameN>`
		If the source release is 5.1.x or higher:
		The following option **(siteId)** allows the user to select all servers associated with a given SOAM site to be upgraded:
		`$ /usr/TKLC/dpi/bin/backupAllHosts --site=<siteId>`
		…where **<siteId>** 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:
		`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.

Procedure 15: SOAM Pre-Upgrade Backups (All Configurations)

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**	
7. ☐	**Active SOAM VIP:** 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.

8. ☐	**Active SOAM VIP:**
	Exit the "root" user session back to the "admusr" user session.
		`# exit`
		`logout`
		`$`

9. ☐	**ALTERNATIVE METHOD (Optional)**
	
	Server CLI:
	If needed, the Alternative backup method can be executed on each individual server instead of using the **"backupAllHosts"** script.
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		
		Output similar to the following 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.`

10. ☐	**Active NOAM VIP:**
	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.

	THIS PROCEDURE HAS BEEN COMPLETED.	

5.2.2 SOAM Pre-Upgrade Health Check (All Configurations)

This procedure is non-intrusive and performs a health check of the site prior to upgrading.

Procedure 16: SOAM Pre-Upgrade Health Check (All Configurations)

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. ☐	Collect pre-upgrade status depending on the source release	If the source release is 70.20 or later, proceed to step 8. Otherwise, continue with step 2.
2. ☐	**Active SOAM VIP:** Verify Server Status is Normal	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.
3. ☐	**Active SOAM VIP:** Log all current 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.
4. ☐	**Active SOAM VIP:** Capture the 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.
5. ☐	**Active SOAM VIP:** 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.**

Procedure 16: SOAM Pre-Upgrade Health Check (All Configurations)

6. ☐	**Active SOAM VIP:** Capture Transport Manager configuration (if MD-IWF equipped) **NOTE:** *Perform this step only if the MD-IWF feature is provisioned*.	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.
7. ☐	**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*.	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.
	PROCEED TO STEP 11	

Procedure 16: SOAM Pre-Upgrade Health Check (All Configurations)

8. ☐	**ACTIVE SOAM CLI:**
	
	Verify SOAM pre-Upgrade Status *(source release 70.20 and later only)*
		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 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		
		This command creates three files in `/var/TKLC/db/filemgmt/UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		
		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.
		
		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.

9. ☐	**ACTIVE SOAM CLI:** Capture Diameter Maintenance Status *(source release 70.20 and later only)*	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.
10. ☐	**ACTIVE SOAM CLI:** View DA-MP Status *(source release 70.20 and later only)*	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
11. ☐	**ACTIVE SOAM VIP:** Capture Diameter Configuration on Active SOAM GUI	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. Verify the requested data is exported using the tasks button at the top of the screen. 4. 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.
12. ☐	Capture Data for each SOAM Site	**Repeat steps 1 through 11 for each configured SOAM Site to be upgraded.**
		THIS PROCEDURE HAS BEEN COMPLETED.

5.2.3 Disable Site Provisioning (All SOAM Configurations)

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 17: Disable Site Provisioning (All SOAM Configurations)

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 MOS AND ASK FOR UPGRADE ASSISTANCE.	
1. ☐	**Active SOAM VIP:** Disable Site Provisioning	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 002] - Global provisioning has been manually disabled**. The Active SOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
	THIS PROCEDURE HAS BEEN COMPLETED.	

SOAM UPGRADE
ACTIVE / STANDBY (1+1 / RMS 1+1)

Use this section to upgrade Active/Standby (1+1) configurations.

5.3 SOAM Upgrade (1+1 / RMS 1+1)

This section contains the steps required to perform an upgrade (major or incremental) for a DSR site with an SOAM, and an Active/Standby (1+1) DA-MP redundancy configuration.

NOTE: For any DSR system consisting of multiple sites (signaling network elements), it is not recommended to apply the upgrade to more than one network element within a single maintenance window.

To maximize Maintenance Window usage, the Standby DA-MP may be upgraded in parallel with the Standby SOAM.

TVOE Hosts may be upgraded during this procedure, if they need to be upgraded. The Elapsed Time mentioned in table below specifies the time with TVOE upgrade and without TVOE upgrade. It assumes that each of the SOAM servers is running on a TVOE Host (i.e. it assumes that there are 2 TVOE hosts to be upgraded at the site.)

During the Site upgrade, global and site provisioning are disabled. Both may re-enable at the completion of the site upgrade.

5.3.1 RMS 1+1

This section contains the steps required to upgrade a DSR, deployed on RMSs, and whose DA-MPs are in the Active/Standby (1+1) configuration.

The following commercial deployment types are supported:

1) 2 RMS servers, one site, no IDIH
2) 3 RMS servers, one site, with one server reserved for IDIH (and IDIH storage)
3) 4 RMS servers, 2 sites with 2 servers per site, no IDIH
4) 6 RMS servers, 2 sites with 3 servers per site, 1 server at each site reserved for IDIH (and IDIH storage)

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 is without 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.

Global provisioning can be re-enabled between scheduled maintenance windows.

NOTE: For any DSR system consisting of multiple sites (signaling network elements), it is not recommended to apply the upgrade to more than one network element within a single maintenance window.

To maximize Maintenance Window usage, the Standby DA-MP and half of the SS7-MPs may be upgraded in parallel with the Standby SOAM.

During the Site upgrade, global and site provisioning are disabled. Both may re-enable at the completion of the site upgrade.

Table 10: Site Upgrade Execution Overview (1+1 / RMS 1+1).

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 15	0:10-0:20	0:10-0:20	SOAM Pre-Upgrade Backups (All Configurations)	None
Procedure 16	0:20-0:25	0:20-0:35	SOAM Pre-Upgrade Health Check (All Configurations)	None
Procedure 17	1:40-2:00	2:00-2:35	Disable Site Provisioning (All SOAM Configurations)	Site Provisioning Disabled, No Traffic Impact
Procedure 18*	1:40-2:00	3:40-4:35	Upgrade SOAMs (1+1 / RMS 1+1)	Site Provisioning Disabled, No Traffic Impact
Procedure 19	1:20-1:40	5:00-6:15	Upgrade DA-MPs (1+1 / RMS 1+1)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 20	0:40-2:40	5:40-8:55	Upgrade Multiple SS7-MPs (1+1 / RMS 1+1)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 35	0:02	5:02-8:57	Allow Site Provisioning (All SOAM Configurations)	Site Provisioning Enabled (SOAM).
Procedure 36	0:10-0:15	5:12-9:12	Verify Post-Upgrade Status (All SOAM Configurations)	None

* **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 7.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 7.0 Application upgrade, then see **[Table 5]** for additional time estimates associated with TVOE upgrade.*

!! WARNING!!

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

Procedure 15; Procedure 16; Procedure 17

5.3.2 Upgrade SOAMs (1+1 / RMS 1+1)

For each site in the DSR, the SOAM(s) (Procedure 18) and associated DA-MPs (Procedure 19) should be upgraded within a single maintenance window. Additionally, Oracle CGBU recommends that only a single site be upgraded in any particular maintenance window.

Procedure 18: Upgrade SOAMs (1+1 / RMS 1+1)

S T E P #	This procedure upgrades the SOAM(s) in a DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. 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	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 17** - *Disable Site Provisioning (All SOAM Configurations)*. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, skip to **Step 3**, otherwise, execute the sub-steps below. 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.**
3. ☐	Upgrade TVOE Host for Standby SOAM server	If the TVOE Host for the Standby SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Standby SOAM **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.**
4. ☐	**Active NOAM VIP:** Upgrade Standby SOAM	Upgrade the Standby SOAM server using Upgrade Single Server procedure : **Execute Appendix F** - Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
5. ☐	Upgrade TVOE Host for Active SOAM Server	If the TVOE Host for the Active SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Active SOAM. **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.**

Procedure 18: Upgrade SOAMs (1+1 / RMS 1+1)

6. ☐	**Active NOAM VIP:** Upgrade Active SOAM	Upgrade the Active SOAM server using Upgrade Single Server procedure : **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
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 Upgrade DA-MPs (1+1 / RMS 1+1)

Detailed steps on upgrading the MPs are shown in the procedure below. In the Active/Standby (1+1) configuration, the Standby DA-MP is upgraded first, followed by the Standby. Preparing the Active DA-MP for upgrade will cause an HA switchover.

Procedure 19: Upgrade DA-MPs (1+1 / RMS 1+1)

S T E P #	This procedure upgrades the DA-MP(s). 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 and Record the status of the DA-MP before upgrade	Verify and record the status and hostname of the Active DA-MP and of the Standby DA-MP by going to **Status & Manage > HA**. **NOTE: The Active DA-MP server can be identified by looking for the "VIP" label. The server with VIP in the row is the Active DA-MP.**
2. ☐	**RMS Expansion MPs Only:** Upgrade TVOE Host for the Expansion MP server.	If the TVOE Host for the Expansion MP needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Expansion MP server. **NOTE: In an RMS-based DSR, the MPs on the Core server TVOE Hosts have already been upgraded as part of the NOAM upgrade. However, the TVOE Host of the Expansion MPs (if equipped), must be verified independently.**
3. ☐	**Active NOAM VIP:** Upgrade the standby DA-MP server	Upgrade the Standby DA-MP server using the Upgrade Single Server procedure: **Execute Appendix F** - Single Server Upgrade for the Standby DA-MP. After successfully completing the procedure in **Appendix F**, return to this point and continue with the next step.
4. ☐	**RMS Expansion MPs Only:** Upgrade TVOE Host for the Expansion MP server.	If the TVOE Host for the Expansion MP needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Expansion MP server. **NOTE: In an RMS-based DSR, the MPs on the Core server TVOE Hosts have already been upgraded as part of the NOAM upgrade. However, the TVOE Host of the Expansion MPs (if equipped), must be verified independently.**

Procedure 19: Upgrade DA-MPs (1+1 / RMS 1+1)

5. ☐	**Active NOAM VIP:** Upgrade the Active DA-MP server	Upgrade the Active DA-MP server using the Upgrade Single Server procedure. **Execute Appendix F** - Single Server Upgrade for the Active DA-MP. After successfully completing the procedure in **Appendix F**, return to this point and continue with the next step.
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.3.4 Upgrade Multiple SS7-MPs (1+1 / RMS 1+1)

The following procedure is used to upgrade the SS7-MPs in the SS7-IWF server groups. The effect on the Diameter network traffic must be considered, since any SS7-MP being upgraded will not be handling live traffic.

Procedure 20 must be executed for all configured SS7-MPs at a site, regardless of how the MPs are grouped for upgrade. So if eight SS7-MPs are upgraded four at a time, then Procedure 20 must be executed twice.

Procedure 20: Upgrade Multiple SS7-MPs (1+1 / RMS 1+1)

S T E P #	This procedure upgrades the SS7-MPs. 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 SS7-MPs to be upgraded together, if equipped	If SS7-MPs are deployed, choose the number of MP(s) on which upgrade can be executed in parallel, considering traffic.
2. ☐	**RMS Expansion MPs Only:** Upgrade TVOE Host for the Expansion MP server.	If the TVOE Host for the Expansion MP needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Expansion MP server. **NOTE: In an RMS-based DSR, the MPs on the Core server TVOE Hosts have already been upgraded as part of the NOAM upgrade. However, the TVOE Host of the Expansion MPs (if equipped), must be verified independently.**
3. ☐	**Active NOAM VIP:** Upgrade selected SS7-MPs	Upgrade the selected SS7-MPs, executing the Upgrade Multiple Server procedure on all selected SS7-MPs in parallel. **Execute Appendix I -** Upgrade Multiple Servers After successfully completing the procedure in **Appendix I**, for all selected SS7-MPs, return to this point and continue with the next procedure.
4. ☐	Repeat for all SS7-MP servers	• Repeat Step 1 - 2 for the next set of SS7-MP servers to be upgraded in parallel.
	THIS PROCEDURE HAS BEEN COMPLETED.	

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

- **Procedure 35 - Allow Site Provisioning (All SOAM Configurations)**
- **Procedure 36 - Verify Post-Upgrade Status (All SOAM Configurations)**

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

- **Procedure 45 - Accepting Upgrade**

SOAM UPGRADE
MULTI-ACTIVE (N+0 / RMS N+0)

Use this section to upgrade Multi-Active (N+0) configurations.

5.4 SOAM Upgrade (N+0 / RMS N+0)

This section contains the steps required to perform an upgrade (major or incremental) for a DSR site with an SOAM, and a multiple-active (N+0) DA-MP configuration.

NOTE: For any DSR system consisting of multiple sites (signaling network elements), it is not recommended to apply the upgrade to more than one network element within a single maintenance window.

To maximize Maintenance Window usage, DA-MPs and IPFEs may be upgraded in parallel with the Standby SOAM.

TVOE Hosts may be upgraded during this procedure, if they need to be upgraded. The Elapsed Time mentioned in table below specifies the time with TVOE upgrade and without TVOE upgrade. It assumes that each of the SOAM servers is running on a TVOE Host (i.e. it assumes that there are 2 TVOE hosts to be upgraded at the site.)

During the Site upgrade, global and site provisioning are disabled. Both may re-enable at the completion of the site upgrade.

5.4.1 RMS N+0

This section contains the steps required to upgrade a DSR, deployed on RMS, with DA-MPs in the multi-active (N+0) configuration.

The following commercial deployment types are supported:

1) 2 RMS servers, one site, no IDIH
2) 3 RMS servers, one site, with one server reserved for IDIH (and IDIH storage)
3) 4 RMS servers, 2 sites with 2 servers per site, no IDIH
4) 6 RMS servers, 2 sites with 3 servers per site, 1 server at each site reserved for IDIH (and IDIH storage)

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 is without 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.

Global provisioning can be re-enabled between scheduled maintenance windows.

NOTE: For any DSR system consisting of multiple sites (signaling network elements), it is not recommended to apply the upgrade to mated sites within a single maintenance window.

To maximize Maintenance Window usage, DA-MPs, SS7-MPs, and IPFEs may be upgraded in parallel with the Standby SOAM.

During the Site upgrade, global and site provisioning are disabled. Both may re-enable at the completion of the site upgrade.

Table 11: Site Upgrade Execution Overview (N+0 / RMS N+0)

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 15	0:10-0:20	0:10-0:20	SOAM Pre-Upgrade Backups (All Configurations)	None
Procedure 16	0:20-0:25	0:30-0:45	SOAM Pre-Upgrade Health Check (All Configurations)	None
Procedure 17	1:40-2:00	2:10-2:45	Disable Site Provisioning (All SOAM Configurations)	Site Provisioning Disabled, No Traffic Impact
Procedure 21*	1:40-2:00	3:50-4:45	Upgrade SOAMs (N+0 / RMS N+0)	Site Provisioning Disabled, No Traffic Impact
Procedure 22	0:40-2:40	4:30-7:25	Upgrade Multiple DA-MPs (N+0 / RMS N+0)	Traffic handled by MP(s) not being upgraded.
Procedure 23	0:40-2:40	5:10-10:05	Upgrade Multiple SS7-MPs (N+0 / RMS N+0)	Traffic handled by MP(s) not being upgraded.
Procedure 24	0:40-1:20	5:50-10:25	Upgrade IPFE(s) (N+0 / RMS N+0)	No Traffic Impact
Procedure 35	0:02	5:52-10:27	Allow Site Provisioning (All SOAM Configurations)	Site Provisioning Enabled (SOAM).
Procedure 36	0:10-0:15	6:02-10:42	Verify Post-Upgrade Status (All SOAM Configurations)	None

* **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 7.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 7.0 Application upgrade, then see **[Table 5]** for additional time estimates associated with TVOE upgrade.*

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

Procedure 15; Procedure 16; Procedure 17

5.4.2 Upgrade SOAMs (N+0 / RMS N+0)

For each site in the DSR, the SOAM(s) and associated MPs and IPFEs should be upgraded within a single maintenance window. Additionally, Oracle CGBU recommends that only a single site be upgraded in any particular maintenance window.

Procedure 21: Upgrade SOAMs (N+0 / RMS N+0)

STEP #		
	This procedure upgrades the SOAM(s) in a DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. 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	1. Log into the SOAM GUI using the VIP. 2. 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 17** - *Disable Site Provisioning (All SOAM Configurations)*. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, skip to **Step 3**, otherwise, execute the sub-steps below. 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.**
3. ☐	Upgrade TVOE Host for Standby SOAM server	If the TVOE Host for the Standby SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Standby SOAM **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.**
4. ☐	**Active NOAM VIP:** Upgrade Standby SOAM	Upgrade the Standby SOAM server using Upgrade Single Server procedure : **Execute Appendix F** - Single Server Upgrade Procedure After successfully completing the procedure in **Appendix F**, return to this point and continue with the next step.
5. ☐	Upgrade TVOE Host for Active SOAM Server	If the TVOE Host for the Active SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Active SOAM. **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.**

Procedure 21: Upgrade SOAMs (N+0 / RMS N+0)

6. ☐	**Active NOAM VIP:** Upgrade Active SOAM	Upgrade the Active SOAM server using the Upgrade Single Server procedure : **Execute Appendix F** - Single Server Upgrade Procedure After successfully completing the procedure in **Appendix F**, return to this point and continue with the next step.
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.

5.4.3 Upgrade Multiple DA-MPs (N+0 / RMS N+0)

The following procedure is used to upgrade the DA-MPs in a multi-active DA-MP cluster. In a multi-active DA-MP cluster, all of the DA-MPs are Active; there are no Standby DA-MPs. So the effect on the Diameter network traffic must be considered, since any DA-MP being upgraded will not be handling live traffic.

If the DSR being upgraded is running OFCS, ensure that the DA-MPs are upgraded on an enclosure basis. That is, upgrade the DA-MPs in one enclosure first, and only after the first enclosure has been successfully upgraded should the DA-MPs in the second enclosure be upgraded. This approach will ensure service is not affected.

Procedure 22 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 22 must be executed four distinct times.

Procedure 22: Upgrade Multiple DA-MPs (N+0 / RMS N+0)

S T E P #	This procedure upgrades the DA-MP. 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	Choose the number of MP(s) on which upgrade can be executed in parallel, considering traffic. **NOTE:** *Never select more than ½ of the installed MPs to be upgraded in parallel to avoid traffic impact.* **NOTE: It is recommended that the DA-MP Leader and the Designated Controller be upgraded in the last group of servers to minimize DA-MP Leader and Designated Controller role changes.**
2. ☐	**RMS Expansion MPs Only:** Upgrade TVOE Host for the Expansion MP server.	If the TVOE Host for the Expansion MP needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Expansion MP server. **NOTE: In an RMS-based DSR, the MPs on the Core server TVOE Hosts have already been upgraded as part of the NOAM upgrade. However, the TVOE Host of the Expansion MPs (if equipped), must be verified independently.**

Procedure 22: Upgrade Multiple DA-MPs (N+0 / RMS N+0)

3. ☐	**Active NOAM VIP:** Upgrade Active DA-MPs	Upgrade the selected DA-MPs, executing the Upgrade Multiple Server procedure on all selected DA-MPs in parallel. **Execute Appendix I -** Upgrade Multiple Servers After successfully completing the procedure in **Appendix I**, for all selected DA-MPs, return to this point and continue with the next procedure.
4. ☐	Repeat for all DA-MP servers	• Repeat steps 1 and 2 for the next set of DA-MP servers to be upgraded in parallel.
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.4.4 Upgrade Multiple SS7-MPs (N+0 / RMS N+0)

The following procedure is used to upgrade the SS7-MPs in the SS7-IWF server groups. The effect on the Diameter network traffic must be considered, since any SS7-MP being upgraded will not be handling live traffic.

Procedure 23 must be executed for all configured SS7-MPs of a site, regardless of how the MPs are grouped for upgrade. So if eight SS7-MPs are upgraded four at a time, then Procedure 23 must be executed twice.

Procedure 23: Upgrade Multiple SS7-MPs (N+0 / RMS N+0)

S T E P #	This procedure upgrades the SS7-MPs. 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 SS7-MPs to be upgraded together, if equipped.	If SS7-MPs are deployed, choose the number of MP(s) on which upgrade can be executed in parallel, considering traffic.
2. ☐	**RMS Expansion MPs Only:** Upgrade TVOE Host for the Expansion MP server.	If the TVOE Host for the Expansion MP needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Expansion MP server. **NOTE: In an RMS-based DSR, the MPs on the Core server TVOE Hosts have already been upgraded as part of the NOAM upgrade. However, the TVOE Host of the Expansion MPs (if equipped), must be verified independently.**
3. ☐	**Active NOAM VIP:** Upgrade selected SS7-MPs	Upgrade the selected SS7-MPs, executing the Upgrade Multiple Server procedure on all selected SS7-MPs in parallel. **Execute Appendix I -** Upgrade Multiple Servers After successfully completing the procedure in **Appendix I**, for all selected SS7-MPs, return to this point and continue with the next procedure.
4. ☐	Repeat for all SS7-MP servers	• Repeat Step 1 - 2 for the next set of SS7-MP servers to be upgraded in parallel.
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.4.5 Upgrade IPFE(s) (N+0 / RMS N+0)

If none of the signaling network elements in the DSR being upgraded has IPFE servers installed, skip this section and proceed to next procedure. Otherwise, the following procedure must be executed independently for each signaling network element that has IPFE servers installed.

Procedure 24: Upgrade IPFE(s) (N+0 / RMS N+0)

S T E P #	This procedure upgrades the IPFE(s). 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 IPFE upgrade order	Choose the number of IPFEs to be upgraded in parallel, considering traffic impact. The selected IPFEs should belong to same enclosure, and only after the first enclosure has been successfully upgraded should the IPFE(s) in the second enclosure be upgraded.
2. ☐	**Active NOAM VIP:** Upgrade IPFE servers	Upgrade the IPFEs identified in step 1 in parallel, using the Upgrade Multiple Server procedure. **Execute Appendix I -** Upgrade Multiple Servers After successfully completing the procedure in Appendix I, return to this point and continue with the next step. **NOTE: In an RMS-based DSR, the IPFE is a guest on a TVOE Host that has already been upgraded as part of the NOAM upgrade.**

3. ☐	Use an SSH client to connect to the upgraded IPFE server.	Use an SSH client to connect to the IPFE server :
		`ssh <IPFE XMI IP address>`
		`login as: admusr`
		`password: <enter admusr password>`

Procedure 24: Upgrade IPFE(s) (N+0 / RMS N+0)

4. ☐	Execute ipfeNetUpdate on each upgraded IPFE server	1. Execute the following command on each upgraded IPFE server:
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh -verify`
		
		Example 1: Output with a result value of "0" (actual file names and numbers may vary):
		
		`[admusr@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 0`
		`Files that need to change:`
		
		Example 2: Output with a result value > "0" (actual file names and numbers may vary):
		
		`[root@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 6`
		`Files that need to change:`
		
		`/etc/sysconfig/network`
		`/etc/modprobe.d/bnx2x.conf`
		`/etc/sysconfig/network-scripts/ifcfg-eth01`
		`/etc/sysconfig/network-scripts/ifcfg-eth02`
		`/etc/sysconfig/network-scripts/ifcfg-eth21`
		`/etc/sysconfig/network-scripts/ifcfg-eth22`

5. ☐	If the number of lines that need to change is greater than **ZERO (> 0)**, then execute this Step.
	
	If the number of lines that need to change equals **ZERO (0)**, then S**kip to Step 6**.
		1. Execute the following commands.
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`$ sudo init 6`
		
		NOTE: ***init 6 will cause a reboot of the IPFE server. It is recommended to run the above steps on just one server of the pair, at a time, to reduce traffic impact.***
		
		2. Once the server is back online, log into the server and execute the following command:
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh -verify`
		
		NOTE: ***If the outcome of the above command is blank or if it indicates that a NON-ZERO number of lines need to change, it is recommended to contact MOS for guidance.***

Procedure 24: Upgrade IPFE(s) (N+0 / RMS N+0)

6. ☐	Repeat for all IPFE servers	**Repeat steps 3 through 5 for the remaining IPFE servers which have completed upgrade.**

THIS PROCEDURE HAS BEEN COMPLETED.

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

- **Procedure 35 - Allow Site Provisioning (All SOAM Configurations)**
- **Procedure 36 - Verify Post-Upgrade Status (All SOAM Configurations)**

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

- **Procedure 45 - Accepting Upgrade**

PCA SITE 1 UPGRADE

Use this section to upgrade Site 1 of a PCA System

5.5 PCA Upgrade *(formerly PDRA)*

This section contains the steps required to upgrade the following PCA specific configuration:

- 3-tier
- 2 sites each with Geo-Diverse SOAM and P-SBR servers (Active/Standby/Spare plus an optional 2nd spare)
- PCA MP's

NOTE: For any DSR system consisting of multiple sites (signaling network elements), it is not recommended to apply the upgrade to more than one network element within a single maintenance window.

To maximize Maintenance Window usage, DA-MPs, SS7-MPs, IPFEs, and SBRs may be upgraded in parallel with the Standby SOAM.

TVOE Hosts may be upgraded during this procedure, if they need to be upgraded. The Elapsed Time mentioned in table below specifies the time with TVOE upgrade and without TVOE upgrade. It assumes that each of the SOAM servers is running on a TVOE Host (i.e. it assumes that there are 2 TVOE hosts to be upgraded at the site.)

During the Site upgrade, global and site provisioning are disabled. Both may re-enable at the completion of the site upgrade. Table 12 provides the upgrade overview for PCA Site 1 and Table 13 provides the upgrade overview for PCA Site 2.

Table 12. Site Upgrade Execution Overview (PCA, Site 1).

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 15	0:10-0:20	0:10-0:20	SOAM Pre-Upgrade Backups (All Configurations)	None
Procedure 16	0:20-0:25	0:30-0:45	SOAM Pre-Upgrade Health Check (All Configurations)	None
Procedure 17	1:40-2:00	2:10-2:45	Disable Site Provisioning (All SOAM Configurations)	Site Provisioning Disabled, No Traffic Impact
Procedure 25*	1:40-2:00	3:50-4:45	PCA SOAM Upgrade - Site 1	Site Provisioning Disabled, No Traffic Impact
Procedure 26	0:40-2:40	4:30-7:25	Upgrade SBRs - Site 1 (PCA)	No Traffic Impact
Procedure 27	0:40-2:40	5:10-10:05	Upgrade Multiple DA-MPs - Site 1 (PCA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 28	0:40-2:40	5:50-12:45	Upgrade Multiple SS7-MPs - Site 1 (PCA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 29	0:40-1:20	6:30-14:05	Upgrade IPFE(s) - Site 1 (PCA)	No Traffic Impact

* **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 7.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 7.0 Application upgrade, then see* ***[Table 5]*** *for additional time estimates associated with TVOE upgrade.*

Table 13. Site Upgrade Execution Overview (PCA, Site 2).

Procedure	Elapsed Time (hrs: min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 15	0:10-0:20	0:10-0:20	SOAM Pre-Upgrade Backups (All Configurations)	None
Procedure 16	0:20-0:25	0:30-0:45	SOAM Pre-Upgrade Health Check (All Configurations)	None
Procedure 17	1:40-2:00	2:10-2:45	Disable Site Provisioning (All SOAM Configurations)	Site Provisioning Disabled, No Traffic Impact
Procedure 30*	1:40-2:00	2:50-4:45	PCA SOAM Upgrade - Site 2	Site Provisioning Disabled, No Traffic Impact
Procedure 31	0:40-2:40	3:30-6:25	Upgrade SBR - Site 2 (PCA)	No Traffic Impact
Procedure 32	0:40-2:40	4:10-8:05	Upgrade Multiple DA-MPs - Site 2 (PCA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 33	0:40-2:40	4:50-10:45	Upgrade Multiple SS7-MPs - Site 2 (PCA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 34	0:40-1:20	5:30-12:05	Upgrade IPFE(s) - Site 2 (PCA)	No Traffic Impact

* **NOTE:** *It is highly recommended that TVOE Hosts at a site be upgraded in a MW prior to the start of the DSR 7.0 Application upgrade. If TVOE host are to be upgraded during the same MW as the DSR 7.0 Application upgrade, then see* ***[Table 5]*** *for additional time estimates associated with TVOE upgrade.*

!! WARNING!!

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

Procedure 15; Procedure 16; Procedure 17

5.5.1 PCA SOAM Upgrade - Site 1

For PCA SOAM Site 1, the SOAM(s), the SBRs, the IPFEs, and the associated DA-MPs should be upgraded within a single maintenance window. **If this is not possible, then it is required that all servers within each Server Group share the same release at the end of the maintenance window (i.e. do not split server release levels within the same SG).** Additionally, Oracle CGBU recommends that only a single site be upgraded in any particular maintenance window.

Procedure 25: PCA SOAM Upgrade - Site 1

S T E P #	This procedure upgrades the SOAM(s) for Site 1, including, if necessary, TVOE on each server that hosts an SOAM guest. 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 Traffic status	1. Log into the SOAM GUI using the VIP. 2. Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	Verify that site Provisioning is disabled	Verify that Site Provisioning was properly disabled in **Procedure 17** - *Disable Site Provisioning (All SOAM Configurations)*. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, skip to **Step 3**, otherwise, execute the sub-steps below. 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.**
3. ☐	Upgrade TVOE for Standby SOAM and Spare SOAM	If the TVOE Host for the Standby or Spare SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Standby and Spare SOAMs.
4. ☐	Upgrade Standby SOAM and Spare SOAM in parallel	**NOTE: the Spare server of this triplet will be located at a different site.** Upgrade the Standby SOAM and Spare SOAM in parallel using the Upgrade Multiple Server procedure : **Execute Appendix I —** Upgrade Multiple Servers Procedure After successfully completing the procedure in Appendix I, return to this point and continue with the next step.
5. ☐	Upgrade TVOE Host for Active SOAM Server	If the TVOE Host for the Active SOAM needs to be upgraded **Execute Appendix H** to upgrade the TVOE Host for the Active SOAM.

Procedure 25: PCA SOAM Upgrade - Site 1

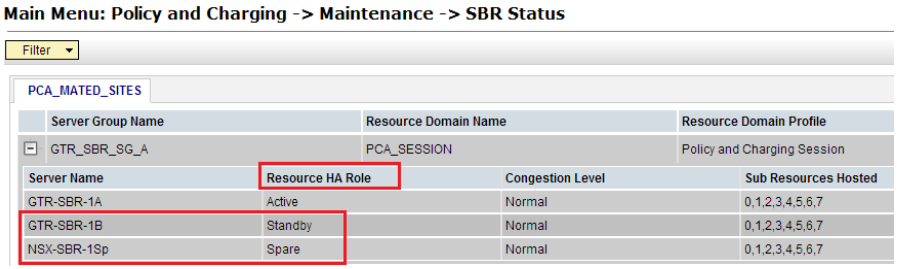
6. ☐	Upgrade Active DSR SOAM	Upgrade the Active SOAM server using the Upgrade Single Server procedure : **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next procedure.
		THIS PROCEDURE HAS 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.

5.5.2 Upgrade SBRs - Site 1 (PCA)

This procedure upgrades the SBR triplet for Site 1. Before upgrading the Active SBR, it is imperative that the database audit of the Spare and Standby server complete successfully. Failure to comply could result in a loss of session data.

Procedure 26: Upgrade SBRs - Site 1 (PCA)

S T E P #	This procedure upgrades the SBR triplet for Site 1. 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 3, pick the server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously. 2. Identify all server groups selected for upgrade in sub-step 1. 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: **GTR-SBR-1A - Active** **GTR-SBR-1B - Standby** **GTR-SBR-1Sp - Spare**  **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 26: Upgrade SBRs - Site 1 (PCA)

2. ☐	Upgrade Spare SBR Server identified in step 1 of this procedure.	**NOTE: The Spare SBR of this triplet will be located at a different site.** 1. Upgrade the Spare SBR server using the Upgrade Single Server procedure : **Execute Appendix F**—Upgrade Single Server Procedure After successfully completing the procedure in Appendix F, 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 F, 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.	1. Upgrade the Standby SBR server using the Upgrade Single Server procedure : **Execute Appendix F -** Upgrade Single Server Procedure After successfully completing the procedure in **Appendix F**, 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. ☐	Verify Standby SBR server status	**From the Active NOAM GUI:** 1. Navigate to **Main Menu > Policy and Charging >Maintenance > SBR Status.** Open the tab of the server group being upgraded. NOTE: After executing Appendix F, 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 26: Upgrade SBRs - Site 1 (PCA)

5. ☐	Verify that bulk download is complete between Active SBR to Standby SBR and Spare SBR	**From the Active NOAM GUI:** 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 4 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 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 F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
7. ☐	Repeat steps 1 through 6 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.

5.5.3 Upgrade Multiple DA-MPs - Site 1 (PCA)

The following procedure is used to upgrade the DA-MPs in a multi-active DA-MP cluster. In a multi-active DA-MP cluster, all of the DA-MPs are Active; there are no Standby DA-MPs. So the effect on the Diameter network traffic must be considered, since any DA-MP being upgraded will not be handling live traffic.

Procedure 27 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 27 must be executed four distinct times.

Procedure 27: Upgrade Multiple DA-MPs - Site 1 (PCA)

S T E P #	PCA (DA-MP Server) upgrade procedure for Site 1 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 **DSR (multi-active cluster)** to Upgrade in Site 1	From the data captured in Table 3, 1. Pick the "DSR (multi-active cluster)" Server Group in Site 1. 2. Identify the servers to be upgraded in the Server Group selected in sub-step 1.
2. ☐	Upgrade PCA Server as identified in Step 1	1. Upgrade (½) one half (no more than 50%) of the PCA (DA-MP) servers in parallel using the Upgrade Multiple Servers procedure : **NOTE: It is recommended that the DA-MP Leader and the Designated Controller be upgraded in the last group of servers to minimize DA-MP Leader and Designated Controller role changes.** **Execute Appendix I : Upgrade Multiple Servers** After successfully completing the procedure in Appendix I, return to this point and continue with the next step.
3. ☐	Repeat step 2 for all servers identified in Step 1 of this procedure.	Repeat step 2 of this procedure for the remaining PCA (DA-MP) servers.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.4 Upgrade Multiple SS7-MPs - Site 1 (PCA)

The following procedure is used to upgrade the SS7-MPs in the SS7-IWF server groups. The effect on the Diameter network traffic must be considered, since any SS7-MP being upgraded will not be handling live traffic.

Procedure 28 must be executed for all configured SS7-MPs of a site, regardless of how the MPs are grouped for upgrade. So if eight SS7-MPs are upgraded four at a time, then Procedure 28 must be executed twice.

Procedure 28: Upgrade Multiple SS7-MPs - Site 1 (PCA)

S T E P #	This procedure upgrades the SS7-MPs. 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 SS7-MPs to be upgraded together, if equipped	If SS7-MPs are deployed, choose the number of MP(s) on which upgrade can be executed in parallel, considering traffic.
2. ☐	Upgrade selected SS7-MPs	Upgrade the selected SS7-MPs, executing the Upgrade Multiple Server procedure on all selected SS7-MPs in parallel. **Execute Appendix I :** Upgrade Multiple Servers After successfully completing the procedure in **Appendix I**, for all selected SS7-MPs, return to this point and continue with the next procedure.
3. ☐	Repeat for all SS7-MP servers	Repeat steps 1 and 2 for the next set of SS7-MP servers.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.5 Upgrade IPFE(s) - Site 1 (PCA)

If none of the signaling network elements in the site being upgraded has IPFE servers installed, skip this section and proceed to next procedure. Otherwise, the following procedure must be executed independently for each signaling network element that has IPFE servers installed.

Procedure 29: Upgrade IPFE(s) - Site 1 (PCA)

S T E P #	This procedure upgrades the IPFE servers for Site 1 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 **IP Front End** Server Group to Upgrade in Site 1	From the data captured in Table 3, 1. Select one "**IP Front End**" Server Group in Site 1. 2. Identify the servers to be upgraded in the Server Group identified in sub-step 1. **NOTE: By selecting one client-facing IPFE and one server-facing IPFE, two servers can be upgraded in parallel.**
2. ☐	Upgrade IPFE Servers identified in Step 1	1. Upgrade IP Front End servers using the Upgrade Multiple Servers procedure : **Execute Appendix I**-- Upgrade Multiple Servers After successfully completing the procedure in Appendix I, return to this point and continue with the next step.

3. ☐	Execute the following steps on the IPFE	Execute the following steps on each IPFE server just upgraded :
		1. Use an ssh client to connect to the IPFE server :
		`ssh <IPFE XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Execute the following command on the IPFE server :
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`

Procedure 29: Upgrade IPFE(s) - Site 1 (PCA)

4. ☐	Execute the following steps on the IPFE	The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to step 6)**.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[admusr@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 0`
		`Files that need to change:`
		
		If the outcome of the above command indicates that a **NON ZERO** number of lines need to change, then continue with step 5.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[root@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 4`
		`Files that need to change:`
		
		`/etc/sysconfig/network`
		`/etc/modprobe.d/bnx2x.conf`
		`/etc/sysconfig/network-scripts/ifcfg-eth01`
		`/etc/sysconfig/network-scripts/ifcfg-eth02`

5. ☐	Execute the following steps on the IPFE	1. Execute the following commands.
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`$ sudo init 6`
		
		NOTE: init 6 will cause a reboot of the IPFE server. It is recommended to run the above steps on just one server of the pair, at a time, to reduce traffic impact.
		
		2. Once the server is back online, log into the server and execute the following command:
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh -verify`
		
		NOTE: If the outcome of the above command is blank or if it indicates that a NON-ZERO number of lines need to change, it is recommended to contact MOS for guidance.

Procedure 29: Upgrade IPFE(s) - Site 1 (PCA)

6. ☐	Repeat for all IPFE servers	Repeat steps 1 through 3 of this procedure for each IPFE server.

THIS PROCEDURE HAS BEEN COMPLETED.

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

- **Procedure 35 - Allow Site Provisioning (All SOAM Configurations)**
- **Procedure 36 - Verify Post-Upgrade Status (All SOAM Configurations)**

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

- **Procedure 45 - Accepting Upgrade**

PCA SITE 2 UPGRADE

Use this section to upgrade Site 2 of a PCA System

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

Procedure 15; Procedure 16; Procedure 17

5.5.6 PCA SOAM Upgrade - Site 2

Procedure 30: PCA SOAM Upgrade - Site 2

S T E P #		
	This procedure verifies that the SOAM server with TVOE platform upgrade steps have been completed, and upgrades 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. ☐	Verify Traffic status	1. Log into the SOAM GUI using the VIP. 2. Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in **Procedure 17** - *Disable Site Provisioning (All SOAM Configurations)*. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, skip to **Step 3**, otherwise, execute the sub-steps below. 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.**
3. ☐	Upgrade TVOE for Standby SOAM and Spare SOAM	If the TVOE Host for the Standby or Spare SOAM needs to be upgraded: **Execute Appendix H** to upgrade the TVOE Host for the Standby and Spare SOAMs.
4. ☐	Upgrade Standby SOAM and Spare SOAM in parallel	**NOTE: the Spare server of this triplet will be located at a different site.** Upgrade the standby SOAM and Spare SOAM servers in parallel using the Upgrade Multiple Server procedure : **Execute Appendix I**—Upgrade Multiple Servers Procedure After successfully completing the procedure in Appendix I, return to this point and continue with the next step.
5. ☐	Upgrade TVOE Host for Active SOAM Server	If the TVOE Host for the Active SOAM needs to be upgraded **Execute Appendix H** to upgrade the TVOE Host for the Active SOAM.

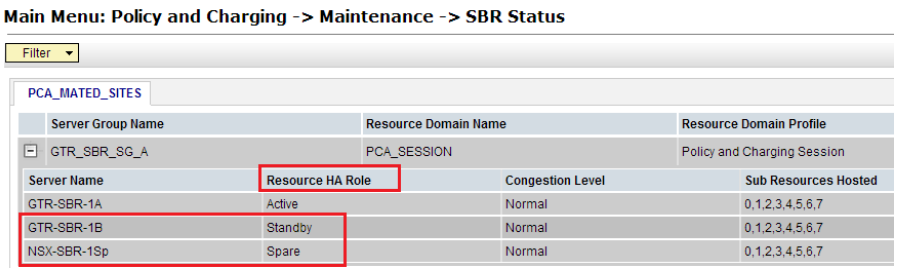
Procedure 30: PCA SOAM Upgrade - Site 2

6. ☐	Upgrade Active SOAM	Upgrade the Active SOAM server using the Upgrade Single Server procedure : **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next procedure.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.7 Upgrade SBR - Site 2 (PCA)

This procedure upgrades the SBR triplet for Site 2. Before upgrading the Active SBR, it is imperative that the database audit of the Spare and Standby server complete successfully. Failure to comply could result in a loss of session data.

Procedure 31: Upgrade SBR - Site 2 (PCA)

S T E P #	This procedure upgrades the SBR triplet for Site 2. 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 to Upgrade	1. From the data captured in Table 3, pick the server group(s) to upgrade. One server group can be upgraded at one time or multiple server groups can be upgraded simultaneously. 2. Identify all server groups selected for upgrade in sub-step 1. 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: **GTR-SBR-1A - Active** **GTR-SBR-1B - Standby** **GTR-SBR-1Sp - Spare**  **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 31: Upgrade SBR - Site 2 (PCA)

2. ☐	Upgrade Spare SBR Server identified in step 1 of this procedure.	**NOTE: Spare SBR of this triplet will be located at a different site.** 1. Upgrade the Spare SBR server using the Upgrade Single Server procedure : **Execute Appendix F**—Upgrade Single Server Procedure After successfully completing the procedure in Appendix F, 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. 3. Monitor the **Resource HA Role** status of the Spare server. 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 is **Spare**.
3. ☐	Upgrade Standby SBR Server identified in step 1 of this procedure.	1. Upgrade the Standby SBR server using the Upgrade Single Server procedure : **Execute Appendix F**—Upgrade Single Server Procedure After successfully completing the procedure in **Appendix F**, 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. ☐	Verify Standby SBR server status	**From the Active NOAM GUI:** 1. Navigate to **Main Menu > Policy and Charging >Maintenance >SBR Status.** Open the tab of the server group being upgraded. 2. Do not proceed to step 5 until the **Resource HA Role** for the Standby server has a status of **Standby**. **Main Menu: Policy and Charging -> Maintenance -> SBR Status** Filter PCA_MATED_SITES Server Group Name / Resource Domain Name / Resource Domain Profile GTR_SBR_SG_A / PCA_SESSION / Policy and Charging Session Server Name / Resource HA Role / Congestion Level / Sub Resources Hosted GTR-SBR-1A / Active / Normal / 0,1,2,3,4,5,6,7 GTR-SBR-1B / Standby / Normal / 0,1,2,3,4,5,6,7 NSX-SBR-1Sp / Spare / Normal / 0,1,2,3,4,5,6,7

Procedure 31: Upgrade SBR - Site 2 (PCA)

5. ☐	Verify that bulk download is complete between Active SBR in server group to Standby SBR and Spare SBR.	**From the Active NOAM GUI:** 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 4 instances of Event 31127: • 1 for the Standby Binding SBR • 1 for the Standby Session SBR • 1 for the Spare Binding SBR server • 1 for the Spare Session SBR server 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 in this procedure	Upgrade the Active SBR server using the Upgrade Single Server procedure : **Execute Appendix F** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
7. ☐	Repeat steps 1 through 6 for all the Binding and Session Server Groups with Active, Standby in Site 2) and Spare in Site 1	Repeat steps 1 through 6 for the remaining binding and session server groups to be upgraded.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.8 Upgrade Multiple DA-MPs - Site 2 (PCA)

The following procedure is used to upgrade the DA-MPs in a multi-active DA-MP cluster. In a multi-active DA-MP cluster, all of the DA-MPs are Active; there are no Standby DA-MPs. So the effect on the Diameter network traffic must be considered, since any DA-MP being upgraded will not be handling live traffic.

Procedure 32: Upgrade Multiple DA-MPs - Site 2 (PCA)

S T E P #	PCA server (DA-MP Server) upgrade procedure for Site 2 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 **DSR (multi-active cluster)** to Upgrade in Site 2	From the data captured in Table 3, 1. Pick the "DSR (multi-active cluster)" Server Group in Site 2. 2. Identify the servers to be upgraded in the Server Group identified in sub-step 1.
2. ☐	Upgrade PCA Server as identified in Step 1	1. Upgrade (½) one half (no more than 50%) of the PCA (DA-MP) servers in parallel using the Upgrade Multiple Servers procedure : **NOTE: It is recommended that the DA-MP Leader and Designated Controller be upgraded in the last group of servers to minimize DA-MP Leader and Designated Controller role changes.** **Execute Appendix I : Upgrade Multiple Servers** After successfully completing the procedure in Appendix I, return to this point and continue with the next step.
3. ☐	Repeat step 2 for all servers identified in Step 1 of this procedure.	Repeat step 2 of this procedure for the remaining PCA (DA-MP) servers.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.9 Upgrade Multiple SS7-MPs - Site 2 (PCA)

The following procedure is used to upgrade the SS7-MPs in the SS7-IWF server groups. The effect on the Diameter network traffic must be considered, since any SS7-MP being upgraded will not be handling live traffic.

Procedure 33 must be executed for all configured SS7-MPs of a site, regardless of how the MPs are grouped for upgrade. So if eight SS7-MPs are upgraded four at a time, then Procedure 33 must be executed twice.

Procedure 33: Upgrade Multiple SS7-MPs - Site 2 (PCA)

S T E P #	This procedure upgrades the SS7-MPs. 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 SS7-MPs to be upgraded together. If equipped	If SS7-MPs are deployed, choose the number of MP(s) on which upgrade can be executed in parallel, considering traffic.
2. ☐	Upgrade selected SS7-MPs	Upgrade the selected SS7-MPs, executing the Upgrade Multiple Server procedure on all selected SS7-MPs in parallel. **Execute Appendix I :** Upgrade Multiple Servers After successfully completing the procedure in **Appendix I**, for all selected SS7-MPs, return to this point and continue with the next procedure.
3. ☐	Repeat for all SS7-MP servers	Repeat steps 1 and 2 for the next set of SS7-MP servers.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.5.10 Upgrade IPFE(s) - Site 2 (PCA)

If none of the signaling network elements in the site being upgraded has IPFE servers installed, skip this section and proceed to next procedure. Otherwise, the following procedure must be executed independently for each signaling network element that has IPFE servers installed.

Procedure 34: Upgrade IPFE(s) - Site 2 (PCA)

S T E P #	IPFE server upgrade procedure for Site 2 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 **IP Front End** Server Group to Upgrade in Site 2	From the data captured in Table 3, 1. Select one "**IP Front End**" Server Group in Site 2. 2. Identify the servers to be upgraded in the Server Group identified in sub-step 1. **NOTE: By selecting one client-facing IPFE and one server-facing IPFE, two servers can be upgraded in parallel.**
2. ☐	Upgrade IPFE Server as identified in Step 1 in this procedure	1. Upgrade the IP Front End servers using the Upgrade Multiple Servers procedure : **Execute Appendix I**-- Upgrade Multiple Servers After successfully completing the procedure in Appendix I, return to this point and continue with the next step.

3. ☐		Execute the following steps on each IPFE server just upgraded :
		1. Use an SSH client to connect to the IPFE server :
		`ssh <IPFE XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Execute the following command on the IPFE server :
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`

Procedure 34: Upgrade IPFE(s) - Site 2 (PCA)

4. ☐		The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to step 6)**.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[admusr@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 0`
		`Files that need to change:`
		
		If the outcome of the above command indicates that a **NON ZERO** number of lines need to change, then continue with step 5.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[admusr@ISoak-IPFE ~]$ sudo ipfeNetUpdate.sh -verify`
		`Inspecting /etc/sysconfig/network`
		`Inspecting /etc/modprobe.d/bnx2x.conf`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth01`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth02`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth21`
		`Inspecting /etc/sysconfig/network-scripts/ifcfg-eth22`
		
		`You are running in verify mode.`
		
		`Count of lines that need to change: 4`
		`Files that need to change:`
		
		`/etc/sysconfig/network`
		`/etc/modprobe.d/bnx2x.conf`
		`/etc/sysconfig/network-scripts/ifcfg-eth01`
		`/etc/sysconfig/network-scripts/ifcfg-eth02`

5. ☐	Execute the following steps on the IPFE	1. Execute the following commands.
		
		`$ /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`$ sudo init 6`
		
		NOTE: init 6 will cause a reboot of the IPFE server. It is recommended to run the above steps on just one server of the pair, at a time, to reduce traffic impact.
		
		2. Once the server is back online, log into the server and execute the following command:
		
		`$ sudo /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh -verify`
		
		NOTE: If the outcome of the above command is blank or if it indicates that a NON-ZERO number of lines need to change, it is recommended to contact MOS for guidance.

Procedure 34: Upgrade IPFE(s) - Site 2 (PCA)

6. ☐	Repeat 3 for all IPFE servers	Repeat steps 1 through 3 for the remaining IPFE servers.

THIS PROCEDURE HAS BEEN COMPLETED.

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

- **Procedure 35 - Allow Site Provisioning (All SOAM Configurations)**
- **Procedure 36 - Verify Post-Upgrade Status (All SOAM Configurations)**

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

- **Procedure 45 - Accepting Upgrade**

6 SOAM POST-UPGRADE VERIFICATION

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

6.1.1 Allow Site Provisioning (All SOAM Configurations)

This procedure enables Site Provisioning for the site just upgraded.

ANY PROVISIONING CHANGES MADE TO THIS SITE BEFORE THE UPGRADE IS ACCEPTED WILL BE LOST IF THE UPGRADE IS BACKED OUT

Procedure 35: Allow Site Provisioning (All SOAM Configurations)

S T E P #	This procedure allows provisioning for SOAM and MP servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active SOAM VIP:** 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**
THIS PROCEDURE HAS BEEN COMPLETED.		

6.1.2 Verify Post-Upgrade Status (All SOAM Configurations)

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

Procedure 36: Verify Post-Upgrade Status (All SOAM Configurations)

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.**	
1. ☐	Collect post-upgrade status depending on the source release	If the source release is 70.20 or later, proceed to step 13. Otherwise, continue with step 2.

2. ☐	Verify Upgrade Status	1. Execute the following commands on the upgraded servers :
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		`ssh <Server XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		NOTE: The static XMI IP address for each server should be available in Table 3.
		`# sudo verifyUpgrade`
		2. Examine the output of the above command to determine if any errors were reported. In case of errors it is recommended to contact MOS for guidance.
		`$ alarmMgr --alarmstatus`
		The following alarm output should be seen, indicating that the upgrade completed.
		`SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33|tpdServerUpgradePendingAccept|1.3.6.1.4.1.323.5.3.18.3.1.3.33`
		Alarm ID 32532 will be cleared once Procedure 45 is executed to accept the upgrade on each server.
		It is recommended to contact MOS if above output is not generated.

3. ☐	**SOAM Server Only:** 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 36: Verify Post-Upgrade Status (All SOAM Configurations)

4. ☐	**Active NOAM VIP:** 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. it is recommended to contact MOS if any server status is not Norm. 5. It is recommended to contact MOS if there are any unexpected Major or Critical alarms. All other upgraded servers will have the following expected alarm: Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** **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 means 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.**
3. ☐	**Active NOAM VIP:** Log all current 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. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)** All other upgraded servers will have the following expected alarm: Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4. ☐	**Active NOAM VIP:** View Communication Agent 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.
5. ☐	**Active NOAM VIP:** Export and archive the 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 NOAM to the client machine.

Procedure 36: Verify Post-Upgrade Status (All SOAM Configurations)

6. ☐	**Active SOAM VIP:** Capture the Diameter Maintenance Status	1. Log into the SOAM GUI of the site just upgraded using the VIP. 2. Select **Main Menu > Diameter > Maintenance** 3. Select **Maintenance >Route Lists** screen. 4. Filter out all the Route Lists with **Route List Status** as **"Is Not Available"** and **"Is Available".** 5. Record the number of "Not Available" and "Available" Route Lists. 6. Select **Maintenance >Route Groups** screen. 7. Filter out all the Route Groups with "**PeerNode/Connection Status** as **"Is Not Available"** and **"Is Available".** 8. Record the number of "Not Available" and "Available" Route Groups. 9. Select **Maintenance >Peer Nodes** screen. 10. Filter out all the Peer Nodes with "**Peer Node Operational Status"** as **"Is Not Available"** and **"Is Available".** 11. Record the number of "**Not Available**" and "**Available**" peer nodes. 12. Select **Maintenance >Connections** screen. 13. Filter out all the Connections with "**Operational Status"** as **"Is Not Available"** and **"Is Available".** 14. Record the number of "**Not Available**" and "**Available** "connections. 15. Select **Maintenance >Applications** screen. 16. Filter out all the Applications with "**Operational State"** as **"Is Not Available"** and **"Is Available".** 17. Record the number of "**Not Available**" and "**Available**" applications. 18. Save the recorded data on the client machine 19. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 20. Select the **Peer DA-MP Status** tab. 21. Verify all Peer MPs are available 22. Select the **DA-MP Connectivity** tab. 23. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count
7. ☐	**Active SOAM VIP:** Verify and collect Signaling Network Configuration data	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. Select **Configuration > Network > Routes**. 8. Click **Report All** at the bottom of the table to generate a report for all entries.
8. ☐	**Active SOAM VIP:** Capture the IPFE Configuration Options Screens (if equipped)	1. Select **Main Menu: IPFE >Configuration >Options** 2. Capture and archive the screen capture of the complete screen. 3. Save this data on the client machine
9. ☐	**Active SOAM VIP:** Capture the IPFE Configuration Target Set screens (if equipped)	1. Select **Main Menu: IPFE >Configuration >Target Sets** 2. Capture and archive the screen capture of the complete screens. Save the captured data on the client machine.
10. ☐	**Active SOAM VIP:** Verify Traffic status	Inspect KPI reports to verify traffic is at the expected condition.

Procedure 36: Verify Post-Upgrade Status (All SOAM Configurations)

11. ☐	**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
12. ☐	**PCA Installations Only** **Active SOAM VIP (PCA Site 2):** Export and archive the Diameter and PCA configuration data on the Active SOAM GUI for **Site 2**.	Export Diameter and PCA configuration data **From the Active SOAM GUI (PCA Site 2):** 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter and PCA data by choosing the drop down entry labeled "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 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
		PROCEED TO STEP 16

13. ☐	**ACTIVE SOAM CLI:**
	
	Verify SOAM post-Upgrade Status (source release 70.20 and later only)
		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 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		
		This command creates three files in `/var/TKLC/db/filemgmt/UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		
		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.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to consult with 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 36: Verify Post-Upgrade Status (All SOAM Configurations)

14. ☐	**ACTIVE SOAM CLI:** 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.
15. ☐	**ACTIVE SOAM CLI:** View DA-MP Status	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
16. ☐	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 13 through 15 is the same as the pre-upgrade health checks taken in **Procedure 16**. If system operation is degraded, it is recommended to contact MOS for guidance.
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: *If another site is to be upgraded, all procedures specified by **Table 9** must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.*

7 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 14. 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 15. 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 14 and Table 15 are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done.

Table 14: Emergency Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 37	0:10-0:30	0:10-0:30	Backout Setup: 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 38	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 43	See Note	See Note	Back Out 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 39	See Note	See Note	Emergency NOAM Backout: NOTE: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
Procedure 44	0:01-0:05	Varies	Perform Health Check (Post-Backout)	None

Table 15. Normal Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 37	0:10-0:30	0:10-0:30	Backout Setup: 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 40	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 43	See Note	See Note	Back Out 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 41	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 44	0:01-0:05	Varies	Perform Health Check (Post-Backout)	None

7.1 Recovery Procedures

Upgrade procedure recovery issues should be directed to MOS by referring to Appendix M 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 M.

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 70.y.z release to the previously installed 5.x.w/6.x.w release). Backout of an initial installation is not supported.

7.2 Backout Setup

This section provides the procedure to prepare a DSR for backout.

Procedure 37: Backout Setup

S T E P #	This procedure is used to prepare a DSR system for 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:** Identify IP addresses of servers to be backed out	1. Login in to the NOAM GUI using the VIP. 2. Select **Administration > Software Management > Upgrade.** 3. Based on the "Application Version" column, identify all the hostnames that need to be backed out. 4. Select **Configuration > Servers.** 5. Identify the XMI/iLO/LOM IP addresses of all the hostnames identified in step 2 from Table 3. These are required to access the server when performing the backout. The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures **WILL** cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended to contact MOS as stated in the **Warning** box above.

Procedure 37: Backout Setup

2. ☐	Verify backup archive files	1. Verify that the two backup archive files, created using Procedure 3 in section 3.3.5, are present on every server that is to be backed out. These archive files are located in the /var/TKLC/db/filemgmt directory and have different filenames than other database backup files. The filenames will have the format: Backup.<application>.<server>.**FullDBParts**.<role>.<date_time>.**UPG**.tar Backup. <application>.<server>.**FullRunEnv**.<role>.<date_time>.**UPG**.tar
THIS PROCEDURE HAS BEEN COMPLETED.		

EMERGENCY SITE BACKOUT

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

7.3 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 7.1, to verify that all corrective setup steps have been taken.

7.3.1 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 38: Emergency Site Backout

S T E P #	This procedure is used to back out the DSR application software from multiple B- and C-level servers for a specific site. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs, 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. ☐	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. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 4. Make note of these servers. They have been identified for backout. 5. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.

Procedure 38: Emergency Site Backout

2. ☐	Disable Global Provisioning (if not already done)	Disable provisioning and configuration updates on the entire network (if not done previously: Since this step is being executed during a backout procedure, it is likely that Provisioning and Configuration updates are disabled already. If they have not been disabled, execute the following steps to disable provisioning: **From the Active NOAM GUI:** 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. 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)**
3. ☐	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.**
		**!WARNING!** **STEP 4 WILL RESULT IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR**
4. ☐	Back out all C-level servers, as applicable	**For all configurations:** Back out all C-level servers (IPFEs, SBRs, SBRs, DA-MPs, and SS7-MPs) identified in step 1: Execute Section 7.6, Back Out Multiple Servers.
5. ☐	Back out the Standby and Spare SOAM servers, as applicable	To back out the Standby and Spare DSR SOAM servers: Execute Section 7.6, Back Out Multiple Servers. If there is no Spare SOAM, back out the Standby SOAM: Execute Section 7.5, Back Out Single Server.

Procedure 38: Emergency Site Backout

6. ☐	Work-around for DSR 7.0 to 5.x backout	**This step should be executed only if backing out from DSR Release 7.0 to DSR Release 5.x.**
		
		1. Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Standby **SOAM**:
		
		`ssh root@<Standby_SOAM>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. Verify the following soft links exist in the specified directory. If not, execute the following commands as needed:
		
		`ln -fs /usr/TKLC/ipfe/modules/ipfe /var/TKLC/appworks/modules/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/gui /var/TKLC/appworks/library/Ipfe`
		
		`ln -fs /usr/TKLC/ipfe/js /var/TKLC/appworks/public/js/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/modules/ipfe/views/images /var/TKLC/appworks/public/images/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/js/IpfeJsonQueryRestStore.js /usr/TKLC/plat/www/dojo/dojox/data/IpfeJsonQueryRestStore.js`
		
		`ln -fs /usr/TKLC/ipfe/css/grid.css /var/TKLC/appworks/public/css/grid.css`
		
		`ln -fs /usr/TKLC/ipfe/css/ipfe.css /var/TKLC/appworks/public/css/ipfe.css`
		
		`ln -fs /usr/TKLC/ipfe/gui/wsdl /usr/TKLC/dpi/wsdl/Ipfe`
		
		3. Repeat this step on the Spare **SOAM**.

7. ☐	Back out the Active SOAM	Back out the Active DSR SOAM server: Execute Section 7.5, Back Out Single Server.
8. ☐	Repeat work-around for other SOAM	Repeat step 6 on the other (now Standby) SOAM.

Procedure 38: Emergency Site Backout

9. ☐	Back out TVOE if upgraded previously	**If the SOAM server hosts the TVOE software, determine if TVOE backout is required (if upgraded previously). If backout is not required, proceed to the next step.**
		
		Execute the following steps for each TVOE blade upgraded previously.
		
		Disable all applications running on the TVOE blade:
		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 blade.
		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**'.
		
		7. List the guests running on the current TVOE host by using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		`# virsh list`
		
		NOTE: the output of above command will list all guests running on the TVOE host.
		
		8. Execute the following command for each guest listed in sub-step 7 :
		
		`# virsh shutdown <guestname>`
		
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE blades on which SOAM(s) are hosted are successfully backed out.
		
		9. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [3].

Procedure 38: Emergency Site Backout

10. ☐	Enable virtual guest watchdogs if disabled previously	If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [5] Otherwise execute the following sub-steps:
		
		1. Log into the TVOE host using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to start the TVOE guest shutdown in step 9 sub-step 8 above (if not already started).
		
		`# virsh start <guestname>`
		
		3. Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list`
		
		Enable all applications running on the backed out TVOE blade.
		
		4. Log into the NOAM VIP GUI
		5. Select **Status & Manage > Server**.
		The Server Status screen is displayed
		6. Select all applications running on the current TVOE blade.
		7. Click the **Restart** button.
		8. Confirm the operation by clicking **Ok** in the popup dialog box.
		9. Verify that the 'Appl State' for all selected servers is changed to '**Enabled**'.
		
		NOTE: This step shall be executed only if the TVOE is backed out in Step 9.
		
		Execute Steps 9 and 10 again for another TVOE blade hosting SOAM (as applicable).

Procedure 38: Emergency Site Backout

<table>
<tr><td>11.</td><td>Prepare to enable site provisioning</td><td>Prepare to enable site provisioning.

A workaround may be required before Site Provisioning can be enabled following a backout. To determine if the workaround is required, execute the following:

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

If the source release is 5.x:
ssh root@<SOAM_VIP>

If the source release is 6.x/7.0:
ssh admusr@<SOAM_VIP>

2. Display the contents of the prov_ctlBsource table

iqt -p prov_ctlBsource

Sample output:
[admusr@NO-FordB ~]$ iqt -p prov_ctlBsource
prov_status
Disable

The second line of output (highlighted) indicates the enabled or disabled state of Site Provisioning. If the second line is present, the workaround is not required; continue with step 12 below.

If the highlighted line is not present, perform the following steps to enact the workaround:
ivi prov_ctrBsource

Insert the following text:

#!/bin/sh
iload -ha -xU -fprov_status prov_ctlBsource \
<<'!!!!'
Enable
!!!!

Save the file and apply the changes:
:wq
APPLY THE CHANGES [yn]? y

This procedure is complete.</td></tr>
<tr><td>12.</td><td>Enable Site Provisioning</td><td>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</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED.</td></tr>
</table>

NOTE: If another site is to be backed out, follow all procedures in Table 14 in another maintenance window.

7.3.2 Emergency NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 39: Emergency NOAM Backout

S T E P #	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. ☐	Back out Standby DR NOAM server (if equipped)	Back out the Standby DR NOAM server: Execute Section 7.5 Back Out Single Server.
2. ☐	Back out Active DR NOAM server (if equipped)	Back out the other DR NOAM server (now the Standby): Execute Section 7.5 Back Out Single Server.
3. ☐	Back out Standby DSR NOAM server (as applicable)	Back out the Standby DSR NOAM server: Execute Section 7.5 Back Out Single Server.
4. ☐	Back out Active DSR NOAM server	Back out the other DSR NOAM server (now the standby): Execute Section 7.5 Back Out Single Server.

Procedure 39: Emergency NOAM Backout

5. ☐	Back out TVOE if upgraded previously	**If the NOAM server hosts the TVOE software, determine if TVOE backout is required (if upgraded previously). If backout is not required then proceed to step 6.**
		
		Execute the following steps for each TVOE blade upgraded previously.
		
		Disable all applications running on the TVOE blade:
		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 blade.
		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**'.
		
		7. List the guests running on the current TVOE host by using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		`# virsh list`
		
		The output of above command will list all guests running on the TVOE host.
		
		8. Execute the following command for each guest listed in sub-step 2 :
		
		`# virsh shutdown <guestname>`
		
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE blades on which NOAM(s) are hosted are successfully backed out.
		
		9. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [3].

Procedure 39: Emergency NOAM Backout

6. ☐	Enable virtual guest watchdogs if disabled previously	If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [5] Otherwise execute the following sub-steps.
		
		1. Log into the TVOE host using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to start the TVOE guest shutdown in step 5 sub-step 3 above (if not already started).
		
		`# virsh start <guestname>`
		
		3. Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list`
		
		Enable all applications running on the backed out TVOE blade.
		
		4. Log into the NOAM VIP GUI
		5. Select **Status & Manage > Server**.
		The Server Status screen is displayed
		6. Select all applications running on the current TVOE blade.
		7. Click the **Restart** button.
		8. Confirm the operation by clicking **Ok** in the popup dialog box.
		9. Verify that the 'Appl State' for all selected servers is changed to **'Enabled'**.
		
		NOTE: This step shall be executed only if the TVOE is backed out in step 5.
		
		Execute steps 5 and 6 again for another TVOE blade hosting NOAM (as applicable).

7. ☐	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**.

Procedure 39: Emergency NOAM Backout

8. ☐	Remove 'Ready' state for any backed out server	Remove 'Ready' state **From the Active NOAM GUI :** 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

7.4 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 7.1, to verify that all corrective setup steps have been taken.

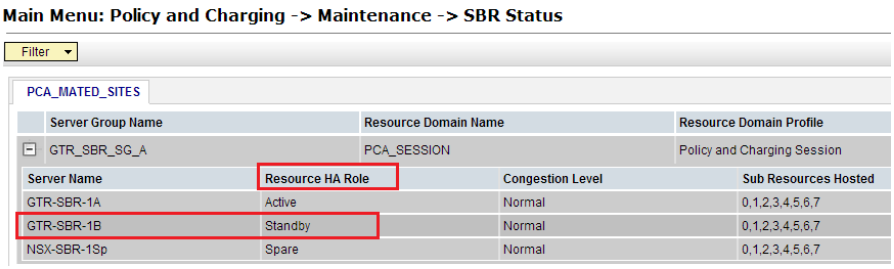
7.4.1 Normal Site Backout

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

Procedure 40: Normal Site Backout

S T E P #	This procedure is used to back out an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs, 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. ☐	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. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 4. Make note of these servers. They have been identified for Backout. 5. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. ☐	Disable Global Provisioning (if not already done)	Disable provisioning and configuration updates on the entire network (if not done previously: Since this step is being executed during a backout procedure, it is likely that Provisioning and Configuration updates are disabled already. If they have not been disabled, execute the following steps to disable provisioning: **From the Active NOAM GUI:** 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. 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)**

Procedure 40: Normal Site Backout

3. ☐	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.**
4. ☐	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.** Back out the first set of servers. The following servers can be backed out in parallel (as applicable) • Standby DA-MP(s) (or half of the DA-MPs for the N+0 configuration) • Standby SBR(s) • Spare SBR(s) • SS7-MPs Execute 7.5, Back Out Single Server for each Standby/Spare C-level server identified above. NOTE: There will be no Standby DA-MPs for the N+0 DA-MP configurations.
		**!WARNING!** **Failure to comply with step 5 and step 6 may result in the loss of PCA traffic, resulting in service impact**
5. ☐	Verify Standby SBR server status	If the server being backed out is the Standby SBR, execute this step. Otherwise, continue with step 6. **From the Active NOAM GUI:** 1. Navigate to **Main Menu -> Policy and Charging->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**. 

Procedure 40: Normal Site Backout

6. ☐	**Execute this Step for PCA installations only:** 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. **From the Active NOAM GUI:** 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 4 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 NOTE: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.
7. ☐	Back out remaining C-level servers, as applicable	**For DSR 1+1 (Active/Standby) configuration** Back out **MP server** (the mate, if dealing with a server pair). Execute Section 7.5 Back Out Single Server. **For DSR N+0 (multi-Active) configuration:** 1. Identify the C-level servers that can be backed out in parallel, considering traffic. 2. Backout all identified IPFE(s),SBR(s), SBR(s) DA MP(s), and SS7-MP(s) in parallel Execute Section 7.5 Back Out Single Server. 3. Execute sub-steps 1 and 2 for remaining Active MP(s).
8. ☐	Back out the Standby SOAM server	Back out the Standby DSR SOAM server: Execute Section 7.5 Back Out Single Server.

Procedure 40: Normal Site Backout

9. ☐	Work-around for DSR 7.0 to 5.x backout	**This step should be executed only if backing out from DSR Release 7.0 to DSR Release 5.x.**
		
		1. Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Standby SOAM:
		
		`ssh root@<Standby_SOAM>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. Verify the following soft links exist in the specified directory. If not, execute the following commands as needed:
		
		`ln -fs /usr/TKLC/ipfe/modules/ipfe /var/TKLC/appworks/modules/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/gui /var/TKLC/appworks/library/Ipfe`
		
		`ln -fs /usr/TKLC/ipfe/js /var/TKLC/appworks/public/js/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/modules/ipfe/views/images /var/TKLC/appworks/public/images/ipfe`
		
		`ln -fs /usr/TKLC/ipfe/js/IpfeJsonQueryRestStore.js /usr/TKLC/plat/www/dojo/dojox/data/IpfeJsonQueryRestStore.js`
		
		`ln -fs /usr/TKLC/ipfe/css/grid.css /var/TKLC/appworks/public/css/grid.css`
		
		`ln -fs /usr/TKLC/ipfe/css/ipfe.css /var/TKLC/appworks/public/css/ipfe.css`
		
		`ln -fs /usr/TKLC/ipfe/gui/wsdl /usr/TKLC/dpi/wsdl/Ipfe`

10. ☐	Back out Active SOAM Server	Back out the Active DSR SOAM server: Execute Section 7.5 Back Out Single Server.
11. ☐	Work-around for DSR 7.0 to 5.x backout	Repeat step 9 on the other (now Standby) SOAM.
12. ☐	Back out Spare SOAM Server (if applicable)	**NOTE: The Spare server is located at the mated site of the site being backed out.** If equipped, back out the spare SOAM server: Execute Section 7.5 Back Out Single Server.
13. ☐	Work-around for DSR 7.0 to 5.x backout	Repeat step 9 on the Spare SOAM.

Procedure 40: Normal Site Backout

14. ☐	Back out TVOE if upgraded previously	**If the SOAM server hosts the TVOE software, determine if TVOE backout is required (if upgraded previously). If backout is not required, then skip to the next step.**
		
		Execute the following steps for each TVOE blade upgraded previously.
		
		Disable all applications running on the TVOE blade:
		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 blade.
		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'**.
		
		7. List the guests running on the current TVOE host by using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		`# virsh list`
		
		The output of above command will list all guests running on the TVOE host.
		
		8. Execute the following command for each guest listed in sub-step 2 :
		
		`# virsh shutdown <guestname>`
		
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE blades on which SOAM(s) are hosted are successfully backed out.
		
		9. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [3].

Procedure 40: Normal Site Backout

15. ☐	Enable virtual guest watchdogs if disabled previously	If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [5] Otherwise execute the following sub-steps.
		
		1. Log into the TVOE host using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to start the TVOE guest shutdown in step 14 sub-step 8 above (if not already started).
		
		`# virsh start <guestname>`
		
		3. Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list`
		
		Enable all applications running on the backed out TVOE blade:
		4. Log into the NOAM VIP GUI
		5. Select **Status & Manage > Server**.
		The Server Status screen is displayed
		6. Select all applications running on the current TVOE blade.
		7. Click the **Restart** button.
		8. Confirm the operation by clicking **Ok** in the popup dialog box.
		9. Verify that the 'Appl State' for all selected servers is changed to **'Enabled'**.
		
		NOTE: This step shall be executed only if the TVOE is backed out in Step 14.
		
		Execute Steps 14 and 15 again for another TVOE blade hosting SOAM (as applicable).

Procedure 40: Normal Site Backout

<table>
<tr><td>16.
☐</td><td>Prepare to enable site provisioning</td><td>Prepare to enable site provisioning.

A workaround may be required before Site Provisioning can be enabled following a backout. To determine if the workaround is required, execute the following:

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

If the source release is 5.x:
ssh root@<SOAM_VIP>

If the source release is 6.x/7.0:
ssh admusr@<SOAM_VIP>

4. Display the contents of the prov_ctlBsource table

iqt -p prov_ctlBsource

Sample output:
[admusr@NO-FordB ~]$ iqt -p prov_ctlBsource
prov_status
Disable

The second line of output (highlighted) indicates the enabled or disabled state of Site Provisioning. If the second line is present, the workaround is not required; continue with step 17 below.

If the highlighted line is not present, perform the following steps to enact the workaround:
ivi prov_ctrBsource

Insert the following text:

#!/bin/sh
iload -ha -xU -fprov_status prov_ctlBsource \
<<'!!!!'
Enable
!!!!

Save the file and apply the changes:
:wq
APPLY THE CHANGES [yn]? y

This procedure is complete.</td></tr>
<tr><td>17.</td><td>Enable Site Provisioning</td><td>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</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED.</td></tr>
</table>

NOTE: If another site is to be backed out, follow all procedures in Table 15 in another maintenance window.

7.4.2 Normal NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 41: Normal NOAM Backout

S T E P #	This procedure is used to perform a normal back out 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 UPGRADE ASSISTANCE**	
1. ☐	Back out Standby DR NOAM server (if equipped).	Back out the Standby DR NOAM server: Execute Section 7.5 Back Out Single Server.
2. ☐	Back out Active DR NOAM server (if equipped).	Back out the other DR NOAM server (now the Standby): Execute Section 7.5 Back Out Single Server.
3. ☐	Back out Standby DSR NOAM server (as applicable).	Back out the Standby DSR NOAM server: Execute Section 7.5 Back Out Single Server.
4. ☐	Back out Active DSR NOAM server.	Back out the other NOAM server (now the Standby): Execute Section 7.5 Back Out Single Server.

Procedure 41: Normal NOAM Backout

5. ☐	Back out TVOE if upgraded previously	If the NOAM server hosts the TVOE software, determine if TVOE backout is required (if upgraded previously). If backout is not required then proceed to step 6.
		
		Execute the following steps for each TVOE blade upgraded previously.
		
		Disable all applications running on the TVOE blade:
		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 blade.
		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'**.
		7. List the guests running on the current TVOE host by using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		`# virsh list`
		
		The output of above command will list all guests running on the TVOE host.
		
		8. Execute the following command for each guest listed in sub-step 2 :
		
		`# virsh shutdown <guestname>`
		
		NOTE: Shutting down applications may lead to lost VIP. Wait until all TVOE blades on which NOAM(s) are hosted are successfully backed out.
		
		9. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [3].

Procedure 41: Normal NOAM Backout

6. ☐	Enable virtual guest watchdogs if disabled previously	If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [5] Otherwise execute the following sub-steps.
		
		1. Log into the TVOE host using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to start the TVOE guest shutdown in step 5 sub-step 3 above (if not already started).
		
		`# virsh start <guestname>`
		
		3. Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list`
		
		Enable all applications running on the backed out TVOE blade:
		4. Log into the NOAM VIP GUI
		5. Select **Status & Manage > Server**.
		The Server Status screen is displayed
		6. Select all applications running on the current TVOE blade.
		7. Click the **Restart** button.
		8. Confirm the operation by clicking **Ok** in the popup dialog box.
		9. Verify that the 'Appl State' for all selected servers is changed to **'Enabled'**.
		
		NOTE: This step shall be executed only if the TVOE is backed out in step 5.
		
		Execute Steps 5 and 6 again for another TVOE blade hosting an NOAM (as applicable).

7. ☐	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**.

Procedure 41: Normal NOAM Backout

8. ☐	Remove 'Ready' state for any backed out server	Remove 'Ready' state **From the Active NOAM GUI :** 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** button. Otherwise, skip this step. The Upgrade [Complete] 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.

7.5 Back Out Single Server

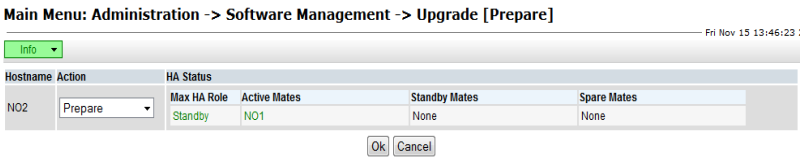
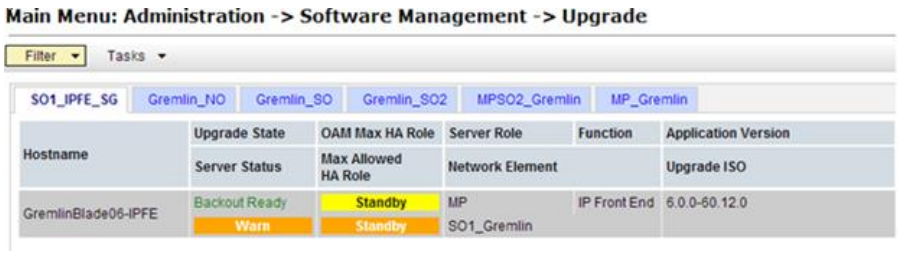
This section provides the procedures to back out the application software on a single server.

Procedure 42: Back Out Single Server

S T E P #	This procedure will back out the upgrade of DSR 7.0 application software. Any server requiring Backout can be included: NOAMs, SOAMs, DA-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. ☐	Logical Volume integrity check	Verify Logical Volume integrity on the server to be backed out.
		
		1. Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: If direct access to the IMI is not available, 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.
		
		2. Execute the following command:
		
		`$ sudo lvs`
		
		`[admusr@NO2 ~]$ sudo lvs`
		`LV VG Attr LSize Pool Origin Data% Move Log Cpy%Sync Convert`
		`apw_tmp vgroot -wi-ao---- 2.41g`
		`filemgmt vgroot -wi-ao---- 9.59g`
		`logs_process vgroot -wi-ao---- 512.00m`
		`logs_security vgroot -wi-ao---- 512.00m`
		`netbackup_lv vgroot -wi-ao---- 2.00g`
		`plat_root vgroot -wi-ao---- 1.00g`
		`plat_tmp vgroot -wi-ao---- 1.00g`
		`plat_usr vgroot -wi-ao---- 4.00g`
		`plat_var vgroot -wi-ao---- 1.00g`
		`plat_var_tklc vgroot -wi-ao---- 4.00g`
		`run_db vgroot -wi-ao---- 5.00g`
		
		3. The integrity of the LV snapshot may be verified by reviewing the **Data%** values displayed in the lvs command output.
		
		IMPORTANT: If any value shown in the Data% column equals 100.00%, then the snapshot is INVALID and backout to the previous release is no longer possible.

Procedure 42: Back Out Single Server

2. ☐	Make server ready for backout	Make the server 'Ready' for Backout: 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. **For DSR 51.13.0 and later only:** 3. Select the Server Group tab of the server(s) to be backed out. 4. Select the server to backout and check its upgrade state : a) If the upgrade state is "**Ready**" then press the "**Complete**" button and continue to the next sub-step. b) Select the server to be backed out and press the "**Prepare"** button. The **Upgrade** [**Prepare]** screen will appear.  5. If this is the **Standby** server, verify that the value in the HA Status field under the Selected Server Status is **Standby;** otherwise it will display **Active.** 6. Click **OK.** This starts the Prepare action on the server. Control will return to the Upgrade Administration screen. **NOTE: If this is the Active server in an Active-Standby pair, the Prepare action WILL cause an HA switchover. The HA switchover is an expected outcome from the Prepare action.** **NOTE: When the Active NOAM is the server being backed out, the HA switchover will cause the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.**
		7. Wait for the screen to refresh and show the Upgrade State as **Backout Ready** for the server to be upgraded. It may take up to a minute for the Upgrade State to change to **Backout Ready**. 

3. ☐	SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		
		NOTE: If direct access to the IMI is not available, 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.

Procedure 42: Back Out Single Server

4. ☐	Execute the backout	Determine the state of the server to be backed out. The server must be either Standby or Spare. Execute following command to find the state :
		
		`$ ha.mystate`
		
		In the example output below, the HA state is Standby.
		
		`[admusr@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		
		If the state of the server is Active, then go back to step 1 above.
		
		`$ 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`

5. ☐	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.

Procedure 42: Back Out Single Server

6. ☐	SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		
		If the source release is 5.x:
		`login as: root`
		`password: <enter password>`
		
		If the source release is 6.x/7.0:
		`login as: admusr`
		`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.

7. ☐	Restore the full DB run environment	1. Execute the backout_restore utility to restore the full database run environment:
		
		If the source release is 5.x:
		`# /var/tmp/backout_restore`
		
		If the source release is 6.x/7.0:
		`$ 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 `/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 M of this document for further instructions.

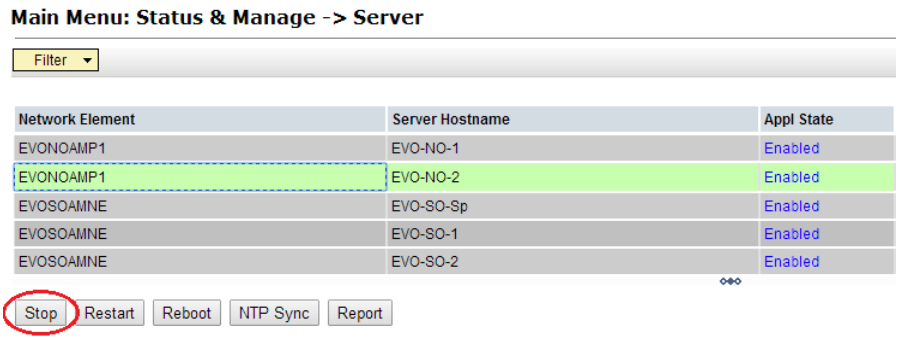
Procedure 42: Back Out Single Server

8. ☐	Verify the backout	1. Examine the output of the following commands to determine if any errors were reported:
		
		If the source release is 5.x:
		`# 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`
		
		If backing out to 70.19 and later:
		`$ sudo verifyBackout`
		
		The following 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`
		
		2. If the backout was not successful because other errors were recorded in the logs, it is recommended to contact MOS by referring to Appendix M of this document for further instructions.
		3. If the backout was successful (no errors or failures), then continue with the next step.

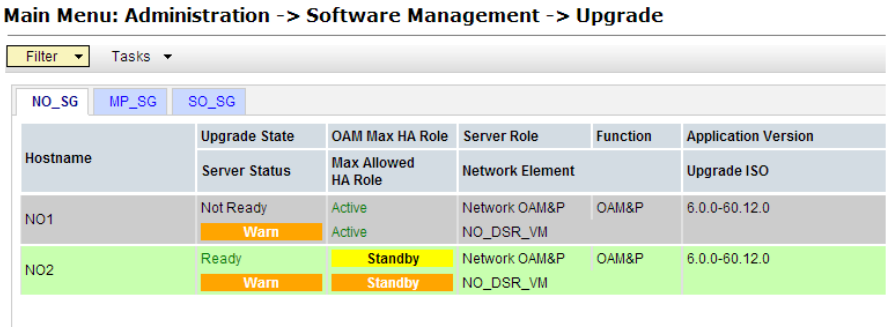
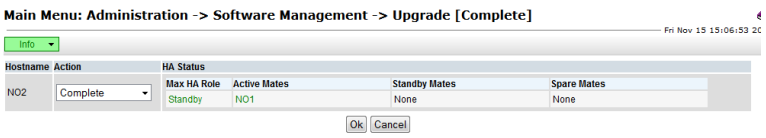
9. ☐	Reboot the server	Enter the following command to reboot the server:
		
		If the source release is 5.x:
		`# init 6`
		
		If the source release is 6.x/7.0:
		`$ sudo init 6`
		
		This step can take several minutes.

Procedure 42: Back Out Single Server

10. ☐	Verify services restart	Verify 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.
		
		If the source release is 5.x:
		`login as: root`
		`password: <enter password>`
		
		If the source release is 6.x/7.0:
		`login as: admusr`
		`password: <enter password>`
		
		3. If this is an NOAM or SOAM, verify the httpd service is running. Execute the command:
		
		If the source release is 5.x:
		`# service httpd status`
		
		If the source release is 6.x/7.0:
		`$ 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 M of this document for further instructions.

11. ☐	Remove Upgrade Ready status	Remove Upgrade Ready status 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. If the server just backed-out shows an "**Appl State"** of **"Enabled"**, then select the server row and press the **Stop** button. 

Procedure 42: Back Out Single Server

		4. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 5. If the server just backed-out shows an Upgrade State of "**Ready**" or "**Success**", then select the backed-out server and press **Complete.** Otherwise, skip to sub-step 6 below.  The **Upgrade [Complete]** screen will appear 
		6. Click **OK.** This will now remove the Forced Standby designation for the backed-out server. **7.** Verify the **Application Version** value for this server has been downgraded to the original release version.
12. ☐	Procedure Complete	**The single 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.

7.6 Back Out Multiple Servers

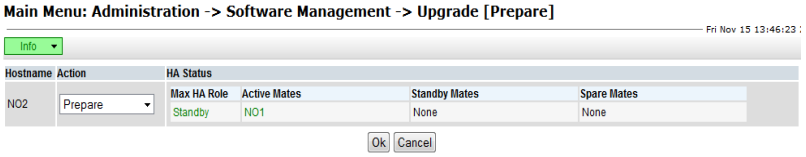
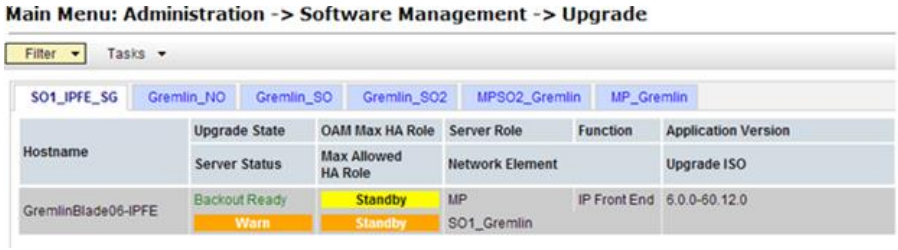
This section provides the procedures to back out the application software on multiple servers.

Procedure 43: Back Out Multiple Servers

S T E P #	This procedure will back out the upgrade of DSR 7.0 application software for multiple servers. Any server requiring backout can be included: NOAMs, SOAMs, DA-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 ☐	Logical Volume integrity check	Verify Logical Volume integrity for each server to be backed out.
		
		1. Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: If direct access to the IMI is not available, 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.
		
		2. Execute the following command:
		
		`$ sudo lvs`
		
		`[admusr@NO2 ~]$ sudo lvs`
		`  LV  VG  Attr  LSize  Pool Origin Data%  Move Log Cpy%Sync Convert`
		`  apw_tmp  vgroot -wi-ao----  2.41g`
		`  filemgmt  vgroot -wi-ao----  9.59g`
		`  logs_process  vgroot -wi-ao---- 512.00m`
		`  logs_security vgroot -wi-ao---- 512.00m`
		`  netbackup_lv  vgroot -wi-ao----  2.00g`
		`  plat_root  vgroot -wi-ao----  1.00g`
		`  plat_tmp  vgroot -wi-ao----  1.00g`
		`  plat_usr  vgroot -wi-ao----  4.00g`
		`  plat_var  vgroot -wi-ao----  1.00g`
		`  plat_var_tklc vgroot -wi-ao----  4.00g`
		`  run_db  vgroot -wi-ao----  5.00g`
		
		3. The integrity of the LV snapshot may be verified by reviewing the **Data%** values displayed in the lvs command output.
		
		IMPORTANT: If any value shown in the Data% column equals 100.00%, then the snapshot is INVALID and backout to the previous release is no longer possible.
		
		4. Repeat sub-steps 1 thru 3 for each server to be backed out.

Procedure 43: Back Out Multiple Servers

2 ☐	Make servers ready for backout	Make the servers 'Ready' for Backout: 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. **For DSR 51.13.0 and later only:** 3. Select the Server Group tab of the servers to back out. Check the upgrade state of the servers to backout: 4. Select all of the servers with an upgrade state of **'Ready'**. 5. Press the **'Complete'** button. The Upgrade [Complete] screen is displayed. 6. Select **Ok**. This starts the Complete action on the server. Control will return to the Upgrade Administration screen. 7. Select all of the remaining servers to be backed out. 8. Press the **'Prepare'** button. The Upgrade [Prepare] screen is displayed.  9. Click **OK.** This starts the Prepare action on the server. Control will return to the Upgrade Administration screen. **NOTE: If this is the Active server in an Active-Standby pair, the Prepare action WILL cause an HA switchover. The HA switchover is an expected outcome from the Prepare action.** **NOTE: When the Active NOAM is the server being backed out, the HA switchover will cause the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** 10. Wait for the screen to refresh and show the Upgrade State as **Backout Ready** for the server to be upgraded. It may take up to a minute for the Upgrade State to change to **Backout Ready**.  11. Repeat sub-steps 3 through 10 for each Server Group tab.

Procedure 43: Back Out Multiple Servers

3 ☐	Login to the server(s)	Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		
		If the source release is 5.x:
		`login as: root`
		`password: <enter password>`
		
		If the source release is 6.x/7.0:
		`login as: admusr`
		`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.

Procedure 43: Back Out Multiple Servers

4 ☐	Execute the backout	Determine the state of the server to be backed out. The server must be either Standby or Spare. Execute following command to find the state :
		
		`# ha.mystate`
		
		In the example output below, the HA state is Standby.
		
		`[admusr@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		
		If the state of the server is Active, then return to step 1 above.
		
		`$ sudo /var/TKLC/backout/reject`
		
		NOTE: If backout prompts to continue, answer "**y**".
		
		(The reject command 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`

5 ☐	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.
6 ☐	Repeat for each server to be backed out.	Repeat steps 2 through 4 for each server to be backed out.

Procedure 43: Back Out Multiple Servers

7 ☐	Login to the server	Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		
		If the source release is 5.x:
		`login as: root`
		`password: <enter password>`
		
		If the source release is 6.x/7.0:
		`login as: admusr`
		`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.

8 ☐	Restore the full DB run environment	Execute the backout_restore utility to restore the full database run environment:
		
		If the source release is 5.x:
		`# /var/tmp/backout_restore`
		
		If the source release is 6.x/7.0:
		`$ 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 `/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 M of this document for further instructions.

Procedure 43: Back Out Multiple Servers

<table>
<tr><td>9</td><td>Verify the backout</td><td>
1. Examine the output of the following commands to determine if any errors were reported:

If the source release is 5.x:
<pre># verifyUpgrade</pre>
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 <code>TKLCplat.sh</code> error:

<pre>[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</pre>
If backing out to 70.19 and later:

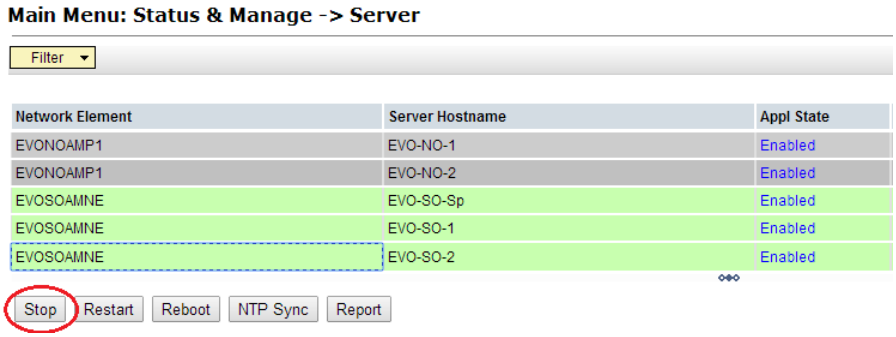
<pre>$ sudo verifyBackout</pre>
The following command will show the current rev on the server:

<pre>$ 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</pre>
2. If the backout was not successful because other errors were recorded in the logs, it is recommended to contact MOS by referring to Appendix M of this document for further instructions.
3. If the backout was successful (no errors or failures), then continue with the next step.
</td></tr>
<tr><td>10</td><td>Reboot the server</td><td>
Enter the following command to reboot the server:

If the source release is 5.x:
<pre># init 6</pre>
If the source release is 6.x/7.0:
<pre>$ sudo init 6</pre>
This step can take several minutes.
</td></tr>
</table>

Procedure 43: Back Out Multiple Servers

11 ☐	Verify services restart	Verify 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.
		
		If the source release is 5.x:
		`login as: root`
		`password: <enter password>`
		
		If the source release is 6.x/7.0:
		`login as: admusr`
		`password: <enter password>`
		
		3. If this is an NOAM or SOAM, verify the httpd service is running. Execute the command:
		
		If the source release is 5.x:
		`# service httpd status`
		
		If the source release is 6.x/7.0:
		`$ 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 M of this document for further instructions.

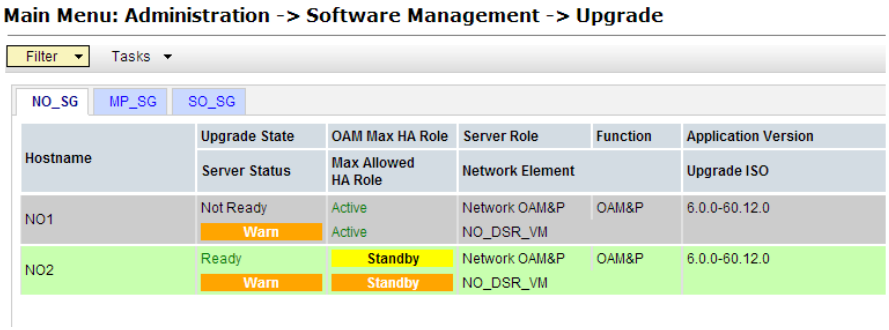
12 ☐	Repeat for each server backed out	Repeat steps 6 through 10 for each server backed out.
13 ☐	Remove Upgrade Ready status	Remove Upgrade Ready status 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. If the servers just backed-out show an "**Appl State"** of **Enabled**, then multi-select the server rows and press the **Stop** button. 4. Click **OK** on the confirmation dialog box. 

Procedure 43: Back Out Multiple Servers

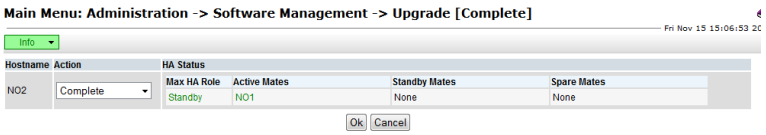
5. Select **Administration > Software Management > Upgrade.**
   The Upgrade Administration screen is displayed.

6. If the servers just backed-out show an Upgrade State of "**Ready**" or "**Success**", then select the backed-out server and press the **Complete** button.

   Otherwise, skip to sub-step 7 below.



The **Upgrade [Complete]** screen will appear.



7. Click **OK.** This will remove the Forced Standby designation for the backed-out servers.

8. Verify the **Application Version** value for these servers has been downgraded to the original release version.

14	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.

7.7 Perform Health Check (Post-Backout)

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

Procedure 44: Perform Health Check (Post-Backout)

S T E P #	This procedure performs a basic Health Check of the DSR to verify the health of the system following a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	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. ☐	Log all current alarms	Log all current alarms in the system: **From the Active NOAM GUI:** 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.	

8 APPENDIXES

Appendix A. ACCEPT UPGRADE

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

An upgrade should be accepted only after it was 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.

THE USER SHOULD BE AWARE THAT IN THE CASE OF "5.x to 7.x" MAJOR UPGRADE, UPGRADE ACCEPTANCE WILL FORCE AN IMMEDIATE REBOOT OF THE SERVER.

THEREFORE, PARALLEL EXECUTION MUST BE COORDINATED IN ORDER TO PREVENT A NODAL OUTAGE!

!! WARNING!!

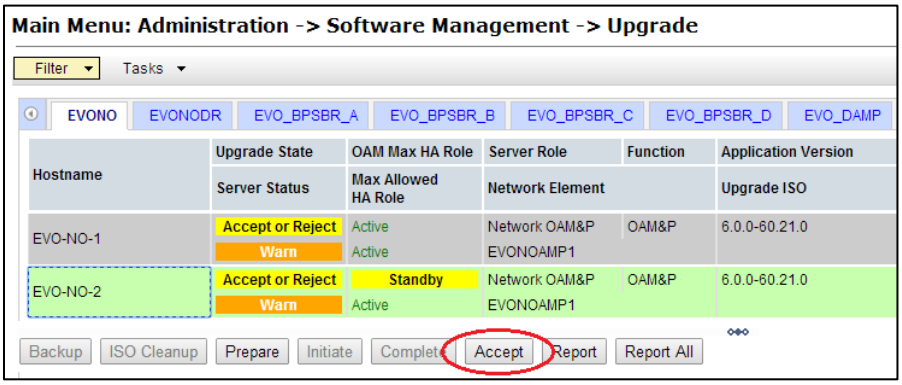
UPGRADE ACCEPTANCE MAY ONLY BE EXECUTED WITH AUTHORIZATION FROM THE CUSTOMER.

THE USER SHOULD BE AWARE THAT ONCE UPGRADE HAS BEEN ACCEPTED, IT WILL NOT BE POSSIBLE TO BACKOUT TO THE PREVIOUS RELEASE.

Procedure 45: 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 MOS AND ASK FOR UPGRADE ASSISTANCE.**	
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. ☐	**Active NOAM VIP:** Execute this Step if accepting a NOAM server. Log all current alarms present at the NOAM.	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.	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)**

Procedure 45: Accepting Upgrade

4. ☐	Accept upgrade for 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 server Groups tabs and select the servers (using the Ctrl button) for which upgrade is to be accepted, considering traffic, as Accept upgrade may lead to a server reboot. **4.** Click the **Accept** button  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.
5. ☐	Accept upgrade of the rest of the system	Repeat step 2 of this procedure until the upgrade of all Servers within the system has been accepted.
End of maintenance window.		

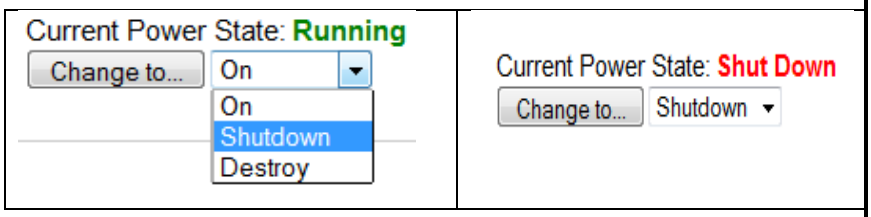
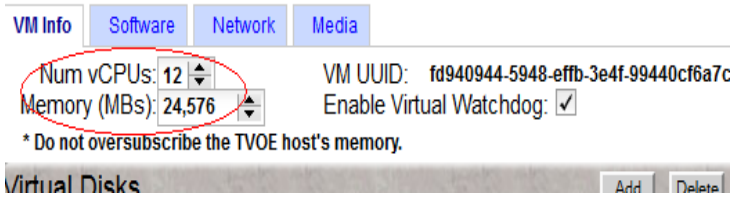
Appendix B. COMMAND OUTPUTS

Not Applicable.

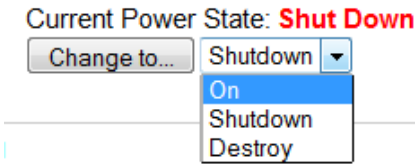
Appendix C. UPDATE NOAM GUEST VM CONFIGURATION

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 46: 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. ☐	Edit the NOAM Guest VM configuration	Edit NOAM Guest VM configuration 1. Log into the PMAC 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 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 minutes as this executes a graceful shutdown of the NOAM guest.  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**  **No other configuration values should be changed.** 8. Select **Save**. The GUI may gray out for a moment while the changes are committed.

Procedure 46: Update NOAM Guest VM Configuration

2. ☐	Modify the Guest power state.	9. Change the Guest power state from **Shutdown** to **On a**nd click the "**Change to…**" button. 
		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix D. 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 first 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 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 47: 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 UPGRADE ASSISTANCE.**	

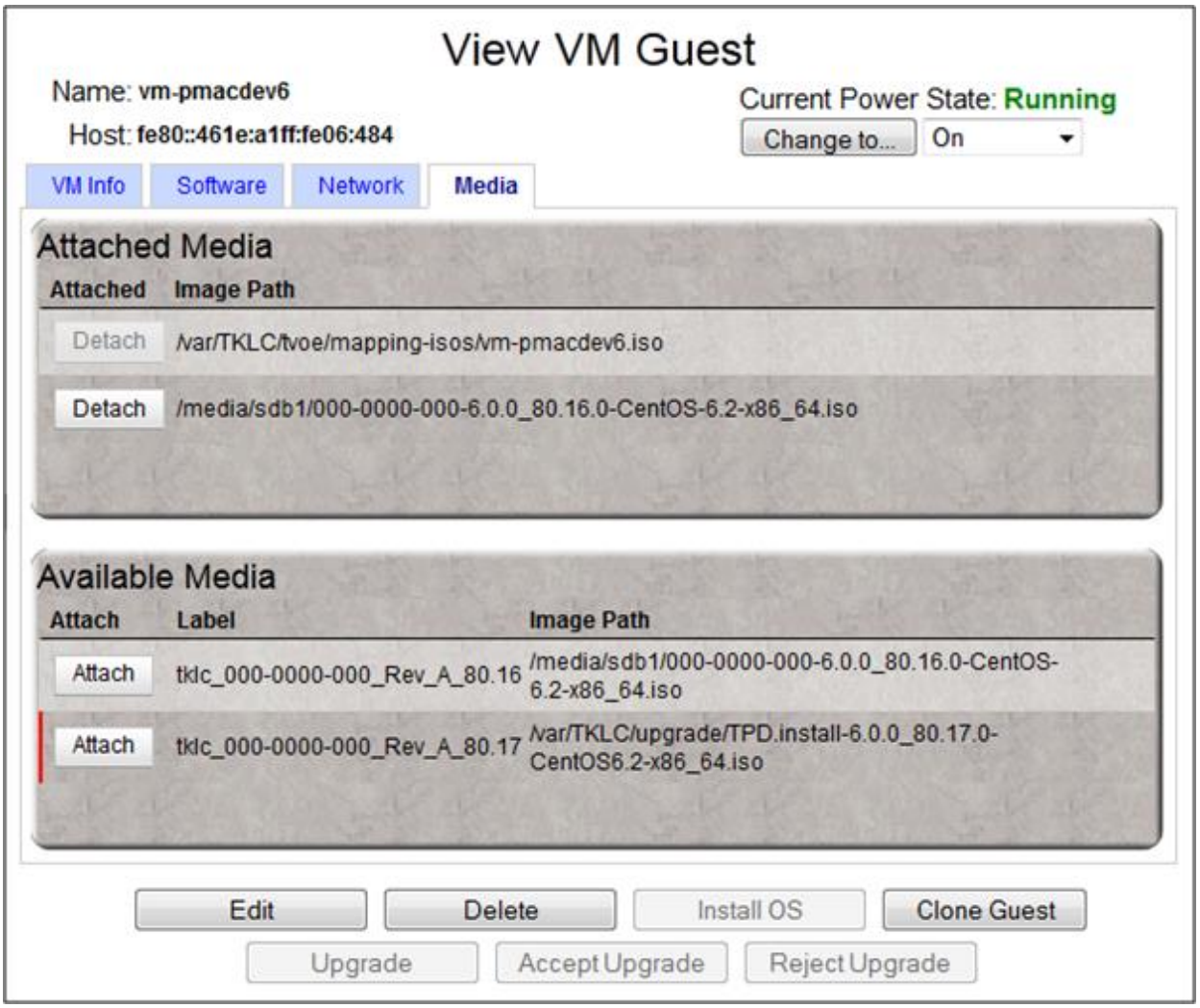
1. ☐	Determine the version of TVOE already running on the bare-metal server that hosts the virtual guest currently being upgraded	1. Log into the host server on which TVOE is installed.
		2. Execute the following command to get the current TVOE installed version :
		`# appRev`
		`Install Time: Thu Aug 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`

2. ☐	Check the TVOE release version required for target DSR release	It is recommended to contact MOS by referring to Appendix M of this document to determine the appropriate release version.
3. ☐	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 H.
	THIS PROCEDURE HAS BEEN COMPLETED.	

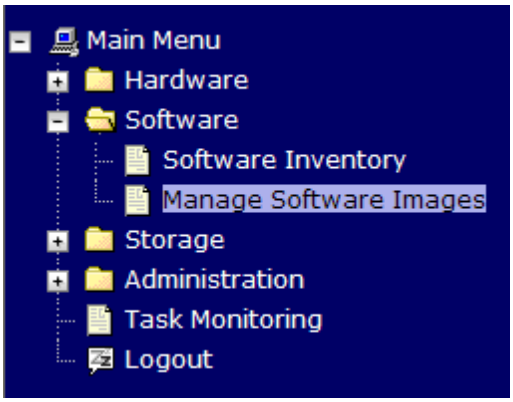
Appendix E. ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY

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.

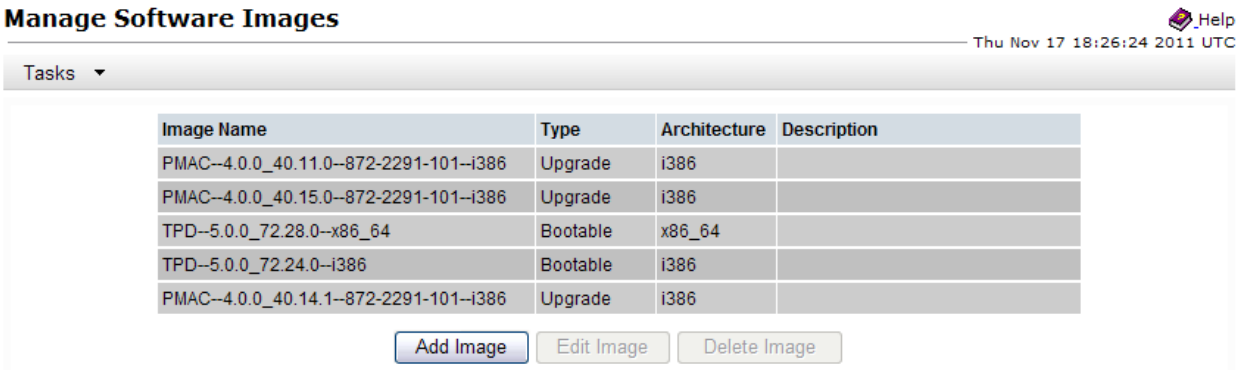
1. In the PM&C GUI, navigate to **Main Menu > VM Management.** In the "**VM Entities**" list, select the PM&C Guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.
2. Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



3. **PM&C GUI:** Navigate to **Manage Software Images**
   Navigate to **Main Menu ➤ Software ➤ Manage Software Images**

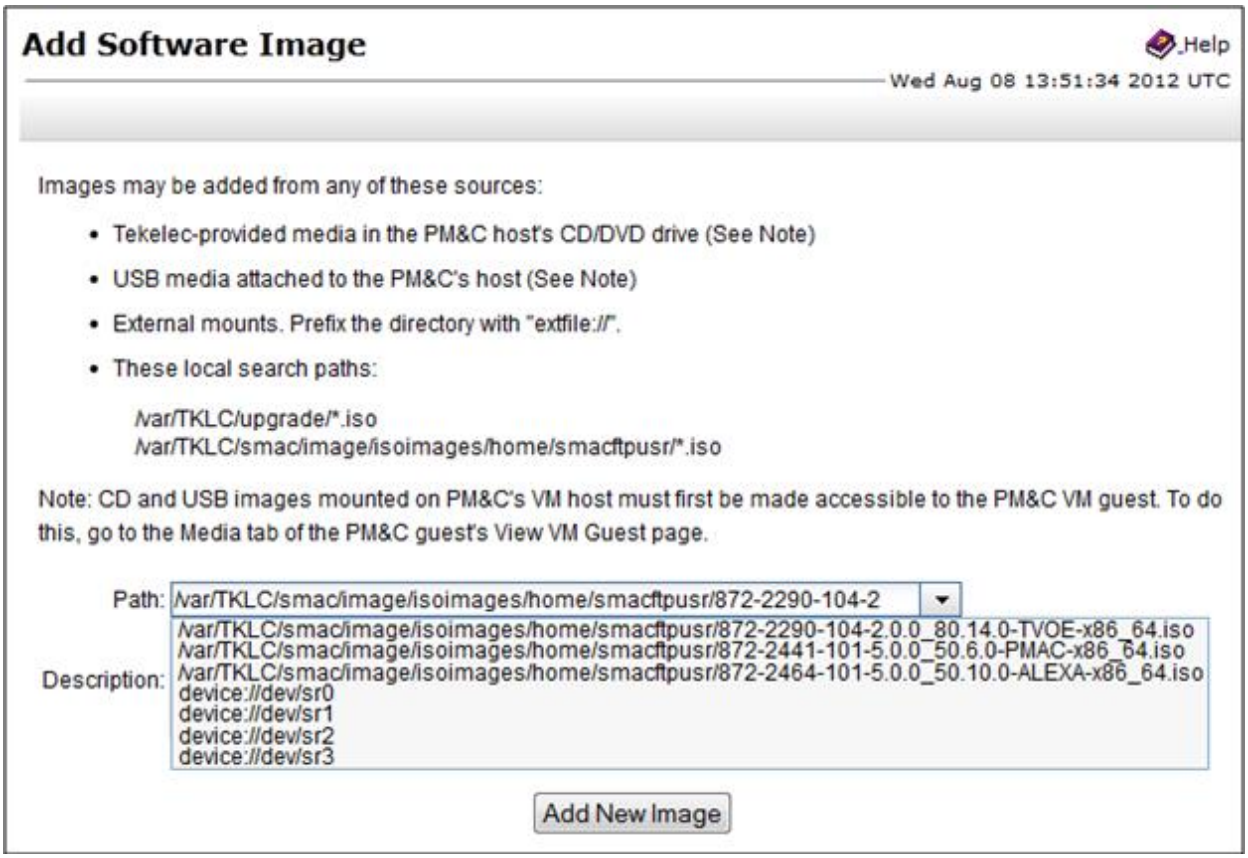


4. **PM&C GUI:** Add image
   Press the **Add Image** button.



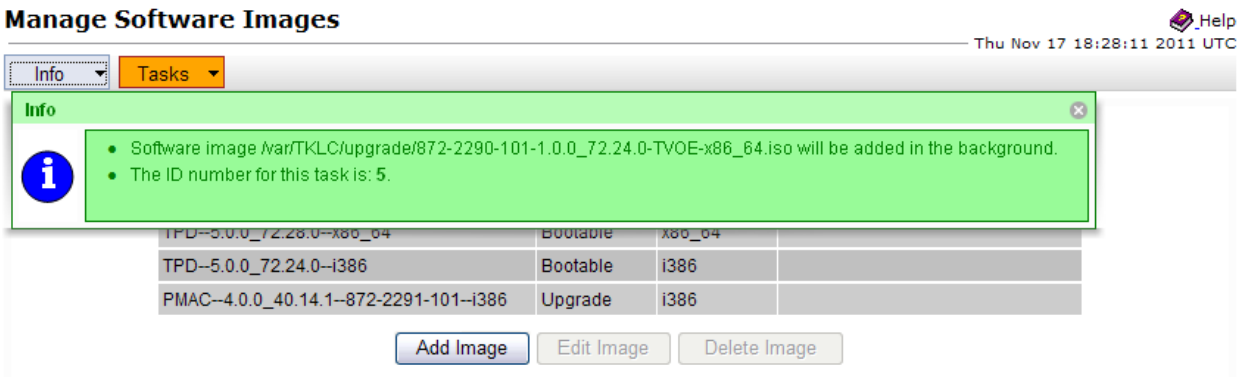
5. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:
   - If the image was transferred to PM&C via sftp, it will appear in the list as a local file "`/var/TKLC/...`".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("`device://...`"). 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.



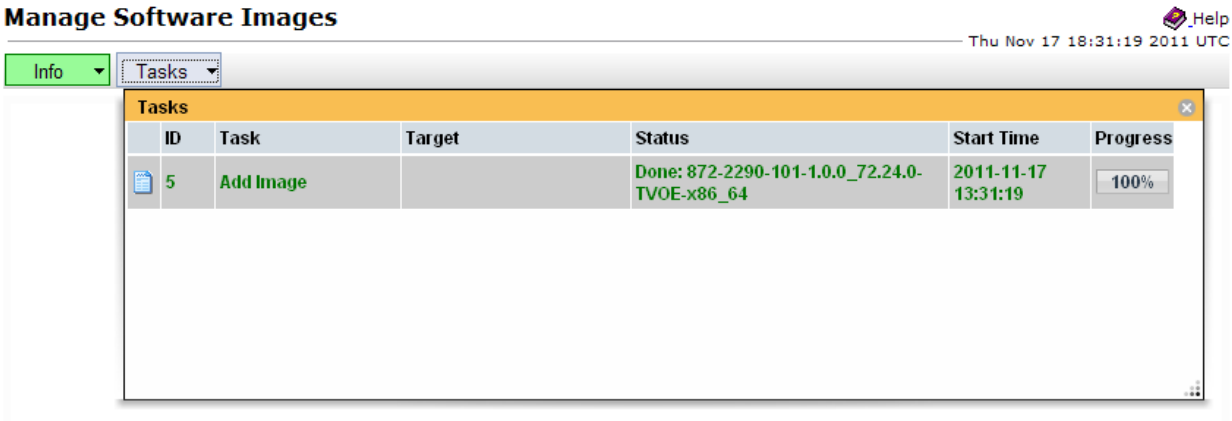
6. **PM&C GUI** Monitor the Add Image status

The Manage Software Images page is then redisplayed with a new background task entry in the table at the bottom of the page:



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:



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 3, 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 F. UPGRADE SINGLE SERVER – UPGRADE ADMINISTRATION

This Appendix provides the procedure for upgrading a DSR single server of any type (NOAM, SOAM, MP, etc).

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 F to mark up, or keep another form of written record of the steps performed.

Procedure 48: Upgrade Single Server – Upgrade Administration

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. ☐	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): **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release. 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)**

Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

Hostname	Server Status OAM Max HA Role Max Allowed HA Role	Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO2
Viper-NO2	Norm Standby Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO1
Viper-SO1-A	Norm Active Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-B
Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-A
Viper-SO2-A	Norm Active Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-B
Viper-SO2-B	Norm Standby Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-A
Viper-MP05	Norm Active Active	MP SO1_Viper 5.0.0-50.15.1	DSR (multi-active cluster)	Not Ready		Viper-MP06

Procedure 48: Upgrade Single Server – Upgrade Administration

<table>
<tr><td></td><td></td><td><u>Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later</u>

Main Menu: Administration -> Software Management -> Upgrade

Filter ▾ Tasks ▾

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

<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>GTR-MP-01</td><td>Backup Needed
Norm</td><td>Spare
Active</td><td>MP
GTR_SOAM_NE</td><td>DSR (multi-active cluster)</td><td>7.0.0.0.0-70.7.0</td></tr>
<tr><td>GTR-MP-02</td><td>Backup Needed
Norm</td><td>Spare
Active</td><td>MP
GTR_SOAM_NE</td><td>DSR (multi-active cluster)</td><td>7.0.0.0.0-70.7.0</td></tr>
<tr><td>GTR-MP-03</td><td>Backup Needed
Norm</td><td>Spare
Active</td><td>MP
GTR_SOAM_NE</td><td>DSR (multi-active cluster)</td><td>7.0.0.0.0-70.7.0</td></tr>
<tr><td>GTR-MP-04</td><td>Backup Needed
Norm</td><td>Spare
Active</td><td>MP
GTR_SOAM_NE</td><td>DSR (multi-active cluster)</td><td>7.0.0.0.0-70.7.0</td></tr>
</table>
</td></tr>
<tr><td>2.</td><td>Verify status of Server to be upgraded</td><td>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. Verify the Upgrade State is Not Ready :

NOTE: The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release.</td></tr>
<tr><td></td><td></td><td><u>Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2</u>

• Continue with sub-step 5 below:

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

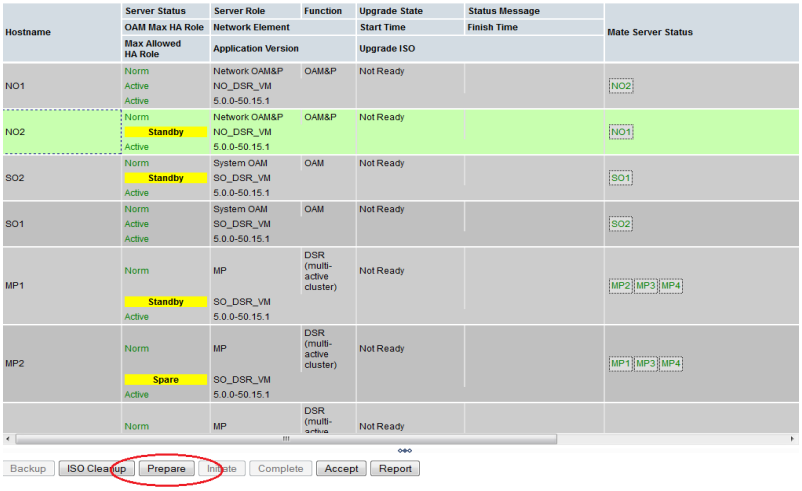
Procedure 48: Upgrade Single Server – Upgrade Administration

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later 4. From the Administration > Software Management > Upgrade screen, select the Server Group of the server which needs to be upgraded. **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks NSX_NO_SG | GTR_MP_SG | GTR_SBR_SG_A | GTR_SBR_SG_B | GTR_SO_SG | NSX_IPFE_A | NSX_IPFE_B | Hostname	Upgrade State / Server Status	OAM Max HA Role / Max Allowed HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO | |---|---|---|---|---|---| | GTR-MP-01 | Backup Needed / Norm | Spare / Active | MP / GTR_SOAM_NE | DSR (multi-active cluster) | 7.0.0.0.0-70.7.0 | | GTR-MP-02 | Backup Needed / Norm | Spare / Active | MP / GTR_SOAM_NE | DSR (multi-active cluster) | 7.0.0.0.0-70.7.0 | | GTR-MP-03 | Backup Needed / Norm | Spare / Active | MP / GTR_SOAM_NE | DSR (multi-active cluster) | 7.0.0.0.0-70.7.0 | | GTR-MP-04 | Backup Needed / Norm | Spare / Active | MP / GTR_SOAM_NE | DSR (multi-active cluster) | 7.0.0.0.0-70.7.0 |
		For All DSR Releases 5. If the server is in the '**Ready**' state, then skip the "Prepare Upgrade" steps (3-5) and start the Upgrade at Step 6. 6. If the server is in "**Backup Needed"** state, then first select the server and click the "Backup" button. Refresh the Upgrade screen to make sure that server is in the "**Not Ready**" state.
3 ☐	Prepare Upgrade (step 1)	For the server to be upgraded: 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) **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release.

Procedure 48: Upgrade Single Server – Upgrade Administration

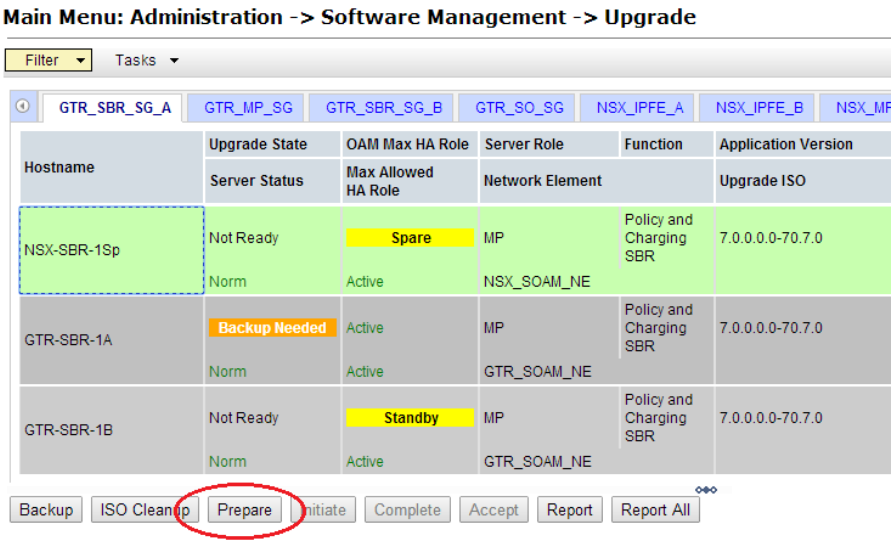
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

When **Prepare** is selected, the "Upgrade [Prepare]" form is displayed (see step 4 below).

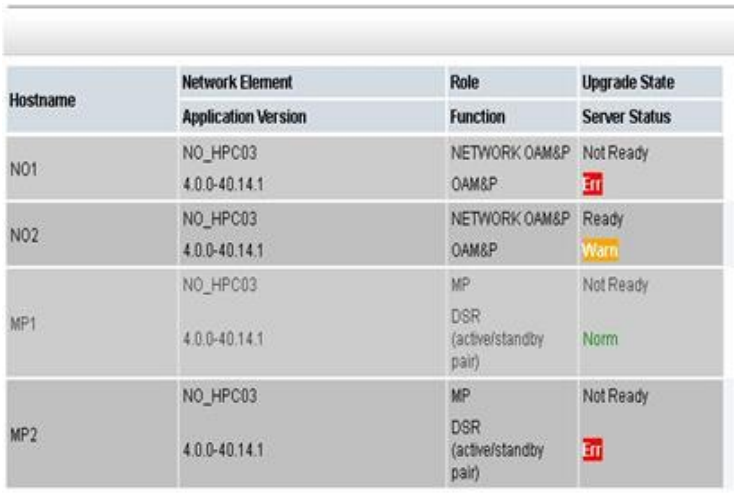


Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later

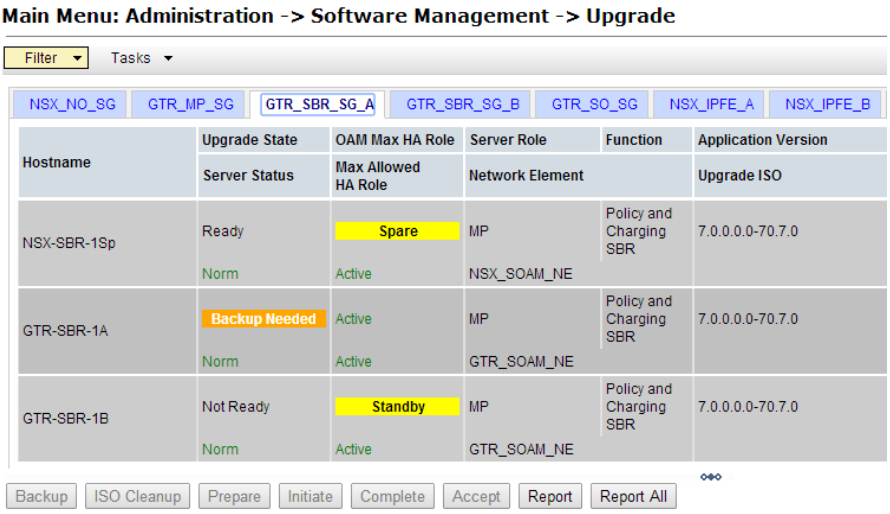
When **Prepare** is selected, the "Upgrade [Prepare]" form is displayed (see step 4 below).



Procedure 48: Upgrade Single Server – Upgrade Administration

4 ☐	Prepare Upgrade (step 2)	The **Upgrade** form is displayed (see example below) **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release. 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 condition of the Server to be upgraded is as expected, then, select: **OK** **NOTE: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** **NOTE: If the selected server is the active server in an Active/Standby pair, the 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.**
5 ☐	Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute) **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2** 

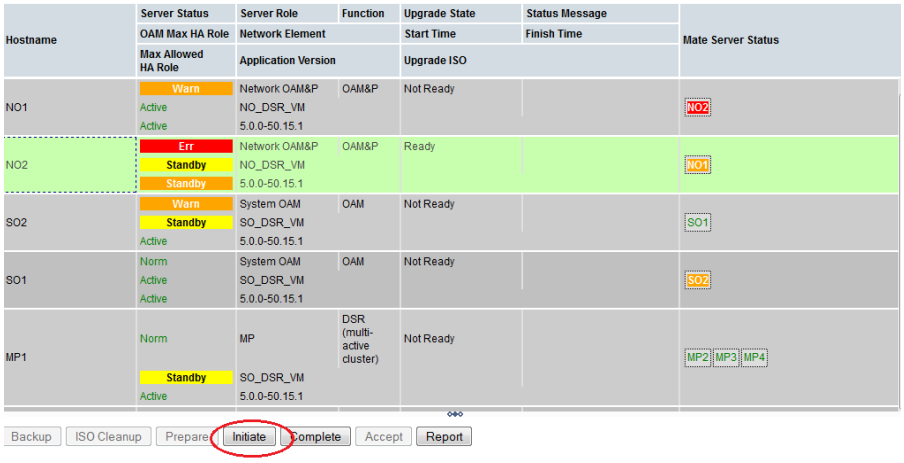
Procedure 48: Upgrade Single Server – Upgrade Administration

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later 
		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)**
6 ☐	Initiate Upgrade (initiate) (part 1)	Initiate the upgrade on the server. **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release.

Procedure 48: Upgrade Single Server – Upgrade Administration

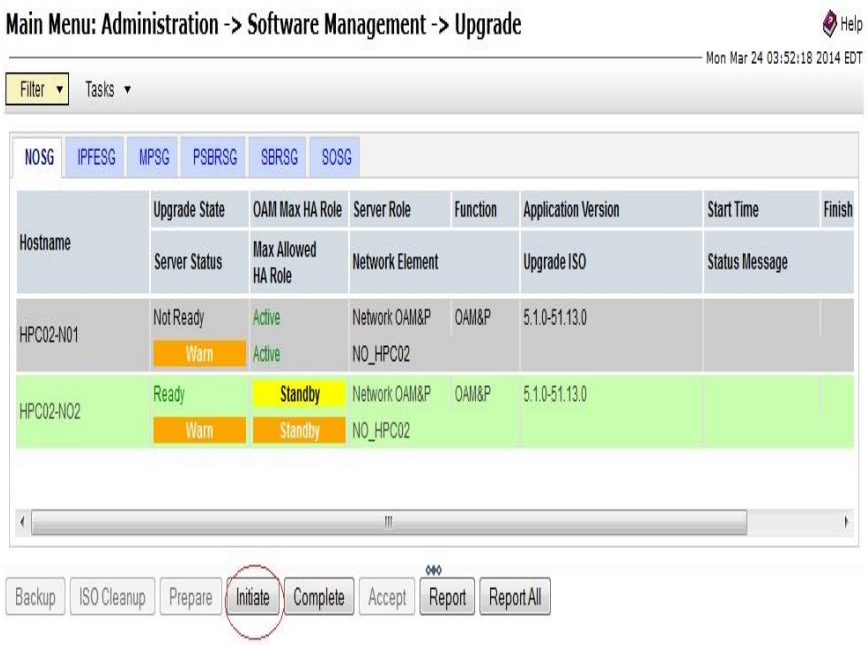
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Ensure that the "**Initiate"** button is enabled.
3. Click the "**Initiate"** button
4. Proceed to step 7.



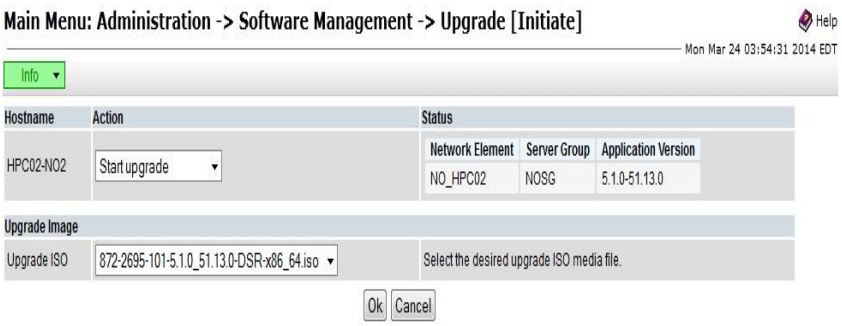
Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later

1. From the Upgrade Administration screen, select the server to be upgraded.
2. Ensure that the "**Initiate"** button is enabled.
3. Click the "**Initiate"** button



7	Initiate Upgrade (part 2) – Select ISO form	The Initial Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]** The target server is identified with its associated data (Hostname, Network Element, Server Group and application version)

Procedure 48: Upgrade Single Server – Upgrade Administration

		Upgrade initiate screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2 1. From the pick list at the lower left of the form, select the ISO to use in the server upgrade. 2. Click the **Start Upgrade** button. The upgrade will begin and control will return to the Upgrade **Administration** screen. 3. Proceed to step 8. 
		Upgrade initiate screen in DSR 5.1 releases 5.1.0-51.13.0 and later 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. 
8	View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release. 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.*

Procedure 48: Upgrade Single Server – Upgrade Administration

Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

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

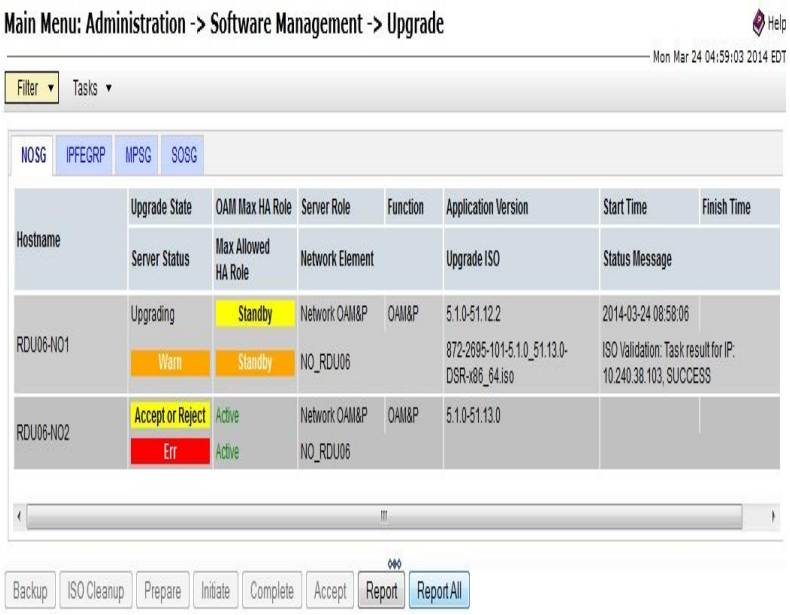
Hostname	Server Status OAM Max HA Role Max Allowed HA Role	Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
NO1	Err Active Active	Network OAM&P NO_DSR_VM 5.0.0-50.15.1	OAM&P	Not Ready		NO2
NO2	Warn Standby Standby	Network OAM&P NO_DSR_VM 5.0.0-50.15.1	OAM&P	Upgrading 2013-11-14 18:49:57 872-2526-101-5.0.0_50.15.1-DSR-x86_64.iso	Upgrade: retrieved TPD task state for IP: 192.168.1.12 is IN_PROGRESS_STATE	NO1
SO2	Warn Standby Active	System OAM SO_DSR_VM 5.0.0-50.15.1	OAM	Not Ready		SO1
SO1	Warn Active Active	System OAM SO_DSR_VM 5.0.0-50.15.1	OAM	Not Ready		SO2

2. Wait for the upgrade to complete. The "**Upgrade State**" column will show "**Success**". This step will take around 40-50 minutes.
3. Proceed to step 9.

Procedure 48: Upgrade Single Server – Upgrade Administration

Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later

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



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

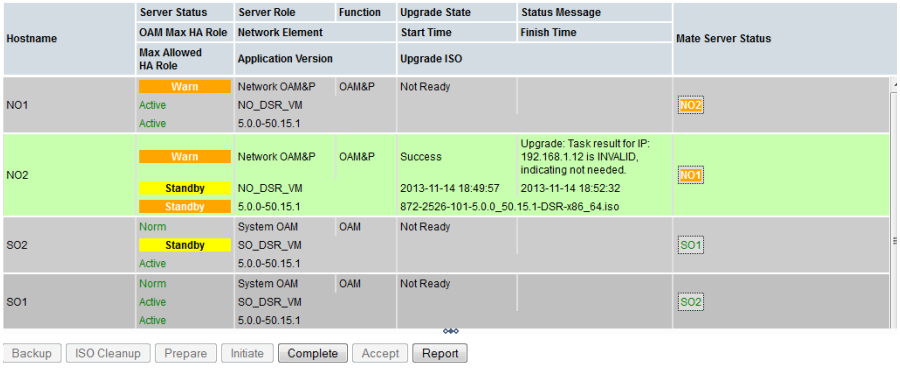
Alarm ID = **10008 (Provisioning Manually Disabled)**
Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)**
Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)**
Alarm ID = **32515 (Server HA Failover Inhibited)**
Alarm ID = **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.

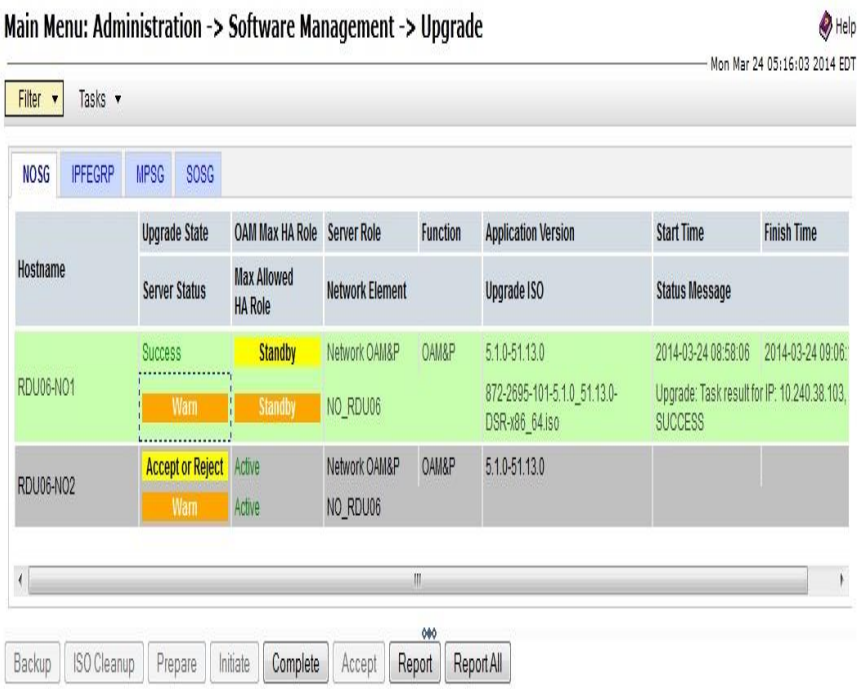
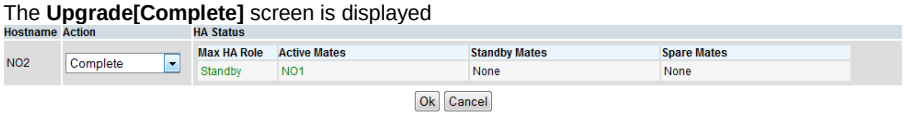
Procedure 48: Upgrade Single Server – Upgrade Administration

9 ☐	**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`

10 ☐	IF 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`
		
		It is recommended to contact MOS by referring to Appendix M of this document and provide these files.

11 ☐	Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 1)	Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type. **NOTE:** The look and feel of the Upgrade screen has changed between the 5.x and 6.x/7.0 releases. The screenshots below provide examples from each release. 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 status: 4. Verify the **Upgrade State** of the server that was upgraded is **Success**.
		<u>Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2</u> 5. Verify the **Complete** button is enabled for the server that was upgraded 6. Click the **Complete** button. 7. Proceed to step 12. 

Procedure 48: Upgrade Single Server – Upgrade Administration

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and later 5. Verify the **Complete** button is enabled for the server that was upgraded 6. Click the **Complete** button. 
12	Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 2)	The **Upgrade[Complete]** screen is displayed  Record the **Upgrade Ready Criteria** and selected **Server Status** values for this server. Keep this information for future reference. 1. Click **OK**. This completes the Remove Ready action on the server. The Upgrade Administration screen is displayed.

Procedure 48: Upgrade Single Server – Upgrade Administration

		2. Wait for the screen to refresh and show the Upgrade Ready State is **Accept or Reject** and the **Upgrade** action link is disabled for the server that was upgraded. It may take up to 2 minutes for the Upgrade Ready State to change to **Accept or Reject**. 
13 ☐	View Post-Upgrade Status	View the Post-Upgrade Status of the server: The Active NOAM or 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 = **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)** The Active NOAM or SOAM will have the following expected alarm until both NOAMs/SOAMs are upgraded: Alarm ID = **31233 – HA Secondary Path Down** NOTE: Do Not Accept upgrade at this time. This alarm is OK.
14 ☐	Procedure Complete	The single server upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix F. Procedure 9: NOAM Upgrade Procedure 10: Alternate NOAM Upgrade Procedure 18: Upgrade SOAMs (1+1 / RMS 1+1) Procedure 19: Upgrade DA-MPs (1+1 / RMS 1+1) Procedure 21: Upgrade SOAMs (N+0 / RMS N+0) Procedure 25: PCA SOAM Upgrade - Site 1 Procedure 26: Upgrade SBRs - Site 1 (PCA) Procedure 27: Upgrade Multiple DA-MPs - Site 1 (PCA)

Appendix G. UPGRADE FIRMWARE

Firmware Upgrade procedures are not included in this document. It is recommended to contact MOS by referring to Appendix M of this document for the latest information on Firmware upgrades.

Appendix H. UPGRADE TVOE PLATFORM

This Appendix provides the procedure 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 on a bare-metal server running the TVOE host software, then TVOE itself may have to be upgraded first. Refer to Appendix D to determine if a TVOE upgrade is required.

If you are upgrading a DSR server that is not virtualized, then this Appendix does not apply.

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.

The user should 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 49: Upgrade TVOE Platform

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 MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Disable all the applications running on current TVOE blade	1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Identify the NOAM or SOAM (virtual) servers that are running on the TVOE environment to be upgraded, and select these. 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**'.

2. ☐	**TVOE Host:**
	Find out the guests running on TVOE host
		List the guests running on the TVOE Host.
		1. SSH to the TVOE and log in.
		If the PM&C release is 5.0:
		`login as: root`
		`password: <enter password>`
		If the PM&C release is 5.5 or later:
		`login as: admusr`
		`password: <enter password>`
		Note: when logged in as admusr, some commands must be executed with the 'sudo' privilege.
		2. List all guests running on the TVOE Host:
		`# virsh list --all`
		or
		`$ sudo virsh list --all`
		Note: the output of above command will list all the guests running on current TVOE host.

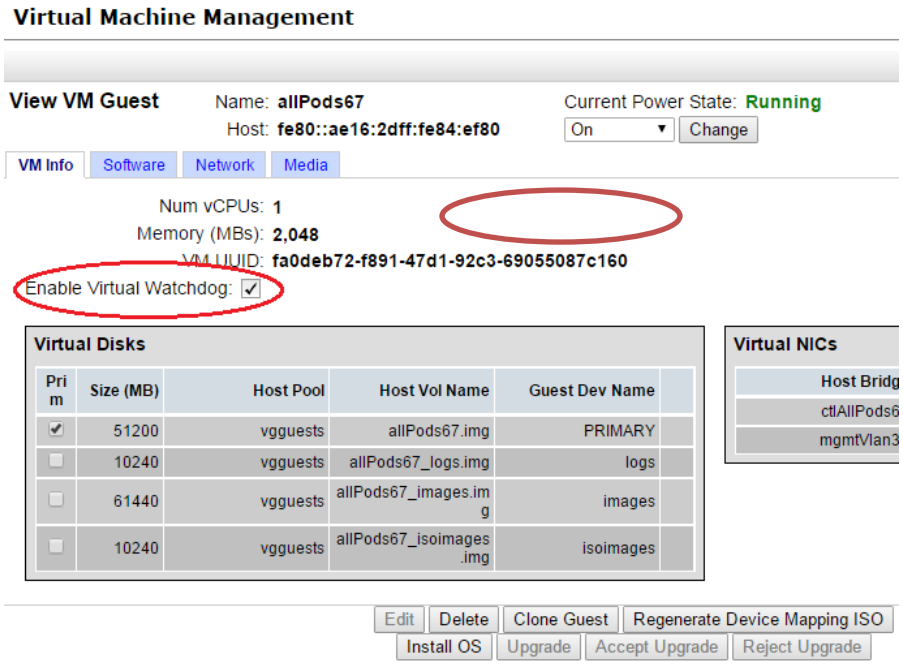
Procedure 49: Upgrade TVOE Platform

3. ☐	**TVOE Host:**
	Shutdown each guest running on TVOE host
		1. Execute the following command for each guest identified in Step 2 :
		
		`# virsh shutdown <guestname>`
		or
		`$ sudo virsh shutdown <guestname>`

4. ☐	**TVOE Host:**
	Upgrade TVOE
		1. Periodically execute following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list --all`
		or
		`$ sudo virsh list --all`
		
		2. Once all VMs have been properly shut down:
		
		Upgrade TVOE using the "PMAC Aided TVOE Upgrade Procedure" from Reference [3].
		
		[If the "PMAC Aided TVOE Upgrade" procedure is not possible, it is also possible to upgrade TVOE using the alternate procedure provided in Reference [3].]
		
		NOTE: If Active NOAM is hosted on the TVOE blade which is being upgraded, then VIP may be lost until TVOE is successfully upgraded.

5. ☐	After completed …	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.

Procedure 49: Upgrade TVOE Platform

6. ☐	**PMAC GUI:** Verify Enable Virtual Guest Watchdog is set for VM	From the PMAC VM Management form, verify that the "Enable Virtual Watchdog" is checked. If the 'Enable Virtual Watchdog checkbox is not checked, perform the following steps; 1. Shutdown the VM. 2. Click the **Edit** button. 3. Check the **Enable Virtual Watchdog** checkbox. 4. Restart the VM. 

7. ☐	**TVOE Host:**
	Start guests on TVOE host
		Execute following steps
		
		1. SSH to the TVOE and log in.
		
		If the PM&C release is 5.0:
		`login as: root`
		`password: <enter password>`
		
		If the PM&C release is 5.5 or later:
		`login as: admusr`
		`password: <enter password>`
		
		2. Execute the following command to start the TVOE guest(s) previously shutdown in step 3 above. If already running, then ignore this step and go to step 8.
		
		`# virsh start <guestname>`
		`or`
		`$ sudo virsh start <guestname>`
		
		3. Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list --all`
		`or`
		`$ sudo virsh list --all`

Procedure 49: Upgrade TVOE Platform

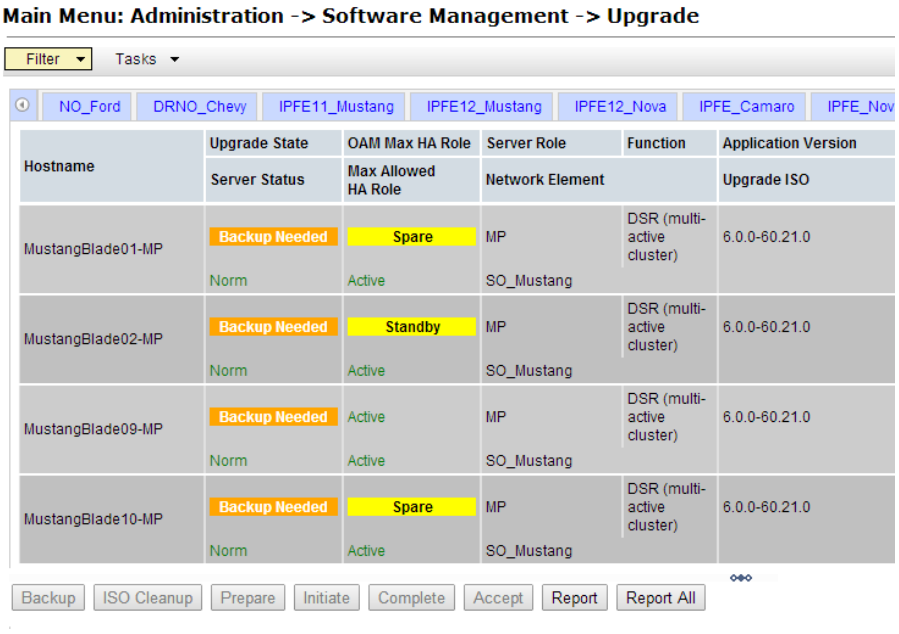
8. ☐	**Active NOAM VIP:** Enable all the applications disabled in step1	Enable all applications running on current TVOE blade 1. Log into the NOAM GUI using the VIP 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Select all the applications (NOAM(s)/SOAM(s)) running on current TVOE blade, 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 I. UPGRADE MULTIPLE SERVERS – UPGRADE ADMINISTRATION

This Appendix provides the procedure for upgrading multiple MP Servers in parallel.

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

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

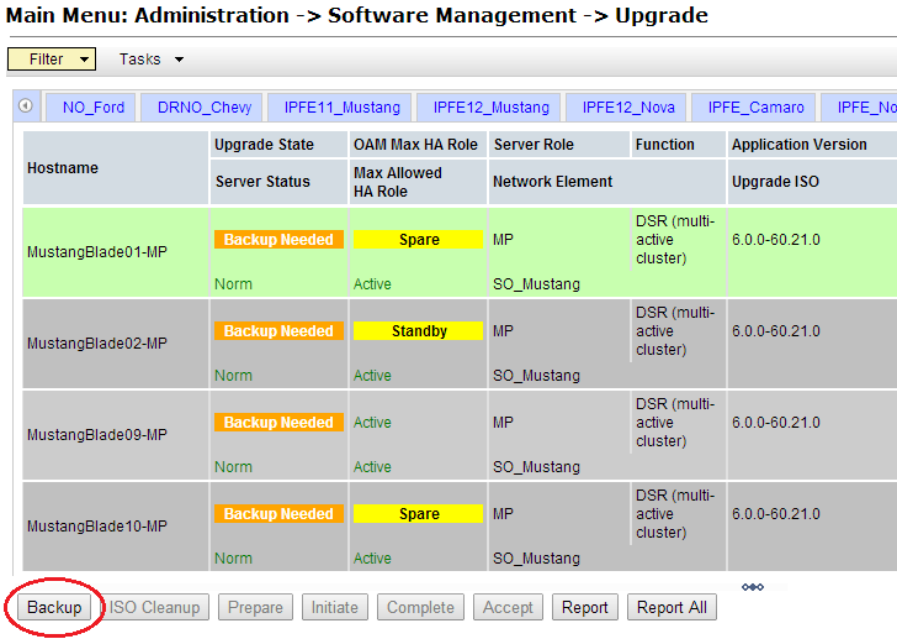
S T E P #	This procedure executes the Upgrade Multiple Servers – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	View the pre-upgrade status of Servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed  Active NOAM server may have some or all of the following expected alarms: Alarm ID = **10008 (Provisioning Manually Disabled)**

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

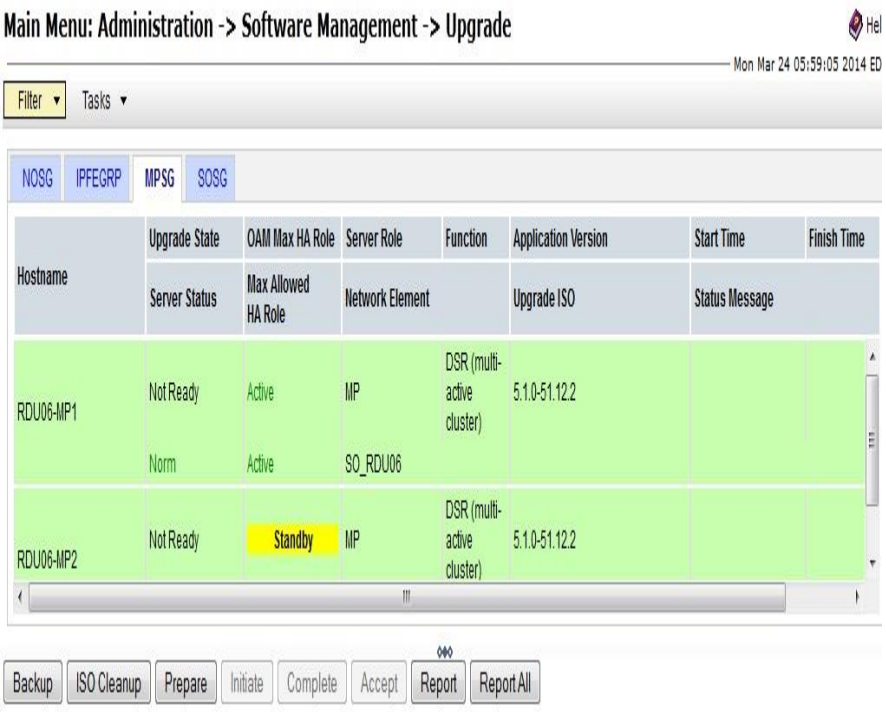
2. ☐	Verify status of Servers to be upgraded	For the servers to be upgraded: 1. Identify the MP servers to be upgraded in parallel _____ (record names) **NOTE: If the servers to be upgraded have "Function" of "Policy SBR" [5.x/6.0] or "Policy and Charging SBR" [7.0], the Standby and Spare servers can be upgraded in parallel. When determining which servers are the Standby and Spare servers, you MUST use the "Resource HA Role" value from the SBR Status screen instead of the value displayed in the "OAM Max HA Role" on the Upgrade screen.** 2. Verify the Application Version value is the expected source software release version for each MP server to be upgraded. 3. Verify the Upgrade State is **Not Ready** for each MP server to be upgraded. 4. From the **Administration > Software Management > Upgrade** screen, select the Server Group of the server to be upgraded. **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks NO_Ford DRNO_Chevy IPFE11_Mustang IPFE12_Mustang IPFE12_Nova IPFE_Camaro IPFE_No Hostname / Server Status / Upgrade State / Max Allowed HA Role / OAM Max HA Role / Network Element / Server Role / Function / Application Version / Upgrade ISO MustangBlade01-MP: Backup Needed / Norm / Spare / Active / MP / SO_Mustang / DSR (multi-active cluster) / 6.0.0-60.21.0 MustangBlade02-MP: Backup Needed / Norm / Standby / Active / MP / SO_Mustang / DSR (multi-active cluster) / 6.0.0-60.21.0 MustangBlade09-MP: Backup Needed / Norm / Active / Active / MP / SO_Mustang / DSR (multi-active cluster) / 6.0.0-60.21.0 MustangBlade10-MP: Backup Needed / Norm / Spare / Active / MP / SO_Mustang / DSR (multi-active cluster) / 6.0.0-60.21.0 Backup ISO Cleanup Prepare Initiate Complete Accept Report Report All

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

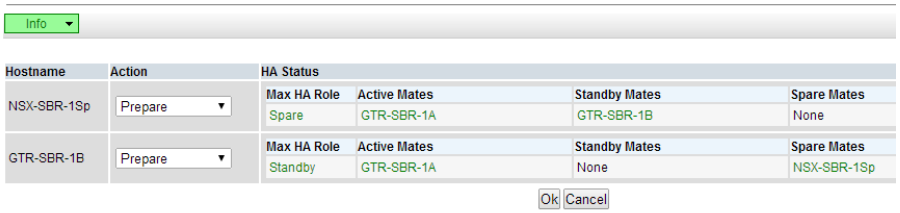
5. If the servers are in 'Ready' state then skip the "Prepare Upgrade" steps and start the upgrade at Step 6.
6. If the servers are in "**Backup Needed"** state then first select all the servers which are in **"Backup Needed"** state and click "Backup" button. Refresh the Upgrade screen to make sure that servers are in "**Not Ready**" state.



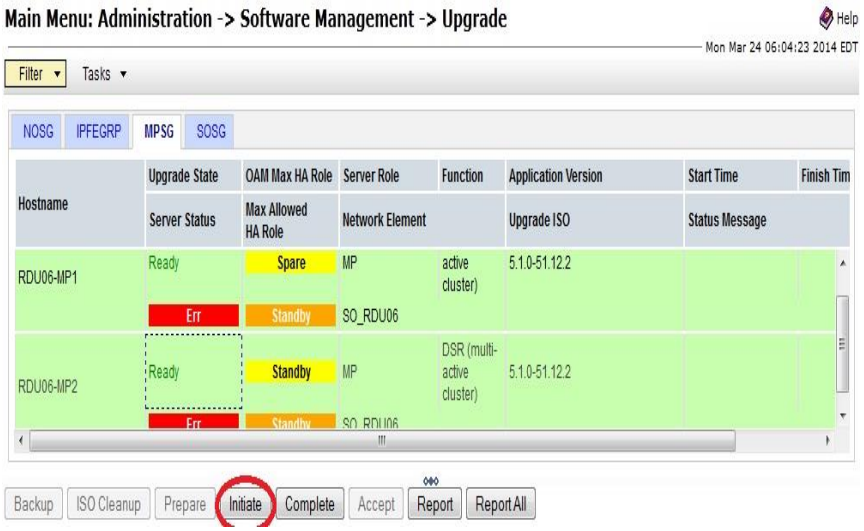
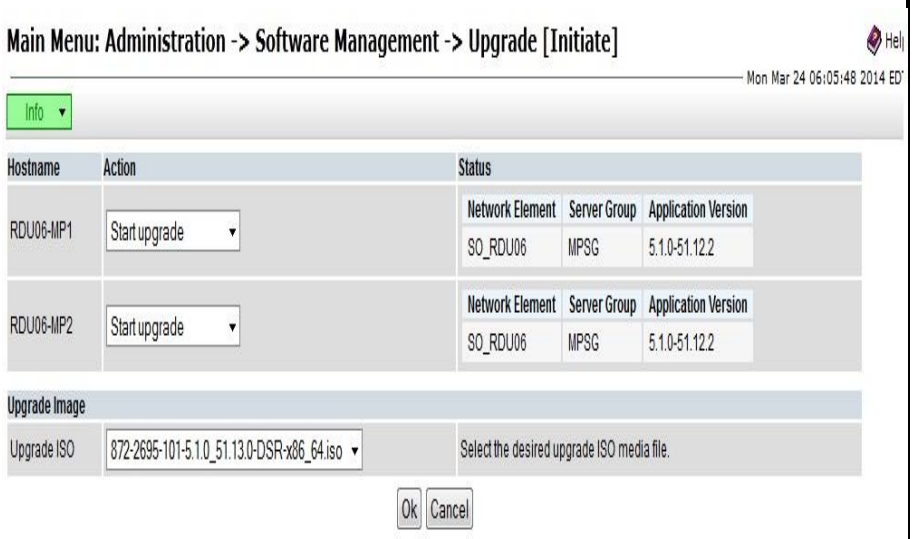
Procedure 50: Upgrade Multiple Servers - Upgrade Administration

3. ☐	Prepare Upgrade (step 1)	For the servers to be upgraded: 1. On the Upgrade form, make the server 'Upgrade Ready', by selecting the servers to be upgraded (using Ctrl button) and select **Prepare** The Upgrade Administration screen is displayed (examples below; In this example, MP1 and MP2 will be made ready for Upgrade)  The "Upgrade [Prepare]" form will be displayed. (see next step)

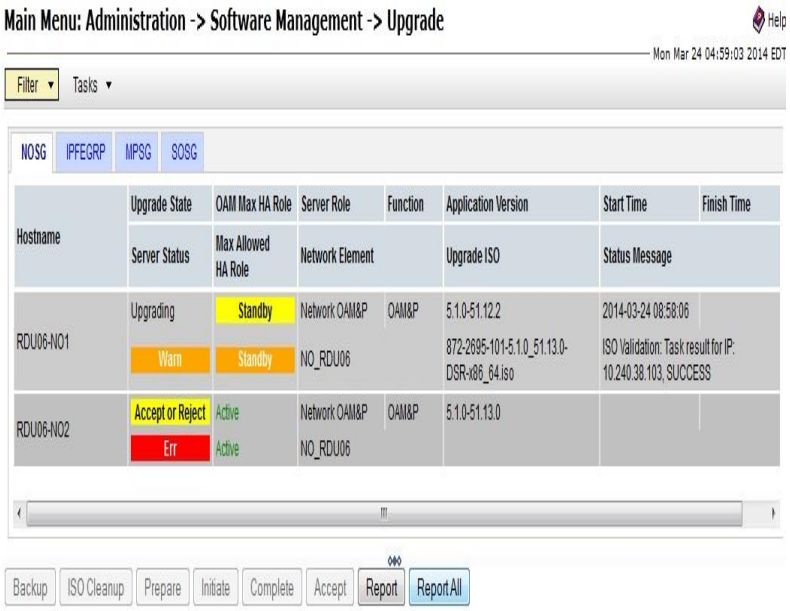
Procedure 50: Upgrade Multiple Servers - Upgrade Administration

4. ☐	Prepare Upgrade (step 2)	The Upgrade form is displayed (see example below) 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) **NOTE: If the servers to be upgraded have "Function" of "Policy SBR" [5.x/6.0] or "Policy and Charging SBR" [7.0], you MUST use the "Resource HA Role" value from the SBR Status screen instead of the value displayed in the "Max HA Role" on the Upgrade [Prepare] screen when determining if the server is in the "expected condition". Ignore any warnings about upgrading an Active server if you are upgrading a server known to be Standby or Spare from the SBR Status screen.** 2. If the condition of the Server to be upgraded is as expected, then select: **OK.** The Upgrade Administration screen is re-displayed. **Main Menu: Administration -> Software Management -> Upgrade [Prepare]**  ***NOTE: If the selected server is the active server in an Active/Standby pair, the 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.***
5. ☐	Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute) The Upgrade Administration screen is displayed (examples below): Depending on the server being upgraded, new alarms may occur. 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 50: Upgrade Multiple Servers - Upgrade Administration

6. ☐	Initiate Upgrade (initiate) (part 1)	Initiate Upgrade on the servers: 1. Select the servers to be upgraded and select the **Initiate** button. 
7. ☐	Initiate Upgrade (part 2) – Select ISO form	The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]** The target server is identified with its associated data (Hostname, Network Element, Server Group and application version) 1. From the pick list at the lower left of the form, select the ISO to use in the server upgrade. 2. Click the **Start Upgrade** button; the upgrade will begin and control will return to the Upgrade **Administration** screen. 

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

8. ☐	View In-Progress Status (monitor)	The View Upgrade Administration form:  Wait for the upgrade to complete. The "**Upgrade State**" column will show "**Success**". This step will take around 40-50 minutes. 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)** See step below for instructions if the Upgrade fails, or 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.*

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

9. ☐	**Optional :** View In-Progress Status from command line of server	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:
		
		`# appRev`
		`Install Time: Mon Oct  7 03:00:14 2013`
		`Product Name: DSR`
		`Product Release: 5.1.0_51.12.0`
		`Part Number ISO: 872-2526-101`
		`Part Number USB: 872-2526-101`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.5.0_82.24.0`
		`Base Distro ISO: TPD.install-6.5.0_82.24.0-CentOS6.4-x86_64.iso`
		`OS: CentOS 6.4`

10. ☐	IF 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`
		
		It is recommended to contact MOS by referring to Appendix M of this document and provide these files.

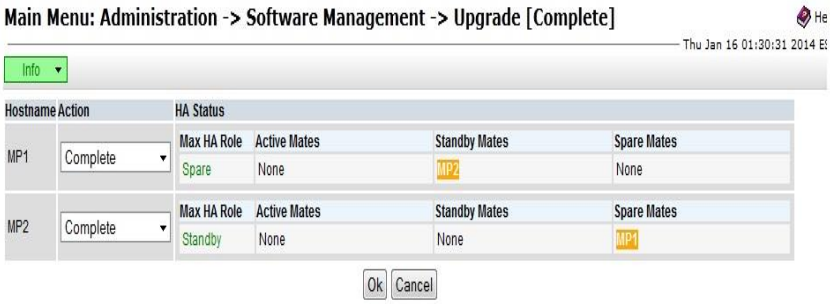
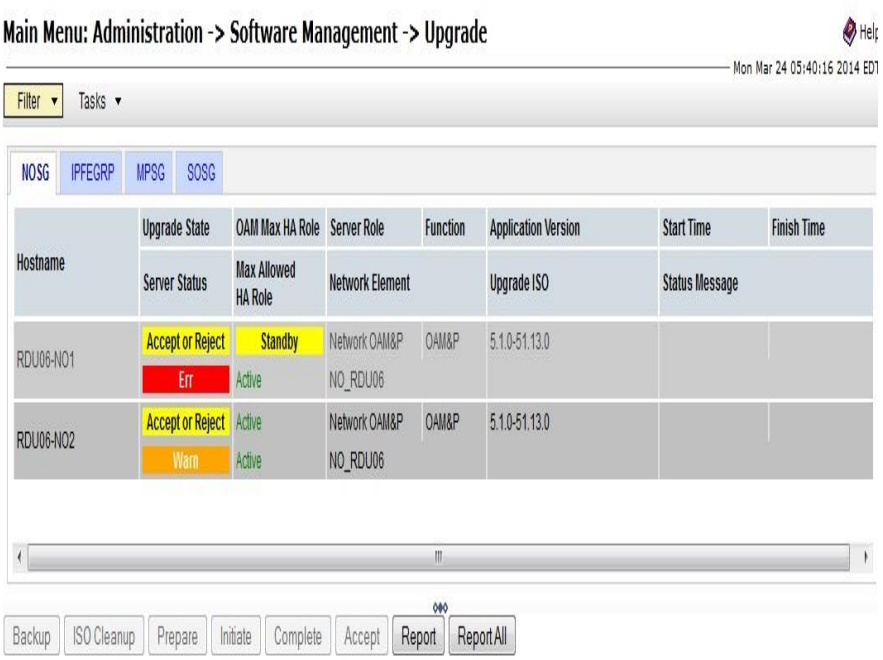
Procedure 50: Upgrade Multiple Servers - Upgrade Administration

11. ☐	Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 1)	Take the upgraded servers out of the upgrade ready state. This step applies to all servers, regardless of type. 1. Select the **Upgrade Administration** screen **Administration > Software Management > Upgrade** 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 servers that was upgraded is **Success**. 5. Verify the **Complete** button is enabled for the servers that were upgraded. 6. Select all servers with an upgrade state of "Success" (using Ctrl button) 7. Click the **Complete** button. Main Menu: Administration -> Software Management -> Upgrade Thu Jan 16 01:03:34 2014 ES Filter ▾ Tasks ▾

Hostname	Server Status / OAM Max HA Role / Max Allowed HA Role	Server Role / Network Element / Application Version	Function	Upgrade State / Start Time / Upgrade ISO	Status Message / Finish Time	Mate Server Status
NO2	Unk null null	Network OAM&P NO_DSR_VM	OAM&P			
SO1	Err Active Active	System OAM SO_DSR_VM 5.1.0-51.12.0	OAM	Not Ready		SO2
SO2	Err Standby Active	System OAM SO_DSR_VM 5.1.0-51.12.0	OAM	Not Ready		SO1
MP1	Err Spare Standby	MP SO_DSR_VM 5.1.0-51.12.0	DSR (multi-active cluster)	Success 2014-01-15 13:02:32 872-2695-101-5.1.0_51.11.0-DSR-x86_64.iso	Upgrade: Task result for IP: 10.240.23.221, SUCCESS 2014-01-15 13:41:10	MP2
MP2	Err Standby Standby	MP SO_DSR_VM 5.1.0-51.12.0	DSR (multi-active cluster)	Success 2014-01-15 13:02:54 872-2695-101-5.1.0_51.11.0-DSR-x86_64.iso	Upgrade: Task result for IP: 10.240.23.222, SUCCESS 2014-01-15 13:40:33	MP1

Backup | ISO Cleanup | Prepare | Initiate | Complete | Accept | Report

Procedure 50: Upgrade Multiple Servers - Upgrade Administration

12. ☐	Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 2)	The **Upgrade[Complete]** screen is displayed  **1.** Record the Selected **Server Status** values for the upgraded servers. Keep this information for future reference. **2.** Verify that Action is "Complete" for each upgraded/selected server. **3.** Click **OK**. This completes the Remove Ready action on each upgraded server. The Upgrade Administration screen is displayed. **5.** Wait for the screen to refresh and show the Upgrade Ready State is **Accept or Reject** and the **Upgrade** action link is disabled for the servers that were upgraded. It may take up to 2 minutes for the Upgrade Ready State to change to **Accept or Reject**. 
13.	View Post-Upgrade Status	View Post-Upgrade Status of the server: The Active SOAM server may have some or all the following expected alarm(s): Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10010 (Stateful database not yet synchronized with mate database)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31000 (Program impaired by S/W Fault)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** NOTE: Do Not Accept upgrade at this time. This alarm is OK.

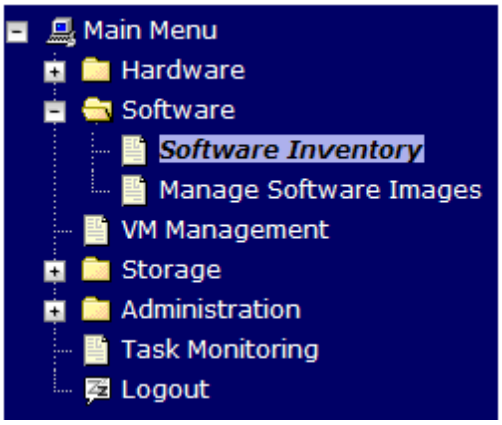
14. ☐	Procedure Complete.	The multiple servers upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix I. Procedure 20: Upgrade Multiple SS7-MPs (1+1 / RMS 1+1) Procedure 22: Upgrade Multiple DA-MPs (N+0 / RMS N+0) Procedure 23: Upgrade Multiple SS7-MPs (N+0 / RMS N+0) Procedure 24: Upgrade IPFE(s) (N+0 / RMS N+0) Procedure 27: Upgrade Multiple DA-MPs - Site 1 (PCA) Procedure 28: Upgrade Multiple SS7-MPs - Site 1 (PCA) Procedure 29: Upgrade IPFE(s) - Site 1 (PCA) Procedure 30: PCA SOAM Upgrade - Site 2 Procedure 32: Upgrade Multiple DA-MPs - Site 2 (PCA) Procedure 33: Upgrade Multiple SS7-MPs - Site 2 (PCA) Procedure 34: Upgrade IPFE(s) - Site 2 (PCA)
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix J. ALTERNATE SERVER UPGRADE USING PM&C

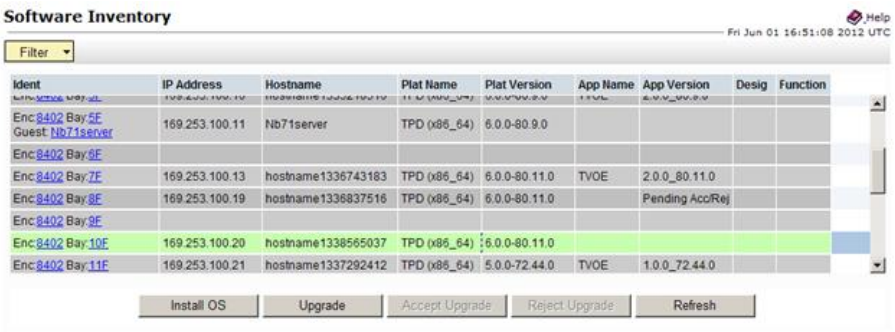
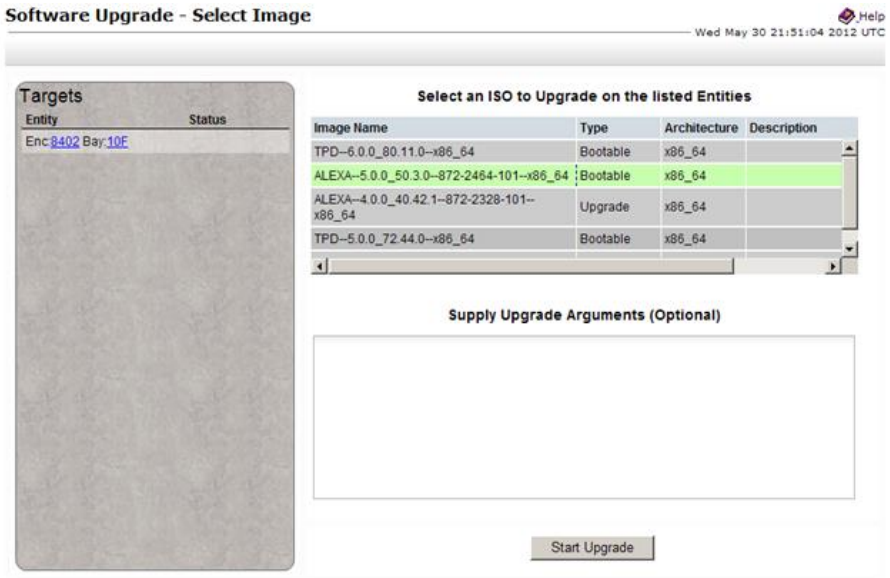
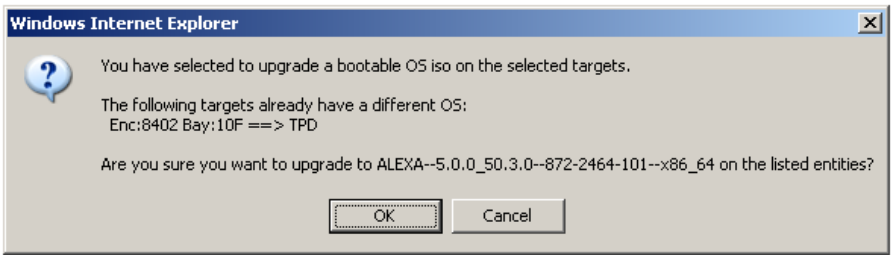
This appendix provides the procedure for upgrading the Standby NOAM and DR-NOAM using the PM&C interface. This upgrade method is an alternative to using the NOAM Upgrade GUI, and is used only when the NOAM Upgrade GUI refresh is sluggish due to the large number of C-level servers.

NOTE: Before executing this procedure, download the target release ISO to the PM&C image repository in accordance with Appendix E.

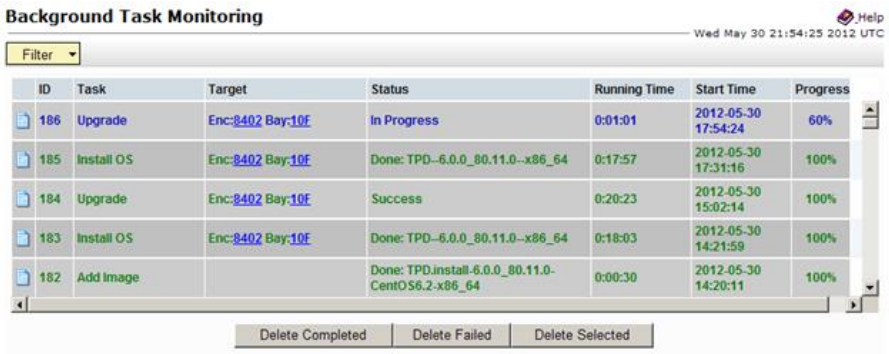
Procedure 51: Alternate Server Upgrade using PM&C

S T E P #	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 ☐	Navigate to Software Inventory	1. Navigate to **Main Menu > Software > Software Inventory**. 

Procedure 51: Alternate Server Upgrade using PM&C

3 ☐	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.  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 ☐	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. 
5 ☐	Start the upgrade	1. Press the **Start Upgrade** button. 2. Press the **OK** button to proceed with the upgrade. 

Procedure 51: Alternate Server Upgrade using PM&C

6 ☐	Monitor the upgrade	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the Upgrade background task. A separate task will appear for each server being upgraded.  When the task is complete and successful, the text will change to green and the Progress column will indicate "100%".
7 ☐	Procedure Complete	The alternate server upgrade procedure is now complete. Return to the overall DSR upgrade procedure step that directed the execution of Appendix J.
		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix K. EXPIRED PASSWORD WORKAROUND PROCEDURE

This appendix provides the procedures to handle password expiration during upgrade. Procedure 52 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 53 after the site is upgraded. Failure to remove the workaround will inhibit password aging on the server.

Appendix K.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 52: Expired Password Workaround Procedure

S T E P #	This procedure disables password aging on a server, allowing "expired" credentials to be used for login. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	SSH to Active SOAM server	5. 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:
		
		If the source release is 5.x:
		`ssh root@<SOAM_VIP>`
		
		If the source release is 6.x/7.0:
		`ssh admusr@<SOAM_VIP>`
		
		(Answer 'yes' if prompted to confirm the identity of the server.)
		
		6. Create a text file with the following content:
		
		`[production]`
		`aw.policy.pwchange.isExpired = [development:production]`
		`[test:development]`
		
		7. Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		
		8. Execute the following command:
		
		`clearCache`

Procedure 52: Expired Password Workaround Procedure

		9. Repeat sub-steps 1 through 4 for the Standby SOAM **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 all non-upgraded sites	Repeat step 1 for all non-upgraded sites.
THIS PROCEDURE HAS BEEN COMPLETED.		

Appendix K.2. Enable Password Aging

This procedure removes the password expiration workaround that is enabled by Procedure 52.

Procedure 53: Expired Password Workaround Removal Procedure

S T E P #	This procedure removes the password aging workaround and re-enables password aging on a server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	SSH to Active SOAM server	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:
		
		If the source release is 5.x:
		`ssh root@<NOAM_VIP>`
		
		If the source release is 6.x/7.0:
		`ssh admusr@<NOAM_VIP>`
		
		(Answer 'yes' if prompted to confirm the identity of the server.)
		
		2. Create a text file with the following content:
		
		`[production]`
		`aw.policy.pwchange.isExpired = [development:production]`
		`[test:development]`
		
		3. Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		
		4. Execute the following command:
		
		`clearCache`
		
		5. Repeat sub-steps 1 through 4 for the Standby SOAM

2 ☐	Repeat for all non-upgraded sites	Repeat step 1 for all non-upgraded sites.
	THIS PROCEDURE HAS BEEN COMPLETED.	

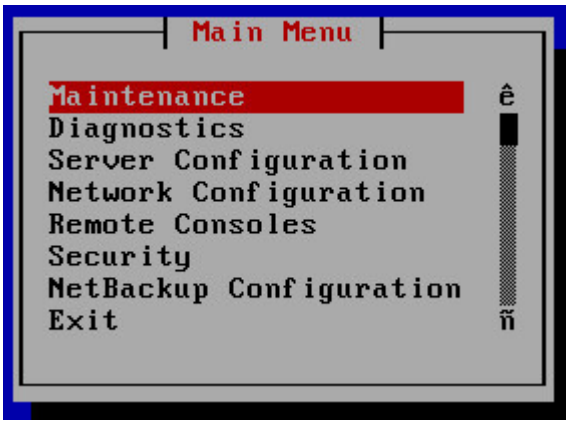
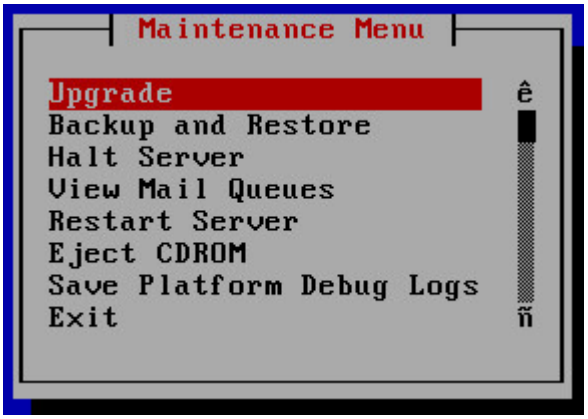
Appendix L. SERVER UPGRADE USING PLATCFG

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

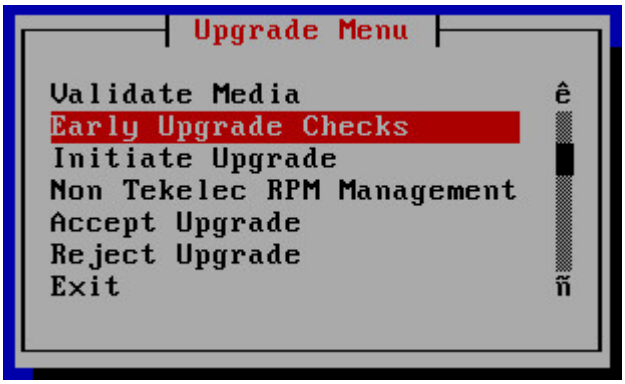
Procedure 54: Server Upgrade using platcfg

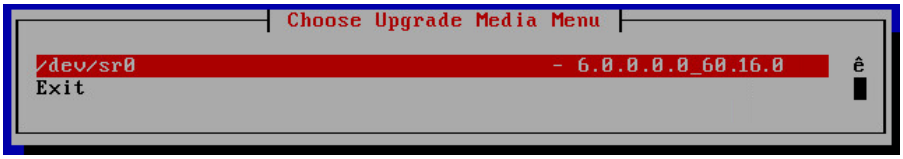
S T E P #		
	This procedure upgrades a server using the platcfg utility. NOTE: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	

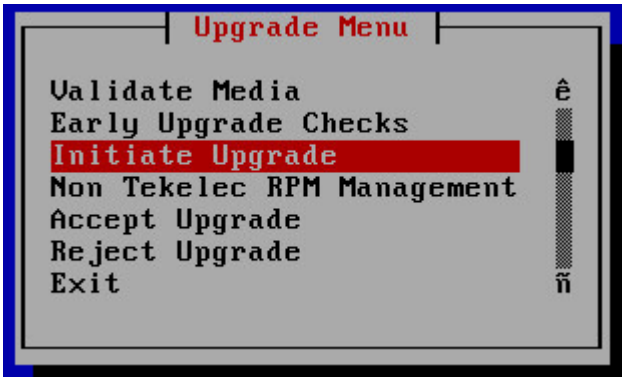
1 ☐	Login to the server to be upgraded	Log into the server console as root.
		
		`NOatlga login: root`
		`Password: <enter password>`

2 ☐	Enter the platcfg menu	Switch to the platcfg user to start the configuration menu. `[root@NOatlga ~]# su - platcfg` From the Main Menu, select **Maintenance** 
3 ☐	Select Upgrade	From the Maintenance Menu, select **Upgrade** 

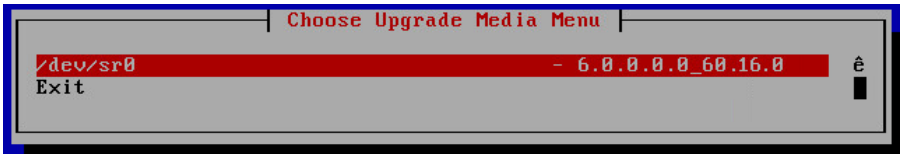
Procedure 54: Server Upgrade using platcfg

4 ☐	Select Early Upgrade Checks	From the Upgrade Menu, select **Early Upgrade Checks** 

5 ☐	Select the Upgrade Media	From the Choose Upgrade Media Menu, select the desired target media. This will initiate the early upgrade checks in the console window.
		 
		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!`
		1. Verify early upgrade checks pass. In case of errors, it is recommended to contact MOS for guidance.
		2. Press 'q' to exit the screen session and return to the platcfg menu.
		3. From the Choose Upgrade Media Menu, select **Exit.**

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

Procedure 54: Server Upgrade using platcfg

7 ☐	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.
		
		1. From the Choose Upgrade Media Menu, select the desired target media. This will initiate the server upgrade.
		
		 
		
		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 ☐	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:
		
		If the source release is 5.x:
		`ssh root@<server_IP>`
		
		If the source release is 6.0/7.0:
		`ssh admusr@<server_IP>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)

9 ☐	Check for upgrade errors	Examine the upgrade logs in the directory /var/TKLC/log/upgrade and verify 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`
		
		It is recommended to contact MOS by referring to Appendix M of this document and provide these files.

10 ☐	IF 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`
		
		It is recommended to contact MOS by referring to Appendix M of this document and provide these files.

Procedure 54: Server Upgrade using platcfg

11 ☐	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 for guidance.
		
		`[admusr@NO2 ~]$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		`1407786220::  UPGRADE IS COMPLETE`

		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix M. 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 Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **Applications** tile.
The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.