Oracle® Communications Diameter Signaling Router

DSR Software Upgrade Procedure

Release 5.1

E54548-01

June 2014

ORACLE®

Oracle® Communications Diameter Signaling Router DSR Software Upgrade Procedure, Release 5.1

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access Oracle CGBU Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.
Refer to Appendix O for instructions on accessing this site.

Contact Oracle CGBU Customer Care Center and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

Phone: 1-888-367-8552 or 919-460-2150 (international)
FAX: 919-460-2126

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 4.x to 5.1, or an incremental upgrade from an earlier DSR 5.x release to a later 5.1 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 5.1 Software Release includes all Oracle CGBU Platform Distribution (TPD) software. Any upgrade of TPD required to bring the DSR to release 5.1 occurs automatically as part of the DSR 5.1 software upgrade. The execution of this procedure assumes that the DSR 5.1 software load (ISO file, CD-ROM or other form of media) has already been delivered to the customer's premises. This includes delivery of the software load to the local workstation being used to perform this upgrade.

1.1.1 What is Not Covered by this Document

- Distribution of DSR 5.1 software loads. Please contact the Oracle CGBU Customer Care Center for the software loads as described in Appendix O.
- Initial installation of DSR software. Refer to [7].
- DIH upgrade. Refer to [9].
- Firmware upgrade. Refer to [1].
- PM&C upgrade. Refer to [4].
- SDS upgrade. Refer to [10].

1.2 References

[1] *HP Solutions Firmware Upgrade Pack Release Notes, 795-0000-0xx,*v2.1.1 (or latest 2.1 version)
[2] *TVOE 2.5 upgrade Document. 909-2276-001. V 1.0 or greater.*
[3] *PM&C 4.x to 5.5 Migration procedure, 909-2280-001, Oracle*
[4] *PM&C 5.5 Incremental upgrade, 909-2281-001, Oracle.*
[5] *DSR 4.x installation document.909-2228-001. Oracle*
[6] *DSR 5.0 installation document. 909-2278-001, Oracle.*
[7] *DSR 5.0 Base Hardware and Software installation document 909-2282-001, Oracle.*
[8] *2-tier to 3-tier migration WI006897, Oracle*
[9] *IDIH upgrade document. 909-2265-001, Oracle.*
[10] *SDS Upgrade document. UG006386.docx, Oracle.*
[11] *Maintenance Window Analysis Tool SS006061.xlsx, 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

Table 1. Acronyms

DB	Database
DP	Data Processor
DIH	Diameter Intelligent Hub, one kind of XIH
DR	Disaster Recovery
DSR	Diameter Signaling Router
DSR DR NO	Disaster Recovery DSR NO
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NO	Network OAM
NOAM	Network OAM
OA	HP Onboard Administrator
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PM&C	Platform Management and Configuration
P-DRA	Policy Diameter Routing Agent
pSBR	Policy Session Binding Repository
RMS	Rack Mount Server
SBR	Session Binding Repository
SDS	Subscriber Database Server
SO	System OAM
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualized Operating Environment
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XIH	Intelligent Hub for Tekelec XG elements
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 4.x to DSR 5.1.
Incremental Upgrade	An upgrade within a given DSR release e.g. 5.1.x to 5.1.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 4.x/5.x 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 5.1 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.
Downgrade/Backout	The process of converting a DSR 5.1 server from its current release to a prior release. This could be performed due to a misbehaving system. Once the upgrade is accepted, servers cannot be backed out to previous release.
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.
NO	Network OAM for DSR.
SO	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 DIH
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.

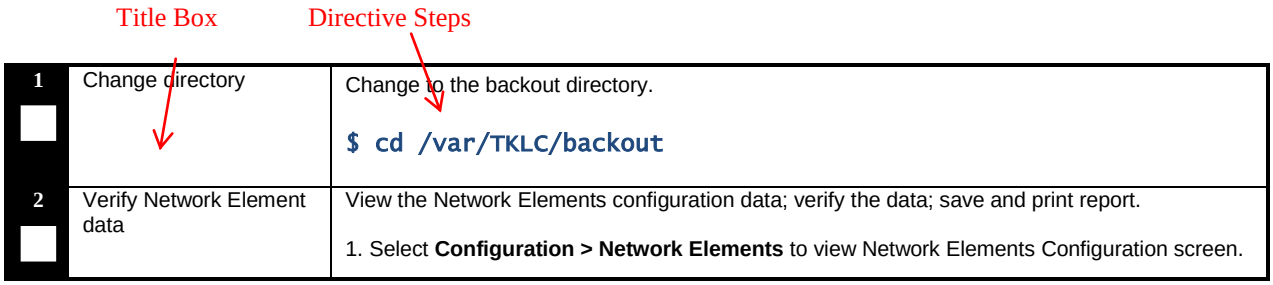
3) If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP and contact the Oracle CGBU Customer Care Center (*US: 1-888-367-8552, Intl: +1-919-460-2150)* for assistance before attempting to continue.

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 exists) 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 4.x to target release 5.1. An incremental upgrade advances the DSR from an earlier DSR 5.1 source release to a more recent 5.1 target release.

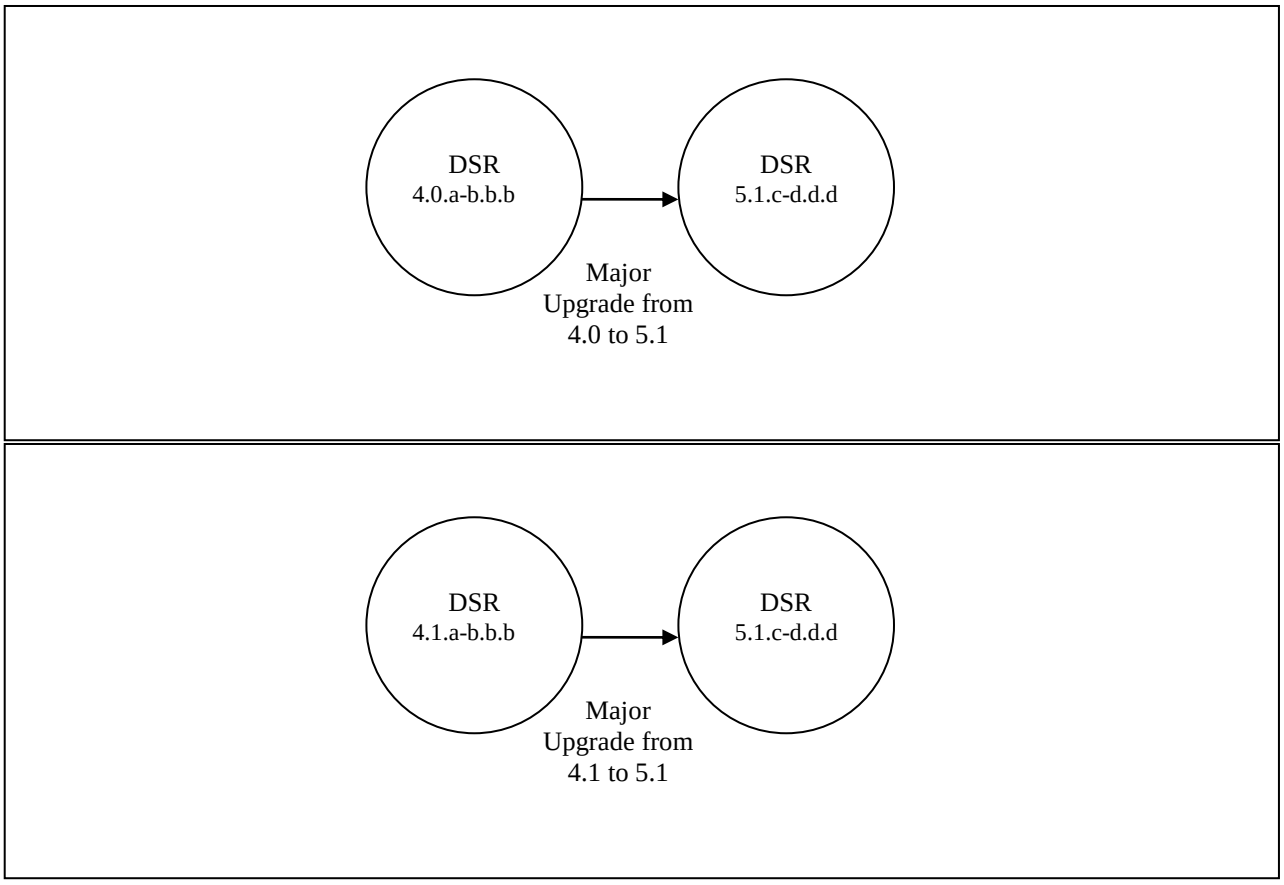
Note that for any incremental upgrade, the source and target releases must have the same value of "x". For example, advancing a DSR from 5.x.0-50.1.0 to 5.x.0-50.2.0 or to 5.x.1-50.2.0 is an incremental upgrade. But advancing a DSR running a 4.1 release to a 5.1 target release constitutes a major upgrade.

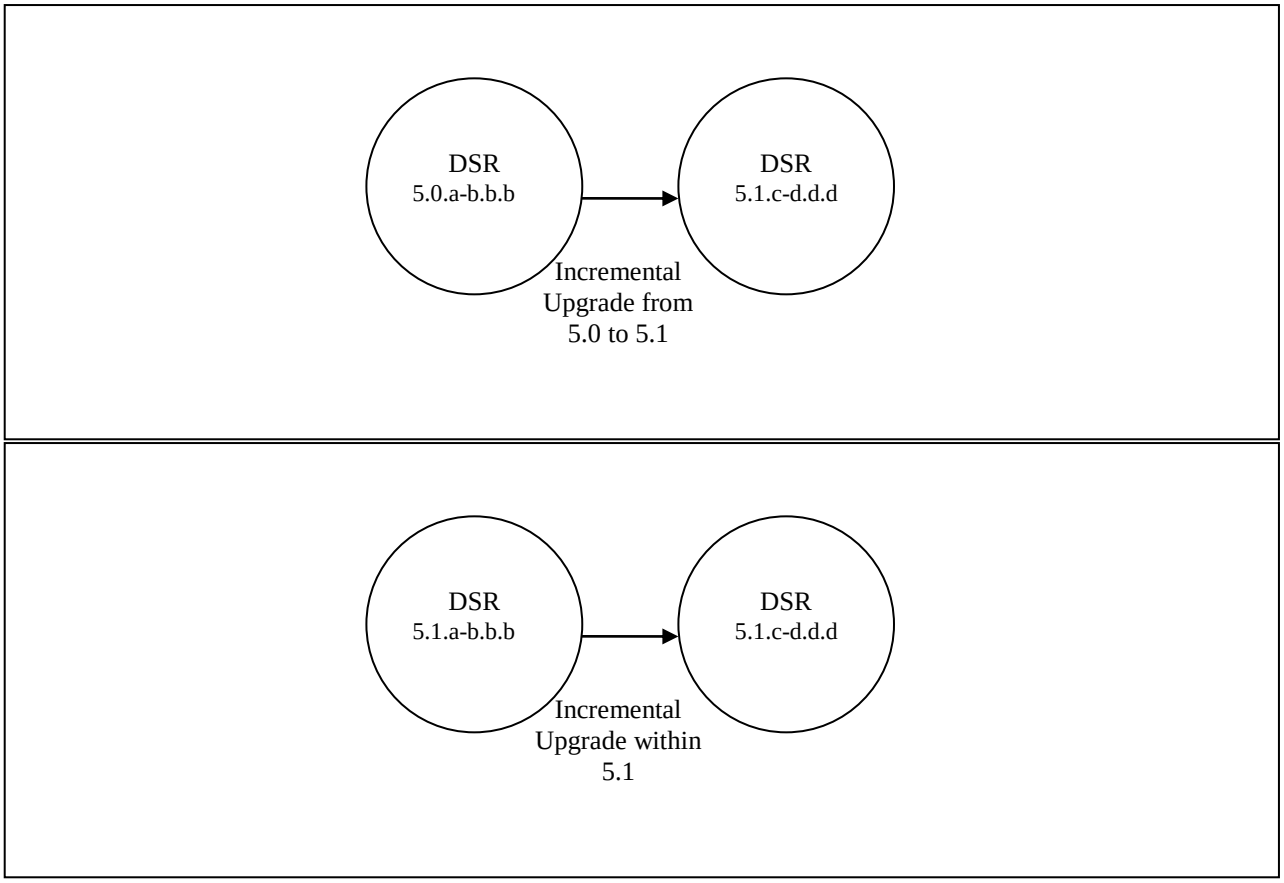
2.1 Supported Upgrade Paths

The supported paths to upgrade to a DSR 5.1 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 2-Tier vs. 3-Tier Upgrades

This document supports both 2-Tier and 3-Tier OAM upgrades. There are some procedure steps that are different depending on which is being upgraded. These are noted in the document.

In DSR 4.0, the 3-Tier (network and signaling network element) was introduced for new installs of the DSR system. [2-Tier OAM supports site-only management] As a result, there are both 2-Tier and 3-Tier DSR 4.0 network deployments. Both may be upgraded to DSR 5.1, while retaining the existing 2-Tier or 3-Tier configuration. For a 2-Tier Upgrade, the procedure will upgrade a site-at-a-time to DSR 5.1.

Note: Migration from 2-Tier to 3-Tier architecture is performed after the upgrade to DSR 5.1 is completed. See Reference [8].

One point that may be confusing is that the meaning of NO (NOAM) is different for 2-Tier and 3-Tier deployments.

- 2-Tier NO (NOAM) – refers to the Site level OAM function. After migration to 3-Tier, this function will be referred to as the SO (SOAM).
- 3-Tier NO (NOAM) – refers to the Network level OAM function (this is site-independent, and collects information from multiple sites (SOAMs) to a single user interface.
- 3-Tier SOAM – refers to the Site level OAM function in a 3-Tier deployment. This replaces the 2-Tier NO.

Assumptions:

- IPFE is only used when active-active load shared redundancy is used for the DA MPs within a given DSR signaling NE.
- It is assumed that all sites of a 3-tier deployment will have the same redundancy (either N+0 or 1+1), but not a mix of the two in the same 3-tier network.

This document refers to 2-Tier NO or 3-Tier NO, where it is necessary to clarify which NO is being referred to.

2.3 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.

2.4 Geo-diverse 3-Tier SOAM (Active/Standby/Spare PDRA configuration)

With Geo-Diverse SOAM, the upgrade of the site with the SOAM Active/Standby servers must also include an upgrade of the Spare SOAM at the geo-site, in the same maintenance window. The PDRA upgrade procedure in this document is specific to a configuration that includes Geo-Diverse SO (Section 4.7).

2.5 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 5.1 release. See Release Notes for any dependencies.

2.6 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.

2.7 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
- DIH

(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 SDS NOAM or 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 3.3.11.

2.8 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.

2.9 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.

2.10 Password Expiration during Upgrade

For DSR systems consisting of multiple sites, it is possible that password aging could disable SOAM logins on non-upgraded sites. Under normal conditions, a changed password is replicated down to all sites to enable logins at the SOAM. However, because of database version differences between the upgraded NOAM and all non-upgraded SOAMs, the new password is not replicated to non-upgraded sites.

To overcome this limitation, a workaround is provided in Appendix M. This workaround should be used only if a password expires before all sites have been upgraded. The workaround should be removed once the site is upgraded.

2.11 Optional NetBackup

There is a change in NetBackup functionality in DSR 5.1 release. Previously, the backup file location path in the Netbackup server for DSR 4.0 was configured as `/var/TKLC/db/filemgmt/`. For DSR 5.1, the path shall be `/var/TKLC/db/filemgmt/backup/`.

There are a couple of steps in the procedures to manage NetBackup during upgrade. NetBackup should be fully functional after the upgrade, without re-install.

2.12 RMS Deployments

DSR 4.1 added support for Rack Mount Server (RMS) deployments of DSR. All Deployments with RMS are 3-Tier. In these smaller deployments, the Message Processing (DA-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:

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

3.1 Required Materials

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 4.x/5.x Network OAM servers with Administrator privileges**.**

  Note: All logins into the DSR 4.x/5.x NO servers are made via the External Management VIP unless otherwise stated.
- User logins, passwords, IP addresses and other administration information. See Section 3.1.2.
- 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 iLO/XMI IP addresses (whichever is applicable) from the workstations directly connected to the DSR servers is required.
- The APN Conflict Resolution Tool. Required in Procedure 6. Download instructions are provided in Appendix N.

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 5.1 ISO image file name will be in the following format:

872-2526-101-5.1.z-5x.w.q-DSRx86_64.iso

Note: Prior to the execution of this upgrade procedure it is assumed that the DSR 5.1 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 supplied 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	
	Root Password[2]	
	Blades iLO Admin Username	
	Blades iLO 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)	
NO	XMI VIP address[3]	
	NO 1 XMI IP Address	
	NO 2 XMI IP Address	
SO	XMI VIP address	
	SO 1 XMI IP Address (Site 1)	
	SO 2 XMI IP Address (Site 1)	
	Policy DRA (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)	
	Policy DRA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	
Binding pSBR Server Groups	Binding pSBR SR1 Server Group Servers (Site 1)	
	Binding pSBR SR2 Server Group Servers (Site 1)	
	Binding pSBR SR3 Server Group Servers (Site 1)	
	Binding pSBR SR4 Server Group Servers (Site 1)	
Session pSBR Server Groups	Session pSBR SR1 Server Group Servers (Site 1)	
	Session pSBR SR2 Server Group Servers (Site 1)	
	Session pSBR SR3 Server Group Servers (Site 1)	
	Session pSBR SR4 Server Group Servers (Site 1)	
P-DRA MP Server Group	Policy DRA MP Server Group Servers (Site 1)	
	Policy DRA MP Server Group Servers (Site 1)	
IPFE Server Groups(For PDRA)	P-DRA IPFE A1 Server Group Server(Site 1)	
	P-DRA IPFE A 2 Server Group Server(Site 1)	
	P-DRA IPFE B 1 Server Group Server(Site 1)	
	P-DRA IPFE B 2 Server Group Server(Site 1)	

[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 **`root`** login on the servers. This is not the same login as the GUI Administrator. The root password is required if recovery procedures are needed. If the `root` password is not the same on all other servers, then all those servers' root passwords must also be recorded; use additional space at the bottom of this table.
[3] Note: All logins into the NO servers are made via the External Management VIP unless otherwise stated.

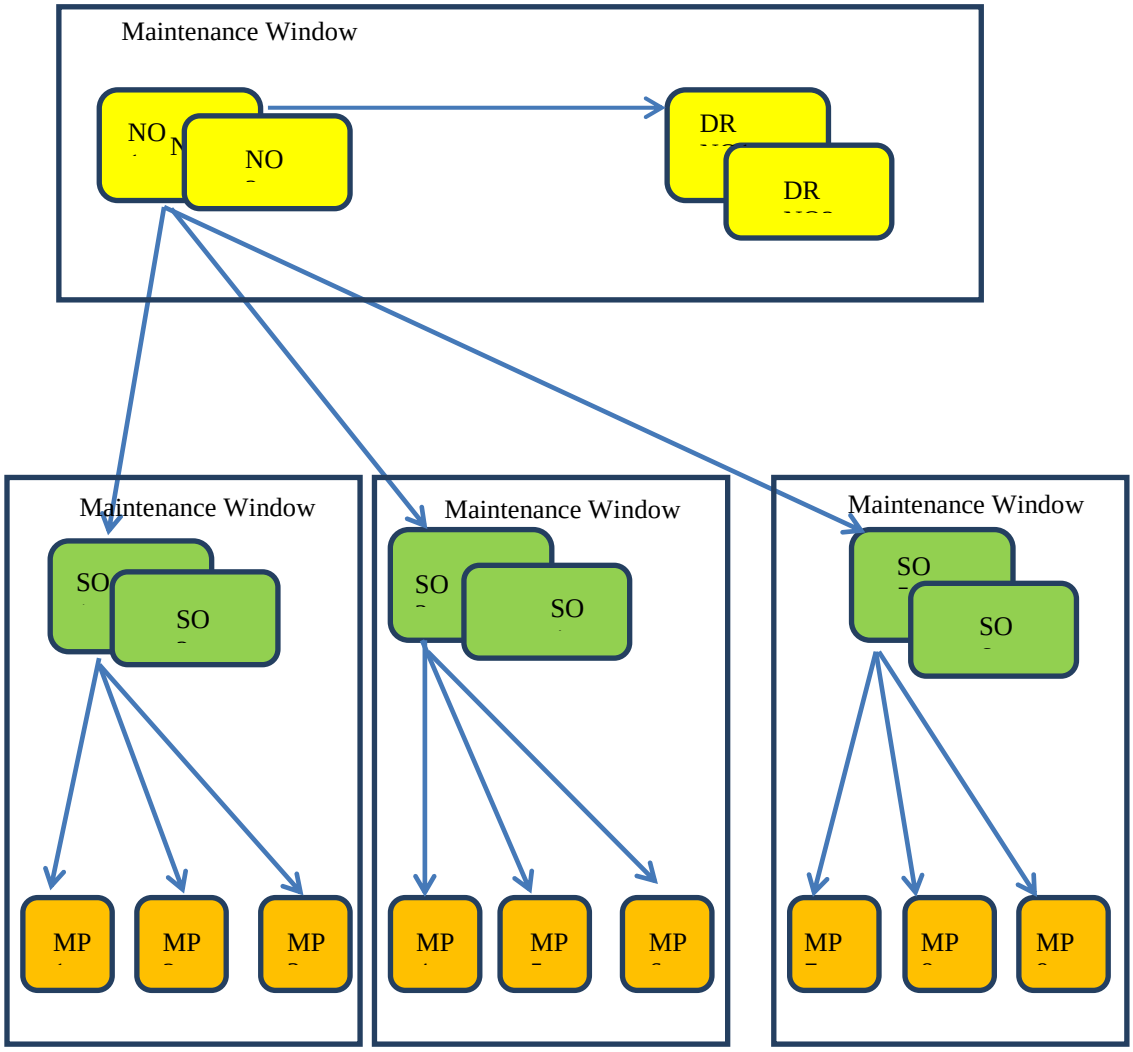
Binding PSBR Server Groups	Binding pSBR SR1 Server Group Servers (Site 2)	
	Binding pSBR SR2 Server Group Servers (Site 2)	
	Binding pSBR SR3 Server Group Servers (Site 2)	
	Binding pSBR SR4 Server Group Servers (Site 2)	
Session PSBR Server Groups	Session pSBR SR1 Server Group Servers (Site 2)	
	Session pSBR SR2 Server Group Servers (Site 2)	
	Session pSBR SR3 Server Group Servers (Site 2)	
	Session pSBR SR4 Server Group Servers (Site 2)	
P-DRA MP Server Group	Policy DRA MP Server Group Servers (Site 2)	
IPFE Server Groups(For PDRA)	P-DRA IPFE A1 Server Group Server(Site 2)	
	P-DRA IPFE A 2 Server Group Server(Site 2)	
	P-DRA IPFE B 1 Server Group Server(Site 2)	
	P-DRA IPFE B 2 Server Group Server(Site 2)	
iLO	NO 1 iLO IP Address	
	NO 2 iLO IP Address	
	SO 1 iLO IP Address	
	SO 2 iLO IP Address	
	MP 1 iLO IP Address	
	MP 2 iLO IP Address	
	……..	
	MP (n) iLO IP Address	
	IPFE MP iLO IP Address (optional)	
	IPFE MP iLO IP Address (optional)	
	……..	
	IPFE MP (n) iLO IP Address (optional)	
	cSBR MP iLO IP Address (optional)	
	cSBR MP iLO IP Address (optional)	
	……..	
	cSBR MP(n) iLO IP Address (optional)	
	DA MP iLO IP Address (optional)	
	DA MP iLO IP Address (optional)	
	……	
	DA MP(n) iLO 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 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 PMAC and TVOE upgrades as separately planned and executed activities.

- PMAC Upgrade procedure is provided in reference [4].
- TVOE Host environment upgrade procedures are included in architecture-specific sections this document.

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

It 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 [11]).

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 MW details and timings can be found in Reference [11]. Please see the instructions tab of the spreadsheet for more information and details.

3.2.3 Maintenance Window 1 (3-Tier NOAM servers)

During the first maintenance window, the 3-Tier NOAM servers are upgraded, and possibly also the PMAC, and the TVOE environments supporting these servers. (Note: PMAC and/or TVOE environments may be upgraded before this Maintenance Window, as a preferred option.)

This Maintenance Window is not required for 2-Tier deployments.

During the first maintenance window, all 3-Tier NOAM servers are upgraded. Also, PMAC and TVOE environments may be upgraded. **Maintenance Window 1** **Date: _____** **NOTE:** *The **NE Name** may be viewed from the DSR NOAM GUI under* **[Main Menu → Configuration → Network Elements].**	• Record the Site **NE Name** of the PM&C, DSR NOAM and the DR Provisioning Site to be upgraded during Maintenance Window 1 in the space provided below: • **"Check off"** the associated **Check Box** as upgrade is completed for each server. ☐ PM&C : _____ ☐ TVOE for Standby DR NOAM: _____ ☐ TVOE for Active DR NOAM: _____ ☐ TVOE for Standby NOAM: _____ ☐ TVOE for Active NOAM: _____ ☐ DR Standby NOAM: _____

	☐ DR Active NOAM: _____ ☐ DSR Standby NOAM: _____ ☐ DSR Active NOAM: _____ ☐ TVOE for Standby SOAMs: _____ ☐ TVOE for Active SOAMs: _____

3.2.4 Maintenance Window 2 (First Site upgrade)

During this maintenance window, all servers associated with the first site are upgraded. If upgrading a two-tier DSR, the SOAM Site 1 entry in the checklist is instead a 2-Tier NOAM.

Maintenance Window 2 **Date: _____**	• Record the Site **NE Name** of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided below: • **"Check off"** the associated **Check Box** as upgrade is completed for each server. ☐ SOAM/2-Tier NOAM Site1: _____ ☐ IPFE1: _____ ☐ IPFE2 : _____ ☐ IPFE3: _____ ☐ IPFE4 : _____ ☐ cSBR: _____ ☐ cSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____

	.... ☐ SpareSBR: _____ ☐ 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: _____ Note: For 1+1 configuration, only 2 DA-MP(s) will be present, one is Active while another is standby.

3.2.5 Maintenance Window 3 (Additional site upgrade)

For three-tier DSRs configured with mated-pair Sites, or three-tier DSRs having multiple, distinct Sites (e.g. geo-redundant PDRA installations), all servers associated with the second site are upgraded during a third maintenance window. If there are more than two sites in the installation, then the following form should be used for the second and subsequent sites, each site being upgraded in its own maintenance window.

The following form also applies to 2-Tier upgrades, where the SOAM is replaced with a 2-Tier NOAM.

Maintenance Window 3 **Date: _____** NOTE: *The NE Name may be viewed from the Primary Provisioning Site GUI under* [Main Menu → Configuration → Network Elements	• Record the Site **NE Name** of the DSR SOAM Site 2 and the MP(s) to be upgraded during Maintenance Window 3 in the space provided below: • **"Check off"** the associated **Check Box** as upgrade is completed for each server. ☐ SOAM/2-Tier NOAM Site2: _____ ☐ IPFE1: _____ ☐ IPFE2 : _____ ☐ cSBR: _____ ☐ cSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____ ☐ 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: _____

3.3 Pre-Upgrade 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. Pre-Upgrade Overview

Procedure Number	Elapsed Time (Hours: Minutes)		Procedure Title	Impact
	This Step	Cum.		
Procedure 1	0:10-0:30	0:10-0:30	Required Materials Check	None
Procedure 2	0:10-0:60	0:20-1:30	Collect/Backup all Global and Site Provisioning Data	None
Procedure 3	0:10-2:00	0:30-3:30	Full Backup of DB Run Environment at Each Server	None
Procedure 4	0:10-1:15 (Depends upon number of servers)	0:40-4:45	Perform Health Check (Upgrade Preparation)	None
Procedure 5	0:20-0:30 (Depends upon number of servers and sites)	1:00-5:15	Perform Health Check (For Configuration Data)	None
Procedure 6	0:45-1:00	1:45-6:15	Policy DRA APN Table Validation (applies to Policy DRA system only)	None
Procedure 7	0:15-0:20	2:00-6:35	Create New Logical Volume for NetBackup Client (if needed)	None
Procedure 8	0:02-0:10*	2:02-6:45	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 5.1

3.3.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the new DSR 5.1 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 3.1.2 is filled-in and accurate.
3 ☐	Contact Oracle CGBU Customer Care Center	Contact the Oracle CGBU Customer Care Center and inform them of plans to upgrade this system. See Appendix O for these instructions. Note that obtaining a new online support account can take up to 48 hours.

3.3.4 Collect/Backup all Global and Site Provisioning Data

This procedure is part of Software Upgrade Preparation and is used to collect data required for network analysis and Disaster Recovery.

- If the network is 3-Tier, then data is collected from both the Active NO and from the Active SO's at each site.
- If the network is 2-Tier, then the data is collected from the Active NO.

Procedure 2: Collect/Backup all Global and Site Provisioning 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Verify and collect Network Element Configuration data	View the Network Elements configuration data; verify the data; save and print report: 1. Log into the NOAM GUI using the VIP. 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 3. Click **Report** at the bottom of the table to generate a report for all entries. 4. Verify the configuration data is correct for the network. 5. Save the report and/or print the report. Keep these copies for future reference.

Procedure 2: Collect/Backup all Global and Site Provisioning Data

2 ☐	Verify and collect Server Group Configuration data	View the Server Group configuration data; verify the data; save and print report: 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 ☐	Verify and collect Server Configuration data	View the Server configuration data; verify the data; save and print report: 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 ☐	Verify and collect Services Configuration data	View the Services configuration data; verify the data; save and print report: 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 ☐	Verify and collect Signaling Network Configuration data for DSR with source release 4.x	View the Signaling Networks configuration data; verify the data; save and print report: 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** and repeat sub steps 2 through 4. 6. Select **Configuration > Network > Routes** and repeat sub steps 2 through 4.
6 ☐	Verify and collect Signaling Network Configuration data for DSR with source release 5.x	View the Signaling Networks configuration data; verify the data; save and print report: 1. Select **Configuration > Network** to view the Signaling Networks. 2. Click "**Report All**" 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.
7 ☐	Collect database reports	Gather data from the primary Active NO server: 1. Select **Status & Manage > Database** to view the Database Status screen. 2. Click to highlight the **Active NO** server to be backed up, and click **Report**. 3. Save the report and print the report. Keep these copies for future reference. 4. Click to highlight each of the **Active SO(s)** (if exists) to be backed up, and click **Report**. Name the backup file to identify the SO. 5. **Save** the report and print the report. Keep these copies for future reference.
8 ☐	Backup all global provisioning databases for NOAM **IMPORTANT: Required for Disaster Recovery**	Backup the global database from the primary Active NO: 1. Select **Status & Manage > Database** to return to the Database Status screen. **2.** Click to highlight the **Active NO** 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.** Verify **Configuration** Data is selected for backup 4. Enter **Comments** (optional) 5. Click **OK**. Note: the Active NO 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.

Procedure 2: Collect/Backup all Global and Site Provisioning Data

9 ☐	Save database backups for NOAM **IMPORTANT: Required for Disaster Recovery**	Save database backups to the local workstation: 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active NO server tab**.** 3. Select the database backup file and click the **Download** button. 4. A confirmation window is displayed. Click **Save**. 5. The **Choose File** window is displayed. Select a destination folder on the local workstation to store the backup file. Click **Save**. 6. The **Download Complete** confirmation is displayed. Click **Close**.
10 ☐	Backup all global and site provisioning databases for SO's **IMPORTANT: Required for Disaster Recovery**	Backup the global database from all Active SO servers (3-Tier only): 1. Log into the Active SOAM GUI using the VIP. 2. Select **Status & Manage > Database** to return to the Database Status screen. **3.** Click to highlight the **Active SO** server; click **Backup**; the Backup and Archive screen is displayed. **(Note: the Backup button will only be enabled when the Active server is selected.)** **4.** Verify the **Configuration** checkbox is selected 5. Enter **Comments** (optional) 6. Click **OK**. **Repeat sub steps 1 through 6 for each Active SOAM (if exists).** Note: the Active SO 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.
11 ☐	Save database backups for SO's) **IMPORTANT: Required for Disaster Recovery**	Save database backups to the local workstation: From the Active SOAM GUI: 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active SO server tab**.** 3. Select the database backup file and click the **Download** button. 4. A confirmation window is displayed. Click **Save**. 5. The **Choose File** window is displayed. Select a destination folder on the local workstation to store the backup file. Click **Save**. 6. The **Download Complete** confirmation is displayed. Click **Close**. Repeat sub-steps 1 to 6 for each Active SOAM.
12 ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE//P-SBR/PDRA which will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Steps 1-7. 2. Plan for any MP upgrades by consulting the Oracle CGBU Customer Care Center 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.

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 NO 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Log into the Active NO	Use the ssh command (on UNIX systems – or putty if running on Windows) to log into the Active NO: **`ssh root@<NO_VIP>`** (Answer 'yes' if you are prompted to confirm the identity of the server.)

2 ☐	**SSH to Active NO:**
	Execute Full Backup for all servers (managed from this NO)
		Execute the **backupAllHosts** utility on the Active NO. [This utility will remotely access every server in the scope of the NO, and run the backup command for the server.]
		SSH to the Active NO server:
		`# 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.)
		`# /usr/TKLC/dpi/bin/backupAllHosts`
		The following output will be generated for DSR 5.1 servers only:
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		It may take from 10 minutes to 2 hours for this command to complete, depending upon 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`
		`---------- ----------`

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

S T E P #	This procedure (executed from the Active NO 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
		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. **# exit** (to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively) **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 system 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 Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.
3 ☐	**Active NO GUI:** Verify that backups are created for all servers	**For the Active NO:** 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. Verify that the following two files have been created: Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2 Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2

3.3.6 Perform Health Check (Upgrade Preparation)

This procedure is part of software upgrade preparation and is used to determine the health and status of the DSR 4.x/5.x network and servers. This may be executed multiple times, but must also be executed at least once within the time frame of 24-36 hours prior to the start of a maintenance window.

Procedure 4: Perform Health Check (Upgrade Preparation)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Verify Software Versions on DSR Servers	From the Active NO GUI: Select the **Upgrade Administration** form: (DSR 4.x: "**Administration > Upgrade**" DSR 5.1: " **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 DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x**

Hostname	Network Element Application Version	Role Function	Upgrade State Server Status
NO1	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Err
NO2	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Norm
MP1	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

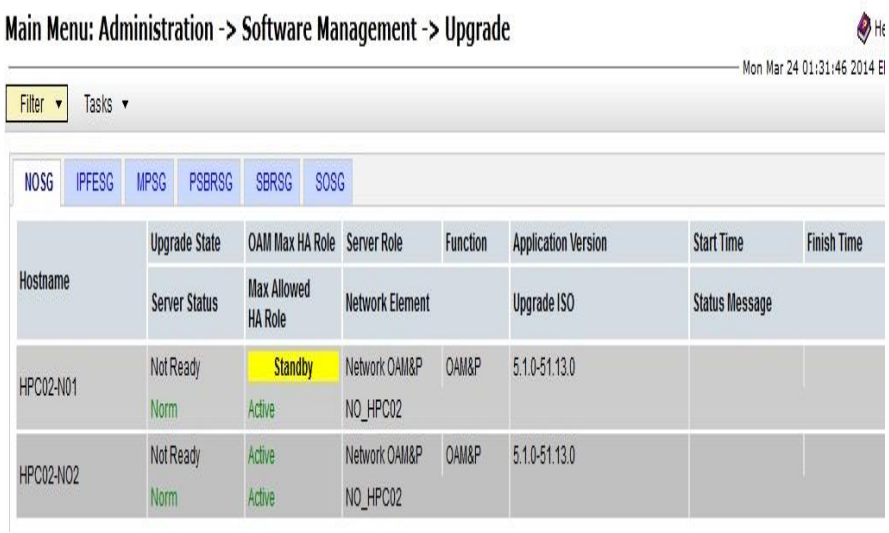
Procedure 4: Perform Health Check (Upgrade Preparation)

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

Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Select each server group and verify the **Application Version** for each server.

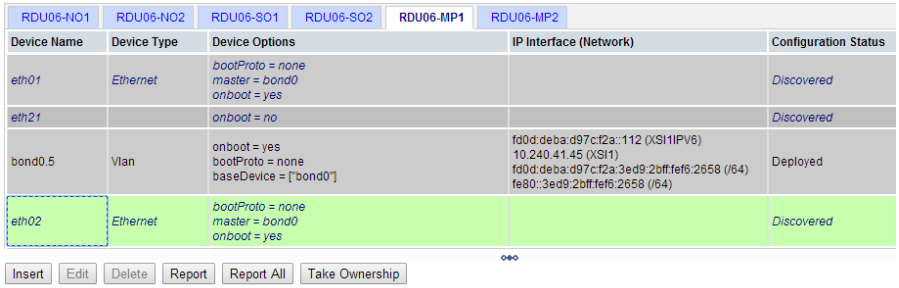


Verify the **Application Version** value for the DSR servers, and record this information.

Procedure 4: Perform Health Check (Upgrade Preparation)

<table>
<tr><td>2 ☐</td><td>Verify Network Device status</td><td>From the Active NOAM GUI:

1. Navigate to Configuration >Network >Devices to display the Network Devices form

2. Select an MP Server Group tab. A list of network devices installed on the MP is displayed.
3. For each device that will be used as an unbonded signaling interface, and has a Configuration Status of Discovered, select the device and click the Take Ownership button.
4. Verify the device status changes to Configured, then Deployed. (Note: it may take a few minutes for the device to transition to the Deployed state.)

Repeat steps 2 through 4 for each MP Server Group.</td></tr>
<tr><td>3 ☐</td><td>Check if a new Firmware Release may be required for the system</td><td>Contact the Oracle CGBU Customer Care Center by referring to Appendix O 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 2.2.4

If an upgrade is required, acquire the Firmware release package and follow procedures provided with the package to determine which specific system components (Switches, Servers, etc) may require an upgrade.

Plan for Firmware Upgrade Maintenance windows, if needed, since this activity is typically performed before the DSR Upgrade.</td></tr>
<tr><td>4 ☐</td><td>Check the existing PM&C version and identify if PM&C upgrade is required, before starting with DSR upgrade(applies to servers that are already running PM&C)</td><td>1. Record the target DSR Release for the servers that need to be upgraded. (5.1.y-5x.nn.a).

2. Determine the PM&C version installed by logging into PM&C GUI.

3. For upgrade to DSR 5.1, the minimum PM&C required is 5.5.

4. If the PM&C version is below 5.5, identify the proper PM&C upgrade document (to be used later) based on the following DSR upgrade path :

a) For a major DSR upgrade (i.e. from DSR 4.x->5.1), follow reference [3].

b) For incremental upgrades (i.e. from DSR 5.0->DSR 5.1), follow reference [4].</td></tr>
</table>

Procedure 4: Perform Health Check (Upgrade Preparation)

5 ☐	Check the TVOE Host server software version	1. Find the target DSR release from Table 3. 2. Contact the Oracle CGBU Customer Care Center by referring to Appendix O 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. Follow Appendix E for the procedure to check the current TVOE HOST OS version, for all TVOE Hosts. IMPORTANT: If TVOE Hosts are not on the correct release, refer to Section 3.2.1 to plan for TVOE Host upgrades.
6 ☐	Check if netbackup client installed on NOAM/SOAM(if exists)	1. Check the Netbackup server version before starting the DSR upgrade. 2. Supported versions of Netbackup client and Netbackup server for DSR 5.1 release are 7.1 or 7.5. 3. If the Netbackup server is not on 7.1 or 7.5 then plan a Netbackup upgrade before starting the DSR upgrade.
7 ☐	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: **ssh root@<target_server_ip>** (Answer 'yes' if you are prompted to confirm the identity of the server.) 2. cd to `/etc/httpd/conf.d` and edit 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 path and name for use in Procedure 89.

3.3.7 Perform Health Check (For Configuration Data)

Execute the following procedure to take diameter configuration data backup and health check.

Procedure 5: Perform Health Check (For Configuration Data)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for all the sites**	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter-> Maintenance** 2. Select **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.
2 ☐	Capture the Policy SBR Status(if exists) **on Active NOAM GUI**	From the Active NOAM GUI: 1. Select **Main Menu-> Policy DRA->Maintenance-> Policy SBR Status** 2. Capture and archive the maintenance status of the following tabs on the client machine by either taking screen captures or documenting it in an editor. a. BindingRegion b. PDRAMatedSites 3. Save recorded data on the client machine.
3 ☐	Capture the IPFE Configuration Options Screens (if exists) on Active SOAM GUI (for 3 tier setup) and on Active NOAM GUI (for 2 tier setup) on all the Sites.	From the Active SOAM (3-tier) or Active NOAM (2-tier) 1. Select **Main Menu: IPFE->Configuration->Options** 2. Capture and archive the screen capture of the complete screen. 3. Save recorded data on the client machine.
4 ☐	Capture the IPFE Configuration Target Set screens (if exists) on Active SOAM GUI (for 3 tier setup) and on Active NOAM GUI (for 2 tier setup) on all the Sites.	From the Active SOAM (3-tier) or Active NOAM (2-tier) 1. Select **Main Menu-> IPFE->Configuration->Target Sets** 2. Capture and archive the screen capture of the complete screens. 3. Save recorded data on the client machine.

Procedure 5: Perform Health Check (For Configuration Data)

5 ☐	Export and archive the Diameter and P-DRA (if exists) configuration data on Active SOAM GUI (for 3 tier setup) and on Active NOAM GUI (for 2 tier setup) on all the Sites.	From the Active SOAM (3-tier) or Active NOAM (2-tier) 1. Select **Main Menu-> Diameter-> Configuration->Export** 2. Capture and archive the Diameter and P-DRA 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
6 ☐	Data shall be captured for each Site.	Repeat steps 1 through 5 for each Site.

3.3.8 Policy DRA APN Table Validation

For a Policy DRA upgrade from DSR 4.1.5 or 5.0, to DSR 5.1 or later, Procedure 6 must be executed before the first server is upgraded.

This procedure applies to Policy DRA systems only. Do not execute this procedure on non-Policy DRA systems.

Procedure 6: Policy DRA APN Table Validation

S T E P #	This procedure performs a validation of the APN table. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Perform the APN Table Validation procedures	If the source release is DSR 4.1.5 or 5.0, follow the instructions in Appendix N to validate the APN table before starting the upgrade to release 5.1. Note: It is critically important to execute the procedures in Appendix N prior to the actual maintenance window when upgrade will be performed. If the upgrade is started without following the procedures, and the APN database table does encounter validation problems, the upgrade will fail. The resolution of the problems will require network analysis that may include consultation with other networks/vendors and hence it is highly recommended to check and prepare the system for upgrade in advance.

3.3.9 Create New Logical Volume for NetBackup Client (if needed)

NOTE: This procedure is only required for NOAM and SOAM servers that have the NetBackup client software installed and do not have a logical volume for NetBackup already created.

This section only applies if the Symantec NetBackup utility is already installed on one or more OAM (NO or SO) servers in the DSR to be upgraded. If NetBackup is **not** installed on any of the OAM servers, skip this section entirely. To determine if NetBackup is installed on any OAM server, follow the first step of Procedure 7 below. If NetBackup is installed on one or more OAM servers, but is already located in its own logical volume on each server where NetBackup is installed, it is not necessary to create a new logical volume, and this section can be skipped.

This procedure **checks to see if NetBackup is already installed.** If it is, it creates a new logical volume for NetBackup client software, and moves the existing NetBackup client software to this new volume.

In order to successfully upgrade, the NetBackup client software must be moved to its own logical volume ***before*** attempting the upgrade. Failure to do so may cause the upgrade to fail due to a lack of space in the /usr directory.

NetBackup Installation **Date: _____**	• **Check off** the associated **Check Box** as NetBackup install is completed for each **NO** and **SO.** ☐ Active NO ☐ Standby NO ☐ Active SO ☐ Standby SO ⋮ ☐ Active SO(n) ☐ Standby SO(n) Note: Need to check for all the sites.

Procedure 7: Create New Logical Volume for NetBackup Client (if needed)

S T E P #	This procedure creates a new logical volume for NetBackup client software and moves the existing NetBackup client software to this new volume. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Check if NetBackup Client is installed	Use the ssh command (on UNIX systems – or putty if running on windows) to login into the target server: `ssh root@<target_server_ip>`

Procedure 7: Create New Logical Volume for NetBackup Client (if needed)

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

Execute the following command to check if NetBackup is installed or not :

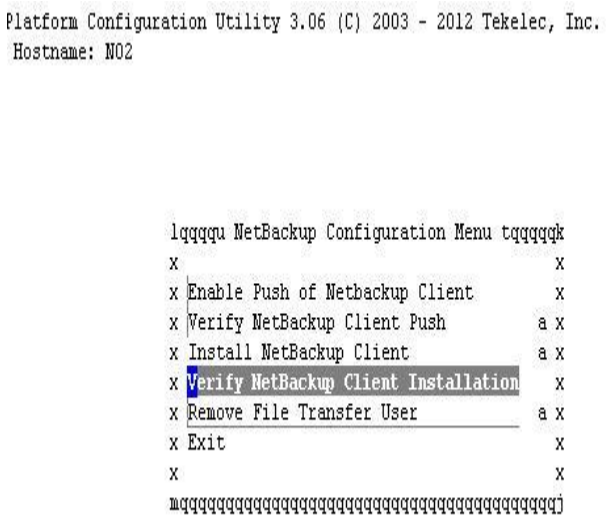
```
# cat /usr/openv/netbackup/bin/version
```

If this file exists, then a version of the NetBackup client is installed on this application. If file doesn't exist, then proceed to Step 9.

```
# su - platcfg
```

The platcfg utility menu is displayed. Then navigate to following submenus :

1. Navigate to NetBackup configuration and select the `Verify NetBackup Client Installation` option



2. If the NetBackup client is installed, the following screen will appear.-

Procedure 7: Create New Logical Volume for NetBackup Client (if needed)

		Platform Configuration Utility 3.06 (C) 2003 - 2012 Tekelec, Inc. Hostname: NO2 Verify NetBackup Client Installation [OK] - Looks like a 7.1 Client is installed [OK] - RC script: netbackup [OK] - rpm: SYMCpddea [OK] - pkgKeep: SYMCpddea [OK] - rpm: SYMCnbjre [OK] - pkgKeep: SYMCnbjre [OK] - rpm: SYMCnbjava [OK] - pkgKeep: SYMCnbjava [OK] - rpm: SYMCnbclt [OK] - pkgKeep: SYMCnbclt [OK] - rpm: VRTSpbx [OK] - pkgKeep: VRTSpbx lqqqqqqqqqk lqqqqqqqqqqk lqqqqqk lqqqqqqqqk lqqqqqqk x Forward x x Backward x x Top x x Bottom x x Exit x mqqqqqqqqqj mqqqqqqqqqqj mqqqqqj mqqqqqqqqj mqqqqqqj Note : Following error in verify NetBackup Client Installation output is acceptable : `[ERROR] - RC script: vxpbx_exchanged` 3. Select Exit to return to the previous menu. If NetBackup is installed proceed to Step 2, otherwise proceed to Step 9.

2	Check if NetBackup Logical volume already exists	Execute the following command to check if the logical volume for NetBackup client already exists :
		`# df -B M`
		The following output shows that the NetBackup Logical Volume already exists :
		`Filesystem 1M-blocks Used Available Use% Mounted on`
		`/dev/mapper/vgroot-netbackup_lv 2016M 692M 1223M 37% /usr/openv`
		If the NetBackup logical Volume exists, then proceed to Step 9; otherwise continue with the next step.

Procedure 7: Create New Logical Volume for NetBackup Client (if needed)

3 ☐	Mount the upgrade media	Insert the Diameter Signaling Router 5.1 ISO into the drive of the application server.
		Log in as root to the application server and execute the following steps:
		Determine the cdrom of the server :
		`# getCDROM`
		`/dev/sr0 (the physical Optical Drive for this server)`
		`/dev/sr1 (Virtual Optical Drive)`
		`/dev/sr2 (Virtual Optical Drive)`
		
		Mount the optical media
		`# mkdir /media/cdrom`
		`# mount /dev/sr0 /media/cdrom`
		
		Run the following command to mount the ISO:
		`# mount -o loop DSR_5.1.iso /media/cdrom`

4 ☐	Verify that the script is available on the media	To verify it is available on the upgrade media, execute the "ls" command to list the relocateNetBackup script: **`# ls <mount point>/upgrade/bin/relocateNetBackup`** Verify that the `relocateNetBackup` script is present; otherwise contact the Oracle CGBU Customer Care Center.
5 ☐	Verify that there is sufficient space available	Verify that the filemgmt filesystem has more than 2049 Megabytes of free space. Execute the `df` command and examine the response. **`# df -B M /var/TKLC/db/filemgmt/`** Verify that the available space is 2049 Megabytes or greater. If there is not sufficient space, remove unneeded files until there is sufficient space.
6 ☐	Execute the relocate script .	Execute the relocate script: **`# <mount point>/upgrade/bin/relocateNetBackup`** Verify that it executes without error. The following warnings are acceptable : **`WARNING: Start of vxpbx_exchanged service exited with value 0`** **`WARNING: Start of netbackup service exited with value 2`** These warnings are a function of the NetBackup client software and can be safely ignored.

Procedure 7: Create New Logical Volume for NetBackup Client (if needed)

7 ☐	Check if NetBackup logical volume exists.	Execute the following command to check if Logical volume for the NetBackup client exists:
		# df -B M
		The following output shows that the NetBackup Logical Volume already exists :
		`Filesystem 1M-blocks Used Available Use% Mounted on`
		`/dev/mapper/vgroot-netbackup_lv 2016M 692M 1223M 37% /usr/openv`
		If the NetBackup logical Volume exists, then proceed to the next step; otherwise contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document.

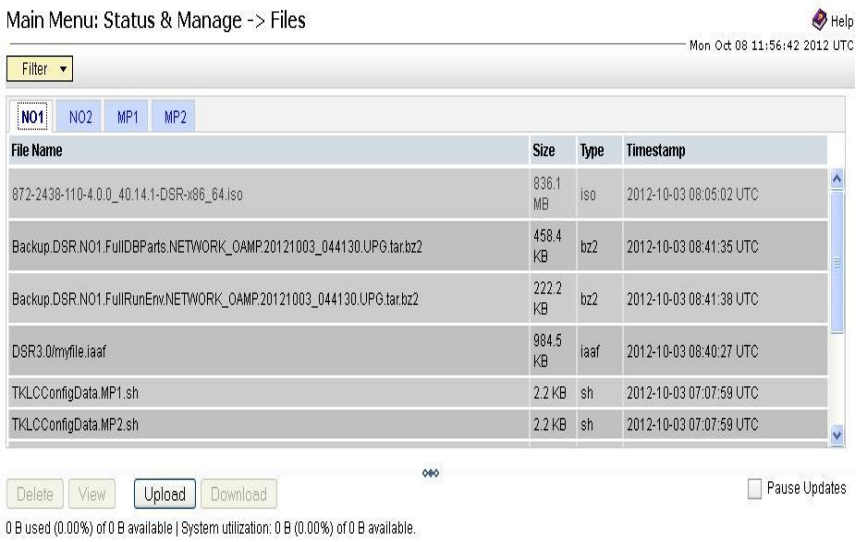
8 ☐	Unmount mount point	Execute the following command to unmount the mount point : **# umount /media/cdrom** Remove the media from the drive.
9 ☐	Check if NetBackup Logical volume already exists on other servers	Repeat this procedure on every NOAM and SOAM server.

3.3.10 ISO Administration

Detailed steps on ISO Administration are given in Procedure 8.

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.

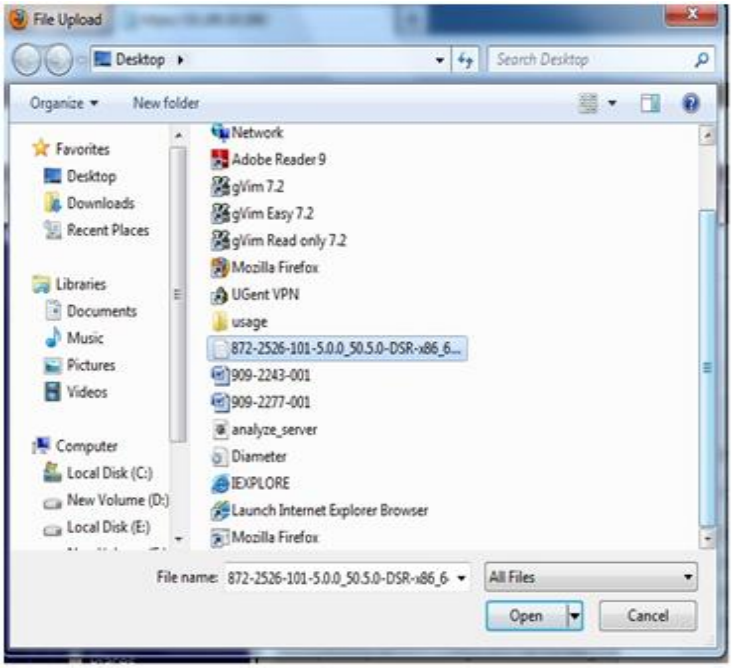
Procedure 8: ISO Administration

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Upload ISO to Active NO server via the DSR 4.x/5.x GUI session.	There are two methods to upload the application ISO to the Active NO based on the type of the media: Execute either: **Option 1** (Use NOAM GUI Upload function for ISO file transfer over the network) **OR** **Option 2** (Local site media ISO transfer, using PM&C). **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 NO server[5]: 1. Log into the Active NOAM GUI. 2. Select **Status & Manage > Files** The Files menu is displayed  3. Click the Active NO 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 NO 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. Browse window will open up :

Procedure 8: ISO Administration

7. Click **Browse** to select the file to upload.

8. The Choose File window displays, allowing selection of the file to upload.



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

Procedure 8: ISO Administration

11. Click **Upload.**
12. The ISO file begins uploading to the file management storage area.
13. 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.
14. To back up the ISO file to the PMAC, ssh from the Active NO 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**.**

Copy the ISO file to the Standby NO using the following command from the Active NO.

```
scp /var/TKLC/db/filemgmt/<DSR_ISO_Filename>
root@<Standby_NO_IP>:/var/TKLC/db/filemgmt
```

Execute Steps 3 to 7 of **Appendix F** to add the ISO image to the PM&C repository.

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 – Applicable for DSR 4.x (PM&C 5.0))

1. Execute Appendix F to load the ISO onto the PM&C server at the site.
2. SSH into the PM&C server and scp the ISO to the Active NO using the following commands:

For PM&C 5.0 :

```
scp
/var/TKLC/smac/image/repository<DSR_ISO_Filena
me> root@<Active_NO_IP>:/var/TKLC/db/filemgmt
```

For PM&C prior to version 5.0 :

```
scp /var/TKLC/smac/image/<DSR_ISO_Filename>
root@<Active_NO_IP>:/var/TKLC/db/filemgmt
```

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

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

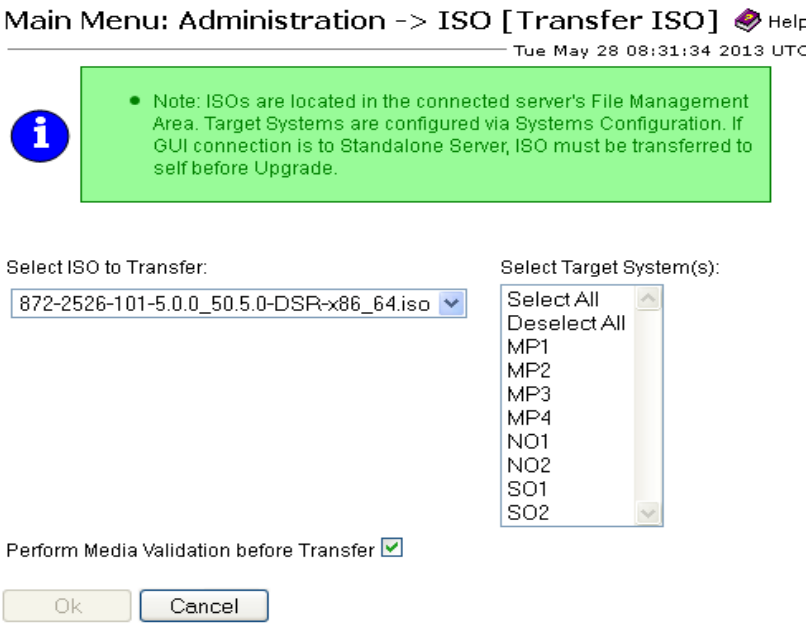
4. From the Active NOAM, copy the ISO file to the Standby NOAM using the following command:

```
scp /var/TKLC/db/filemgmt/<DSR_ISO_Filename>
root@<Standby_NO_IP>:/var/TKLC/db/filemgmt
```

Procedure 8: ISO Administration

2 ☐	Using NOAM GUI, transfer ISO to all DSR 4.x/5.x Servers to be upgraded.	Transfer the target release ISO image file from the Active NO to all other DSR 4.x/5.x servers. 1. From the Active NOAM GUI, navigate to **Administration** -> **ISO** for DSR 4.x, or navigate to **Administration->Software Management-> ISO Deployment** for DSR 5.x GUI.

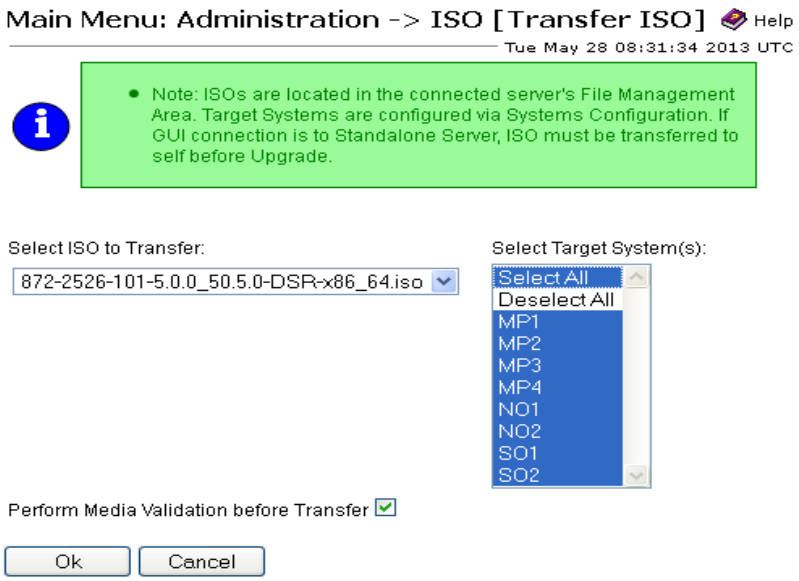
2. Click on "**Transfer ISO"**



Procedure 8: ISO Administration

3. Under the "**Select ISO to Transfer:**" drop down menu select the DSR 5.1 ISO. Under the "**Select Target System(s):**" select "**Select All**".

4. Select the checkbox next to "**Perform Media Validation before Transfer**".



5. Click **Ok**

6. 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, contact the Oracle CGBU Customer Care Center support for assistance.

3.3.11 Upgrade TVOE Hosts at a Site (prior to application upgrade MW)

This procedure applies if the TVOE Hosts at a site will be upgraded BEFORE the start of the DSR 5.1 Upgrade of the NOs and other servers. Performing the TVOE upgrade BEFORE reduces the time required for DSR Application Upgrade procedures.

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 Overview

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 9	30 min per TVOE Host (see note)	0:30- 3:00	Upgrade TVOE Hosts at a Site (prior to 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.

Note: 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 below.

Procedure 9: Upgrade TVOE Hosts at a Site (prior to 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 9: Upgrade TVOE Hosts at a Site (prior to application upgrade MW)

3 ☐	Determine if there are SDS Applications on the TVOE Hosts	Log into the TVOE Hosts and execute: `# virsh list --all` **If the application list includes SDS SOAM applications, then make this team aware of the planned 30 minute outage of the SDS SOAM applications during the TVOE Upgrade.**
4 ☐	Upgrade the TVOE hosting the DSR standby server(s)	Upgrade the TVOE Host of a standby server: **Execute Appendix J**
5 ☐	Upgrade the TVOE hosting the DSR active server(s)	Upgrade TVOE of an Active server **Execute Appendix J** **Note: This will cause a failover of the DSR or other active applications on the TVOE.**
6 ☐	Repeat for TVOE Hosts at a Site	**Repeat steps 4 and 5 for multiple TVOE Hosts at a site, as time permits.**
End of maintenance window		

4. SOFTWARE UPGRADE EXECUTION

Call the **Oracle CGBU Customer Care Center at 1-888-FOR-TKLC (1-888-367-8552); or 1-919-460-2150 (international)** *prior* to executing this upgrade to ensure that the proper media are available for use.

Before upgrade, users must perform the system health check in Section 3.3.6. 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, contact the Oracle CGBU Customer Care Center 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 Oracle CGBU Customer Care Center representative is not present during the upgrade.

4.1 Select Upgrade Path

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

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

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

Use the answers to the following questions to select the required upgrade procedure from Table 6 and Table 7. Table 6 applies to 3-Tier deployments, and Table 7 applies to 2-Tier deployments. The right-most column indicates the sections of this document that apply.

Is this a 2-Tier or 3-Tier NOAM deployment? _____

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

Is this setup deployed on RMS server(s)? _____

Are there PDRA 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 the Tables below: _____

Table 6. 3-Tier Upgrade Path Reference

Type	Supported Configurations	Upgrade Path	Section Reference
1	DSR 5.1 upgrade for 3-tier (1+1) setup (major or incremental)	DSR Upgrade (3-Tier, 1+1) (possibly including TVOE)	Section 4.3
2	DSR 5.1 upgrade for 3 tier (N+0) setup (major or incremental)	DSR Upgrade (3-Tier, N+0) (possibly including TVOE)	Section 4.4
3	DSR 5.1 upgrade for 3 tier (N+0) RMS server setup (major or incremental)	DSR Upgrade (3-Tier, N+0, RMS) (including TVOE)	Section 4.5

4	DSR 5.1 upgrade for 3-tier (1+1) RMS server setup (major or incremental)	DSR Upgrade (3-Tier, 1+1, RMS) (including TVOE)	Section 4.6
5	Policy DRA DSR 5.1 upgrade (major or incremental)	Policy DRA Upgrade (3-Tier)	Section 4.7

Table 7. 2-Tier Upgrade Path Reference

Type	Supported Configurations	Upgrade Path	Section Reference
6	DSR 5.1 upgrade for 2-tier (1+1) setup (major or Incremental)	DSR Site Upgrade (2-Tier, 1+1)	Section 4.8 (Each Site)
7	DSR 5.1 Upgrade for 2-tier (N+0) setup (major or incremental)	DSR Site Upgrade (2-Tier, N+0)	Section 4.9 (Each Site)

4.2 Accepting the Upgrade

After the upgrade of all servers is complete, and following an appropriate soak time, the Post-Upgrade procedures in section 4.10 are performed in a separate Maintenance Window to finalize the upgrade. Procedure 89 performs a final Health Check of the system to monitor alarms and server status. Procedure 90 accepts the upgrade. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4.3 DSR Upgrade (3-Tier, 1+1) (possibly including TVOE)

This section contains upgrade steps for DSR 5.1 (3-tier setup) with (1+1) configuration (major or incremental).

4.3.1 NO Upgrade Execution (3-Tier, 1+1)

Procedures for the 3-tier NO 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 NO servers (which will also disable provisioning at the SO servers). Provisioning activities at the NO and SO servers will have certain limitations during the period where the NOs 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.

These times are estimates.

Table 8. NO Upgrade Execution Overview (3-Tier, 1+1).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 11	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAMs)	None
Procedure 12	0:05-0:10	0:06-0:15	0:06-0:15	0.06-0.20	Disable Provisioning (3-tier, 1+1)	Global and Site Provisioning Disabled, No Traffic Impact
Procedure 13	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:20	Upgrade TVOE and NOs (3-Tier, 1+1)	No Traffic Impact
Procedure 14	0:01-0:05	0:32-1:20	0:01-0:05	1:32-2:25	Verify Post Upgrade Status (3-Tier, 1+1, NOAM)	Global Provisioning Enabled

4.3.2 Pre-Upgrade Checks (3-Tier, 1+1, NOAM)

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

Procedure 10: Pre-Upgrade Checks (3-Tier, 1+1, NOAM)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.1), then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (This can be done from PMAC Software Inventory form.) Complete this information: NO-A TVOE Host Rev _____ NO-B TVOE Host Rev _____ DR-NO-A TVOE Host Rev _____ DR-NO-B TVOE Host Rev _____ Will TVOE Upgrades be performed during the DSR Application Upgrades? _____
2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade). **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x**

Procedure 10: Pre-Upgrade Checks (3-Tier, 1+1, NOAM)

Main Menu: Administration -> Upgrade

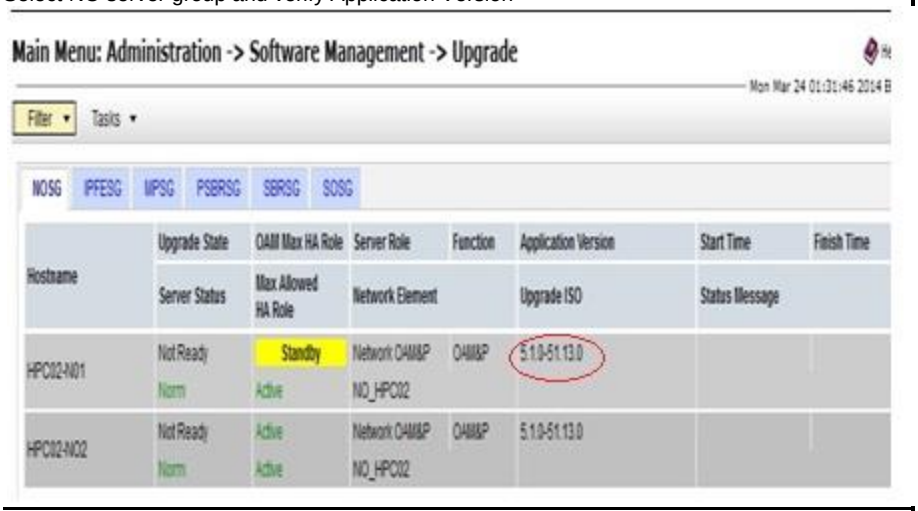
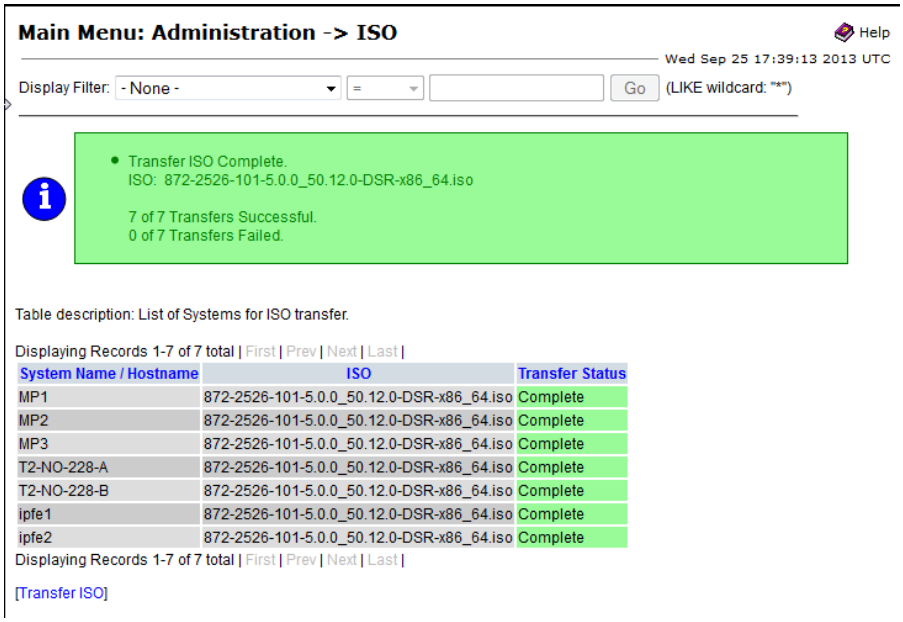
Hostname	Network Element Application Version	Role Function
T2-NO-228-A	T2_NO_228 4.0.2-40.27.3	NETWORK OAM&P OAM&P
T2-NO-228-B	T2_NO_228 Unknown	NETWORK OAM&P OAM&P
MP2	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
MP3	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
ipfe1	T2_NO_228 4.0.2-40.27.3	MP IP Front End
ipfe2	T2_NO_228 4.0.2-40.27.3	MP IP Front End
MP1	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)

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 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 10: Pre-Upgrade Checks (3-Tier, 1+1, NOAM)

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up Select NO server group and verify Application Version 
3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify the DSR ISO file has been transferred to all servers: Example:  If not, see Section 3.3.10, ISO Administration.

Procedure 10: Pre-Upgrade Checks (3-Tier, 1+1, NOAM)

4 ■	**Verify that a recent version of the Full DB backup has been performed**	Verify that a recent version of the Full DB backup has been performed.
		
		1. Log into the Active NOAM GUI using the VIP.
		2. Select **Status and Manage → Files.**
		3. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.3.3 Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAMs)

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(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.** **THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.**

Procedure 11: Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAMs)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ■	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log into the Active 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 displayed 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. Repeat sub-steps 1 through 5 from each Active SOAM.

Procedure 11: Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAMs)

2 ☐	Log all current alarms at NOAM	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference. Repeat sub-steps 1 through 3 for all Active SOAMs.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
4 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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**

4.3.4 Disable Provisioning (3-tier, 1+1)

The following procedure upgrades the 3-tier NOAM, including the Disaster Recovery site NOAM (DR-NO). If the DR NOAM is not present, all DR NOAM-related steps can be safely ignored.

Procedure 12: Disable Provisioning (3-tier, 1+1)

S T E P #	This procedure disables provisioning for 3-Tier NO (and DR-NO) servers, prior to upgrade. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments only. It applies to (1+1) DA-MP server configurations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	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**. 6. The Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 12: Disable Provisioning (3-tier, 1+1)

2 ☐	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 should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled.** 6. Repeat sub-steps 1 through 5 for all sites present in the setup.

4.3.5 Upgrade TVOE and NOs (3-Tier, 1+1)

This procedure is used to upgrade the NOAM and DR NOAM servers, including TVOE if required.

Procedure 13. Upgrade TVOE and NOs (3-Tier, 1+1)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Upgrade Standby DSR NO and DR NO servers (using Upgrade Single Server procedure).	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DR NO(s) (if exists) in parallel using Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**
2 ☐	Upgrade Active NO and DR NO servers. (NOTE: If logged out of NOAM VIP, login again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**

4.3.6 Verify Post Upgrade Status (3-Tier, 1+1, NOAM)

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

Procedure 14: Verify Post Upgrade Status (3-Tier, 1+1, NOAM)

S T E P #	This procedure verifies Post Upgrade Status for 3-Tier NO upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		1. Execute the following commands on the Active NOAM, Standby NOAM, Active DR NOAM, Standby DR NOAM servers :
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		Note: The static XMI IP address for each NO server should be available in Table 3.
		`# verifyUpgrade`
		Examine the output of the above command to determine if any errors were reported. In case of errors please contact the Oracle CGBU Customer Care Center.
		`# 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.]
		Contact the Oracle CGBU Customer Care Center if above output is not generated.

Procedure 14: Verify Post Upgrade Status (3-Tier, 1+1, NOAM)

2 ☐	Verify Server Status is Normal	Verify Server Status is Normal: From the Active NOAM GUI: **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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 1 and 2 from each Active SOAM.
3 ☐	**NO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the Active NOAM GUI via 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. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 2 through 4 from each Active SOAM.
4 ☐	**SO GUI:** Verify Alarm status	Log all current alarms in the system: From the Active SOAM 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/or print the report. Keep these copies for future reference. Expected Alarms include: Active SO server: Alarm ID = **10008** (Provisioning Manually Disabled)
5 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.

Procedure 14: Verify Post Upgrade Status (3-Tier, 1+1, NOAM)

6 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Enable global provisioning and configuration	Enable provisioning and configuration updates on the entire network : **Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning, new data provisioned at NOAM will be replicated only to upgraded SO(s).** **Note: Step 8 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM**. From the Active NOAM GUI: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Click the **Enable Provisioning** button. 3. Verify the text of the button changes to **Disable Provisioning.**
9 ☐	Add new Network Element (if required).	Skip this step if: • 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 NO(s). Follow the DSR 4.x Installation Procedure ([5]) or DSR 5.x Installation Procedure ([6]) to install the software on the new servers and add the new Network Element under the existing NO(s). Skip the sections of the Installation Procedure related to installing and configuring the NO(s). This will add a new DSR SO site under the existing NO(s).
10 ☐	*Note on Provisioning status*	Provisioning on the SOs, will typically remain disabled until further upgrades are performed on the sites.
End of maintenance window		

4.3.7 Site Upgrade (3-Tier, 1+1)

This section contains upgrade steps for a single site with 3-tier SO and (1+1) DA-MP redundancy configuration. The following upgrade paths are supported:

- DSR 4.x->5.1 Major upgrade
- DSR 5.1 Incremental upgrade

[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.]

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 SO 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, the site provisioning should be disabled. It may re-enable at the completion of the site upgrade.

Table 9. Site Upgrade Execution Overview (3-Tier, 1+1).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 16	0:10-0:15	0:10-0:15	0:10-0:15	0:10-0:15	Perform Health Check (Pre-Upgrade, 3-Tier, 1+1 SOAMs)	None
Procedure 17	0:25-1:00	0:35-1:15	1:25-2:00	1:35-2:15	Upgrade SOs (3-Tier, 1+1)	Site Provisioning Disabled, No Traffic Impact
Procedure 18	0:25-1:00	1:00-2:15	0:25-1:00	2:00-3:15	Upgrade DA-MPs (3-Tier, 1+1)	Global and Site Provisioning Enabled, No Traffic Impact
Procedure 19	0:01-0:05 Per MP	1:16-3:35	0:01-0:05 Per MP	2:16-4:35	Verify Post-Upgrade Status (3-Tier, 1+1)	None

4.3.8 Perform Site Backup (Pre-Upgrade, 3-Tier, 1+1)

This procedure is used to perform a backup of all servers associated with the site 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: Perform Site Backup (Pre-Upgrade, 3-Tier, 1+1)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active NO	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NO: `ssh root@<NO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this NO)	Execute the **backupAllHosts** utility on the Active NO. [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**

Procedure 15: Perform Site Backup (Pre-Upgrade, 3-Tier, 1+1)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	

		The following output will be generated for DSR 5.1 servers only:
		
		`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.
		
		`# exit`
		(to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		
		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`
		`Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.3.9 Perform Health Check (Pre-Upgrade, 3-Tier, 1+1 SOAMs)

This procedure is used to perform a pre-upgrade health check of the site SOAM servers.

Procedure 16: Perform Health Check (Pre-Upgrade, 3-Tier, 1+1 SOAMs)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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**. Note: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**. The Alarms & Events > View Active screen is displayed. 2. Click the **Report button** to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**

4.3.11 Upgrade SOs (3-Tier, 1+1)

For each site in the 3-tier DSR, the SOAM(s) (Procedure 17) and associated DA-MPs (Procedure 18) 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 17: Upgrade SOs (3-Tier, 1+1)

S T E P #		
	This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify that Site Provisioning is disabled	Site Provisioning was disabled in Section 4.3.4,Disable Provisioning (3-tier, 1+1). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with step 2. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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.**
2 ☐	Upgrade TVOE Host for Standby Server	If the TVOE Host for the Standby SO needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Standby SO.
3 ☐	Upgrade Standby SO	Upgrade the Standby SO **Execute Appendix G** – Single Server Upgrade for Standby SO After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Upgrade TVOE Host for Active SO Server	It the Active SO is hosted on a TVOE blade, and the TVOE Host needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Active SO.
5 ☐	Upgrade Active SO	Upgrade the Active SO server using Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
6 ☐	Install NetBackup on NO and SO (If required)	If Netbackup is to be installed on the DSR, execute the procedure in Appendix I. **Note: In DSR 5.0, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`**. The Netbackup server configuration must to be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.**

4.3.12 Upgrade DA-MPs (3-Tier, 1+1)

Detailed steps on upgrading the MPs are shown in the procedure below.

Procedure 18: Upgrade DA-MPs (3-Tier, 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	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 ☐	Upgrade the standby DA-MP server (using Upgrade Single Server procedure)	Upgrade the Standby DA-MP server[6] using the Upgrade Single Server procedure: **Execute Appendix G –** Single Server Upgrade for the Standby DA-MP. After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
3 ☐	Upgrade the Active DA-MP server.	Upgrade the Active DA-MP server using the Upgrade Single Server procedure. **Execute Appendix G** – Single Server Upgrade for the Active DA-MP. After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Enable global provisioning and configuration (if not already enabled).	Enable provisioning and configuration updates on the entire network: **Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning, new data provisioned at NOAM will be replicated only to upgraded SO(s).** **Note: Step 4 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM.** 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. Verify the text of the button changes to **Disable Provisioning.**
5 ☐	Enable Site Provisioning	**Enable Site provisioning.** 1. Log into the SOAM VIP GUI of the site just upgraded. 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**

Procedure 18: Upgrade DA-MPs (3-Tier, 1+1)

6 ☐	Update Max Allowed HA Role for NO and SO.	From the Active NOAM GUI: 1. Go to the **Status & Manage-> HA** screen. 2. Click the **Edit** button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By default, it should be 'Active'. Otherwise, update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click the **Ok** button.

4.3.13 Verify Post-Upgrade Status (3-Tier, 1+1)

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

Procedure 19: Verify Post-Upgrade Status (3-Tier, 1+1)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	Verify Server Status is Normal	Verify Server Status is Normal:
		
		1. Log into the Active 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), High Availability (HA), and Processes (Proc).
		3. Execute the following commands on the upgraded servers :
		
		Use an SSH client to connect to each of the upgraded DA-MP servers (e.g. ssh, putty):
		
		`ssh <server DA-MP IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# verifyUpgrade`
		
		Examine the output of the above command, and determine if any errors were reported. Please contact the Oracle CGBU Customer Care Center in case of errors.
		
		`# alarmMgr --alarmstatus`
		
		The following output is expected :
		
		`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 90 is executed to accept the upgrade on each server.

Procedure 19: Verify Post-Upgrade Status (3-Tier, 1+1)

2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. The following Alarm ID will be observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and print the report. Keep these copies for future reference.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for upgraded site.**	1. Log into the Active 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
4 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.

Procedure 19: Verify Post-Upgrade Status (3-Tier, 1+1)

6 ☐	Export and archive the Diameter configuration data. On Active SOAM GUI on upgraded site	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->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
7 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->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.
8 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Please verify that the health check status of the upgraded site as collected from steps 2 through 7 is the same as the pre-upgrade health checks taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window		

Note: If another site is to be upgraded, please follow all steps sequentially, starting from Procedure 15, **in another maintenance window.**

4.4 DSR Upgrade (3-Tier, N+0) (possibly including TVOE)

This section contains upgrade steps for a DSR 5.1 (3-tier setup) upgrade with (N+0) configuration (major or incremental).

4.4.1 NO Upgrade Execution (3-Tier, N+0)

Procedures for the 3-tier NO 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 NO servers (which also disables provisioning at the SO servers). Provisioning activities at the NO and SO servers will have certain limitations during the period in which the NOs 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.

These times are estimates.

Table 10. NO Upgrade Execution Overview (3-Tier, N+0).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 21	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAMs)	None
Procedure 22	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Disable Provisioning (3-Tier, N+0)	Global and Site Provisioning Disabled, No Traffic Impact
Procedure 23	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade TVOE and NOs (3-Tier, N+0)	No Traffic Impact
Procedure 24	0:01-0:05	0:32-1:20	0:01-0:05	1:32-2:20	Verify Post Upgrade Status (3-Tier, N+0, NOAM Upgrade)	Global Provisioning Enabled

4.4.2 Pre-Upgrade Checks (3-Tier, N+0, NOAMs)

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

Procedure 20: Pre-Upgrade Checks (3-Tier, N+0, NOAMs)

S T E P #	This procedure performs a pre-upgrade Health Check of the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.1), then the optional steps in this procedure to upgrade the TVOE Hosts are required. See Appendix E for the steps to verify the TVOE Host revision level. (This can be done from PMAC Software Inventory form.) Complete this information: NO-A TVOE Host Rev _____ NO-B TVOE Host Rev _____ DR-NO-A TVOE Host Rev _____ DR-NO-B TVOE Host Rev _____ Will TVOE Upgrades be performed during the DSR Application Upgrades? _____
2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade). 1. Navigate to Administration > Software Management > Upgrade **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.x releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x**

Procedure 20: Pre-Upgrade Checks (3-Tier, N+0, NOAMs)

Main Menu: Administration -> Upgrade

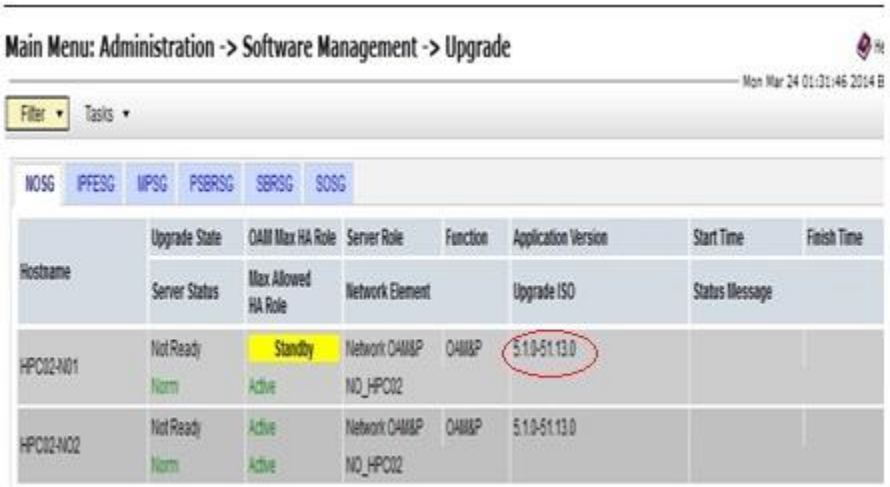
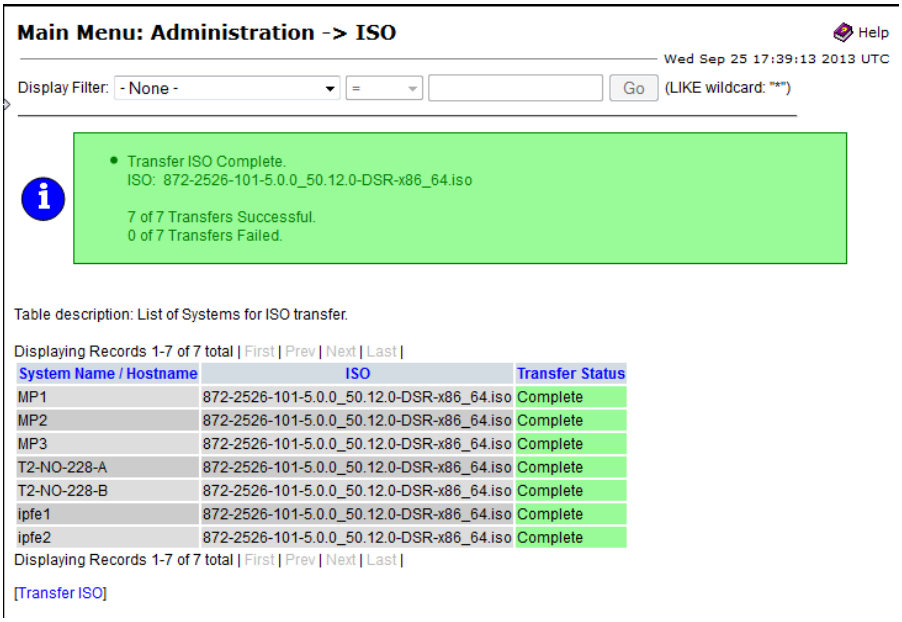
Hostname	Network Element Application Version	Role Function
T2-NO-228-A	T2_NO_228 4.0.2-40.27.3	NETWORK OAM&P OAM&P
T2-NO-228-B	T2_NO_228 Unknown	NETWORK OAM&P OAM&P
MP2	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
MP3	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
ipfe1	T2_NO_228 4.0.2-40.27.3	MP IP Front End
ipfe2	T2_NO_228 4.0.2-40.27.3	MP IP Front End
MP1	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)

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 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 20: Pre-Upgrade Checks (3-Tier, N+0, NOAMs)

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up Select NO server group and verify Application Version 
3	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify that the DSR ISO file has been transferred to all servers: Example:  If not, refer to Section 3.3.10, ISO Administration.

Procedure 20: Pre-Upgrade Checks (3-Tier, N+0, NOAMs)

4 ☐	Verify that a recent version of the Full DB backup has been performed	Verify that a recent version of the Full DB backup has been performed.
		
		1. Select **Status and Manage → Files**
		2. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.4.3 Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAMs)

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(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.

THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.

Procedure 21: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAMs)

S T E P #	This procedure performs a pre-upgrade Health Check of the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
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), High Availability (HA), and Processes (Proc). 4. Do not proceed to upgrade if any of the server statuses displayed 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. Repeat sub-steps 1 through 5 from the Active SOAM GUI.

Procedure 21: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAMs)

2 ☐	Log all current alarms at NOAM	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/or print the report. Keep these copies for future reference. Repeat sub-steps 1through 3 from the Active SOAM GUI.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
4 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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**

4.4.4 Disable Provisioning (3-Tier, N+0)

This procedure disables global and site provisioning in preparation for upgrading the NO and DR-NO.

Procedure 22: Disable Provisioning (3-Tier, N+0)

S T E P #	This procedure disables provisioning for 3-Tier NO (and DR-NO) servers, prior to upgrade. This Procedure is specific to 3-tier deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**
1 ☐	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.** 6. The Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 22: Disable Provisioning (3-Tier, N+0)

2 ☐	Disable Site Provisioning	Disable Site provisioning for all 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 should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled.** 6. Repeat sub-steps 1 through 5 for all sites present in the setup.

4.4.5 Upgrade TVOE and NOs (3-Tier, N+0)

This procedure is used to upgrade the NOAM and DR NOAM servers, including TVOE if required.

Procedure 23. Upgrade TVOE and NOs (3-Tier, N+0)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Upgrade Standby DSR NO and DR NO servers (using Upgrade Single Server procedure).	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DR NO(s) (if exists) in parallel using Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**
2 ☐	Upgrade Active NO and DR NO servers. (NOTE: If logged out of NOAM VIP, login again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**

4.4.6 Verify Post Upgrade Status (3-Tier, N+0, NOAM Upgrade)

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

Procedure 24: Verify Post Upgrade Status (3-Tier, N+0, NOAM Upgrade)

S T E P #	This procedure verifies Post Upgrade Status for 3-Tier (1+1) NO upgrades. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	**SSH:** Verify NO and DR-NO Server Status (optional)	Verify Server Status after NO servers are upgraded:
		1. Execute the following commands on the Active NOAM, Standby NOAM, Active DR NOAM, Standby DR NOAM servers :
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		Note: The static XMI IP address for each NO server should be available in Table 3.
		`# verifyUpgrade`
		Examine the output of the above command to determine if any errors were reported. In case of errors, please contact the Oracle CGBU Customer Care Center.
		`# alarmMgr --alarmstatus`
		The following alarm output is expected, 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.]
		Contact the Oracle CGBU Customer Care Center if the above output is not generated.

2 ☐	Verify Server Status is Normal	Verify Server Status is Normal: **1.** Log into the Active 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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 2 through 3 from the Active SOAM GUI.

Procedure 24: Verify Post Upgrade Status (3-Tier, N+0, NOAM Upgrade)

3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4 ☐	**SO GUI:** Verify Alarm status	Log all current alarms in the system: From the Active SOAM GUI: 1. Log into the SOAM GUI via 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. Expected Alarms include: Active SO server has: Alarm ID = **10008** (Provisioning Manually Disabled)
5 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.

Procedure 24: Verify Post Upgrade Status (3-Tier, N+0, NOAM Upgrade)

8 ☐	Update Appworks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NO 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 NO 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** 1. Log into Active NO console and execute the following command: **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** NOTE: This command may execute without any output if no changes are required (no devices were found to update).
9 ☐	Enable global provisioning and configuration	Enable provisioning and configuration updates on the entire network : **Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning, new data provisioned at NOAM will be replicated only to upgraded SO(s).** **Note: Step 9 is NOT executed on the Active DR NOAM. It is only executed on the "primary" Active NOAM.** From the Active NOAM GUI: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Click the **Enable Provisioning** button. 3. Verify the text of the button changes to **Disable Provisioning.**
10 ☐	Add new Network Element (if required).	*Skip this step if:* • 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 NO(s). Follow the DSR 4.x Installation Procedure [5] or the DSR 5.x Installation Procedure [6] to install the software on the new servers and add the new Network Element under the existing NO(s). Skip the sections of the Installation Procedure related to installing and configuring the NO(s). This will add a new DSR SO site under the existing NO(s).
11 ☐	*Note on Provisioning status*	Provisioning on the SOs, will typically remain disabled until further upgrades are performed on the sites.
End of maintenance window		

4.4.7 Site Upgrade (3-Tier, N+0)

This section contains the steps required to upgrade a 3-tier DSR site with an SOAM, and a multiple-active (N+0) DA-MP configuration. It also includes a procedure to upgrade cSBR servers (if used in the deployment).

Each signaling network element (SOAM pair and its associated MPs (SBR/DA-MP/IPFE) (i.e. site) should be upgraded in its own separate maintenance window.

Table 11. Upgrade Execution Overview (3-Tier, N+0).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 26	0:10-0:15	0:10-0:15	0:10-0:15	0:10-0:15	Perform Health Check (Pre-Upgrade, 3-Tier, N+0, SOAM)	None
Procedure 27	0:25-1:00	0:35-1:15	1:25-2:00	1:35-2:15	Upgrade SOs (3-Tier, N+0)	Site Provisioning Disabled, No Traffic Impact
Procedure 28	0:25-1:00	1:00-2:15	0:25-1:00	2:00-3:15	Upgrade cSBR(s) (3-Tier, N+0)	No Traffic Impact
Procedure 29	0:25-1:10	1:25-3:25	0:25-1:10	2:25-4:25	Upgrade Multiple DA-MPs (3-Tier, N+0)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 30	0:25-1:00	1:50-4:25	0:25-1:00	2:50-5:25	Upgrade IPFE(s) (3-Tier, N+0)	No Traffic Impact
Procedure 31	0:05	1:55-4:30	0:05	2:55-5:30	Allow Provisioning for Upgraded Site (3-Tier, N+0)	Global and Site Provisioning Enabled, No
Procedure 32	0:01-0:05 Per MP	2:11-5:50	0:01-0:05 Per MP	3:11-6:50 worst-case cumulative time (16 DA-MPs is considered)	Verify Post Upgrade status (3-Tier, N+0)	None

4.4.8 Perform Site Backup (Pre-Upgrade, 3-Tier, N+0)

This procedure is used to perform a backup of all servers associated with the site 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 25: Perform Site Backup (Pre-Upgrade, 3-Tier, N+0)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active NO	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NO: `ssh root@<NO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this NO)	Execute the **backupAllHosts** utility on the Active NO. [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**

Procedure 25: Perform Site Backup (Pre-Upgrade, 3-Tier, N+0)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	

		The following output will be generated for DSR 5.1 servers only:
		`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.
		`# exit`
		(to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		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 Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.4.9 Perform Health Check (Pre-Upgrade, 3-Tier, N+0, SOAM)

This procedure performs a health check of the site prior to upgrading.

Procedure 26: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, SOAM)

S T E P #	This procedure performs a Health Check prior to upgrading 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**

4.4.10 Upgrade SOs (3-Tier, N+0)

Procedure 27: Upgrade SOs (3-Tier, N+0)

S T E P #	This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Traffic status	Log into the Active SOAM GUI, and inspect KPI reports to verify traffic is at the expected condition.
2 ☐	Verify site Provisioning is disabled	Site Provisioning was disabled in Section 4.4.4, Disable Provisioning (3-Tier, N+0). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with **step** 3. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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 SO (if needed)	If the Standby SO is hosted on a TVOE blade, and the TVOE Host needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Standby SO.
4 ☐	Upgrade Standby SO	Upgrade the Standby SO server using Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
5 ☐	Active SO TVOE Host Upgrade (if needed)	If the Active SO is hosted on a TVOE blade, and the TVOE Host needs to be upgraded: **Execute Appendix J** to upgrade the TVOE Host for the Active SO.
6 ☐	Upgrade Active SO.	Upgrade the Active SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.

Procedure 27: Upgrade SOs (3-Tier, N+0)

7 ☐	Install NetBackup on NO and SO (If required).	If NetBackup is to be installed on the DSR, execute the procedure found in Appendix I. **Note: In DSR 5.1, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`**. Configuration of the Netbackup server is required to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document**

4.4.11 Upgrade cSBR(s) (3-Tier, N+0)

If the DSR being upgraded is running OFCS, ensure that the cSBR(s) are upgraded on an enclosure basis. That is, upgrade the cSBR(s) in one enclosure first, and only after the first enclosure has been successfully upgraded should the cSBR(s) in the second enclosure be upgraded. This approach will ensure service is not affected. cSBR in different enclosures cannot be upgraded in parallel.

This section covers only the upgrade of Charging SBRs (cSBR), associated with the OFCS application, and NOT Policy SBRs (pSBR), associated with PDRA. Any DSR running PDRA must follow the upgrade procedures found in Section 4.7 of this document.

Procedure 28: Upgrade cSBR(s) (3-Tier, N+0)

S T E P #	This procedure upgrades the cSBR(s). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Find the enclosures in the system.	Identify the enclosures in the system. Each enclosure shall contain an IPFE, Active DA-MPs, active cSBRs and a standby cSBR.
2 ☐	Find the active cSBR(s) in the enclosure	Find and record the hostname of the Active and Standby cSBR(s) in the enclosure by going to the Status & Manage -> HA screen and finding the servers with role of cSBR.
3 ☐	Upgrade cSBRs in OFCS configuration	1. Upgrade each of the Standby cSBR servers identified in step 2 using the Upgrade Single Server procedure. All Standby cSBR servers can be upgraded in parallel. **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue the procedure. 2. Upgrade each of the remaining cSBRs identified in step 2 using the Upgrade Single Server procedure. All remaining cSBR servers can be upgraded in parallel. **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next procedure.

4.4.12 Upgrade Multiple DA-MPs (3-Tier, 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 29 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 29 must be executed four distinct times.

Procedure 29: Upgrade Multiple DA-MPs (3-Tier, 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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.
2 ☐	Upgrade Active DA-MPs	Upgrade the selected DA-MPs, executing the Upgrade Multiple Server procedure on all selected DA-MPs in parallel. **Execute Appendix K :** Upgrade Multiple Servers After successfully completing the procedure in **Appendix K** for all selected DA-MPs, return to this point and continue with the next procedure.
3 ☐	Repeat for all DA-MP servers	Repeat steps 1 and 2 for the next set of DA-MP servers.

4.4.13 Upgrade IPFE(s) (3-Tier, 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, following procedure must be executed independently for each signaling network element that has IPFE servers installed.

Procedure 30: Upgrade IPFE(s) (3-Tier, 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify IPFE upgrade order	Choose the number of IPFEs on which upgrade can be executed 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.

Procedure 30: Upgrade IPFE(s) (3-Tier, N+0)

2 ☐	Upgrade IPFE servers	1. Upgrade the IPFEs identified in step 1 in parallel, using the Upgrade Multiple Server procedure. **Execute Appendix K :** Upgrade Multiple Servers

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	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: root`
		`password: <enter password>`
		
		2. Execute the following command on the IPFE server :
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`
		
		The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to the next step** (step 4).
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[root@ISoak-en1-b10-IPFE ~]# 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 sub-step 3.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[root@ISoak-en1-b10-IPFE ~]# 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: 8`
		`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`

Procedure 30: Upgrade IPFE(s) (3-Tier, N+0)

		3. Execute the following commands.
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# 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.
		
		4. Once the server is back online, log into the server and execute the following command:
		
		`# /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, then contact the Oracle CGBU Customer Care Center.

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

4.4.14 Allow Provisioning for Upgraded Site (3-Tier, N+0)

This procedure allows provisioning for SO servers. Global Provisioning can be enabled after a site upgrade, if required.

Procedure 31: Allow Provisioning for Upgraded Site (3-Tier, N+0)

S T E P #	This procedure allow provisioning for SO 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Enable global provisioning and configuration (if not already enabled).	Enable provisioning and configuration updates on the entire network (if not already enabled, else ignore this step): **Provisioning and configuration updates may be enabled for the entire network. Please note that by enabling global provisioning, new data provisioned at the NOAM will be replicated only to the upgraded SO(s).** **Note: Step 1 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM.** 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. Verify the text of the button changes to **Disable Provisioning.**
2 ☐	Enable site provisioning	**Enable Site provisioning :** 1. Log into the SOAM VIP GUI of the site just upgraded. 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**
3 ☐	Update Max Allowed HA Role for NO and SO.	From the Active NOAM GUI: 1. Go to the Status & Manage-> HA screen. 2. Click the **Edit** button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By default, it should be 'Active'. Otherwise, update the 'Max Allowed HA Role' as Active from the Drop Down list. 4. Click the **Ok** button.

4.4.15 Verify Post Upgrade status (3-Tier, N+0)

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

Procedure 32: Verify Post Upgrade status (3-Tier, N+0)

S T E P #	This procedure verifies Post Upgrade Status Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	Verify Server Status is Normal	Verify Server Status is Normal:
		
		1. Log into the Active 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), High Availability (HA), and Processes (Proc).
		4. Execute the following commands on the upgraded servers :
		
		Use an SSH client to connect to the upgraded MP (DA-MPs, IPFEs and cSBRs) servers (e.g. ssh, putty):
		
		`ssh <MP server IMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# verifyUpgrade`
		
		Examine the output of the above command to determine if any errors were reported. Contact the Oracle CGBU Customer Care Center in case of errors.

Procedure 32: Verify Post Upgrade status (3-Tier, N+0)

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.
		
		The following Alarm ID will be observed on the upgraded MP servers (i.e. IPFEs, DA-MPs and c-SBRs (whichever exists)):
		
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note : If ALARM ID 32532 is not raised on any of the upgraded MP servers, then execute following commands on that particular server to check the existence of the alarm :
		
		Use an SSH client to connect to each upgraded MP server (DA-MPs, IPFEs and cSBRs) which did not raise Alarm Id 32532 (e.g. ssh, putty):
		
		`ssh <MP server IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# alarmMgr --alarmstatus`
		
		The following output should be displayed :
		
		`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`
		
		Contact the Oracle CGBU Customer Care Center if the above output is not raised.
		
		Alarm ID 32532 will be cleared once Procedure 90 is executed to accept the upgrade on each MP server (DA-MPs, IPFEs and cSBRs).
		
		2. Click the **Report** button to generate an Alarms report.
		3. Save the report and print the report. Keep these copies for future reference.

Procedure 32: Verify Post Upgrade status (3-Tier, N+0)

3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for upgraded site.**	1. Log into the SOAM GUI 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 this off to a 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.
4 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	Capture the IPFE Configuration Options Screens. On upgraded site.	1. Select **Main Menu -> IPFE->Configuration->Options** 2. Save a screen capture of the complete screen on the client machine
6 ☐	Capture the IPFE Configuration Target Set screens On upgraded site.	1. Select **Main Menu -> IPFE->Configuration->Target Sets** 2. Save a screen capture of the complete screens on the client machine
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Export and archive the Diameter configuration data. On Active SOAM GUI on upgraded site	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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

Procedure 32: Verify Post Upgrade status (3-Tier, N+0)

9 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 NOAM to the client machine.
10 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Compare the health check status of the upgraded site (as collected in steps 2 through 9) to the pre-upgrade health check status taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window.		

Note: If another site is to be upgraded, please follow all steps sequentially starting with Procedure 25 **in another maintenance window.**

4.5 DSR Upgrade (3-Tier, N+0, RMS) (including TVOE)

This section contains the steps required to upgrade a 3-tier DSR, deployed on RMSs, with DA-MPs in the multi-active (N+0) configuration.

The following commercial deployment types are supported:

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

In DSR 4.x/5.x, 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: DSR 4.1 is the earliest release supported on RMS, so all RMS-based upgrades will have a source release of DSR 4.1 or later.

Note: - Ensure that session output is logged for future debugging.

4.5.1 NO Upgrade Execution (3-Tier, N+0, RMS)

This section contains upgrade steps for DSR 5.1 (3-tier setup) NO upgrade with (N+0) configuration (major or incremental).

Procedures for the 3-tier NO 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 NO servers (which will also disable provisioning at the SO servers). Provisioning activities at the NO and SO servers will have certain limitations during the period in which the NOs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in the 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.

These times are estimates.

Table 12. NO Upgrade Execution Overview (3-Tier, N+0, RMS).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 34	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAM on RMS)	None
Procedure 35	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Disable Provisioning (3-Tier, N+0, RMS)	Global and Site Provisioning Disabled, No Traffic Impact
Procedure 36	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade TVOE and NOs (3-Tier, N+0, RMS)	No Traffic Impact
Procedure 37	0:01-0:05	0:57-2:20	0:01-0:05	2:57-4:20	Verify Post Upgrade Status (3-tier, N+0, NOAM on RMS)	None

4.5.2 Pre-Upgrade Checks (3-Tier, N+0, RMS)

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

Procedure 33: Pre-Upgrade Checks (3-Tier, N+0, RMS)

S T E P #	This procedure verifies that the NOAM is ready for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.1), then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (This can be done from PMAC Software Inventory form.) Complete this information: NO-A TVOE Host Rev _____ NO-B TVOE Host Rev _____ DR-NO-A TVOE Host Rev _____ DR-NO-B TVOE Host Rev _____ Will TVOE Upgrades be performed during the DSR Application Upgrades? _____

Procedure 33: Pre-Upgrade Checks (3-Tier, N+0, RMS)

2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade). Example: **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x** **Main Menu: Administration -> Upgrade** Hostname / Network Element / Role Application Version / Function T2-NO-228-A: T2_NO_228, 4.0.2-40.27.3, NETWORK OAM&P, OAM&P T2-NO-228-B: T2_NO_228, Unknown, NETWORK OAM&P, OAM&P MP2: T2_NO_228, 4.0.2-40.27.3, MP, DSR (multi-active cluster) MP3: T2_NO_228, 4.0.2-40.27.3, MP, DSR (multi-active cluster) ipfe1: T2_NO_228, 4.0.2-40.27.3, MP, IP Front End ipfe2: T2_NO_228, 4.0.2-40.27.3, MP, IP Front End MP1: T2_NO_228, 4.0.2-40.27.3, MP, DSR (multi-active cluster)

Procedure 33: Pre-Upgrade Checks (3-Tier, N+0, RMS)

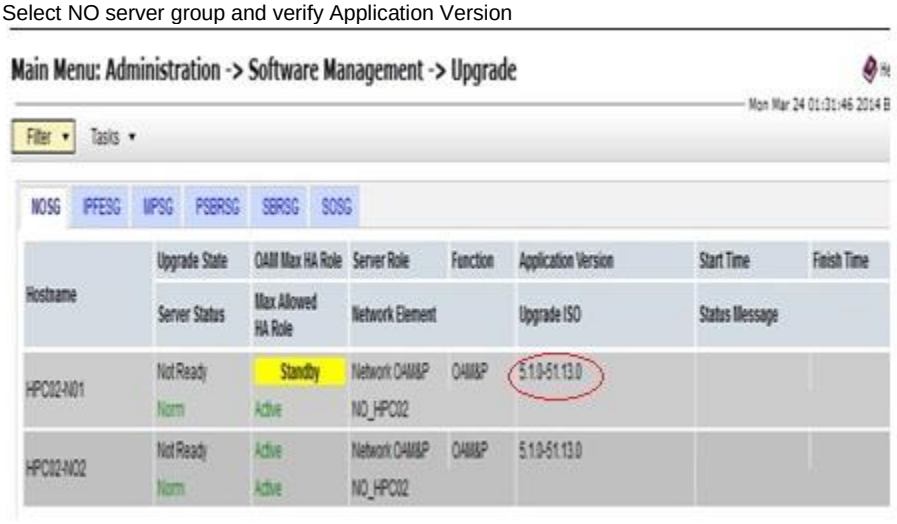
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

Main Menu:Administration->Upgrade

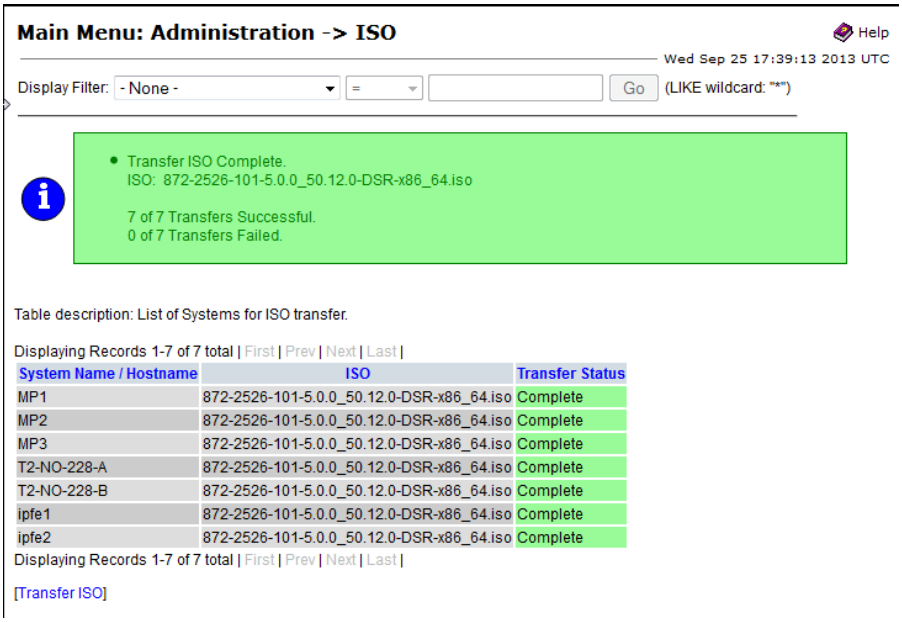
Hostname	Server Status OAM Max HA Role Max Allowed HA Role	Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO2
Viper-NO2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

Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Select NO server group and verify Application Version



Procedure 33: Pre-Upgrade Checks (3-Tier, N+0, RMS)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify the DSR ISO file has been transferred to all servers: Example:  If not, refer to section 3.3.10, ISO Administration.

4 ☐	**Verify that a recent version of the Full DB backup has been performed**	Verify that a recent version of the Full DB backup has been performed.
		
		1. Select **Status and Manage → Files**
		2. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.5.3 Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAM on RMS)

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(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.

THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.

Procedure 34: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAM on RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
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), High Availability (HA), 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. Repeat sub-steps 1 through 5 from the Active SOAM GUI.
2 ☐	Log all current alarms at NOAM	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/or print the report. Keep these copies for future reference. Repeat sub-steps 1 through 3 from the Active SOAM GUI.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.

Procedure 34: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, NOAM on RMS)

4 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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**

4.5.4 Disable Provisioning (3-Tier, N+0, RMS)

The following procedure upgrades the 3-tier NOAM, including the Disaster Recovery site NOAM (DR-NO). If the DR NOAM is not present, all DR NOAM-related steps can be safely ignored.

Procedure 35: Disable Provisioning (3-Tier, N+0, RMS)

S T E P #	This procedure disables provisioning for 3-Tier NO (and DR-NO) servers, prior to upgrade. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments only. It applies to (N+0) redundant DA-MP server configurations on RMS servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	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**. 6. The Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	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 should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled**. 6. Repeat sub steps 2 through 5 for all the sites present in the setup.

4.5.5 Upgrade TVOE and NOs (3-Tier, N+0, RMS)

This procedure is used to upgrade the NOAM and DR NOAM servers, including TVOE if required.

Procedure 36. Upgrade TVOE and NOs (3-Tier, N+0, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Upgrade Standby DSR NO and DR NO servers (using Upgrade Single Server procedure).	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DR NO(s) (if exists) in parallel using Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**
2 ☐	Upgrade Active NO and DR NO servers. (NOTE: If logged out of NOAM VIP, login again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**

4.5.6 Verify Post Upgrade Status (3-tier, N+0, NOAM on RMS)

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

Procedure 37: Verify Post Upgrade Status (3-tier, N+0, NOAM on RMS)

S T E P #	This procedure verifies Post Upgrade Status for 3-Tier (N+0) NO upgrade on RMS servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		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 <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		Note: The static XMI IP address for each NO server should be available in Table 3.
		`# verifyUpgrade`
		Examine the output of the above command to determine if any errors were reported. In case of errors, please contact the Oracle CGBU Customer Care Center.
		`# 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`
		Note: Alarm ID 32532 will be cleared once Procedure 90 is executed to accept the upgrade on each server.
		Contact the Oracle CGBU Customer Care Center if the above output is not generated.

Procedure 37: Verify Post Upgrade Status (3-tier, N+0, NOAM on RMS)

2 ☐	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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 2 through 3 from the Active SOAM GUI.
3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4 ☐	**SO GUI:** Verify Alarm status	Log all current alarms in the system: From the Active SOAM 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/or print the report. Keep these copies for future reference. Expected Alarms include: Active SO server: Alarm ID = **10008** (Provisioning Manually Disabled)
5 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.

Procedure 37: Verify Post Upgrade Status (3-tier, N+0, NOAM on RMS)

6 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Update AppWorks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NO 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 NO 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 its locally store information for those devices.** 1. Log into the Active NO console and execute the following command: **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** **NOTE: This command may execute with no output when no changes are required (no devices were found to update).**
9 ☐	*Note on Provisioning status*	Provisioning on the NO and SOs will typically remain disabled until further upgrades are performed on the sites. SO provisioning shall also remain disabled.
End of maintenance window		

4.5.7 Site Upgrade (3-Tier, N+0, RMS)

This section contains the steps required to upgrade a 3-tier DSR site that has an SOAM function, and multiple-active (N+0) DA-MP configuration on RMS servers.
Each signaling network element (SOAM pair and its associated MPs) (i.e. site) should be upgraded in its own separate maintenance window.
Global provisioning can be re-enabled (if required) after any one of the sites has been upgraded.

Table 13. Site Upgrade Execution Overview (3-Tier, N+0, RMS).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 39	0:10-0:15	0:10-0:15	0:10-0:15	0:10-0:15	Perform Health Check (Pre-Upgrade, 3-Tier, N+0, RMS)	None
Procedure 40	0:25-1:05	0:35-1:20	0:25-1:05	0:35-1:20	Upgrade SOs (3-Tier, N+0, RMS)	Site Provisioning Disabled, No Traffic Impact
Procedure 41	0:20-1:10	0:55-2:30	0:20-1:10	0:55-2:30	Upgrade Multiple DA-MPs (3-Tier, N+0, RMS)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 42	0:10-1:00	1:05-3:30	0:10-1:00	2:05-3:30	Upgrade IPFE(s) (3-Tier, N+0, RMS)	No Traffic Impact
Procedure 43	0:05	1:10-3:35	0:05	2:10-3:35	Allow Provisioning for Upgraded Site (3-Tier, N+0, RMS)	Global and Site Provisioning Enabled, No Traffic Impact
Procedure 44	0:01-0:05 Per MP	1:26-4:55	0:01-0:05 Per MP	2:26-4:55 worst-case cumulative time (16 DA-MPs is considered)	Verify Post Upgrade status (3-Tier, N+0, RMS)	None

4.5.8 Perform Site Backup (Pre-Upgrade, 3-Tier, N+0, RMS)

This procedure is used to perform a backup of all servers associated with the site 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 38: Perform Site Backup (Pre-Upgrade, 3-Tier, N+0, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active NO	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NO: `ssh root@<NO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this NO)	Execute the **backupAllHosts** utility on the Active NO. [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**
		
		The following output will be generated for DSR 5.1 servers only:
		
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`

Procedure 38: Perform Site Backup (Pre-Upgrade, 3-Tier, N+0, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	

		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.
		
		`# exit`
		(to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		
		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`
		`Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.5.9 Perform Health Check (Pre-Upgrade, 3-Tier, N+0, RMS)

Detailed steps are shown in the procedure below.

Procedure 39: Perform Health Check (Pre-Upgrade, 3-Tier, N+0, RMS)

S T E P #	This procedure performs a Health Check before upgrading 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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**. Note: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**

4.5.10 Upgrade SOs (3-Tier, N+0, RMS)

Detailed steps are shown in the procedure below.

Procedure 40: Upgrade SOs (3-Tier, N+0, RMS)

S T E P #		
	This procedure upgrades the SOAM(s) in a 3-tier DSR. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) RMS deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Traffic status	Log into the Active SOAM GUI, and inspect KPI reports to verify traffic is at the expected condition.
2 ☐	Verify that site Provisioning is disabled	Site Provisioning was disabled in Section 4.5.4, Disable Provisioning (3-Tier, N+0, RMS). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with **step** 3. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 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 standby SO	Upgrade the Standby SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **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 ☐	Upgrade Active SO.	Upgrade the Active SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **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.**
5 ☐	Install NetBackup on NO and SO (If required).	If NetBackup is to be installed on the DSR, execute the procedure found in Appendix I. **Note: In DSR 5.1, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`**. Configuration of the Netbackup server is required to update the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.**

4.5.11 Upgrade Multiple DA-MPs (3-Tier, N+0, RMS)

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. The effect on the Diameter network traffic must be considered, since any DA-MP being upgraded will not be handling live traffic.

Procedure 41 **needs to 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 41 **must be executed four distinct times**.

Procedure 41: Upgrade Multiple DA-MPs (3-Tier, N+0, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify all the DA-MPs to be upgraded together.	Choose any number of MP(s) to be upgraded in parallel, considering traffic.
2 ☐	Upgrade Active MPs	Upgrade the selected DA-MPs, executing the Upgrade Multiple Servers procedure on all selected DA-MPs in parallel. **Execute Appendix K :** Upgrade Multiple Servers After successfully completing the procedure in **Appendix K** for all selected DA-MPs, return to this point and continue with the next procedure.
3 ☐	Repeat DA-MP upgrade	Repeat steps 1 and 2 for the next set of DA-MPs to be upgraded.

4.5.12 Upgrade IPFE(s) (3-Tier, N+0, RMS)

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 42: Upgrade IPFE(s) (3-Tier, N+0, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify IPFE upgrade order	Choose any number of IPFEs to be upgraded in parallel, considering traffic impact. All the IPFEs should belong to same RMS geographic site and only after the first RMS geographical site has been successfully upgraded should the IPFE(s) in the second RMS geographic site be upgraded.

Procedure 42: Upgrade IPFE(s) (3-Tier, N+0, RMS)

2 ☐	Upgrade IPFE servers	1. Upgrade the IPFEs identified in sub-step 1 in parallel, using the Upgrade Multiple Server procedure. **Execute Appendix K :** Upgrade Multiple Servers

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	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: root`
		`password: <enter password>`
		
		2. Execute the following command on the IPFE server :
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`
		
		The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to the next step** (step 4).
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[root@ISoak-en1-b10-IPFE ~]# 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 sub-step 3.
		
		Example output with highlight added (actual file names and numbers may vary):
		
		`[root@ISoak-en1-b10-IPFE ~]# 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: 8`
		`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`

Procedure 42: Upgrade IPFE(s) (3-Tier, N+0, RMS)

		3. Execute the following commands.
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# 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.
		
		4. Once the server is back online, log into the server and execute the following command:
		
		`# /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, then contact the Oracle CGBU Customer Care Center.

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

4.5.13 Allow Provisioning for Upgraded Site (3-Tier, N+0, RMS)

This procedure is used to allow Site provisioning and global provisioning disabled previously.

Procedure 43: Allow Provisioning for Upgraded Site (3-Tier, N+0, RMS)

S T E P #	This procedure allow provisioning for SO and MP servers of 3-Tier (N+0) setup. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Enable global provisioning and configuration.	Enable provisioning and configuration updates on the entire network: **Provisioning and configuration updates may be enabled to the entire network.** **Note: By enabling global provisioning, new data provisioned at NOAM will be replicated only to upgraded SO(s).** **Note: Step 1 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM.** 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. Verify the text of the button changes to **Disable Provisioning.**
2 ☐	Enable site provisioning.	**Enable Site provisioning :** 1. Log into the Active SOAM VIP GUI of the site just upgraded. 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.**
3 ☐	Update Max Allowed HA Role for NO and SO.	From the Active NOAM GUI: 1. Go to **Status & Manage-> HA**. 2. Click the **Edit** button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By default, It should be 'Active'. Otherwise, update the 'Max Allowed HA Role' as Active from the Drop Down list. 4. Click the **Ok** button.

4.5.14 Verify Post Upgrade status (3-Tier, N+0, RMS)

This procedure is used to determine the health and status of the network and servers on RMS servers.

Procedure 44: Verify Post Upgrade status (3-Tier, N+0, RMS)

S T E P #	This procedure verifies Post Upgrade Status Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log into the Active 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), High Availability (HA), and Processes (Proc). 4. Execute the following commands on the upgraded servers : Use an SSH client to connect to the upgraded MP (DA-MPs, IPFEs and cSBRs) servers (e.g. ssh, putty): **ssh <MP server IMI IP address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. Contact the Oracle CGBU Customer Care Center in case of errors.

Procedure 44: Verify Post Upgrade status (3-Tier, N+0, RMS)

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.
		
		The following Alarm ID will be observed on all upgraded MP servers (i.e. IPFEs, DA-MPs and c-SBRs (whichever exists)):
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note : If Alarm ID 32532 is not raised on any of the upgraded MP servers (DA-MPs, IPFEs and cSBRs), then execute following commands on that particular server to check for the existence of the alarm :
		
		Use an SSH client to connect to each upgraded MP server (DA-MPs, IPFEs and cSBRs) that did not raise Alarm Id 32532 (e.g. ssh, putty):
		
		`ssh <MP server IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# alarmMgr --alarmstatus`
		
		The following output should be raised :
		
		`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`
		
		Contact the Oracle CGBU Customer Care Center if the above output is not raised.
		
		2. Alarm ID 32532 will be cleared once Procedure 90 is executed to accept the upgrade on each MP server (DA-MPs, IPFEs and cSBRs).
		
		3. Click the **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

Procedure 44: Verify Post Upgrade status (3-Tier, N+0, RMS)

3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for upgraded site.**	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter-> Maintenance** 2. Select **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 this off to a client machine 18. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 19. Select the **Peer DA-MP Status** tab. 20. Verify all Peer MPs are available 21. Select the **DA-MP Connectivity** tab. 22. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count.
4 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	Capture the IPFE Configuration Options Screens. On upgraded site.	1. Select **Main Menu -> IPFE->Configuration->Options** 2. Save a screen capture of the complete screen on the client machine.
6 ☐	Capture the IPFE Configuration Target Set screens On upgraded site.	1. Select **Main Menu -> IPFE->Configuration->Target Sets** 2. Save a screen capture of the complete screens on the client machine.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Export and archive the Diameter configuration data. On Active SOAM GUI on upgraded site	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 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

Procedure 44: Verify Post Upgrade status (3-Tier, N+0, RMS)

9 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 the exported files to the client machine, or use the SCP utility to download the files from the Active NOAM to the client machine.
10 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Compare the health check status of the upgraded site, as collected from steps 2 through 9, to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window.		

Note: If another site is to be upgraded, follow all steps sequentially starting from Procedure 38 **in another maintenance window.**

4.6 DSR Upgrade (3-Tier, 1+1, RMS) (including TVOE)

This section contains the steps required to upgrade a 3-tier DSR, deployed on RMSs, and whose DA-MPs are in the multi-active (N+0) configuration.

The following commercial deployment types are supported:

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

In DSR 4.x/5.x, 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: DSR 4.1 is the earliest release supported on RMS, so all RMS-based upgrades will have a source release of DSR 4.1 or later.

Note: - Ensure that session output is logged for future debugging.

4.6.1 NO Upgrade Execution (3-Tier, 1+1, RMS)

This section contains upgrade steps for DSR 5.1 (3-tier setup) NO upgrade with (1+1) configuration (major or incremental).

Procedures for the 3-tier NO 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 NO servers (which will also disable provisioning at the SO servers). Provisioning activities at the NO and SO servers will have certain limitations during the period in which the NOs 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.

These times are estimates.

Table 14. NO Upgrade Execution Overview (3-Tier, 1+1, RMS).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 46	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAM on RMS)	None
Procedure 47	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Disable Provisioning (3-Tier, 1+1, RMS)	Global and Site Provisioning Disabled, No Traffic Impact
Procedure 48	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade TVOE and NOs (3-Tier, 1+1, RMS)	No Traffic Impact
Procedure 49	0:01-0:05	0:32-1:20	0:01-0:05	1:32-2:20	Verify Post Upgrade Status (3-tier, 1+1, NOAM on RMS)	None

4.6.2 Pre-Upgrade Checks (3-Tier, 1+1, NOAM on RMS)

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

Procedure 45: Pre-Upgrade Checks (3-Tier, 1+1, NOAM on RMS)

S T E P #	This procedure verifies that the NOAM is ready for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.1), then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (This can be done from PMAC Software Inventory form.) Complete this information: NO-A TVOE Host Rev _____ NO-B TVOE Host Rev _____ DR-NO-A TVOE Host Rev _____ DR-NO-B TVOE Host Rev _____ Will TVOE Upgrades be performed during the DSR Application Upgrades? _____

Procedure 45: Pre-Upgrade Checks (3-Tier, 1+1, NOAM on RMS)

2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm the Application Version (pre-upgrade). Example: **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x** **Main Menu: Administration -> Upgrade** (table below)

Hostname	Network Element Application Version	Role Function
T2-NO-228-A	T2_NO_228 4.0.2-40.27.3	NETWORK OAM&P OAM&P
T2-NO-228-B	T2_NO_228 Unknown	NETWORK OAM&P OAM&P
MP2	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
MP3	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
ipfe1	T2_NO_228 4.0.2-40.27.3	MP IP Front End
ipfe2	T2_NO_228 4.0.2-40.27.3	MP IP Front End
MP1	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)

Procedure 45: Pre-Upgrade Checks (3-Tier, 1+1, NOAM on RMS)

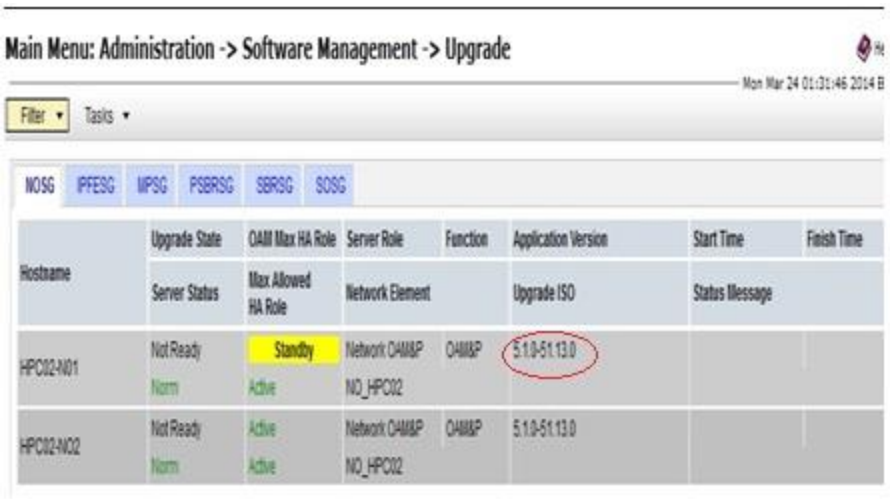
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

Main Menu: Administration->Upgrade

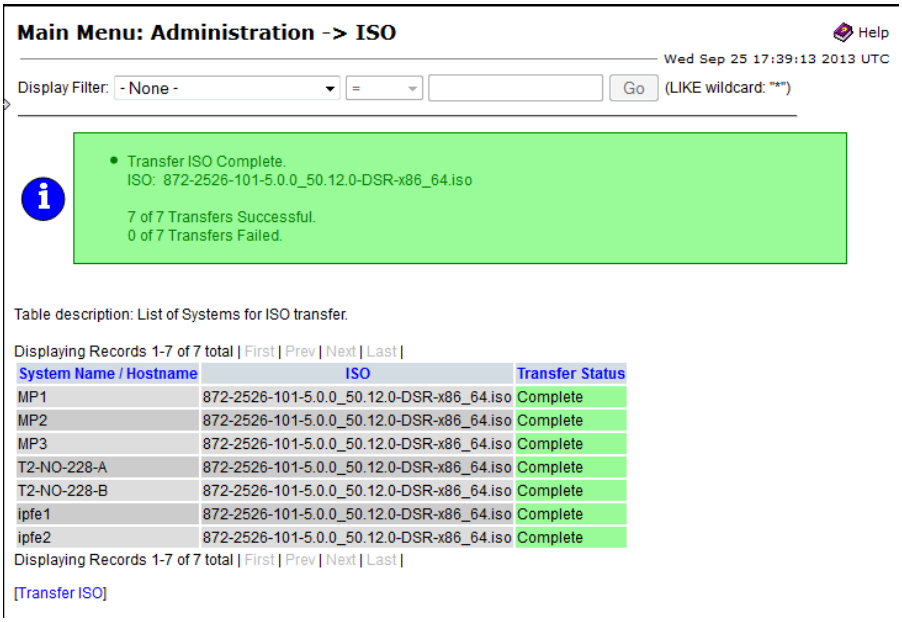
Hostname	Server Status OAM Max HA Role Max Allowed HA Role	Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO2
Viper-NO2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

Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Select NO server group and verify Application Version



Procedure 45: Pre-Upgrade Checks (3-Tier, 1+1, NOAM on RMS)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify the DSR ISO file has been transferred to all servers: Example:  If not, refer to Section 3.3.10, ISO Administration.

4 ☐	**Verify that a recent version of the Full DB backup has been performed**	Verify that a recent version of the Full DB backup has been performed.
		
		1. Select **Status and Manage → Files**
		2. Check the time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.6.3 Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAM on RMS)

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(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.

THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.

Procedure 46: Perform Health Check (Pre-Upgrade, 3-Tier, 1+1, NOAM on RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log into the Active 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), High Availability (HA), 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. Repeat sub-steps 2 through 5 from the Active SOAM GUI.
2 ☐	Log all current alarms at NOAM	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/or print the report. Keep these copies for future reference. Repeat sub-steps 1 through 3 from the Active SOAM GUI.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
4 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.**

4.6.4 Disable Provisioning (3-Tier, 1+1, RMS)

The following procedure will upgrade the 3-tier NOAM, including the Disaster Recovery site NOAM (DR-NO). If the DR NOAM is not present, all DR NOAM-related steps can be safely ignored.

Procedure 47: Disable Provisioning (3-Tier, 1+1, RMS)

S T E P #		
	This procedure disable provisioning for 3-Tier NO (and DR-NO) servers, prior to upgrade. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to either (1+1) or (N+0) redundant DA-MP server configurations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	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**. 6. The Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the Active SOAM GUI for each site using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled**. 6. Repeat sub steps 1 through 5 for all sites present in the setup.

4.6.5 Upgrade TVOE and NOs (3-Tier, 1+1, RMS)

This procedure is used to upgrade the NOAM and DR NOAM servers, including TVOE if required.

Procedure 48. Upgrade TVOE and NOs (3-Tier, 1+1, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Upgrade Standby DSR NO and DR NO servers (using Upgrade Single Server procedure).	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DR NO(s) (if exists) in parallel using Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**
2 ☐	Upgrade Active NO and DR NO servers. (NOTE: If logged out of NOAM VIP, login again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release. **If the upgrade fails – do not proceed. Consult with the Oracle CGBU Customer Care Center on the best course of action.**

4.6.6 Verify Post Upgrade Status (3-tier, 1+1, NOAM on RMS)

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

Procedure 49: Verify Post Upgrade Status (3-tier, 1+1, NOAM on RMS)

S T E P #	This procedure verifies Post Upgrade Status for 3-Tier (1+1) NO upgrade on RMS servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers are upgraded:
		
		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 <NO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		Note: The static XMI IP address for each NO server should be available in Table 3.
		
		`# verifyUpgrade`
		
		Examine the output of the above command to determine if any errors were reported. In case of errors, please contact the Oracle CGBU Customer Care Center.
		
		`# 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.]
		
		Contact the Oracle CGBU Customer Care Center if the above output is not generated.

2 ☐	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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 2 through 3 from the Active SOAM GUI.

Procedure 49: Verify Post Upgrade Status (3-tier, 1+1, NOAM on RMS)

3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 1 through 3 from each Active SOAM GUI.
4 ☐	**SO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the SOAM GUI via 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. Expected Alarms include: Active SO server has: Alarm ID = **10008** (Provisioning Manually Disabled)
5 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	*Note on Provisioning status ….*	Provisioning on the NO and SOs will typically remain disabled until further upgrades are performed on the sites.
End of maintenance window		

4.6.7 Site Upgrade (3-Tier, 1+1, RMS)

This section contains the steps required to upgrade a 3-tier DSR site that has an SOAM function, and an Active/Standby (1+1) DA-MP configuration.
Each signaling network element (SOAM pair and its associated MPs) (i.e. site) should be upgraded in its own separate maintenance window.
Global provisioning can be re-enabled after one of the sites is completely upgraded.

Table 15. Upgrade Execution Overview (3-Tier, 1+1, RMS).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 51	0:05-0:15	0:05-0:15	0:05-0:15	0:05-0:15	Perform Health Check (3-Tier, 1+1, SOAM on RMS)	None
Procedure 52	0:25-1:05	0:30-1:20	0:25-1:05	0:30-1:20	Upgrade SO (3-Tier, 1+1, RMS)	Site Provisioning Disabled, No Traffic Impact
Procedure 53	0:20-1:10	0:50-2:30	0:20-1:10	0:50-2:30	Upgrade DA-MP(s) (3-Tier, 1+1, RMS)	Global and Site Provisioning Enabled, No Traffic Impact
Procedure 54	0:01-0:05 Per MP	0:52-3:50	0:01-0:05 Per MP	0:52-3:50 worst-case cumulative time (16 DA-MPs is considered)	Verify Post Upgrade status (3-Tier, 1+1, RMS)	None

4.6.8 Perform Site Backup (3-Tier, 1+1, RMS)

This procedure is used to perform a backup of all servers associated with the site 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 50: Perform Site Backup (3-Tier, 1+1, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active NO	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NO: `ssh root@<NO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this NO)	Execute the **backupAllHosts** utility on the Active NO. [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**

Procedure 50: Perform Site Backup (3-Tier, 1+1, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	

		The following output will be generated for DSR 5.1 servers only:
		`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.
		`# exit`
		(to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		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 Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.6.9 Perform Health Check (3-Tier, 1+1, SOAM on RMS)

This procedure performs a health check of the SOAM prior to upgrade.

Procedure 51: Perform Health Check (3-Tier, 1+1, SOAM on RMS)

S T E P #	This procedure performs a Health Check before upgrading 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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**. Note: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**

4.6.10 Upgrade SO (3-Tier, 1+1, RMS)

Detailed steps are shown in the procedure below.

Procedure 52: Upgrade SO (3-Tier, 1+1, RMS)

S T E P #		
	This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that hosts an SOAM guest. This procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify site provisioning is disabled.	Site Provisioning was disabled in Section 4.6.4, Disable Provisioning (3-Tier, 1+1, RMS). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with **step** 2. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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**.
2 ☐	Upgrade Standby SO	Upgrade the Standby SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **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.**
3 ☐	Upgrade Active SO.	Upgrade the Active SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. **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 ☐	Install NetBackup on NO and SO (If required).	If NetBackup is to be installed on the DSR, execute the procedure found in Appendix I. **Note: In DSR 5.1, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`. **The Netbackup server configuration must be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.**

4.6.11 Upgrade DA-MP(s) (3-Tier, 1+1, RMS)

Detailed steps on upgrading the MPs are shown in the procedure below.

Procedure 53: Upgrade DA-MP(s) (3-Tier, 1+1, RMS)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify and Record the status of the MP before upgrade	Verify and Record the status and hostname of the Active DA-MP and 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 ☐	Upgrade the Standby DA-MP server (using Upgrade Single Server procedure)	Upgrade the Standby MP server[7] using the Upgrade Single Server procedure: **Execute Appendix G** – Single Server Upgrade for the Standby DA-MP After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
3 ☐	Upgrade the Active DA-MP server.	Upgrade the Active MP server using the Upgrade Single Server procedure. **Execute Appendix G** – Single Server Upgrade for the Active DA-MP After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Enable global provisioning and configuration.	Enable provisioning and configuration updates on the entire network: **Provisioning and configuration updates may be enabled to the entire network.** **Note: Please note that by enabling global provisioning, new data provisioned at NOAM will be replicated only to the upgraded SO(s).** **Note: Step 4 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM.** 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. Verify the text of the button changes to **Disable Provisioning.**

Procedure 53: Upgrade DA-MP(s) (3-Tier, 1+1, RMS)

5 ☐	Enable site provisioning.	**Enable Site provisioning :** 1. Log into the Active SOAM VIP GUI of the site just upgraded. 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**
6 ☐	Update Max Allowed HA Role for NO and SO.	From the Active NOAM GUI: 1. Go to the Status & Manage-> HA screen. 2. Click the **Edit** button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By default, it should be 'Active'. Otherwise, update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click the **Ok** button.

4.6.12 Verify Post Upgrade status (3-Tier, 1+1, RMS)

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

Procedure 54: Verify Post Upgrade status (3-Tier, 1+1, RMS)

S T E P #	This procedure verifies Post Upgrade Status Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	Verify Server Status is Normal	Verify Server Status is Normal:
		
		1. Log into the Active 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. Execute the following commands on the upgraded servers.
		
		Use an SSH client to connect to the upgraded MP (DA-MPs ,IPFEs and cSBRs) servers (e.g. ssh, putty):
		
		`ssh <MP server IMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# verifyUpgrade`
		
		Examine the output of the above command to determine if any errors were reported. Contact the Oracle CGBU Customer Care Center in case of errors.

Procedure 54: Verify Post Upgrade status (3-Tier, 1+1, RMS)

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. From the Active NOAM GUI, select **Alarms & Events > View Active.**
		The Alarms & Events > View Active screen is displayed.
		
		The following Alarm ID will be observed on all upgraded MP servers (i.e. IPFEs ,DA-MPs and c-SBRs (whichever exists)):
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note : If Alarm ID 32532 is not present on any of the upgraded MP servers, then execute the following commands on that particular server to check for the existence of the alarm :
		
		Use an SSH client to connect to each upgraded MP server (DA-MPs, IPFEs and cSBRs) which did not raise Alarm Id 32532 (e.g. ssh, putty):
		
		`ssh <MP server IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# alarmMgr --alarmstatus`
		
		The following output should be raised :
		
		`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`
		
		Contact the Oracle CGBU Customer Care Center if the above output is not raised.
		
		2. Alarm ID 32532 will be cleared once Procedure 90 is executed to accept the upgrade on each MP server (DA-MPs, IPFEs and cSBRs).
		
		3. Click the **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

Procedure 54: Verify Post Upgrade status (3-Tier, 1+1, RMS)

3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for upgraded site.**	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter-> Maintenance** 2. Select **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 this off to a client machine 18. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 19. Select the **Peer DA-MP Status** tab. 20. Verify all Peer MPs are available. 21. Select the **DA-MP Connectivity** tab. 22. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count.
4 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
6 ☐	Export and archive the Diameter configuration data. On Active SOAM GUI on upgraded site	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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

Procedure 54: Verify Post Upgrade status (3-Tier, 1+1, RMS)

7 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 Active NOAM to the client machine.
8 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Compare the health check status of the upgraded site, as collected in steps 2 through 7, to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window.		

Note: If another site is to be upgraded, please follow all the steps sequentially, starting with Procedure 50, **in another maintenance window.**

4.7 Policy DRA Upgrade (3-Tier)

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

- 3-tier OAM
- 2 sites each with Geo-Diverse SO and P-SBR servers (Active/Standby/Spare)
- PDRA MP's

As with other DSR 5.1 Major upgrades, the TVOE Host environments may optionally be planned and executed in separate maintenance windows, before executing these procedures.

Table 16. Upgrade Execution Overview (3-Tier, PDRA, NOAM).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 56	0:05-0:15	0:05-0:15	0:05-0:15	0:05-0:15	Perform Health Check (Pre-Upgrade, 3-Tier, PDRA NOAM)	None
Procedure 57 or Procedure 58	1:10-1:20	1:15-1:35	2:10-2:20	2:15-2:35	Upgrade TVOE and NOs (3-Tier, PDRA) or Alternate Upgrade of NO (3-Tier, PDRA)	Global Provisioning Disabled, TVOE upgrade will stop all the applications running on it.
Procedure 59	0:05	1:20-1:40	0:05	2:20-2:40	Verify Post Upgrade Status (3-Tier, PDRA, NOAM)	Global Provisioning Enabled, No Traffic Impact

Table 17. Upgrade Execution Overview (3-Tier, PDRA, Site 1).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 61	0:05-0:15	0:05-0:15	0:05-0:15	0:05-0:15	Perform Health Check – Site 1 (3-Tier, PDRA, SOAM)	None
Procedure 62	1:00-1:10	1:05-1:25	2:00-2:10	2:05-2:25	Upgrade SOAM – Site 1 (3-Tier, PDRA)	Site Provisioning Disabled, TVOE upgrade will stop all the applications running on it.
Procedure 63	1:00-1:20	2:05-2:45	1:00-1:20	3:05-3:45	Upgrade Policy SBR – Site 1 (3-Tier, PDRA)	No Traffic Impact
Procedure 64	1:00-2:00	3:05-4:45	1:00-2:00	4:05-5:45	Upgrade Multiple DA-MPs – Site 1 (3-tier, PDRA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 65	0:30-1:00	3:35-5:45	0:30-1:00	4:35-6:45	Upgrade IPFE(s) – Site 1 (3-Tier, PDRA)	No Traffic Impact
Procedure 66	0:01-0:05	3:36-5:50	0:01-0:05	4:36-6:50	Post Upgrade Wrap-Up – Site 1 (3-Tier, PDRA)	Global and Site Provisioning Enabled, No Traffic Impact
Procedure 67	0:10-0:15	3:46-6:05	0:10-0:15	4:46-7:05	Verify Post Upgrade Status – Site 1 (3-Tier, PDRA)	None

Table 18 Upgrade Execution Overview (3-Tier, PDRA, Site 2).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 69	0:05-0:15	0:05-0:15	0:05-0:15	0:05-0:15	Perform Health Check - Site 2 (Pre-Upgrade, 3-Tier, PDRA, SOAM)	None
Procedure 70	1:00-1:10	1:05-1:25	1:00-1:10	1:05-1:25	Upgrade SOAM – Site 2 (3-Tier, PDRA)	Global and Site Provisioning Disabled, TVOE upgrade will stop all the applications running on it.
Procedure 71	1:00-1:20	2:05-2:45	1:00-1:20	2:05-2:45	Upgrade Policy SBR – Site 2 (3-Tier, PDRA)	No Traffic Impact
Procedure 72	1:00-2:00	3:05-4:45	1:00-2:00	3:05-4:45	Upgrade Multiple DA-MPs – Site 2 (3-tier, PDRA)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 73	0:30-1:00	3:35-5:45	0:30-1:00	3:35-5:45	Upgrade IPFE(s) – Site 2 (3-Tier, PDRA)	No Traffic Impact
Procedure 74	0:01-0:05	3:36-5:50	0:01-0:05	3:36-5:50	Post Upgrade Wrap-up – Site 2 (3-Tier, PDRA)	Global and Site Provisioning Enabled, No Traffic Impact
Procedure 75	0:10-0:15	3:46-6:05	0:10-0:15	3:46-6:05	Verify Post Upgrade Status – Site 2 (3-Tier, PDRA)	None

4.7.1 Pre-Upgrade Checks (3-Tier, PDRA)

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

Procedure 55: Pre-Upgrade Checks (3-Tier, PDRA)

S T E P #	This procedure verifies that the NOAM is ready for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.1), then the optional steps in this procedure to upgrade the TVOE Hosts are required. See Appendix E for the steps to verify the TVOE Host revision level. (This can be done from PMAC Software Inventory form.) Complete this information: NO-A TVOE Host Rev _____ NO-B TVOE Host Rev _____ DR-NO-A TVOE Host Rev _____ DR-NO-B TVOE Host Rev _____ Will TVOE Upgrades be performed during the DSR Application Upgrades? _____
2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade). Example: **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.x releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x**

Procedure 55: Pre-Upgrade Checks (3-Tier, PDRA)

Main Menu: Administration -> Upgrade

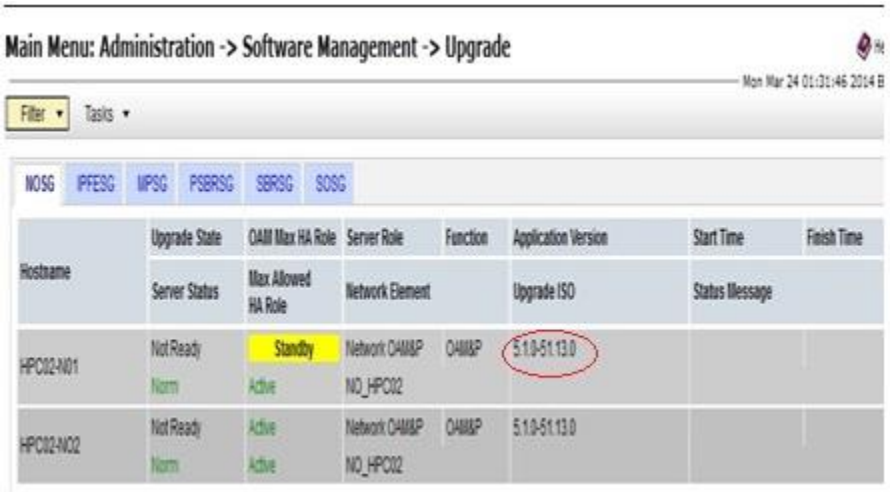
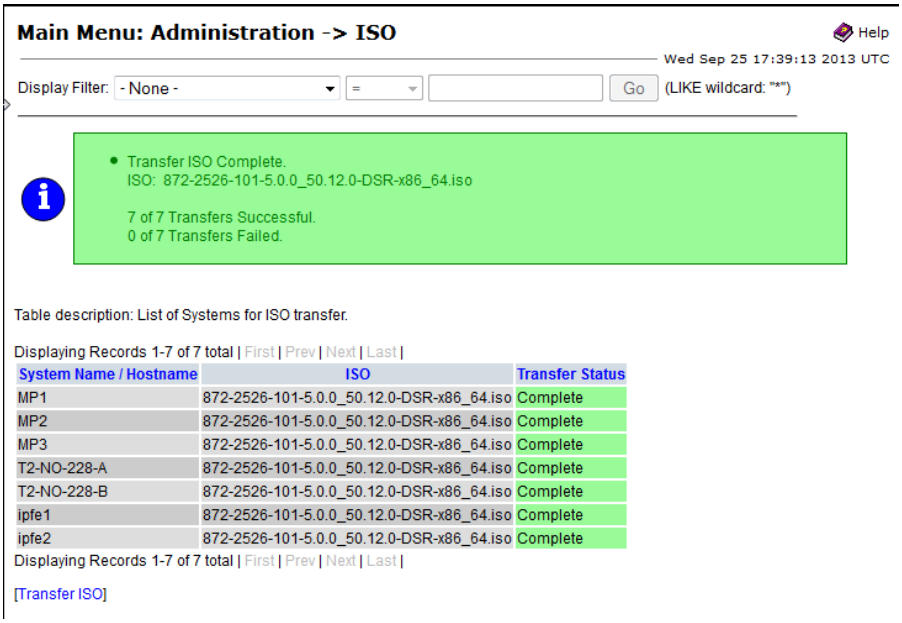
Hostname	Network Element Application Version	Role Function
T2-NO-228-A	T2_NO_228 4.0.2-40.27.3	NETWORK OAM&P OAM&P
T2-NO-228-B	T2_NO_228 Unknown	NETWORK OAM&P OAM&P
MP2	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
MP3	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)
ipfe1	T2_NO_228 4.0.2-40.27.3	MP IP Front End
ipfe2	T2_NO_228 4.0.2-40.27.3	MP IP Front End
MP1	T2_NO_228 4.0.2-40.27.3	MP DSR (multi-active cluster)

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 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 55: Pre-Upgrade Checks (3-Tier, PDRA)

		Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up Select NO server group and verify Application Version 
3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify that the DSR ISO file has been transferred to all servers: Example:  If not, refer to Section 3.3.10, ISO Administration.

Procedure 55: Pre-Upgrade Checks (3-Tier, PDRA)

4 ☐	Verify that a recent version of the Full DB backup has been performed	Verify that a recent version of the Full DB backup has been performed.
		
		1. Log into the NOAM GUI using the VIP.
		2. Select **Status and Manage → Files**
		3. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.7.2 Perform Health Check (Pre-Upgrade, 3-Tier, PDRA NOAM)

This procedure is used to determine the health and status of the network and servers. This procedure must be executed at the start of every maintenance window on both the Active NOAM and the Active SOAM.

WARNING!	**THE NOAM(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.** **THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.**

Procedure 56: Perform Health Check (Pre-Upgrade, 3-Tier, PDRA NOAM)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
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**. 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. Repeat sub-steps 2 through 4 from the Active SOAM GUI.

Procedure 56: Perform Health Check (Pre-Upgrade, 3-Tier, PDRA NOAM)

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/or print the report. Keep these copies for future reference. Repeat sub-steps 1 through 3 from the Active SOAM GUI.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
4 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established**
5 ☐	View Policy SBR status	View pSBR status. From the Active NOAM GUI: 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.
6 ☐	Verify PDRA status	View PDRA status. From the Active SOAM GUI: 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications

4.7.3 Upgrade TVOE and NOs (3-Tier, PDRA)

This procedure is used to upgrade the NOAM servers.

Procedure 57. Upgrade TVOE and NOs (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Disable global provisioning and configuration.	Disable 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 **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**. 6. The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled.** 6. Repeat sub-steps 1 through 5 for all sites present in the setup.
3 ☐	Upgrade Standby DSR NO server (using Upgrade Single Server procedure).	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DR NO(s) (if exists) in parallel using Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Upgrade Active NO server. (NOTE: If logged out of Active NOAM VIP, Log back into Active NOAM VIP again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release.

Procedure 57. Upgrade TVOE and NOs (3-Tier, PDRA)

5 ☐	Update AppWorks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NO 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 NO 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 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 following step will update the locally stored information with the performance optimization parameters. This script checks for the Ethernet devices on the servers that are functioning as IPFE and update its locally store information for those devices.** 1. Log into the Active NO console and execute the following script: **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** **If the script outputs any error messages, please consult with the Oracle CGBU Customer Care Center before proceeding with the upgrade.**

4.7.4 Alternate Upgrade of NO (3-Tier, PDRA)

This procedure can be used to upgrade the Standby NO 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 refresh. This alternate procedure upgrades the Standby NO 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.

Procedure 58. Alternate Upgrade of NO (3-Tier, PDRA)

S T E P #	This procedure upgrades the standby NO server using the PM&C interface. This procedure is specific to LARGE 3-tier deployments only. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 F: Adding ISO Images to PM&C Image Repository.
2 ☐	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**. 6. The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 58. Alternate Upgrade of NO (3-Tier, PDRA)

3 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled.** 6. Repeat sub-steps 1 through 5 for all sites present in the setup.
4 ☐	Upgrade Standby DSR NO server (using PM&C Application upgrade procedure)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DR NO and/or Standby DSR NO are hosted on TVOE blades. Upgrade the Standby DSR NO server and Standby DSR DR NO(s) (if exists) in parallel using the PM&C Application Upgrade procedure: **Execute Appendix G**-- Single Server Upgrade Procedure After successfully completing the procedure in, return to this point and continue with the next step.
5 ☐	Upgrade Active NO server. (NOTE: If logged out of Active NOAM VIP, Log back into Active NOAM VIP again.)	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Active DR NO (mate) and/or Active DSR NO (mate) are hosted on TVOE blades. Upgrade the Active NO server (the mate) and Active DR NO (if exists) using the Upgrade Single Server procedure: **1. Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step. The NOAM GUI will show the new DSR 5.1 release.
6 ☐	Update AppWorks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NO 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 NO 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 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 following step will update the locally stored information with the performance optimization parameters. This script checks for the Ethernet devices on the servers that are functioning as IPFE and update its locally store information for those devices.** 1. Log into the Active NO console and execute the following script: **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** **If the script outputs any error messages, please consult with the Oracle CGBU Customer Care Center before proceeding with the upgrade.**

4.7.5 Verify Post Upgrade Status (3-Tier, PDRA, NOAM)

This procedure is used to determine the health and status of the network and servers following the NOAM upgrade.

Procedure 59: Verify Post Upgrade Status (3-Tier, PDRA, NOAM)

S T E P #	This procedure performs a Health Check after upgrading the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		1. Execute the following commands on the Active NOAM, Standby NOAM, Active DR NOAM, Standby DR NOAM servers :
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		Note: The static XMI IP address for each NO server should be available in Table 3.
		`# verifyUpgrade`
		Examine the output of the above command to determine if any errors were reported. In case of errors please contact the Oracle CGBU Customer Care Center.
		`# 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.]
		Contact the Oracle CGBU Customer Care Center if above output is not generated.

2 ☐	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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Repeat sub-steps 1 through 3 from each Active SOAM GUI.

3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4 ☐	**SO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the SOAM GUI via 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. Expected Alarms include: Active SO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Repeat sub-steps 1 through 4 from each Active SOAM GUI.
5 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	View DA-MP Status	View DA-MP status. From the Active SOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	View Policy SBR status	View pSBR status. From the Active NOAM GUI: 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.
9 ☐	Verify PDRA status	View PDRA status. From the Active SOAM GUI: 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications

10 ☐	Enable global provisioning and configuration	Enable provisioning and configuration updates on the entire network : **Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning, new data provisioned at NOAM will be replicated only to upgraded SO(s).** **Note: Step 10 is NOT executed on the Active DR NOAM; it is only executed on the "primary" Active NOAM**. From the Active NOAM GUI: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Click the **Enable Provisioning** button. 3. Verify the text of the button changes to **Disable Provisioning.**
11 ☐	Add new Network Element (if required).	Skip this step if: • 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 NO(s). Follow the DSR 4.x Installation Procedure ([5]) or DSR 5.x Installation Procedure ([6]) to install the software on the new servers and add the new Network Element under the existing NO(s). Skip the sections of the Installation Procedure related to installing and configuring the NO(s). This will add a new DSR SO site under the existing NO(s).
12 ☐	*Note on Provisioning status*	Provisioning on the NO and SOs will typically remain disabled until further upgrades are performed on the sites. SO provisioning shall also remain disabled.
End of maintenance window		

4.7.6 Perform Site Backup – Site 1 (3-Tier, PDRA)

This procedure is used to perform a backup of all servers associated with the site 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 60: Perform Site Backup – Site 1 (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active SO of Site 1	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active SO of Site 1: `ssh root@<SO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this SO)	Execute the **backupAllHosts** utility on the Active SO(Site 1). [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**

Procedure 60: Perform Site Backup – Site 1 (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
		The following output will be generated for DSR 5.1 servers only: **`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.  **`# exit`** (to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively) **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` `Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.7.7 Perform Health Check – Site 1 (3-Tier, PDRA, SOAM)

This procedure is used to upgrade the Site 1 SOAM servers in a mated pair.

Note: - Ensure that session output is logged for future debugging.

Procedure 61: Perform Health Check – Site 1 (3-Tier, PDRA, SOAM)

S T E P #	This procedure performs a Health Check before upgrading 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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**. Note: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**
4 ☐	Verify PDRA status	View PDRA status. 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications

4.7.8 Upgrade SOAM – Site 1 (3-Tier, PDRA)

Procedure 62: Upgrade SOAM – Site 1 (3-Tier, PDRA)

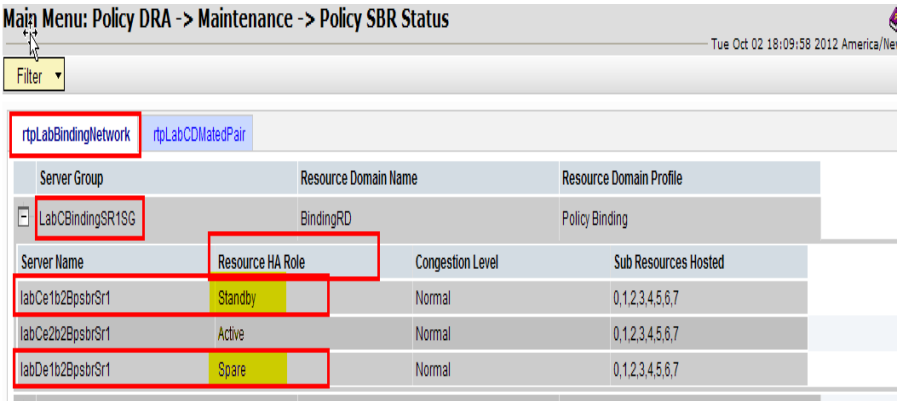
S T E P #		
	This procedure upgrades the TVOE Host of SOAM guests (if required) and upgrades SOAM servers of Site 1. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify that site Provisioning is disabled	Site Provisioning was disabled in Section 4.7.3, Upgrade TVOE and NOs (3-Tier, PDRA). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with step 2. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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**.
2 ☐	Upgrade TVOE for Standby SO and Spare SO	Before proceeding with the following steps, execute Appendix J to upgrade the TVOE Host for the Standby DSR SO and Spare DSR SO if the Standby DSR SO and Spare DSR SO are hosted on TVOE blades.
3 ☐	Upgrade Standby SO and Spare SO in parallel	**Note: The Spare server is located at the mated site of the site being upgraded** 1. Upgrade the Standby DSR SO server and Spare SO in parallel using the Upgrade Multiple Server procedure : **Execute Appendix K**—Upgrade Multiple Servers Procedure After successfully completing the procedure in **Appendix K**, return to this point and continue with the next step.
4 ☐	Upgrade Active DSR SO.	Note: Before proceeding with the following steps, execute Appendix J to upgrade the TVOE Host for the Active DSR SO, if the Active DSR SO is hosted on a TVOE blade. 1. Upgrade the Active DSR SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next procedure.

Procedure 62: Upgrade SOAM – Site 1 (3-Tier, PDRA)

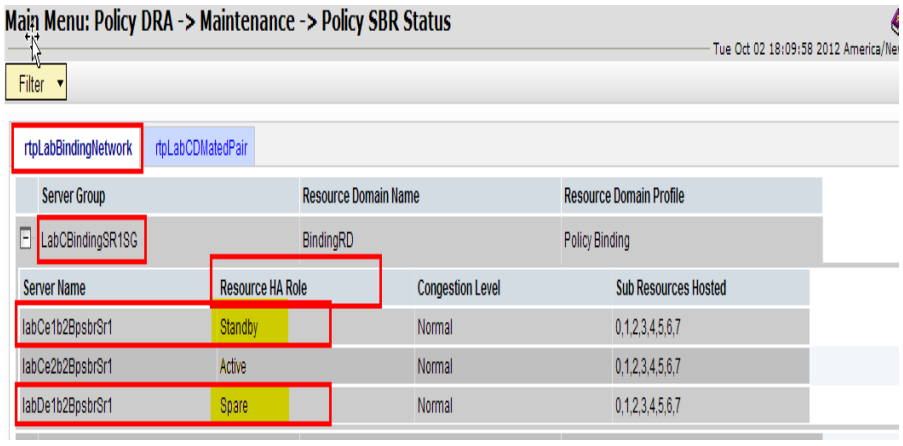
5 ☐	Install NetBackup on NO and SO (If required)	If Netbackup is to be installed on the DSR, execute the procedure in Appendix I. Note: In DSR 5.0, the backup file location is changed from `/var/TKLC/db/filemgmt` to `/var/TKLC/db/filemgmt/backup`. The Netbackup server configuration must to be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.

4.7.9 Upgrade Policy SBR – Site 1 (3-Tier, PDRA)

Procedure 63: Upgrade Policy SBR – Site 1 (3-Tier, PDRA)

S T E P #	Policy SBR 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify the pSBR Server Group(s) to Upgrade	From the data captured in Table 3, 1. Pick the "**Policy SBR**" Server Group(s) (e.g. Binding pSBR Server Group, or multiple server groups). One server group can be executed at a time or multiple server groups can be executed simultaneously. 2. Identify all server group(s) selected for upgrade in sub-step 1. 3. Log into the NOAM GUI using the VIP. 4. Navigate to **Main Menu -> Policy DRA->Maintenance->Policy 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: **labCe2b2BpsbrSr1 - Active** **labCe1b2BpsbrSr1 - Standby** **labDe1b2BpsbrSr1 – Spare**  Main Menu: Policy DRA -> Maintenance -> Policy SBR Status Tue Oct 02 18:09:58 2012 America/Ne Filter rtpLabBindingNetwork rtpLabCDMatedPair Server Group / Resource Domain Name / Resource Domain Profile LabCBindingSR1SG / BindingRD / Policy Binding Server Name / Resource HA Role / Congestion Level / Sub Resources Hosted labCe1b2BpsbrSr1 / Standby / Normal / 0,1,2,3,4,5,6,7 labCe2b2BpsbrSr1 / Active / Normal / 0,1,2,3,4,5,6,7 labDe1b2BpsbrSr1 / Spare / Normal / 0,1,2,3,4,5,6,7 **Note: Policy 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 Policy SBR Status screen MUST be used to determine the high availability status (Active, Standby, or Spare) of pSBR 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 63: Upgrade Policy SBR – Site 1 (3-Tier, PDRA)

2 ☐	Upgrade Spare Policy SBR Server identified in step 1 of this procedure.	**Note: Spare P-SBR of this triplet will be located at a different site.** 1. Upgrade the Spare Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G**—Upgrade Single Server Procedure After successfully completing the procedure in **Appendix G**, return to this point to monitor server status. From the Active NOAM GUI: 2. Navigate to **Main Menu > Policy DRA > Maintenance > Policy SBR Status**. Open the tab of the server group being upgraded. 3. Monitor the **Resource HA Role** status of the Spare server. Do not proceed to step 3 until the **Resource HA Role** of the Spare pSBR server is **Spare**.
3 ☐	Upgrade Standby Policy SBR Server identified in step 1 of this procedure.	1. Upgrade the Standby Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G**—Upgrade Single Server Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
		**WARNING!** **Failure to comply with step 4 and step 5 may result in the loss of Policy DRA traffic, resulting in service impact**
4 ☐	Verify Standby pSBR server status	From the Active NOAM GUI: 1. Navigate to **Main Menu -> Policy DRA->Maintenance->Policy 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**. 

Procedure 63: Upgrade Policy SBR – Site 1 (3-Tier, PDRA)

5 ☐	Verify that bulk download is complete between Active Policy SBR in server group to Standby Policy SBR and Spare Policy 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 Policy SBR group that is in upgrade **Display Filter**: Event ID = 31127 **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: a. 2 for the Standby Policy SBR for both binding and session policies b. 2 for the Spare Policy SBR server for both binding and session policies. 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 Policy SBR Server as identified in Step 1 of this procedure	1. Upgrade the Active Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
7 ☐	Repeat steps 1 through 6 for all Binding and Session 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.

4.7.10 Upgrade Multiple DA-MPs – Site 1 (3-tier, PDRA)

Procedure 64: Upgrade Multiple DA-MPs – Site 1 (3-tier, PDRA)

S T E P #	Policy DRA server (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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 in Server Group **identified in sub-step 1.**
2 ☐	Upgrade Policy DRA Server as identified in Step 1	1. Upgrade half of the Policy DRA (DA-MP) servers in parallel using the Upgrade Multiple Server procedure : **Note: It is recommended that the DA-MP Leader be upgraded in the last group of servers to minimize DA-MP Leader role changes.** **Execute Appendix K : Upgrade Multiple Servers** After successfully completing the procedure in **Appendix K**, return to this point and continue with the next step.

Procedure 64: Upgrade Multiple DA-MPs – Site 1 (3-tier, PDRA)

3 ☐	Repeat step 2 for all servers identified in Step 1 of this procedure.	Repeat step 2 of this procedure for the remaining Policy DRA (DA-MP) servers.
4 ☐	Update Max Allowed HA Role for NO and SO.	1. Log into the NOAM GUI using the VIP 2. Go to the Status & Manage-> HA screen. 3. Click the Edit button. 4. Check the 'Max Allowed HA Role' for each NO (SO). By default, it should be 'Active'. Otherwise, update the 'Max Allowed HA Role' as Active from Drop Down list. 5. Click the Ok button 6. Repeat sub-steps 2 through 5 for each SOAM.

4.7.11 Upgrade IPFE(s) – Site 1 (3-Tier, PDRA)

Procedure 65: Upgrade IPFE(s) – Site 1 (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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. Pick one "**IP Front End**" Server Group in Site 1. 2. Identify the servers in the Server Group identified in sub-step 1 above **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 of this procedure	Step 1: Upgrade IP Front End server using the Upgrade Multiple Servers procedure : **Execute Appendix K**-- Upgrade Multiple Servers After successfully completing the procedure in **Appendix K**, 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: root`
		`password: <enter password>`
		2. Execute the following command on the IPFE server :
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`
		The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to the next step** (step 4).
		Example output with highlight added (actual file names and numbers may vary):
		`[root@ISoak-en1-b10-IPFE ~]# 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 sub-step 3.
		Example output with highlight added (actual file names and numbers may vary):

Procedure 65: Upgrade IPFE(s) – Site 1 (3-Tier, PDRA)

		[root@ISoak-en1-b10-IPFE ~]# 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: 8 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 3. Execute the following commands. # /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # 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.** 4. Once the server is back online, log into the server and execute the following command: # /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, then contact the Oracle CGBU Customer Care Center.**
4 ☐	Repeat for all "**IP Front End**" servers	Repeat steps 1 through 3 of this procedure for each IPFE server.

4.7.12 Post Upgrade Wrap-Up – Site 1 (3-Tier, PDRA)

Execute this procedure after the site has been upgraded.

Procedure 66: Post Upgrade Wrap-Up – Site 1 (3-Tier, PDRA)

S T E P #	Post Upgrade steps after Site 1 is upgraded. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Enable global provisioning and configuration.	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**.
2 ☐	Enable site provisioning and configuration.	Enable Site provisioning after the upgrade is completed: 1. Log into the SOAM VIP GUI for the upgraded site. 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**
3 ☐	Execute FQDN – NE ID Mapping script	**NOTE: Execute this step if upgrading from a release < 4.0.5_41.6.0 to a release > 4.1.0-41.24.0.** 1. SSH into the Active NOAM using the XMI VIP IP Address: 2. Execute the following script **`#/var/TKLC/appworks/library/Pdra/scripts/syncFqdnReferences.sh`**
4 ☐	Truncate PDRA local table – TopoHidingListLocal (Only if source upgrade release was less than 4.1.0-41.24.0)	**NOTE: Execute this step if upgrading from a release < 4.1.0-41.24.0, to a release > 4.1.0-41.24.0.** **This procedure must be executed after the entire site has been upgraded.** 1. Download the script `truncateLocalTable.sh`. 2. Transfer the script file to **`/root`** of the Active SOAM Server. 3. Log into the Active SO upgraded in Site 1 : 4. Use an SSH client to connect to the upgraded server (e.g. ssh, putty): **`ssh <server address>`** **`login as: root`** **`password: <enter password>`** 5. Change directory to /root **`# cd /root`**

Procedure 66: Post Upgrade Wrap-Up – Site 1 (3-Tier, PDRA)

6. Convert the script to unix format:

```
# dos2unix truncateLocalTable.sh
```

7. Execute the following command to ensure that the script has the required permissions:

```
# chmod +x truncateLocalTable.sh
```

8. Execute the script:

```
# ./truncateLocalTable.sh
```

```
[root@sanityE3B01SOa ~]# ./truncateLocalTable.sh

== Start of Post upgrade procedure for release 5.1.0-51.10.0 (logs can be found in file /var/TKLC/db/filemgmt/PDRA_229070_UPGRAGE_LOG_
070404.txt) ==

Server Name of this system       : sanityE3B01SOa
Server Role of this system       : SYSTEM_OAM
HA State of this system          : Active
Network Element ID of this system : 1
-------------------------------------------------------------------------------
Finding DSR MP server with 'DbReplication' resource active within this site only...
Skipping sanityE3B03PDRA01 as the DbReplication role on this server is Stby
Applying post-upgrade procedure on sanityE3B04PDRA02 DSR MP Server ...


*************************************************************************************************************
*
* Policy DRA PostUpgrade Procedure for release 5.1.0-51.10.0 completed successfully!
*  Logs can be found at /var/TKLC/db/filemgmt/PDRA_229070_UPGRAGE_LOG_sanityE3B01SOa_20140129070404.txt
*
*************************************************************************************************************

=============================================================E-N-D=============================================
```

Analyze the Log file mentioned in the output to verify no errors are present.

4.7.13 Verify Post Upgrade Status – Site 1 (3-Tier, PDRA)

This procedure is part of the health check and is used to determine the health and status of the Policy DRA (DSR) network and servers after the upgrade. This procedure must also be executed after Site 1 has been upgraded to compare upgraded server data with pre-upgrade health check data captured in Procedure 5.

Procedure 67: Verify Post Upgrade Status – Site 1 (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Verify all servers status are normal	1. Log into the Active NOAM GUI using the VIP. 2. Select the **Status & Manage -> Server** menu item. 3. Verify all status is Normal (Norm) for all servers. 4. Do not proceed without consent from Engineering/ Consulting Services with the upgrade if any server status is not **Norm**. 5. Do not proceed without consent from Engineering/ Consulting Services if there are any unexpected 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 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.
2 ☐	Log all current alarms on Active NOAM VIP	**1.** Select the **Alarms & Events -> View Active** menu item. 2. Click the **Export** button to generate an Alarms Export file. 3. Record the filename of the Alarms CSV file generated and all the current alarms in the system. 4. Save this information on the client machine for future reference.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for site 1.**	1. Log into the SOAM GUI 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 this 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.

Procedure 67: Verify Post Upgrade Status – Site 1 (3-Tier, PDRA)

4 ☐	Capture the Policy SBR Status **On Active NOAM GUI**	From the Active NOAM GUI: 1. Select **Main Menu-> Policy DRA->Maintenance-> Policy SBR Status** 2. Capture and archive the maintenance status of the following tabs on the client machine either by taking screen captures or by documenting it in an editor. a. Binding Region b. PDRAMatedSites Save this data on the client machine. 3. Expand each Server Group. Verify **Congestion Level** is 'Normal' for all servers.
5 ☐	Verify PDRA status	View PDRA status. From the Active SOAM GUI: 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications
6 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Capture the IPFE Configuration Options Screens. On Active SOAM GUI on Site 1	From the Active SOAM GUI: 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 ☐	Capture the IPFE Configuration Target Set screens On Active SOAM GUI on Site 1	From the Active SOAM GUI: 1. Select **Main Menu: IPFE->Configuration->Target Sets** 2. Capture and archive the screen capture of the complete screens. 3. Save the captured data on the client machine.
10 ☐	Export and archive the Diameter and P-DRA configuration data. On Active SOAM GUI on Site 1	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter and P-DRA 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
11 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 NOAM to the client machine.
12 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Compare the health check status of the upgraded site as collected from steps 2 through 11 to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window		

4.7.14 Perform Site Backup – Site 2 (Pre-Upgrade, 3-Tier, PDRA)

This procedure is used to perform a backup of all servers associated with the site 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 68: Perform Site Backup – Site 2 (Pre-Upgrade, 3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup the configuration database from the Active SO server: 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 SO** 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 SO 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 ☐	SSH to the Active SO of Site 2	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active SO of Site 2: `ssh root@<SO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

3 ☐	Execute a backup of all servers (managed from this SO)	Execute the **backupAllHosts** utility on the Active SO of Site 2. [This utility will remotely access each specified server, and run the backup command for that server.]
		
		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.)
		
		`# /usr/TKLC/dpi/bin/backupAllHosts --hosts=<hostname1>,<hostname2>,<hostname3>`
		
		where <hostname1>,<hostname2>, etc. is a comma-separated list of hostnames of every server associated with the site being upgraded. **Note: Use commas with no spaces to separate the hostnames in the list.**

Procedure 68: Perform Site Backup – Site 2 (Pre-Upgrade, 3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**	

		The following output will be generated for DSR 5.1 servers only:
		`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.
		`# exit`
		(to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		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 Backup.dsr.blade01.FullRunEnv.NETWORK_OAMP.20110417_021502.UPG.tar.gz written in /var/TKLC/db/filemgmt.`

4.7.15 Perform Health Check - Site 2 (Pre-Upgrade, 3-Tier, PDRA, SOAM)

This procedure is used to perform a health check of the SOAM prior to upgrade.

Procedure 69: Perform Health Check - Site 2 (Pre-Upgrade, 3-Tier, PDRA, SOAM)

S T E P #	This procedure performs a Health Check before upgrading 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	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**. Note: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. **2.** Click the **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View DA-MP Status	View DA-MP status. 1. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 2. Select the **Peer DA-MP Status** tab. 3. Verify all Peer MPs are available 4. Select the **DA-MP Connectivity** tab. 5. Note the number of **Total Connections Established.**
4 ☐	Verify PDRA status	View PDRA status. 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications

4.7.16 Upgrade SOAM – Site 2 (3-Tier, PDRA)

The following procedure upgrades the Site 2 SOAM servers and TVOE - but only if a Site 2 SOAM is hosted on a blade for which the TVOE has not already been upgraded as part of Procedure 62.

Procedure 70: Upgrade SOAM – Site 2 (3-Tier, PDRA)

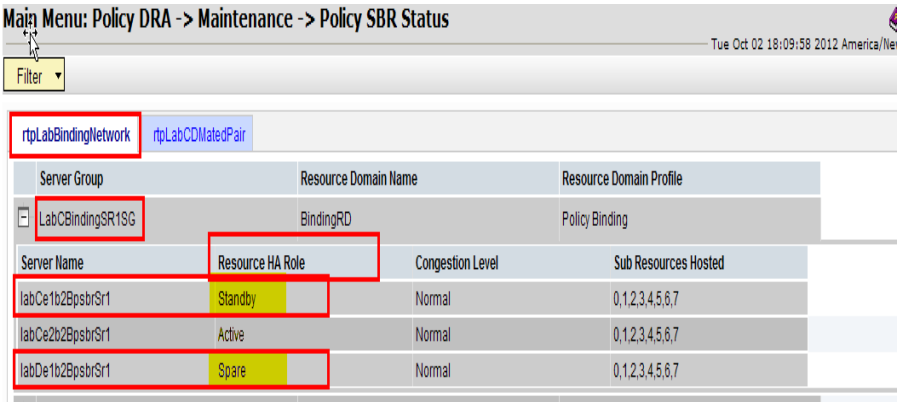
S T E P #	This procedure verifies that the SOAM server with TVOE platform upgrade steps have been completed, and upgrades the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Global Provisioning is disabled	Global Provisioning was disabled in Section 4.7.3, Upgrade TVOE and NOs (3-Tier, PDRA). Verify global provisioning is still disabled before upgrading Site 2. 1. Log into the NOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Global Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with step 2. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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**. 7. The Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Verify Site Provisioning is disabled	Site Provisioning was disabled in Section 4.7.3, Upgrade TVOE and NOs (3-Tier, PDRA). Verify that site provisioning for the site being upgraded is still disabled. 1. Log into the SOAM GUI using the VIP 2. In the GUI status bar, where it says "Connected using …", check for the message "Site Provisioning disabled" **If the message is not present, then execute the following sub-steps;** otherwise, continue with step 3. 3. Select **Status & Manage > Database.** The Database Status screen is displayed 4. Click the **Disable Site Provisioning** button. 5. Confirm the operation by clicking **Ok** in the popup dialog box. 6. 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 platform on SOAM blades	1. Determine if the blade hosting the SOAM requires an upgrade of the TVOE Host (See Appendix E). If an upgrade is required, perform Appendix J.

Procedure 70: Upgrade SOAM – Site 2 (3-Tier, PDRA)

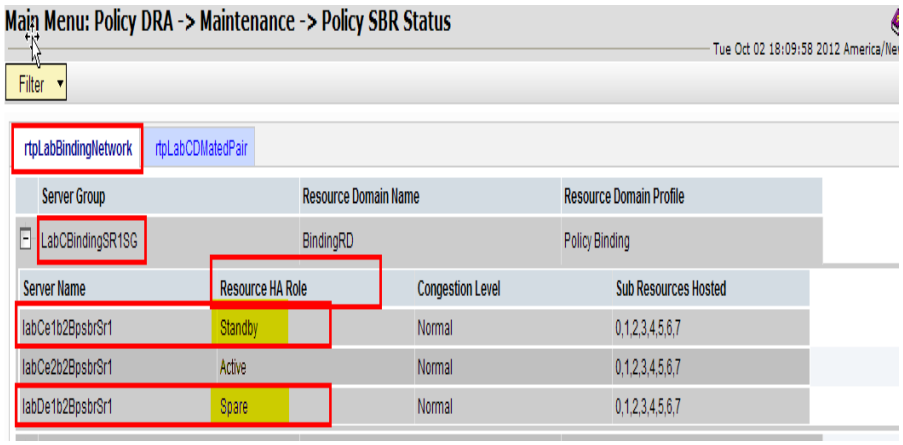
4 ☐	Upgrade Standby SO and Spare SO in parallel.	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Hosts if the Standby DSR SO and/or Spare DSR SO are hosted on TVOE blades. **Note: the Spare SO of this triplet will be located at a different site.** 1. Upgrade the standby SO and Spare SO servers using the Upgrade Multiple Server procedure : **Execute Appendix K—**Upgrade Multiple Servers Procedure After successfully completing the procedure in **Appendix K**, return to this point and continue with the next step.
5 ☐	Upgrade Active DSR SO.	Note: Before proceeding with this step, execute Appendix J to upgrade the TVOE Host if the Active DSR SO is hosted on a TVOE blade. 1. Upgrade the Active DSR SO server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next procedure.
6 ☐	Install NetBackup on NO and SO (If required)	If Netbackup is to be installed on the DSR, execute the procedure in Appendix I. Note: In DSR 5.0, the backup file location is changed from `/var/TKLC/db/filemgmt` to `/var/TKLC/db/filemgmt/backup`. The Netbackup server configuration must to be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.

4.7.17 Upgrade Policy SBR – Site 2 (3-Tier, PDRA)

Procedure 71: Upgrade Policy SBR – Site 2 (3-Tier, PDRA)

S T E P #	Policy SBR 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify the pSBR Server Group to Upgrade	From the data captured in Table 3. 1. Pick the "**Policy SBR**" Server Group (e.g. Binding pSBR Server Group, **or** multiple server groups). One server group can be upgraded at one time or multiple server groups can be upgraded simultaneously. 2. Identify the Server Group(s) in site 2 selected for upgrade in sub-step 1. 3. Login into the NOAM using the VIP. 5. Navigate to **Main Menu -> Policy DRA->Maintenance->Policy 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: **labCe2b2BpsbrSr1 - Active** **labCe1b2BpsbrSr1 - Standby** **labDe1b2BpsbrSr1 - Spare**  **Note: Policy 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 Policy SBR Status screen MUST be used to determine the high availability status (Active, Standby, or Spare) of pSBR 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 71: Upgrade Policy SBR – Site 2 (3-Tier, PDRA)

2 ☐	Upgrade Spare Policy SBR Server as identified in Step 1 of this procedure.	**Note: The Spare P-SBR of this triplet will be located at a different site.** 1. Upgrade the Spare Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G**—Upgrade Single Server Procedure After successfully completing the procedure in **Appendix G**, return to this point to monitor server status. 2. Navigate to **Main Menu > Policy DRA > Maintenance > Policy SBR Status**. Open the tab of the server group being upgraded. 3. Monitor the **Resource HA Role** status of the Spare server. Do not proceed to step 3 until the **Resource HA Role** of the Spare pSBR server is **Spare**.
3 ☐	Upgrade Standby Policy SBR Server identified in step 1 of this procedure.	1. Upgrade the Standby Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G**—Upgrade Single Server Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
		**WARNING!** **Failure to comply with step 4 and Step 5 may result in the loss of Policy DRA traffic, resulting in service impact**
4 ☐	Verify Standby pSBR server status	From the Active NOAM GUI: 1. Navigate to **Main Menu -> Policy DRA->Maintenance->Policy 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**. 

Procedure 71: Upgrade Policy SBR – Site 2 (3-Tier, PDRA)

5 ☐	Verify that bulk download is complete between Active Policy SBR in server group to Standby Policy SBR and Spare Policy 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 Policy SBR group that is in upgrade **Display Filter**: Event ID = 31127 **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: a. 2 for the Standby Policy SBR for both binding and session policies b. 2 for the Spare Policy SBR server for both binding and session policies. 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 Policy SBR Server as identified in Step 1 in this procedure	1. Upgrade the Active Policy SBR server using the Upgrade Single Server procedure : **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
7 ☐	Repeat 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.

4.7.18 Upgrade Multiple DA-MPs – Site 2 (3-tier, PDRA)

Procedure 72: Upgrade Multiple DA-MPs – Site 2 (3-tier, PDRA)

S T E P #	Policy DRA 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 in Server Group **identified in sub-step 1.**

Procedure 72: Upgrade Multiple DA-MPs – Site 2 (3-tier, PDRA)

2 ☐	Upgrade Policy DRA Server as identified in Step 1	1. Upgrade half of the Policy DRA (DA-MP) servers in parallel using the Upgrade Multiple Server procedure : **Note: It is recommended that the DA-MP Leader be upgraded in the last group of servers to minimize DA-MP Leader role changes.** **Execute Appendix K : Upgrade Multiple Servers** After successfully completing the procedure in **Appendix K**, return to this point and continue with the next step.
3 ☐	Repeat step 2 for all servers identified in Step 1 in this procedure.	Repeat step 2 in this procedure for the remaining Policy DRA (DA-MP) servers.
4 ☐	Update Max Allowed HA Role for NO and SO.	1. Log into the NOAM GUI using the VIP 2. Go to the **Status & Manage-> HA** screen. 3. Click the **Edit** button. 4. Check the '**Max Allowed HA Role**' for each NO (SO). By default, it should be '**Active**'. Otherwise, update the '**Max Allowed HA Role**' as Active from Drop Down list. 5. Click the **Ok** button 6. Repeat sub-steps 2 through 5 for each SOAM.

4.7.19 Upgrade IPFE(s) – Site 2 (3-Tier, PDRA)

Procedure 73: Upgrade IPFE(s) – Site 2 (3-Tier, PDRA)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 2. 2. Identify the servers 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 K**-- Upgrade Multiple Servers After successfully completing the procedure in **Appendix K**, 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>`

Procedure 73: Upgrade IPFE(s) – Site 2 (3-Tier, PDRA)

```
login as:       root
password:    <enter password>
```

2. Execute the following command on the IPFE server :

```
# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify
```

The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to the next step** (step 4).

Example output with highlight added (actual file names and numbers may vary):

```
[root@ISoak-en1-b10-IPFE ~]# 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 sub-step 3.

Example output with highlight added (actual file names and numbers may vary):

```
[root@ISoak-en1-b10-IPFE ~]# 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: 8
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
```

3. Execute the following commands.

```
# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh
# 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.

Procedure 73: Upgrade IPFE(s) – Site 2 (3-Tier, PDRA)

		4. Once the server is back online, log into the server and execute the following command: `# /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, then contact the Oracle CGBU Customer Care Center.**
4 ☐	Repeat steps 1 through 3 for all "**IP Front End**" servers	Repeat steps 1 through 3 for the remaining IPFE servers.

4.7.20 Post Upgrade Wrap-up – Site 2 (3-Tier, PDRA)

Procedure 74: Post Upgrade Wrap-up – Site 2 (3-Tier, PDRA)

S T E P #	Post Upgrade Steps 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Enable global provisioning and configuration.	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**.
2 ☐	Enable site provisioning and configuration.	Enable Site provisioning after the upgrade is completed: 1. Log into the SOAM VIP GUI for the upgraded site. 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**

3 ☐	Install backward compatibility path	**NOTE: This step is only applicable to following upgrade path:**
		Source Release: DSR Release < 4.1.0_41.15.0
		Target DSR Release >= 4.1.0_41.15.2
		1. Transfer the /pub/Engineering/Nextgen/PdraPatches/install_backward_compat_patch.sh file to /root of the Active NOAM Server **:**
		a) Login (SSH) to the Active NOAM Server
		b) Change the directory using the command:
		`cd /root`
		c) Convert the file to Unix format:
		`#dos2unix install_backward_compat_patch.sh`
		`install_backward_compat_patch.sh`
		d) Set permissions to executable
		`chmod +x install_backward_compat_patch.sh`
		e) Run the script:
		`./install_backward_compat_patch.sh`

4 ☐	Truncate PDRA local table – TopoHidingListLocal (Only if source upgrade release was less than 4.1.0-41.24.0)	**NOTE: Execute this step if upgrading from a release < 4.1.0-41.24.0, to a release > 4.1.0-41.24.0.** **This procedure must be executed after the entire site has been upgraded.** 1. Download the script `truncateLocalTable.sh`. 2. Transfer the script file to `/root` of the Active SOAM Server. 3. Log into Active SO upgraded in Site 1 :

Procedure 74: Post Upgrade Wrap-up – Site 2 (3-Tier, PDRA)

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

```
ssh <server address>

login as:  root
password:  <enter password>
```

4. Change directory to /root

```
# cd /root
```

5. Convert the script to unix format:

```
# dos2unix truncateLocalTable.sh
```

6. Execute the following command to ensure that the script has the required permissions:

```
# chmod +x truncateLocalTable.sh
```

7. Execute the script:

```
# ./truncateLocalTable.sh
```

```
[root@sanityE3B01SOa ~]# ./truncateLocalTable.sh

== Start of Post upgrade procedure for release 5.1.0-51.10.0 (logs can be found in file /var/TKLC/db/filemgmt/PDRA_229070_UPGRAGE_LOG_sanityE3B0
070404.txt) ==

Server Name of this system       : sanityE3B01SOa
Server Role of this system       : SYSTEM_OAM
HA State of this system          : Active
Network Element ID of this system : 1
--------------------------------------------------------------------------------
Finding DSR MP server with 'DbReplication' resource active within this site only...
Skipping sanityE3B03PDRA01 as the DbReplication role on this server is Stby
Applying post-upgrade procedure on sanityE3B04PDRA02 DSR MP Server ...


********************************************************************************************************************
*
* Policy DRA PostUpgrade Procedure for release 5.1.0-51.10.0 completed successfully!
*  Logs can be found at /var/TKLC/db/filemgmt/PDRA_229070_UPGRAGE_LOG_sanityE3B01SOa_20140129070404.txt
*
********************************************************************************************************************


=====================================================E-N-D=====================================================
```

Analyze the Log file mentioned in output to make sure no errors are present.

4.7.21 Verify Post Upgrade Status – Site 2 (3-Tier, PDRA)

This procedure is part of the Post Maintenance Window 3 health check. This procedure determines the health and status of the Policy DRA (DSR) network and servers once Site 2 is upgraded completely. These steps compare data captured after the upgrade with pre-upgrade health check data captured in Procedure 5.

Procedure 75: Verify Post Upgrade Status – Site 2 (3-Tier, PDRA)

S T E P #	This procedure verifies Post Upgrade Status Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify server status is normal	1. Log into the NOAM GUI using VIP 2. Select the **Status & Manage -> Server** menu item. 3. Verify server status is Normal (Norm) for all servers. 4. If any server's status is not **Norm,** do not proceed with the upgrade without consent from the Oracle CGBU Customer Care Center. 5. If there are any unexpected Major or Critical alarms, do not proceed with the upgrade without consent from the Oracle CGBU Customer Care Center. 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.
2 ☐	Log all current alarms Active NOAM VIP **on site 2.**	1. Select the **Alarms & Events -> View Active** menu item. 2. Click the **Export** button to generate an Alarms Export file. 3. Record the filename of the Alarms CSV file generated and all the current alarms in the system. 4. Save this information on the client machine for future reference.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP of site 2).**	1. Log into the SOAM GUI 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 this information 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

Procedure 75: Verify Post Upgrade Status – Site 2 (3-Tier, PDRA)

		22. Select the **DA-MP Connectivity** tab. 23. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count.
4 ☐	Capture the Policy SBR Status **On Active NOAM GUI**	From the Active NOAM GUI: 1. Select **Main Menu-> Policy DRA->Maintenance-> Policy SBR Status** 2. Capture and archive the maintenance status of the following tabs on the client machine either by taking screen captures or documenting it in an editor. a. BindingRegion b. PDRAMatedSites 3. Save this information on the client machine. 4. Expand each Server Group. Verify **Congestion Level** is 'Normal' for all servers.
5 ☐	Verify PDRA status	View PDRA status. From the Active SOAM GUI: 1. Select **Diameter > Maintenance > Applications** 2. Verify Operational Status is '**Available**' for all applications
6 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
7 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
8 ☐	Capture the IPFE Configuration Options Screens. On Active SOAM GUI on Site 2.	From the Active SOAM GUI: 1. Select **Main Menu -> IPFE->Configuration->Options** 2. Capture and archive the screen capture of the complete screen. 3. Save the capture on the client machine.
9 ☐	Capture the IPFE Configuration Target Set screens On Active SOAM GUI on Site 2	From the Active SOAM GUI: 1. Select **Main Menu -> IPFE->Configuration->Target Sets** 2. Capture and archive the screen capture of the complete screens. 3. Save the capture on the client machine.
10 ☐	Export and archive the Diameter and P-DRA configuration data. On Active SOAM GUI on Site 2	From the Active SOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter and P-DRA 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
11 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded site	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 NOAM to the client machine.

Procedure 75: Verify Post Upgrade Status – Site 2 (3-Tier, PDRA)

12 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the third maintenance window.	Compare the health check status of the upgraded site as collected in steps 2 through 11 to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window		

4.8 DSR Site Upgrade (2-Tier, 1+1)

This section contains major upgrade procedures for a DSR 4.x -> 5.1 (2-tier setup) upgrade with the (1+1) (Active/Standby) configuration, and for a DSR 5.1 incremental upgrade for the (1+1) 2-tier configuration.

Table 19 specifies estimated Elapsed Times with TVOE upgrade and without TVOE upgrade. In some setups, NO(s) are hosted on TVOE blades. TVOE applications also sometimes need to be upgraded. Hence TVOE upgrade estimates are included in a separate column.

Table 19. Upgrade Execution Overview (2-Tier, 1+1).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 77	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 2-Tier, 1+1, NOAM)	None
Procedure 78	0:30-1:00	0:31-1:05	1:30-2:00	1:31-2:05	Upgrade NOAMs (2-Tier, 1+1)	Provisioning Disabled, No Traffic Impact
Procedure 79	0:01-0:05	0:32-1:10	0:01-0:05	1:32-2:10	Verify Post Upgrade Status (2-Tier, 1+1, NOAM)	No Traffic Impact
Procedure 80	0:30-1:00	1:02-2:10	0:30-1:00	2:02-3:10	Upgrade DA-MPs (2-Tier, 1+1)	Provisioning Enabled, No Traffic Impact
Procedure 81	0:01-0:05 Per MP	1:04-3:30	0:01-0:05 Per MP	2:04-4:30	Verify Post Upgrade Status (2-Tier, 1+1)	None

4.8.1 Pre-Upgrade Checks (2-Tier, 1+1)

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

Procedure 76: Pre-Upgrade Checks (2-Tier, 1+1)

S T E P #	This procedure verifies that the NOAM is ready for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**Verify that a recent version of the Full DB backup has been performed**	Verify that a recent version of the Full DB backup has been performed.
		
		1. Log into the NOAM GUI using the VIP.
		2. Select **Status and Manage → Files**
		3. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.8.2 Perform Health Check (Pre-Upgrade, 2-Tier, 1+1, NOAM)

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

WARNING!

THE NOAM(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.

THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.

Procedure 77: Perform Health Check (Pre-Upgrade, 2-Tier, 1+1, NOAM)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
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 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 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.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. 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.

Procedure 77: Perform Health Check (Pre-Upgrade, 2-Tier, 1+1, NOAM)

4 ☐	View DA-MP Status	View DA-MP status. 1. Log into the SOAM GUI using the VIP. 2. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 3. Select the **Peer DA-MP Status** tab. 4. Verify all Peer MPs are available 5. Select the **DA-MP Connectivity** tab. 6. Note the number of Total Connections Established

4.8.3 Upgrade NOAMs (2-Tier, 1+1)

Detailed steps are shown in the procedure below.

Procedure 78: Upgrade NOAMs (2-Tier, 1+1)

S T E P #	This procedure verifies that the NOAM upgrade steps have been completed. This procedure is specific to 2-tier DSR OAM deployments. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Disable global provisioning and configuration.	Disable Global Provisioning and Configuration updates on the entire network: 1. Log into the NOAM VIP GUI. 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**. 6. The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Upgrade TVOE Host (if needed)	If the TVOE Host for the Standby NO is to be upgraded. **Execute Appendix J** to upgrade the TVOE Host for the standby NO.
3 ☐	Upgrade Standby NO server (using Upgrade Single Server procedure).	**Execute Appendix G** –Single Server Upgrade for the Standby NO After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Upgrade TVOE Host (if needed) .	If the TVOE Host for the Active NO is to be upgraded. **Execute Appendix J** to upgrade the TVOE Host for the active NO.

Procedure 78: Upgrade NOAMs (2-Tier, 1+1)

5 ☐	Upgrade Active NO server.	For the Active NO, **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next sub-step. The NOAM GUI will show the new DSR 5.1 release. Expected Alarms include: Active NO server: Alarm ID = 10008 (Provisioning Manually Disabled)
6 ☐	Install NetBackup on NO (If required)	If Netbackup is to be installed on the DSR, execute the procedure found in Appendix I. **Note: In DSR 5.1, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`. **The Netbackup server configuration must be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.**

4.8.4 Verify Post Upgrade Status (2-Tier, 1+1, NOAM)

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

Procedure 79: Verify Post Upgrade Status (2-Tier, 1+1, NOAM)

S T E P #	This procedure verifies the NOAM status following the upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status	Execute the following commands on both the Active and Standby NOAM servers: 1. Use an SSH client to connect to the upgraded server (e.g. ssh, putty): **ssh < NO XMI IP address > login as: root password: <enter password>** Note: XMI IP address for the NO server should be available in Table 3. **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. Contact the Oracle CGBU Customer Care Center if any errors are observed. Note: It is safe to ignore this error if it appears after upgrade from DSR 4.x to 5.1: ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors! ERROR: 1347523804::ERROR-{HA::Mgr}: No Clusternode found for resource entry, (tklc-ha-active)! 1347523805::ERROR-{HA::Mgr}: Failed to initialize ResourceConf! 2. Servers have the following expected alarms: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) On all upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** **Note : If Alarm ID 32532 is not raised on any upgraded server, then execute following commands on that server to check for the existence of the alarm :** **# alarmMgr --alarmstatus** The following output will be raised : **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** 3. Alarm ID 32532 will be cleared once Procedure 90 is executed to accept the upgrade on each server.

Procedure 79: Verify Post Upgrade Status (2-Tier, 1+1, NOAM)

2 ☐	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). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4 ☐	View Communication Agent status	View Communication Agent status for all connections. 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 ☐	View DA-MP Status	View DA-MP status. 1. Log into the SOAM GUI using the VIP. 2. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 3. Select the **Peer DA-MP Status** tab. 4. Verify all Peer MPs are available 5. Select the **DA-MP Connectivity** tab. 6. Verify the number of Total Connections Established is consistent with the pre-upgrade connection count.
6 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.

4.8.5 Upgrade DA-MPs (2-Tier, 1+1)

This procedure upgrades the 2-Tier DA-MP(s).

Procedure 80: Upgrade DA-MPs (2-Tier, 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify and Record the status of the DA-MP before upgrade	Verify and record the status of each DA-MP Server by going to **Status & Manage -> HA** and record the hostname of the Active DA-MP server and the Standby DA-MP server. 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 ☐	Upgrade the standby DA-MP server (using Upgrade Single Server procedure)	Upgrade the Standby DA-MP server using the Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
3 ☐	Upgrade the active DA-MP server.	Upgrade the Active DA-MP server using the Upgrade Single Server procedure. **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
4 ☐	Enable global provisioning and configuration.	Enable provisioning and configuration updates on the entire network: Provisioning and configuration updates may be enabled to 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. Verify the text of the button changes to **Disable Provisioning.**
5 ☐	Update Max Allowed HA Role for NO	1. Go to the **Status & Manage-> HA** screen. 2. Click the **Edit** button. 3. Check the 'Max Allowed HA Role' for the NO. By default, it should be 'Active'. If not, update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click the **Ok** button.

4.8.6 Verify Post Upgrade Status (2-Tier, 1+1)

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

Procedure 81: Verify Post Upgrade Status (2-Tier, 1+1)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	Verify Server Status is Normal	Verify Server Status is Normal:
		
		1. Log into the Active 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), High Availability (HA), and Processes (Proc).
		3. Execute the following commands on all upgraded DA-MP servers :
		
		Use an SSH client to connect to the upgraded DA-MP server (e.g. ssh, putty):
		
		`ssh <DA-MP server XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# verifyUpgrade`
		
		Examine the output of the above command. If any errors were reported, contact the Oracle CGBU Customer Care Center.

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Select **Alarms & Events > View Active.**
		The Alarms & Events > View Active screen is displayed.
		
		The following Alarm ID will be observed on all the upgraded servers :
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note : If Alarm ID 32532 is not raised on any of the upgraded servers, then execute the following commands on that server to check the existence of the alarm :
		
		`# alarmMgr --alarmstatus`
		
		The following output shall be raised :
		
		`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`
		
		2. Alarm ID 32532 will be cleared once Procedure 90is executed to accept the upgrade on each server.
		
		3. Click the **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

Procedure 81: Verify Post Upgrade Status (2-Tier, 1+1)

3 ☐	Capture the Diameter Maintenance Status **On Active NOAM VIP for upgraded setup.**	1. Log into the SOAM GUI 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 this 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.
4 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded setup	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 NOAM to the client machine. 5. Select **Diameter > Maintenance > Applications** 6. Verify Operational Status is '**Available**' for all applications
6 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.
7 ☐	Compare this data to the Pre-Upgrade health check to verify if the system has degraded after the first maintenance window.	Compare the health check status of the upgraded servers to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.

4.9 DSR Site Upgrade (2-Tier, N+0)

This section contains major upgrade procedures for a DSR 4.x->5.1 (2-tier setup) upgrade with the (N+0) (Active/Standby) configuration, and for a DSR 5.1 incremental upgrade for the 2-tier (N+0) configuration.

Table 20 specifies estimated Elapsed Times with TVOE upgrade and without TVOE upgrade. In some setups, NO(s) are hosted on TVOE blades. TVOE applications also sometimes need to be upgraded. Hence TVOE upgrade estimates are included in a separate column.

Table 20. Upgrade Execution Overview (2-Tier, N+0).

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 83	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade, 2-Tier, N+0, NOAM)	None
Procedure 84	0:25-1:00	0:26-1:05	1:25-2:00	1:26-2:05	Upgrade NOAM (2-Tier, N+0)	Provisioning Disabled, No Traffic Impact
Procedure 85	0:02-0:05	0:28-1:10	0:02-0:05	1:28-2:10	Verify Post Upgrade Status (2-Tier, N+0, NOAM)	No Traffic Impact
Procedure 86	0:20-1:00	0:48-2:10	0:20-1:00	1:48-3:10	Upgrade Multiple DA-MPs (2-Tier, N+0)	Traffic will not be handled by the MP(s) being upgraded.
Procedure 87	0:20-1:00	1:08-3:10	0:20-1:00	2:08-4:10	Upgrade IPFE(s) (2-Tier, N+0)	Provisioning Enabled, No Traffic Impact
Procedure 88	0:01-0:05 Per MP	1:09-4:30	0:01-0:05 Per MP	2:09-5:30	Verify Post Upgrade Status (2-Tier, N+0)	None

4.9.1 Pre-Upgrade Checks (2-Tier, N+0)

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

Procedure 82: Pre-Upgrade Checks (2-Tier, N+0)

S T E P #	This procedure verifies that the NOAM is ready for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**Verify that a recent version of the Full DB backup has been performed**	Verify that a recent version of the Full DB backup has been performed.
		
		1. Log into the NOAM GUI using the VIP.
		2. Select **Status and Manage → Files**
		3. Check time stamp on the following files:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		See section 3.3.5 to perform (or repeat) a full Backup, if needed.

4.9.2 Perform Health Check (Pre-Upgrade, 2-Tier, N+0, NOAM)

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

WARNING!

THE NOAM(s) (and DR-NOAMs) MUST BE UPGRADED IN THE SAME MAINTENANCE WINDOW.

THE SOAM SITE(s) SHOULD BE UPGRADED SUBSEQUENTLY, EACH SITE IN ITS OWN MAINTENANCE WINDOW.

Procedure 83: Perform Health Check (Pre-Upgrade, 2-Tier, N+0, NOAM)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
	Start of maintenance window	
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 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.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	View Communication Agent status	View Communication Agent status for all connections. 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.
4 ☐	View DA-MP Status	View DA-MP status. 1. Log into the SOAM GUI using the VIP. 2. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 3. Select the **Peer DA-MP Status** tab. 4. Verify all Peer MPs are available 5. Select the **DA-MP Connectivity** tab. 6. Note the number of **Total Connections Established**

4.9.3 Upgrade NOAM (2-Tier, N+0)

Detailed steps are shown in the procedure below.

Procedure 84: Upgrade NOAM (2-Tier, N+0)

S T E P #	This procedure is used to upgrade the NOAM(s). This procedure is specific to 2-tier DSR OAM deployments. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: Log into the NOAM GUI using the VIP. 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**. 5. The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Upgrade Standby NO server (using Upgrade Single Server procedure).	1. If the TVOE Host for the Standby NO is to be upgraded, **Execute Appendix J** to upgrade the TVOE Host 2. Upgrade the **Standby** NO**:** **Execute Appendix G –** Upgrade Single Server procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
3 ☐	Upgrade Active NO TVOE server.	1. If the TVOE Host for the Active NO is to be upgraded, **Execute Appendix J** to upgrade the TVOE Host
4 ☐	Upgrade Active NO server.	1. Upgrade the Active NO server (the mate) using the Upgrade Single Server procedure: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in **Appendix G**, return to this point and continue with the next step.
5 ☐	Install NetBackup 7.5 on NO (If required).	If Netbackup is to be installed on the DSR, execute the procedure found in Appendix I. **Note: In DSR 5.1, the backup file location is changed from** `/var/TKLC/db/filemgmt` **to** `/var/TKLC/db/filemgmt/backup`**. The Netbackup server configuration must be updated to point to the correct file path. Updating the Netbackup server configuration is out of scope of this upgrade document.**

4.9.4 Verify Post Upgrade Status (2-Tier, N+0, NOAM)

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

Procedure 85: Verify Post Upgrade Status (2-Tier, N+0, NOAM)

S T E P #	This procedure verifies the NOAM status following the upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	Verify Server Status	Verify Server Status after the NOAM servers are upgraded:
		1. Execute the following commands on both the Active and Standby NOAM servers:
		Use an SSH client to connect to the upgraded NOAM server (e.g. ssh, putty):
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		Note: The static XMI IP address for each NOAM server should be available in Table 3
		`# verifyUpgrade`
		Examine the output of the above command to determine if any errors were reported. Contact the Oracle CGBU Customer Care Center if any errors are observed.
		2. Log into the Active NOAM VIP GUI and select the **Alarms & Events-> View Active** screen to verify alarms. Servers have following expected alarms:
		Active NO server:
		Alarm ID = **10008** (Provisioning Manually Disabled)
		All upgraded servers :
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		Note : If Alarm ID 32532 is not raised on any of the upgraded servers, then execute following commands on that server to check for the existence of the alarm :
		`# alarmMgr --alarmstatus`
		The following output will be raised :
		`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`
		Contact the Oracle CGBU Customer Care Center in case above output is not raised.
		3. Alarm ID 32532 will be cleared once Procedure 90is executed to accept the upgrade on each server.

Procedure 85: Verify Post Upgrade Status (2-Tier, N+0, NOAM)

2 ☐	Verify Server Status is Normal	Verify Server Status is Normal: **1.** Select **Status & Manage > Server.** The Server Status screen is displayed. **2.** Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
3 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
4 ☐	View Communication Agent status	View Communication Agent status for all connections. 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 ☐	View DA-MP Status	View DA-MP status. 1. Log into the SOAM GUI using the VIP. 2. Select **Diameter > Maintenance > DA-MPs**. The DA-MP status screen is displayed. 3. Select the **Peer DA-MP Status** tab. 4. Verify all Peer MPs are available 5. Select the **DA-MP Connectivity** tab. 6. Verify the number of **Total Connections Established** is consistent with the pre-upgrade connection count.
6 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.

Procedure 85: Verify Post Upgrade Status (2-Tier, N+0, NOAM)

7 ☐	Update Appworks NetworkDeviceOption Table for the configured IPFE Ethernet devices on the Active NO 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 NO 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** 2. Log into Active NO console and execute the following command: **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** NOTE: This command may execute without any output if no changes are required (no devices were found to update).

4.9.5 Upgrade Multiple DA-MPs (2-Tier, 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. During upgrade, 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: successfully upgrade the DA-MPs in one enclosure first. Then upgrade the DA-MPs in the second enclosure. This approach ensures that service is not affected.

Procedure 86 **must be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. That is, if 16 DA-MPs are upgraded four at a time, then** Procedure 86 **must be executed four distinct times.**

Procedure 86: Upgrade Multiple DA-MPs (2-Tier, N+0)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify DA-MPs to be upgraded together.	Identify all DA-MPs to be upgraded together. **Note: The user can choose any number of MP(s) to be upgraded in parallel, depending upon the configuration.**
2 ☐	Upgrade Active MPs	Upgrade the selected DA-MPs, executing the Upgrade Single Server procedure on all selected DA-MPs in parallel. **Execute Appendix K** -- eMultiple Server Upgrade Procedure After successfully completing the procedure in Appendix K for all selected DA-MPs, return to this point and continue with the next step.
3 ☐	Repeat DA-MP upgrade	Repeat steps 1 and 2 for the next set of DA-MPs to be upgraded.
4 ☐	Update Max Allowed HA Role for NO.	1. Log into the Active NOAM GUI using the VIP. 2. Go to **Status & Manage-> HA screen**. 3. Click the **Edit** button. 4. Check the 'Max Allowed HA Role' for all NO(s). By default, it should be 'Active'. If not, update the 'Max Allowed HA Role' as Active from the Drop Down list. 5. Click the **Ok** button.

4.9.6 Upgrade IPFE(s) (2-Tier, N+0)

If none of the signaling Network Elements in the DSR being upgraded has IPFE servers installed, skip this section and proceed to the next procedure. Otherwise, Procedure 87 must be executed independently for each signaling Network Element that has IPFE servers installed.

Procedure 87: Upgrade IPFE(s) (2-Tier, 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Identify IPFE upgrade order	Choose the number of IPFEs on which upgrade can be executed in parallel, considering traffic impacts. All chosen IPFEs should belong to the same enclosure. Only after the first enclosure has been successfully upgraded should the IPFE(s) in the second enclosure be upgraded.
2 ☐	Upgrade IPFE servers (if exists)	Upgrade the IPFEs identified in step 1 in parallel, using the Upgrade Single Server procedure. 1. Execute **Appendix G** -- Single Server Upgrade Procedure

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	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: root`
		`password: <enter password>`
		2. Execute the following command on the IPFE server :
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh –verify`
		The outcome of the above command will indicate the number of lines that need to change. If the count is **ZERO**, then **proceed to the next step** (step 4).
		Example output with highlight added (actual file names and numbers may vary):
		`[root@ISoak-en1-b10-IPFE ~]# 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 sub-step 3.
		Example output with highlight added (actual file names and numbers may vary):
		`[root@ISoak-en1-b10-IPFE ~]# 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`

Procedure 87: Upgrade IPFE(s) (2-Tier, N+0)

		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: 8 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 3. Execute the following commands. # /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # 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.** 4. Once the server is back online, log into the server and execute the following command: # /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, then contact the Oracle CGBU Customer Care Center.**
4 ☐	Repeat for all IPFE servers	Repeat steps 1 through 3 for the remaining IPFE servers.
5 ☐	Enable global provisioning and configuration.	Enable 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. Verify the text of the button changes to **Disable Provisioning**.

4.9.7 Verify Post Upgrade Status (2-Tier, N+0)

This procedure is used to determine the health and status of the MP servers. This includes all DA-MPs and IPFE servers.

Procedure 88: Verify Post Upgrade Status (2-Tier, N+0)

S T E P #	This procedure verifies Post Upgrade Status (N+0, 2-Tier) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	**SSH MP Server:** 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).
		3. Execute the following commands on the upgraded MP servers (both IPFE and DA-MPs) :
		
		Use an SSH client to connect to the upgraded server (e.g. ssh, putty):
		
		`ssh <MP IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# verifyUpgrade`
		
		Examine the output of the above command, and determine if any errors were reported. Contact the Oracle CGBU Customer Care Center in case of errors.
		
		`# alarmMgr --alarmstatus`
		
		The following output will be raised, 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`

2 ☐	**NO GUI:** Verify Alarm status	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/or print the report. Keep these copies for future reference. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

Procedure 88: Verify Post Upgrade Status (2-Tier, N+0)

3 ☐	Capture the Diameter Maintenance Status **On NOAM VIP for upgraded setup.**	1. Log into the Active NOAM GUI 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 this information 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.
4 ☐	Capture the IPFE Configuration Options Screens. On upgraded setup.	1. Select **Main Menu -> IPFE->Configuration->Options** 2. Capture and archive the screen capture of the complete screen. 3. Save this information on the client machine.
5 ☐	Capture the IPFE Configuration Target Set screens On upgraded setup.	1. Select **Main Menu -> IPFE->Configuration->Target Sets** 2. Capture and archive the screen capture of the complete screens. 3. Save this information on the client machine.
6 ☐	View Communication Agent status	View Communication Agent status for all connections. From the Active NOAM GUI: 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.
7 ☐	Export and archive the Diameter configuration data. On Active NOAM GUI on upgraded setup	From the Active NOAM GUI: 1. Select **Main Menu-> Diameter Configuration->Export** 2. Capture and archive the Diameter 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 NOAM to the client machine. 5. Select **Diameter > Maintenance > Applications** 6. Verify Operational Status is '**Available**' for all applications
8 ☐	Verify Traffic status	From the Active SOAM GUI, inspect KPI reports to verify traffic is at the expected condition.

Procedure 88: Verify Post Upgrade Status (2-Tier, N+0)

9 ☐	Compare this data to the Pre-Upgrade health check to verify if the system has degraded after the upgrade maintenance window.	Compare the health check status of the upgraded server to the pre-upgrade health check taken in Procedure 5. If it is any worse, report it to the Oracle CGBU Customer Care Center.
End of maintenance window.		

4.10 Post-Upgrade Procedures

The post-upgrade procedures consist of a final Health Check of the system prior to accepting the upgrade.

4.10.1 Perform Post-Upgrade Health Check

Procedure 89: Perform Post-Upgrade Health Check

S T E P #	This procedure performs Post Upgrade 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
	Start of maintenance window	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: **1.** Log into the Active 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).
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.
3 ☐	Check if the setup previously has a customer supplied Apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	1. If the setup had a customer-supplied Apache certificate installed and protected with passphrase before the start of the upgrade (refer to Procedure 4), then rename the certificate back to the original name.

4.10.2 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. The Alarm 32532 (Server Upgrade Pending Accept/Reject) will be displayed for each server until one of these two actions is performed.

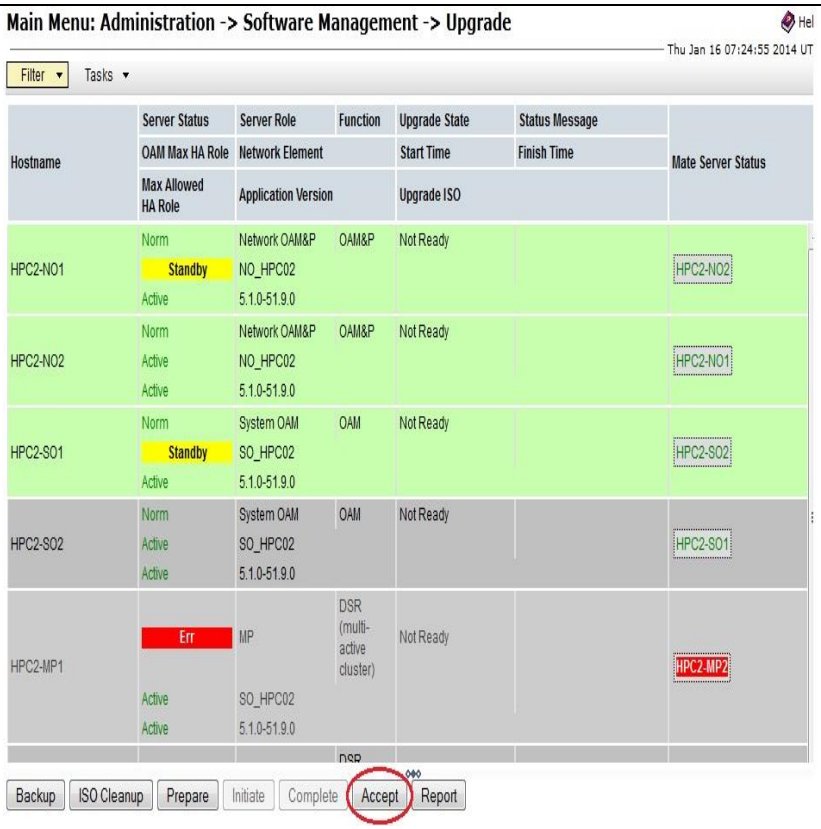
An upgrade should be accepted only after it was determined to be successful as the Accept is final. This frees up file storage but prevents a backout from the previous upgrade.

Note: Once the upgrade is accepted for a server, that server will not be allowed to backout to a previous release.

Procedure 90: Accept Upgrade

S T E P #	This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	It is recommended that this procedure is performed 2 weeks after the upgrade.	Verify that the upgraded system has been stable for 2 weeks or more. [It will not be possible to backout after this is procedure is executed.]
2 ☐	Accept upgrade for multiple servers	Accept the upgrade for multiple servers (considering traffic) **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2** 1. Select **Administration->Software Management->Upgrade.** The Upgrade Administration screen is displayed. 2. Select the servers (using the Ctrl button) for which upgrade is to be accepted, considering traffic, as the Accept upgrade may lead to a server reboot. 3. Click the "**Accept**" button

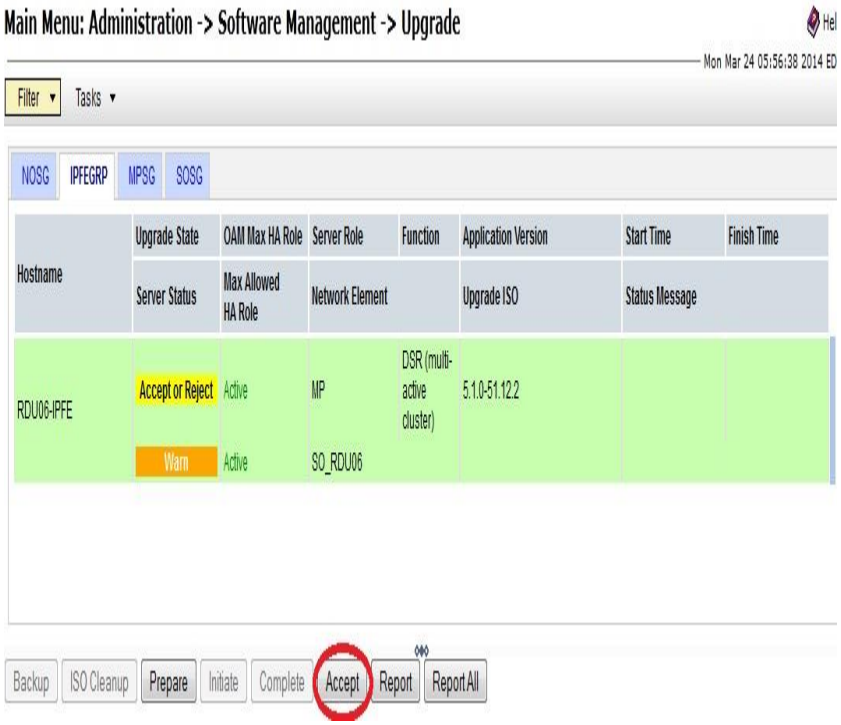
Procedure 90: Accept Upgrade



Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

1. Select **Administration->Software Management->Upgrade.**
   The Upgrade Administration screen is displayed.
2. 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

Procedure 90: Accept Upgrade



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**"
7. The Upgrade Administration screen re-displays.
8. Select **Alarms & Events > View** Active.
   The Alarms & Events > View Active screen displays.
9. As upgrade is accepted on each server, the corresponding Alarm ID **32532 (Server Upgrade Pending Accept/Reject)** should automatically clear.

3 ☐	Accept upgrade of the rest of the system	Accept Upgrade all Servers in the system: 1. Repeat step 2 of this procedure until the upgrade of all Servers within the system has been accepted.
End of maintenance window.		

5. BACKOUT PROCEDURE OVERVIEW

The procedures shown in Table 21 are executed inside a maintenance window. Backout procedure times are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done. This backout procedure covers all upgrade scenarios and topologies.

Table 21. Backout Procedure Overview

Procedure	Elapsed Time (Hours or Minutes)		Procedure Title	Impact
	This Step	Cum.		
Backout Setup	0:10-0:30	0:10-0:30	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 91	See Note	See Note	Back Out Entire Network 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 93	0:01-0:05	Varies	Perform Health Check (Post-Backout)	None

5.1 Recovery Procedures

Upgrade procedure recovery issues should be directed to the Oracle CGBU Customer Care Center by referring to Appendix O of this document. Before executing any of these procedures, contact the Oracle CGBU Customer Care Center at 1-888-FOR-TKLC (1-888-367-8552); or 1-919-460-2150 (international). 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

Do not attempt to perform these backout procedures without first contacting the Oracle CGBU Customer Care Center at

1-888-FOR-TKLC or 1-888-367-8552; or for international callers 1-919-460-2150.

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 10.y.z release to the previously installed 10.x.w release). Backout of an initial installation is not supported.

5.2 Backout Setup

Identify IP addresses of all servers that are to be backed out.

1. Select **Administration->Software Management->Upgrade**
2. Based on the "Application Version" column, identify all the hostnames that need to be backed out.
3. Select **Configuration > Servers**
4. Identify the XMI/iLO 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 procedure **WILL** cause traffic loss. Since all possible reasons cannot be predicted ahead of time, contact the Oracle CGBU Customer Care Center as stated in the **Warning** box above.

For DSR 4.x/5.x:

NOTE: **Verify that the two backup archive files, created using the procedure 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

And

Backup. <application>.<server>.**FullRunEnv**.<role>.<date_time>.**UPG**.tar

5.3 Perform Backout

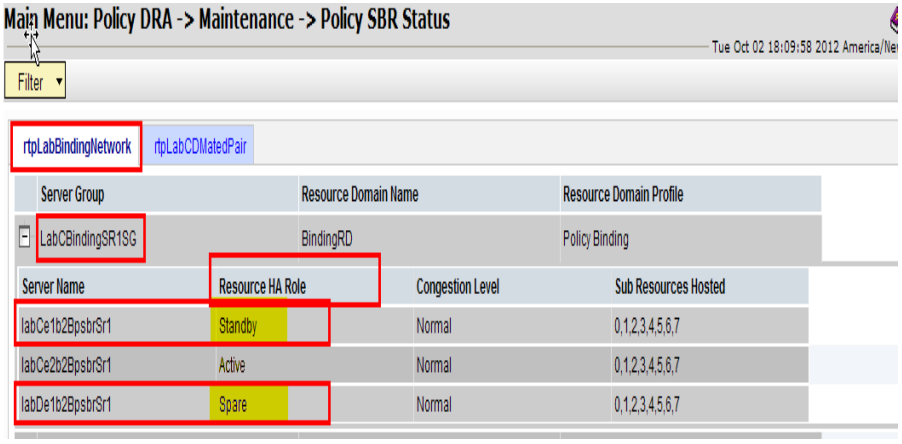
The following procedures to perform a backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. Contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document, as stated in the Warning box above, to identify if all corrective setup steps have been taken.

5.3.1 Back Out Entire Network

Procedure 91: Back Out Entire Network

S T E P #	This procedure is used to back out an upgrade of DSR 4.x/5.x application software from multiple servers in the network. Any server requiring backout can be included: NOAMs, SOAMs, DA-MPs, IPFEs, cSBRs, pSBRs, and even TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
1 ☐	Identify all servers that require Backout.	Identify all servers that require Backout (within a Site): 1. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. 2. Identify the servers in respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. Note: The upgrade screen displays all servers in the DSR 4.x releases, In DSR 5.x, servers are sorted by Server Group tabs. 3. Make note of these servers. They have been identified for Backout. 4. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2 ☐	Disable global provisioning and configuration (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: 1. Log into the NOAM VIP GUI. 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**. 6. The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
3 ☐	Disable Site Provisioning for the Site which is to be backed out.	**Disable Site provisioning :** 1. Log into the SOAM VIP GUI of the site. 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.**

Procedure 91: Back Out Entire Network

4 ☐	Backout Standby DA-MP Servers, Standby cSBR(s) and Standby pSBR(s) ,as applicable	**Note: The Spare server is located at the mated site of the site being backed out.** Back out the **Standby MP** servers. The following servers can be backed out in parallel (as applicable) 1. Standby DA-MP(s) 2. Standby cSBR(s) 3. Standby pSBR(s) 4. Spare pSBR(s) Execute Procedure 92, 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 Policy DRA traffic, resulting in service impact**
5 ☐	Verify Standby pSBR server status	If the server being backed out is the Standby pSBR, execute this step. Otherwise, continue with step 6. From the Active NOAM GUI: 1. Navigate to **Main Menu -> Policy DRA->Maintenance->Policy 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**. 
6 ☐	Verify that bulk download is complete between Active Policy SBR in server group to Standby Policy SBR and Spare Policy 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 Policy SBR group that is in upgrade **Display Filter**: Event ID = 31127 **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: a. 2 for the Standby Policy SBR for both binding and session policies b. 2 for the Spare Policy SBR server for both binding and session policies. NOTE: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.

Procedure 91: Back Out Entire Network

7 ☐	Back out DA-MPs, IPFEs, cSBRs, pSBRs, as applicable" or "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 5.3.2 Back Out Single Server. **For DSR N+0 (multi-Active) configuration** 1. Identify which Active MP(s) can be backed out in parallel, considering traffic. 2. Backout all identified IPFE(s),SBR(s), pSBR(s) and DA MP(s) in parallel : Execute Section 5.3.2 Back Out Single Server. 3. Execute sub-steps 1 again to backout the remaining Active MP(s).
8 ☐	Back out the Standby SOAM server (as applicable).	Back out the Standby **DSR SO** server: Execute Section 5.3.2 Back Out Single Server.
9 ☐	Back out Active SO Server (as applicable).	Back out the Active **DSR SO** server: Execute Section 5.3.2 Back Out Single Server.
10 ☐	Back out Spare SO Server (as applicable).	**Note: The Spare server is located at the mated site of the site being backed out.** Back out the Spare DSR SO server: Execute Section 5.3.2 Back Out Single Server.

11 ☐	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 next step.**
		Execute the following steps for each TVOE blade upgraded previously :
		1. Disable all applications running on the TVOE blade:
		a) Log into the NOAM GUI using VIP.
		b) Select **Status & Manage > Server.** The Server Status screen is displayed
		c) Select all applications running on the current TVOE blade.
		d) Click the **Stop** button.
		e) Confirm the operation by clicking **Ok** in the popup dialog box.
		f) Verify that the 'Appl State' for all selected servers changes to '**Disabled**'.
		2. 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.
		3. Execute the following command for each guest listed in sub-step 2 :

Procedure 91: Back Out Entire Network

		`# virsh shutdown <guestname>`
		
		Note: Shutting down applications may lead to lost VIP. Wait until all TVOE blades on which SO(s) are hosted are successfully backed out.
		
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [2].

12 ☐	Enable virtual guest watchdogs if disabled previously	1. If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [6] Otherwise execute the following sub-steps:
		
		a) Log into the TVOE host using following command :
		
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		
		b) Execute the following command to start the TVOE guest shutdown in step 11 sub-step 3 above (if not already started).
		
		`# virsh start <guestname>`
		
		c) Periodically execute the following command until the command displays all the VM guests running.
		
		`# virsh list`
		
		2. Enable all applications running on the backed out TVOE blade :
		a) Log into the NOAM VIP GUI
		b) Select **Status & Manage > Server.**
		The Server Status screen is displayed
		c) Select all applications running on the current TVOE blade.
		d) Click the **Restart** button.
		e) Confirm the operation by clicking **Ok** in the popup dialog box.
		f) 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 11.
		
		Execute Steps 11 and 12 again for another TVOE blade hosting SO (as applicable).

13 ☐	Enable Site Provisioning	**Enable Site provisioning :** 1. Log into the SOAM VIP GUI of the site. 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**

Procedure 91: Back Out Entire Network

14 ☐	Back out Standby DR NO server (as applicable).	Back out the **primary Standby DR NO** server: Execute Section 5.3.2 Back Out Single Server.
15 ☐	Back out Active DR NO server (as applicable).	Back out the **Active primary DR NO server** (the mate): Execute Section 5.3.2 Back Out Single Server.
16 ☐	Back out Standby NO server.	Back out the **primary Standby NO** server: Execute Section 5.3.2 Back Out Single Server.
17 ☐	Back out Active NO server.	Back out the **other NO server** (now the standby): Execute Section 5.3.2 Back Out Single Server.

18 ☐	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 19.**
		
		Execute the following steps for each TVOE blade upgraded previously :
		
		1. Disable all applications running on the TVOE blade:
		a) Log into the NOAM GUI using the VIP.
		b) Select **Status & Manage > Server.**
		The Server Status screen is displayed
		c) Select all applications running on the current TVOE blade.
		d) Click the **Stop** button.
		e) Confirm the operation by clicking **Ok** in the popup dialog box.
		f) Verify that the 'Appl State' for all selected servers changes to '**Disabled**'.
		
		2. 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.
		
		3. 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 NO(s) are hosted are successfully backed out.
		
		4. Periodically execute the following command until the command displays no entries. This means that all VMs have been properly shut down :
		
		`# virsh list`
		
		Back out TVOE on the blade according to reference [2].

Procedure 91: Back Out Entire Network

19 ☐	Enable virtual guest watchdogs if disabled previously	1. If the virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [6] Otherwise execute the following sub-steps:
		a) Log into the TVOE host using following command :
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		b) Execute the following command to start the TVOE guest shutdown in step 18 sub-step 3 above (if not already started).
		`# virsh start <guestname>`
		c) Periodically execute the following command until the command displays all the VM guests running.
		`# virsh list`
		2. Enable all applications running on the backed out TVOE blade :
		a) Log into the NOAM VIP GUI
		b) Select **Status & Manage > Server.** The Server Status screen is displayed
		c) Select all applications running on the current TVOE blade.
		d) Click the **Restart** button.
		e) Confirm the operation by clicking **Ok** in the popup dialog box.
		f) 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 18.
		Execute Steps 18 and 19 again for another TVOE blade hosting NO (as applicable).

20 ☐	Enable global provisioning and configuration	Enable global provisioning and configuration updates on the entire network: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Click the **Enable Provisioning** button. 3. Verify the button text changes to **Disable Provisioning.**

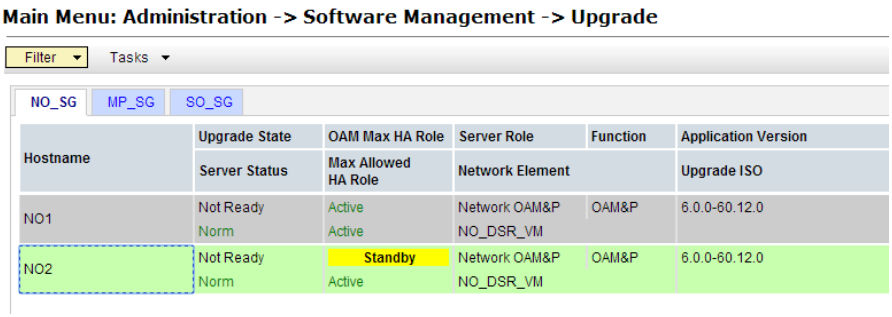
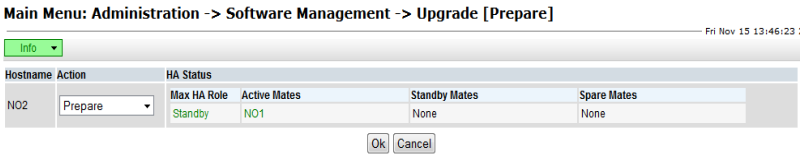
Procedure 91: Back Out Entire Network

21 ☐	Remove 'Ready' state (if exists) for any backed out server	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 > Upgrade (**in DSR 4.x) or **Administration->Software Management->Upgrade** (in DSR 5.x). 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, you may see the following SOAP error in the GUI banner. `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message. Verify the **Application Version** value for servers has been downgraded to the original release version.

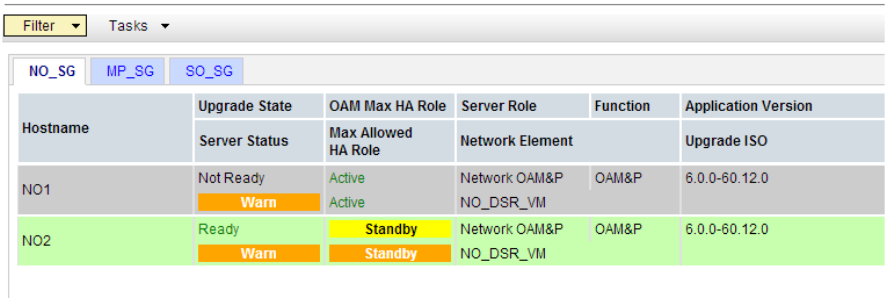
Note: If another site is to be backed out, please follow all steps sequentially from step 1 of Procedure 91 to step 13 of Procedure 91 in another maintenance window.

5.3.2 Back Out Single Server

Procedure 92: Back Out Single Server

S T E P #	This procedure will back out the upgrade of DSR 5.1 application software. Any server requiring Back out can be included: NOAMs, SOAMs, DA-MPs, IPFEs, cSBRs, pSBRs, and even TVOE hosts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
1 ☐	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. 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. b) Otherwise, 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: When the Active NOAM is the server being backed out, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, clo se 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/**Ready** for the server to be upgraded. It may take up to a minute for the Upgrade State to change to Backout Ready/**Ready**.

Procedure 92: Back Out Single Server

		Main Menu: Administration -> Software Management -> Upgrade  Filter Tasks NO_SG MP_SG SO_SG Hostname / Server Status / Upgrade State / Max Allowed HA Role / OAM Max HA Role / Network Element / Server Role / Function / Application Version / Upgrade ISO NO1: Not Ready, Warn / Active, Active / Network OAM&P, NO_DSR_VM / OAM&P / 6.0.0-60.12.0 NO2: Ready, Warn / Standby, Standby / Network OAM&P, NO_DSR_VM / OAM&P / 6.0.0-60.12.0 **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: The preparation steps required to upgrade a server are also required when preparing to back out a server.**
2 ☐	SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty): `ssh <server address>` 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 NO. SSH to the Active NO XMI first. From there, SSH to the target server's IMI address.

3 ☐	Log in as root	Login as root:
		
		`login as: root`
		`password: <enter password>`

Procedure 92: 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.
		
		`[root@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`pSbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`pSbrBindingRes OOS B2435.024 0 0127:113601.918`
		`pSbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`pSbrSessionRes 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.
		
		Execute the backout using the following command:
		
		`# screen`
		`# /var/TKLC/backout/reject`
		
		NOTE: If backout prompts to continue, answer "**y**".

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 ☐	SSH to server	Use an SSH client to connect to the server (e.g. ssh, putty): `ssh <server address>` 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 NO. SSH to the Active NO XMI first. From there, SSH to the target server's IMI address.

7 ☐	Log in as root	Login as root:
		
		`login as: root`
		`password: <enter password>`

Procedure 92: Back Out Single Server

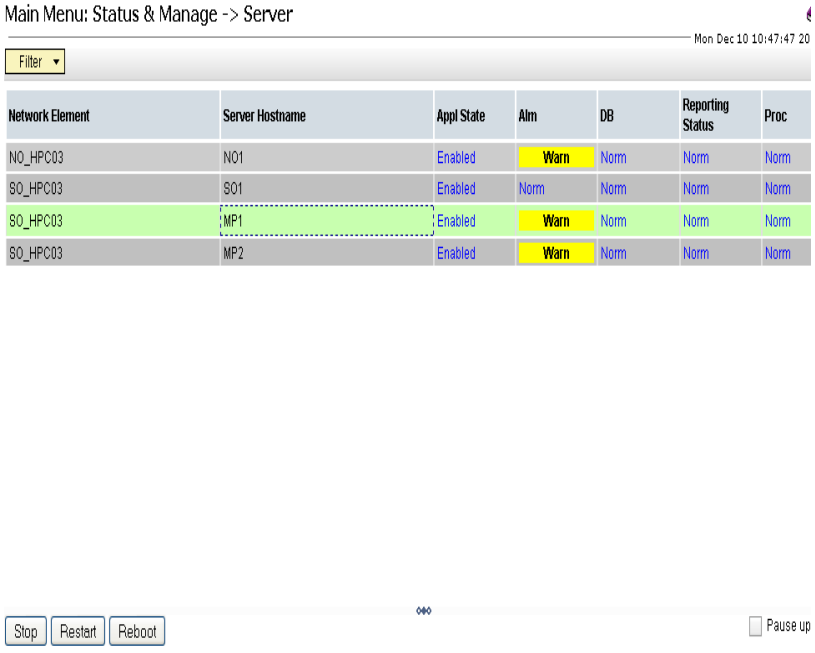
8 ☐	Restore the full DB run environment.	Execute the backout_restore utility to restore the full database run environment:
		`# /var/tmp/backout_restore`
		NOTE: If prompted to proceed, answer "**y**".
		If the restore was successful, the following will be displayed:
		`Success: Full restore of COMCOL run env has completed. Return to the backout procedure document for further instruction.`
		If an error is encountered and reported by the utility, then consult with the Oracle CGBU Customer Care Center by referring to Appendix O of this document for further instructions.

9 ☐	Verify the backout	1. Examine the output of the following commands to determine if any errors were reported:
		`# verifyUpgrade`
		The following command will show the current rev on the server:
		`# 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`
		2. If the backout was not successful because other errors were recorded in the logs, then contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document for further instructions.
		3. If the backout was successful (no errors or failures), then continue with the remaining steps.

10 ☐	Reboot the server	Enter the following command to reboot the server: `# init 6` This step can take several minutes.

Procedure 92: Back Out Single Server

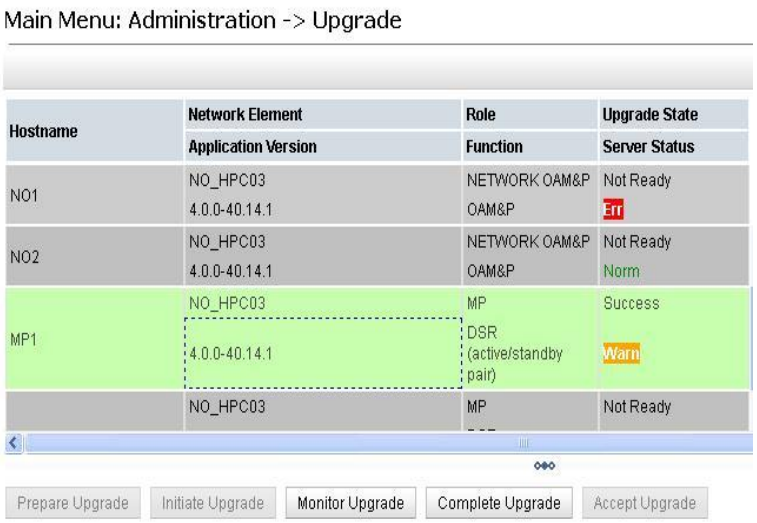
11 ☐	Verify services restart	Verify services have restarted:
		1. Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in as root. The method is the same as Steps 2 and 3 of Section 5.3.1.
		3. If this is an NO or SO, verify the httpd service is running. Execute the command:
		`# 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. Contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document for further instructions.

12 ☐	Remove Upgrade Ready status	From the DSR Active NOAM GUI: 1. Select **Status & Manage > Server.** The Server Status screen is displayed. 2. If the server just backed-out shows "**Appl State" Enabled**, then select the server row and press the **Stop** button. 
13 ☐	Remove Upgrade Ready status	1. Select **Administration > Upgrade** (on DSR 4.x GUI) or **Administration >Software Management >Upgrade** (on DSR 5.1 GUI.; The Upgrade Administration screen is displayed. 2. If the server just backed-out shows an Upgrade State of "**Ready**" or "**Success**", then select the backed-out server and press the **Complete Upgrade (on DSR 4.x GUI) or Complete (on DSR 5.1 GUI)** button. Otherwise, skip to sub-step 4 below. **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR

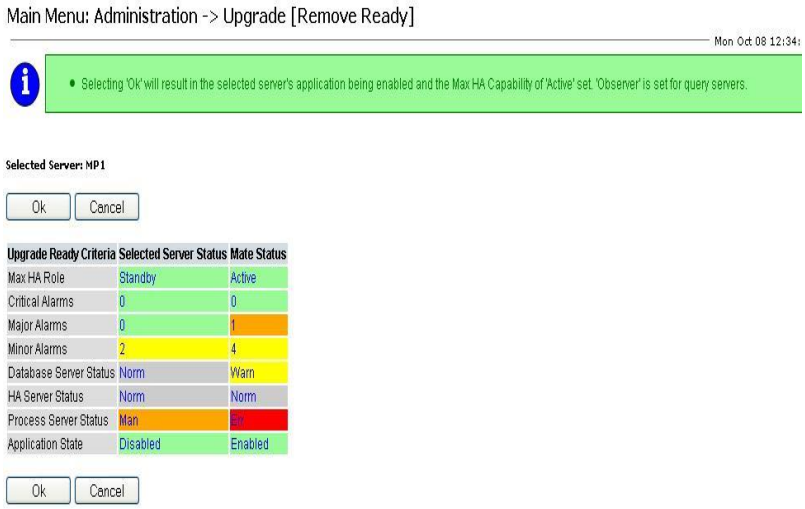
Procedure 92: Back Out Single Server

5.1 releases. The example below provides a snapshot from both releases.

Upgrade Screen in DSR 4.x

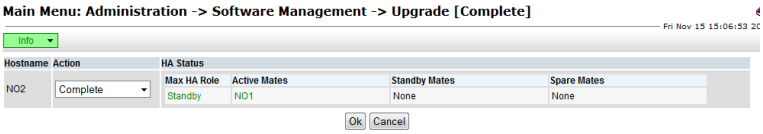


The **Upgrade** [**Remove Ready]** screen will appear.



Upgrade Screen in DSR 5.1

Procedure 92: Back Out Single Server

		Main Menu: Administration -> Software Management -> Upgrade Filter Tasks NO_SG MP_SG SO_SG Hostname / Upgrade State / Server Status / OAM Max HA Role / Max Allowed HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO NO1: Not Ready, Warn / Active, Active / Network OAM&P, NO_DSR_VM / OAM&P / 6.0.0-60.12.0 NO2: Ready, Warn / Standby, Standby / Network OAM&P, NO_DSR_VM / OAM&P / 6.0.0-60.12.0 The **Upgrade [Complete]** screen will appear  **Main Menu: Administration -> Software Management -> Upgrade [Complete]** Info Hostname: NO2 / Action: Complete / HA Status: Max HA Role: Standby / Active Mates: NO1 / Standby Mates: None / Spare Mates: None Ok Cancel 3. Click **OK.** This will remove the Forced Standby designation for the backed-out server. **4.** Verify the **Application Version** value for this server has been downgraded to the original release version.

14	Workaround for major backout (DSR 5.1 -> DSR 4.x)	If the backed out server is the Standby NO (first NO)
		
		1. Log into the Active NO :
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following commands on the command line :
		
		`# ivi NodeInfo`
		
		Change the NodeCapability of the Active NO to 'Stby'.
		Change the NodeCapability of the Standby NO to 'Active'.
		Save the table.
		
		Note: This action will cause a switchover, so if logged in to the VIP, then it will be logged out. Login back in to the VIP and continue.

5.4 Post-Backout Procedures

To complete an Upgrade Backout, complete the Post-Backout procedure below.

5.4.1 Perform Health Check (Post-Backout)

This procedure is used to determine the health and status of the DSR 4.x/5.x network and servers.

Procedure 93: Perform Health Check (Post-Backout)

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Select **Status & Manage > Server.** The Server Status screen is displayed. 2. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 3. Do not proceed with the upgrade if any server status is not **Norm**. 4. 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: 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.

6. APPENDICES

APPENDIX A. COMMAND OUTPUTS

Not applicable.

APPENDIX B. SWOPS SIGN OFF.

Discrepancy List

Date	Test Case	Description of Failures and/or Issues. Any CSR's / RMA's issued during Acceptance. Discrepancy	Resolution and SWOPS Engineer Responsible	Resolution Date:

APPENDIX C. CUSTOMER SIGN OFF

Sign-Off Record

*** **Please review this entire document**. ***
This is to certify that all steps required for the upgrade successfully completed without failure.

Sign your name, showing approval of this procedure, and fax this page and the SWOPS Sign Off matrix to Oracle CGBU, FAX # 919-460-3669.

Customer: Company Name:_____ Date: _____

Site: Location:_____

Customer:(Print)_____ Phone:_____

Fax: _____

Start Date: _____ Completion Date: _____

This procedure has been approved by the undersigned. Any deviations from this procedure must be approved by both Oracle CGBU and the customer representative. A copy of this page should be given to the customer for their records. The SWOPS supervisor will also maintain a signed copy of this completion for future reference.

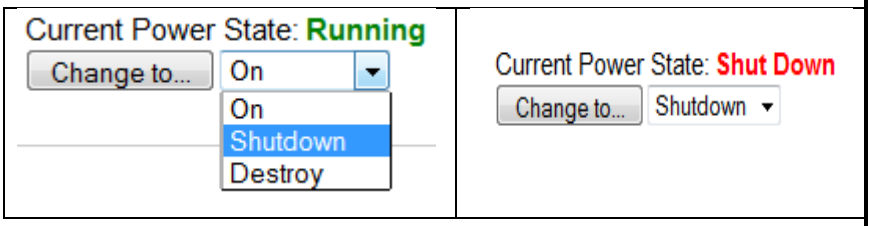
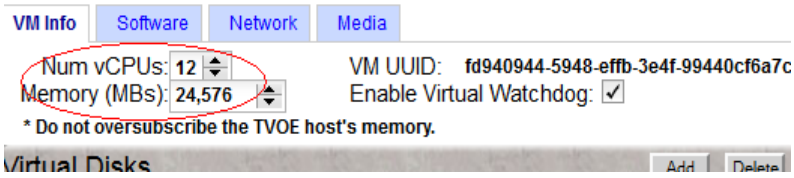
Oracle CGBU Signature: _____ Date: _____

Customer Signature: _____ Date: _____

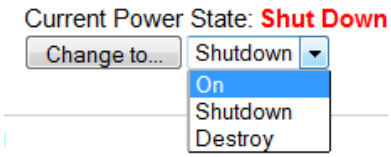
APPENDIX D. UPDATE NOAM GUEST VM CONFIGURATION

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 co-resident B-level or C-level servers.

Procedure 94: 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	**PM&C GUI:** Edit the 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**. Confirm the pop-up and wait for the power state to change to **Shutdown**. This may take a few moments as this executes a graceful shutdown of the NOAM guest.  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.**

Procedure 94: Update NOAM Guest VM Configuration

		8. Select **Save**. The GUI may gray out for a moment while the changes are committed. 9. Change the Guest power state from **Shutdown** to **On**. 

APPENDIX E. DETERMINE IF TVOE UPGRADE IS REQUIRED

When upgrading a server that exists as a virtual guest on a TVOE Host, it is first necessary to determine whether the TVOE Host (i.e. the "bare-metal") server must 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 95: 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	

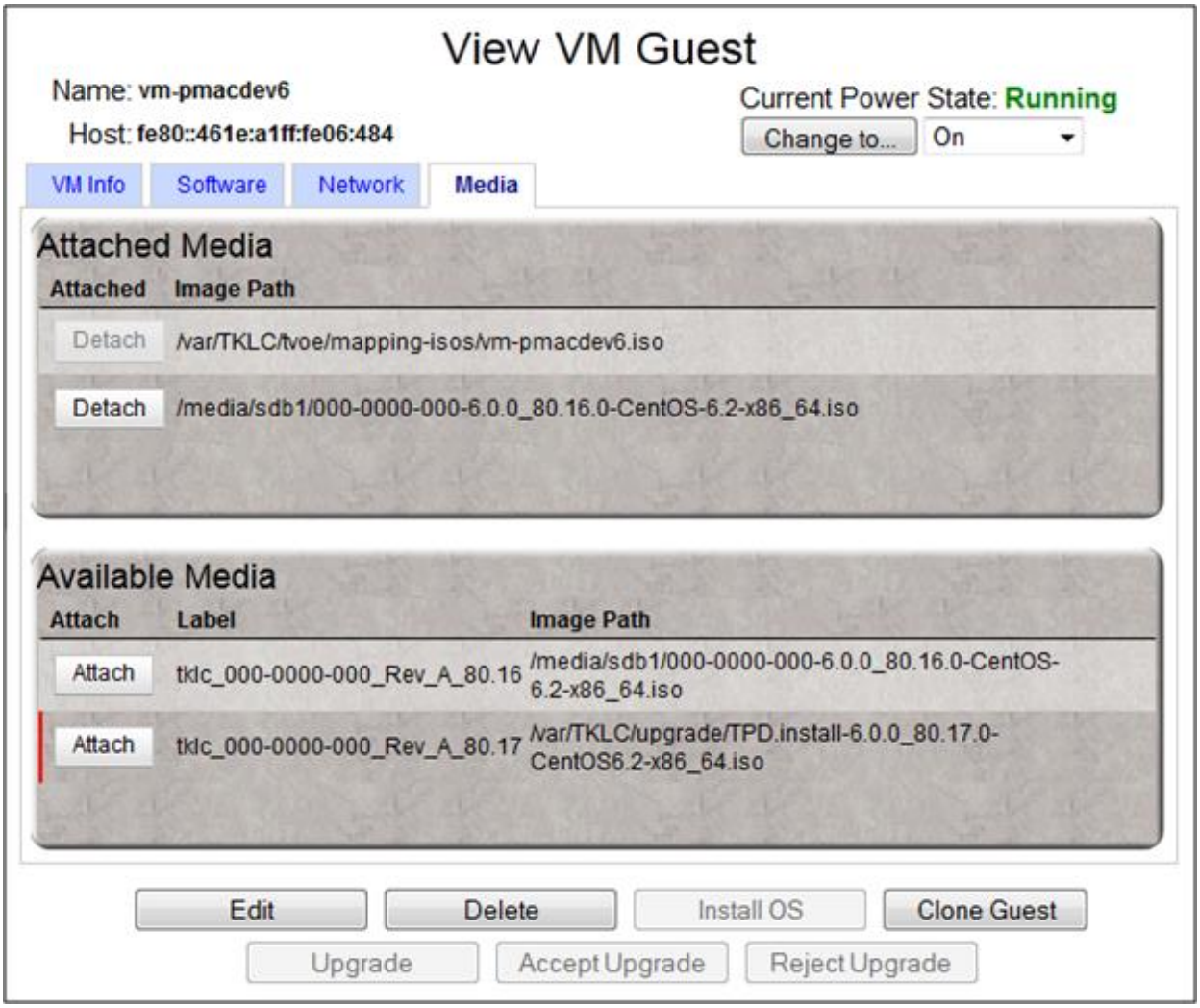
1 ☐	Determine the version of TVOE already running on the bare-metal server that hosts the virtual guest currently being upgraded.	1. Log into the host server on which TVOE is installed.
		2. Execute the following command to get the current TVOE installed version :
		`[root@dsrTVOEblade2 ~]# appRev`
		`Install Time: Tue Aug 7 08:17:52 2012`
		`Product Name: TVOE`
		`Product Release: 2.0.0_80.16.0`
		`Part Number ISO: 872-2290-104`
		`Part Number USB: 872-2290-104`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.0.0_80.16.0`
		`Base Distro ISO: TPD.install-6.0.0_80.16.0-CentOS6.2-x86_64.iso`
		`OS: CentOS 6.2`

2 ☐	Check the TVOE release version required for target DSR release	Contact the Oracle CGBU Customer Care Center by referring to Appendix O 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 J.

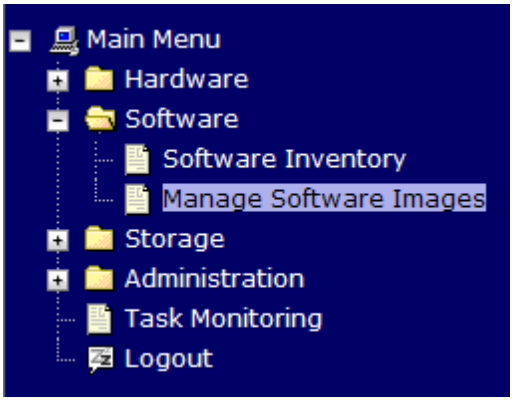
APPENDIX F. ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY

If the ISO image is delivered on optical media, or USB device, continue with step 1 of this Appendix; otherwise, if the ISO image was delivered to the PM&C using sftp, continue with step 5.

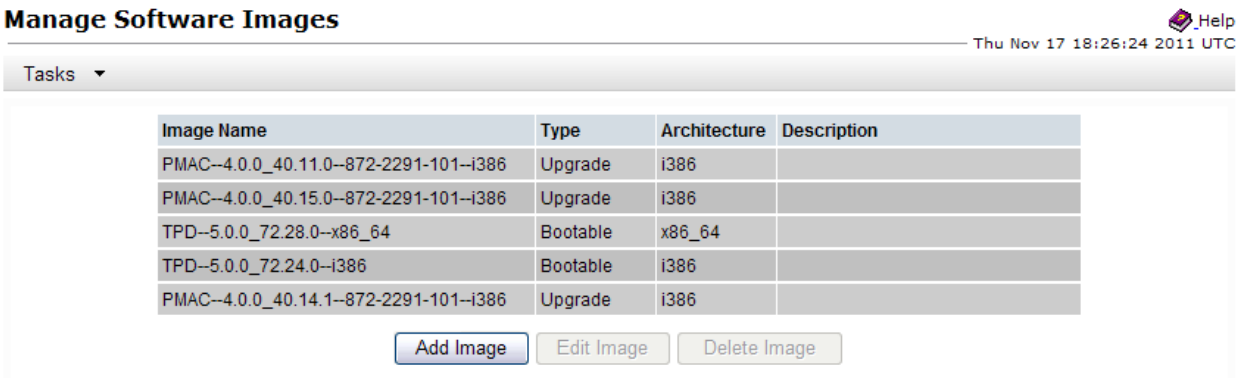
1. In the PM&C GUI, navigate to **Main Menu ➢ VM Management.** In the "**VM Entities**" list, select the PM&C Guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.
2. Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button.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



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

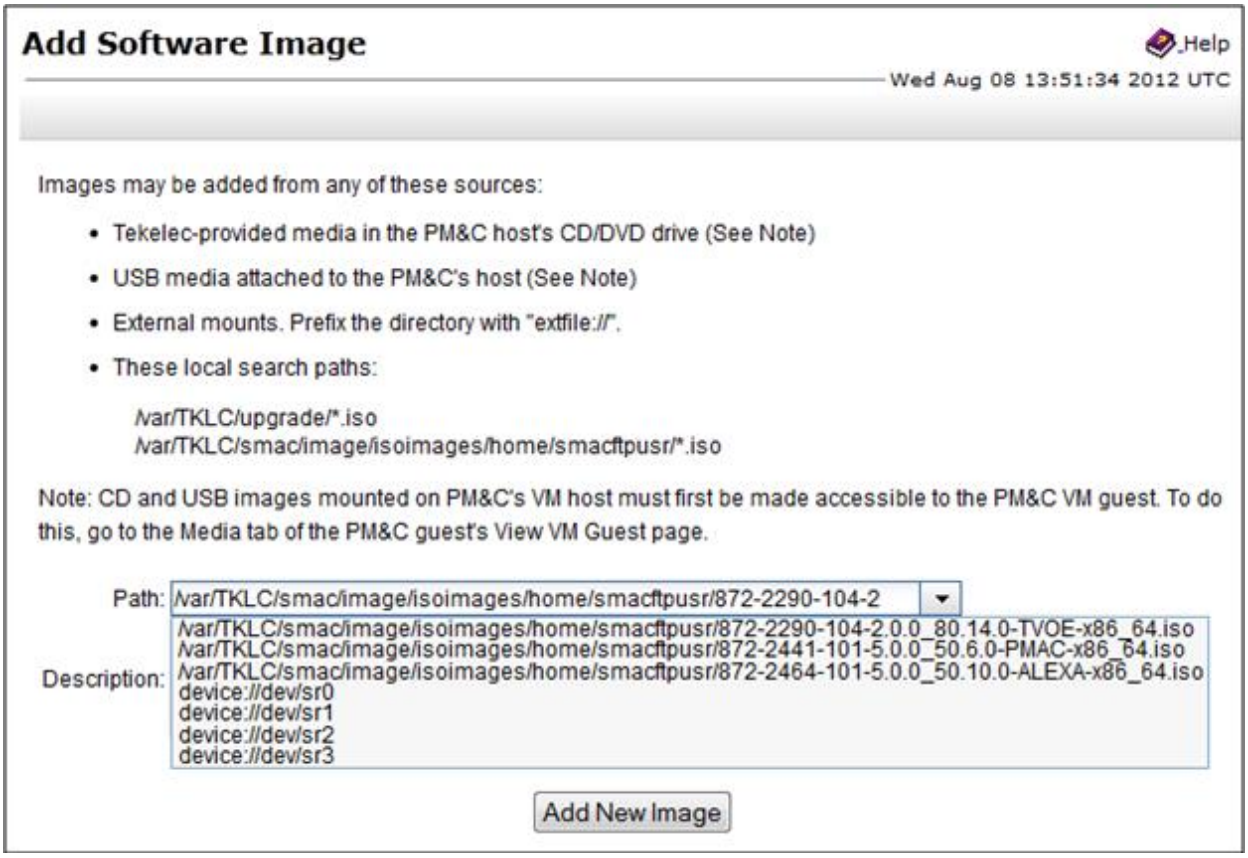


4. **PM&C GUI:**Add image
   Press the **Add Image** button.



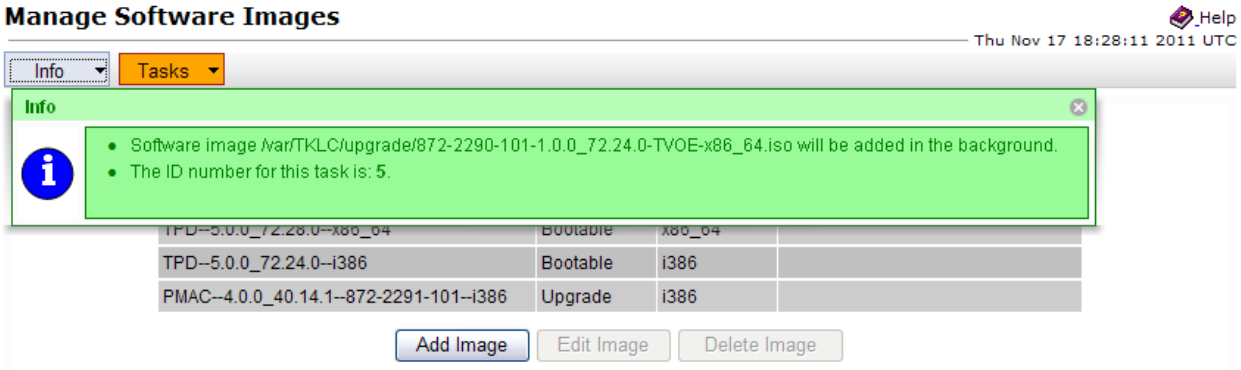
5. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:
   - If the image was transferred to PM&C via sftp, it will appear in the list as a local file"/var/TKLC/...".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…").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



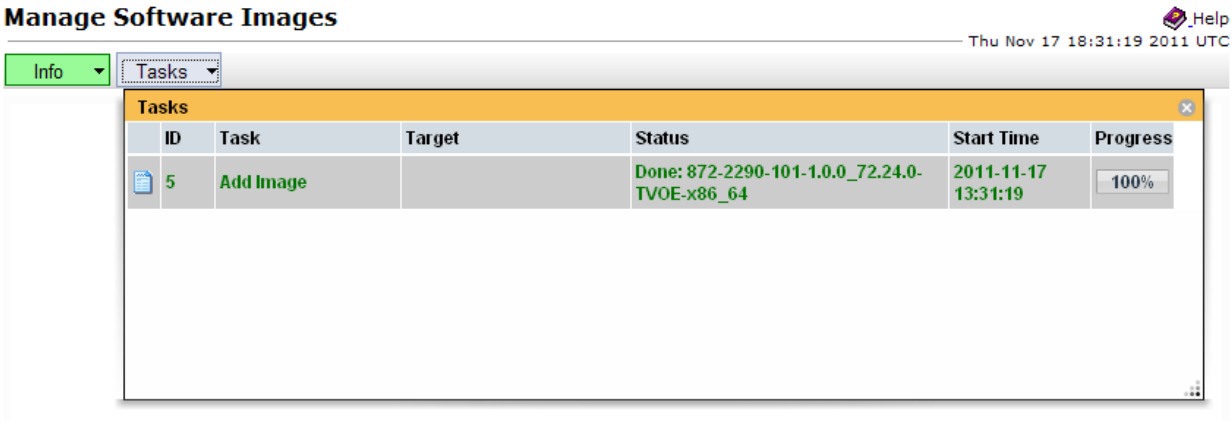
6. **PM&C GUI** Monitor the Add Image status

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 G. UPGRADE SINGLE SERVER – UPGRADE ADMINISTRATION

This Appendix provides the procedure for upgrading a DSR single server of any type (NO, SO, MP, etc).

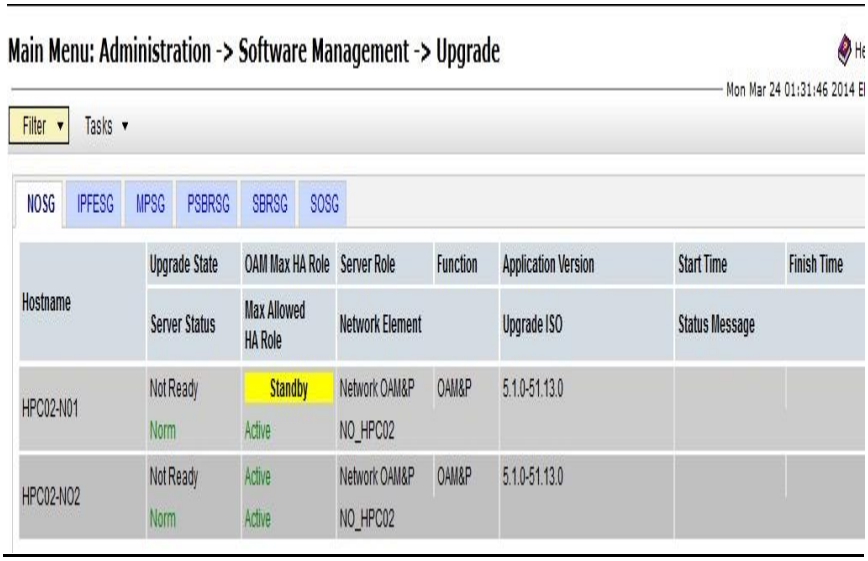
Note that this procedure will be executed multiple times during the overall upgrade, depending on the number of servers in the DSR. Make multiple copies of Appendix G to mark up, or keep another form of written record of the steps performed.

Procedure 96: Upgrade Single Server – Upgrade Administration

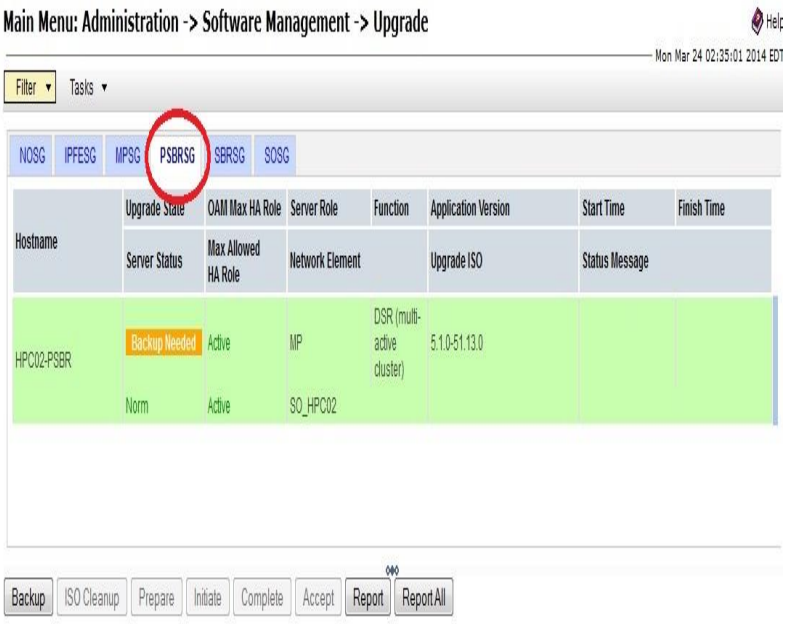
S T E P #		
	This procedure executes the Upgrade Single Server – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**NO GUI – Upgrade Administration:** View the pre-upgrade status of Servers	From the Active NOAM GUI: Select **Upgrade Administration** form (DSR 4.x: "**Administration > Upgrade**" DSR 5.1: " **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 DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x** (screenshot)

Hostname	Network Element Application Version	Role Function	Upgrade State Server Status
NO1	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Err
NO2	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Norm
MP1	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

Procedure 96: Upgrade Single Server – Upgrade Administration

		Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2  **Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up**  **The following status may be observed:** The Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
2	**NO GUI – Upgrade Administration:** Verify status of Server to be upgraded	For the server to be upgraded: 1. Identify the server (NO, SO, 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** : • **Only required for DSR >= 5.1.0-51.13.0 :** • From the Administration -> Software Management -> Upgrade screen, select the Server Group of the server which needs to be upgraded.

Procedure 96: Upgrade Single Server – Upgrade Administration

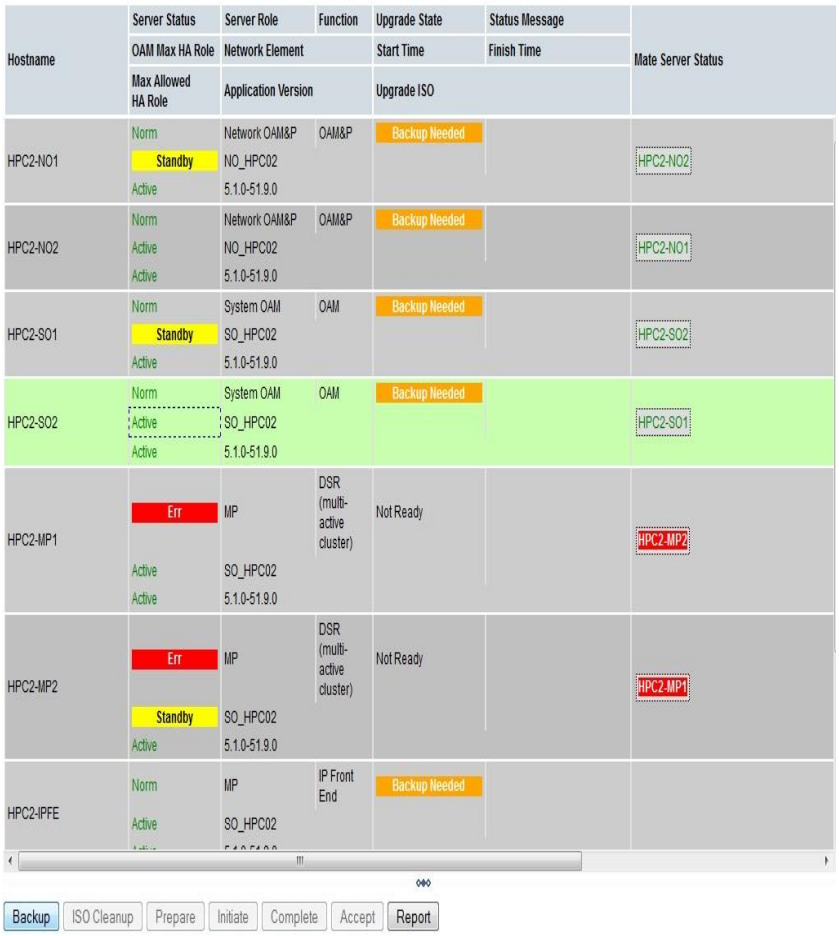


Required for all DSR releases :

- If the server is in the '**Ready**' state, then skip the "Prepare Upgrade" steps (3-5) and start the Upgrade at Step 6.
- If the server is in "**Backup Needed"** state, then first select the server and click "Backup" button. Refresh the Upgrade screen to make sure that server is in the "**Not Ready**" state.

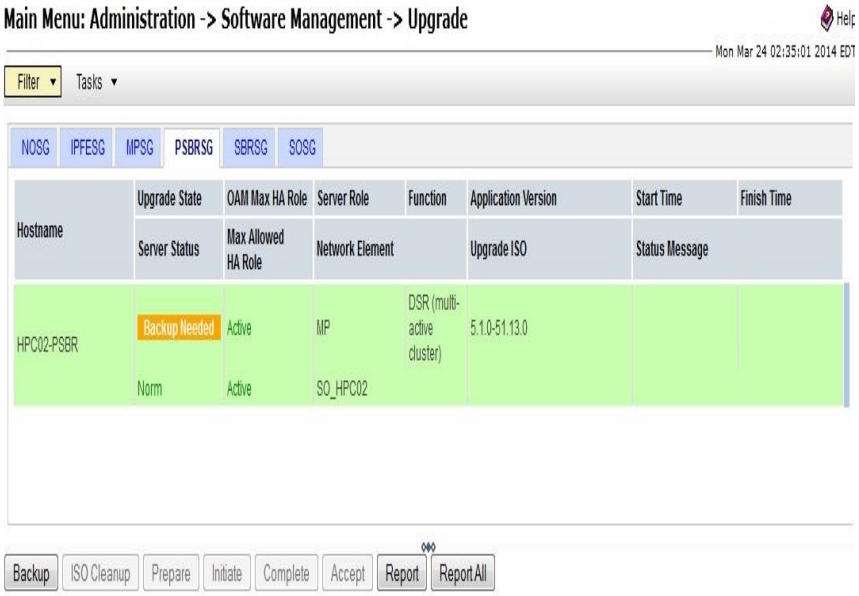
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

Procedure 96: Upgrade Single Server – Upgrade Administration

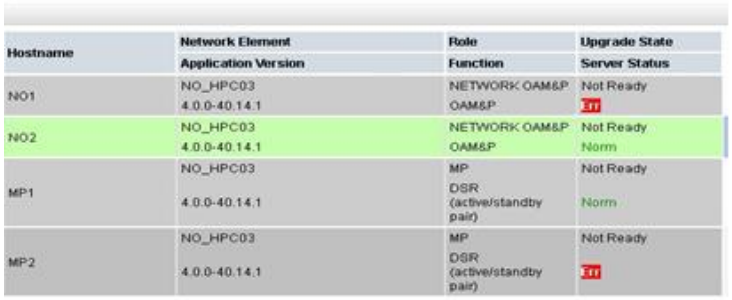


Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Procedure 96: Upgrade Single Server – Upgrade Administration

		
3	**NO GUI – Upgrade Administration:** Prepare Upgrade (step 1)	For the server to be upgraded: On the Upgrade form, make the server 'Upgrade Ready', by selecting the server to be upgraded and, Select: **Prepare Upgrade** (if DSR 4.x) **Prepare** (If DSR 5.1) (In this example, an NO with name "NO2" will be made ready for Upgrade) **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x**

Procedure 96: Upgrade Single Server – Upgrade Administration



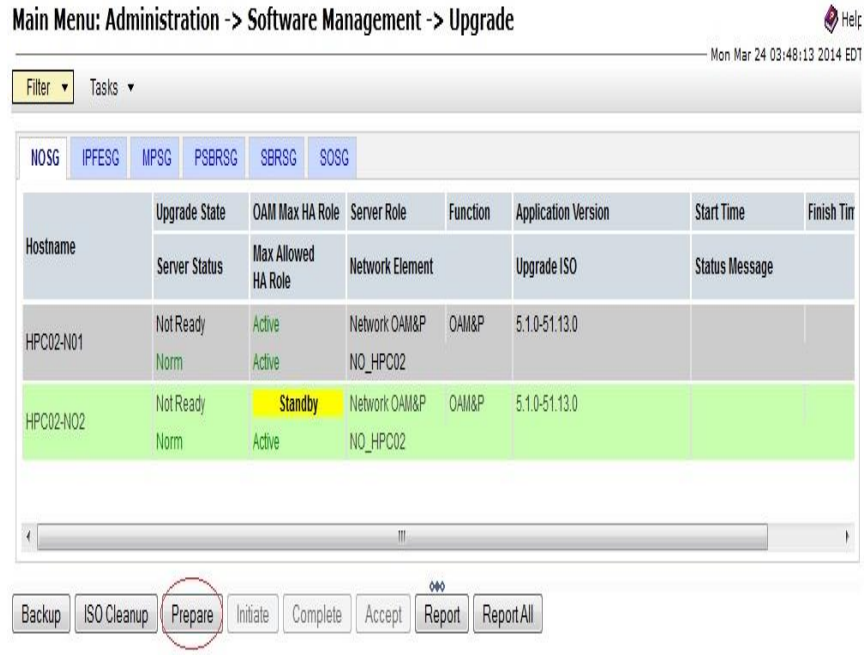
Hostname	Network Element Application Version	Role Function	Upgrade State Server Status
NO1	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Err
NO2	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Norm
MP1	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

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
NO1	Norm Active Active	Network OAM&P NO_DSR_VM 5.0.0-50.15.1	OAM&P	Not Ready		NO2
NO2	Norm Standby Active	Network OAM&P NO_DSR_VM 5.0.0-50.15.1	OAM&P	Not Ready		NO1
SO2	Norm Standby Active	System OAM SO_DSR_VM 5.0.0-50.15.1	OAM	Not Ready		SO1
SO1	Norm Active Active	System OAM SO_DSR_VM 5.0.0-50.15.1	OAM	Not Ready		SO2
MP1	Norm Standby Active	MP SO_DSR_VM 5.0.0-50.15.1	DSR (multi-active cluster)	Not Ready		MP2 MP3 MP4
MP2	Norm Spare Active	MP SO_DSR_VM 5.0.0-50.15.1	DSR (multi-active cluster)	Not Ready		MP1 MP3 MP4
	Norm	MP	DSR (multi-	Not Ready		

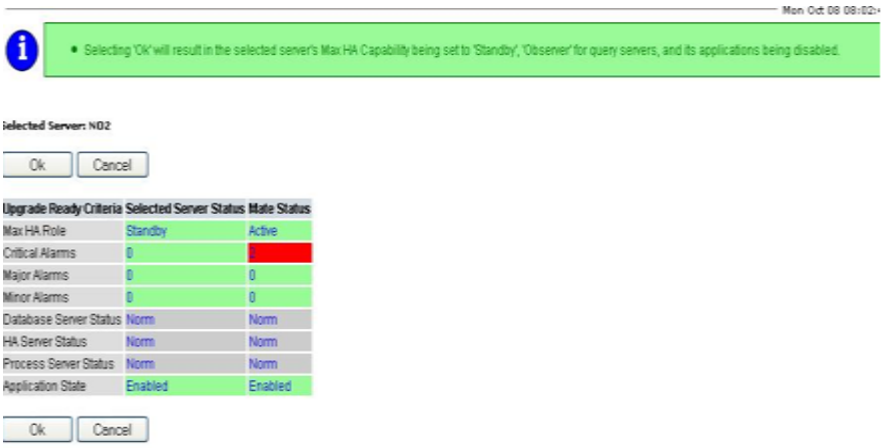
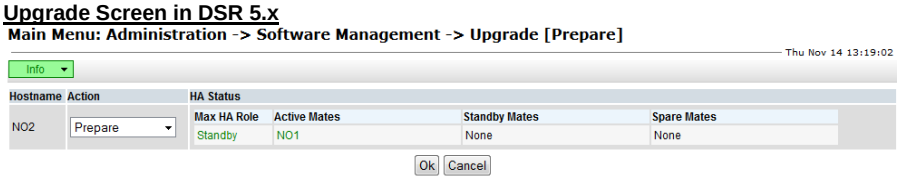
Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Procedure 96: Upgrade Single Server – Upgrade Administration

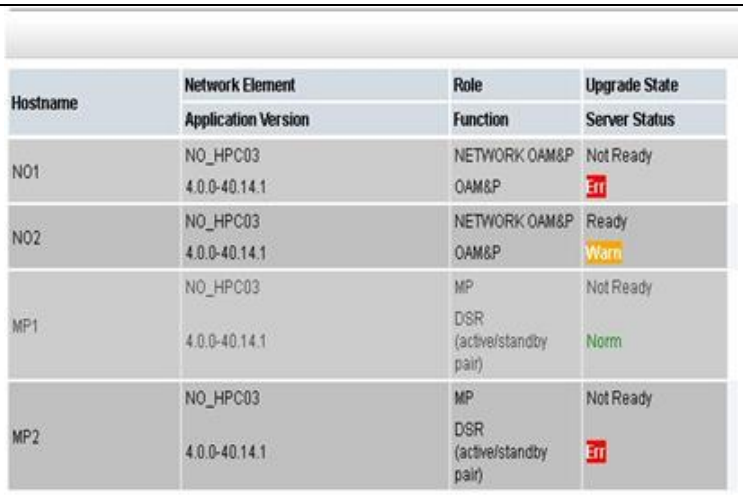
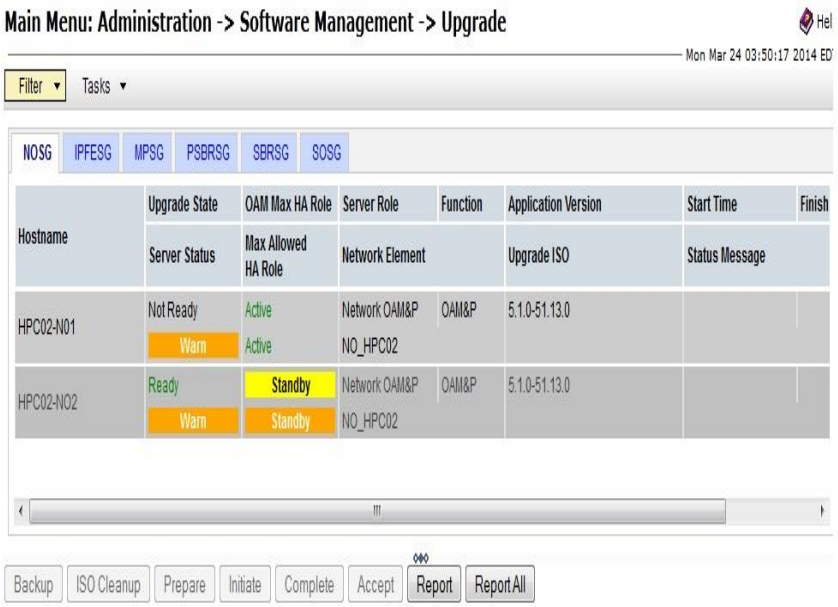


The Upgrade “Make Ready” form will be displayed. (see next step)

Procedure 96: Upgrade Single Server – Upgrade Administration

4 ☐	**NO GUI – Upgrade Administration:** 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 DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. 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.** **Upgrade Screen in DSR 4.x**  Mon Oct 08 08:02: • Selecting 'Ok' will result in the selected server's Max HA Capability being set to 'Standby', 'Observer' for query servers, and its applications being disabled. Selected Server: NO2 Ok Cancel Upgrade Ready Criteria / Selected Server Status / Mate Status Max HA Role: Standby / Active Critical Alarms: 0 / 0 Major Alarms: 0 / 0 Minor Alarms: 0 / 0 Database Server Status: Norm / Norm HA Server Status: Norm / Norm Process Server Status: Norm / Norm Application State: Enabled / Enabled Ok Cancel **Upgrade Screen in DSR 5.x**  Main Menu: Administration -> Software Management -> Upgrade [Prepare] Thu Nov 14 13:19:02 Info Hostname / Action / HA Status Max HA Role / Active Mates / Standby Mates / Spare Mates NO2 / Prepare / Standby / NO1 / None / None Ok Cancel ***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.*** ***For a 2-tier Active-Standby Setup, the Make Ready action on a DA-MP server MAY cause the value in the HA Status field under the Selected Server Status be shown as 'Active' for both DA-MP(s). This is OK. Please proceed with upgrade.***
5 ☐	**NO GUI – Upgrade Administration:** 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 4.x,5.0 and DSR 5.1 releases up to 5.1.0-51.12.2**

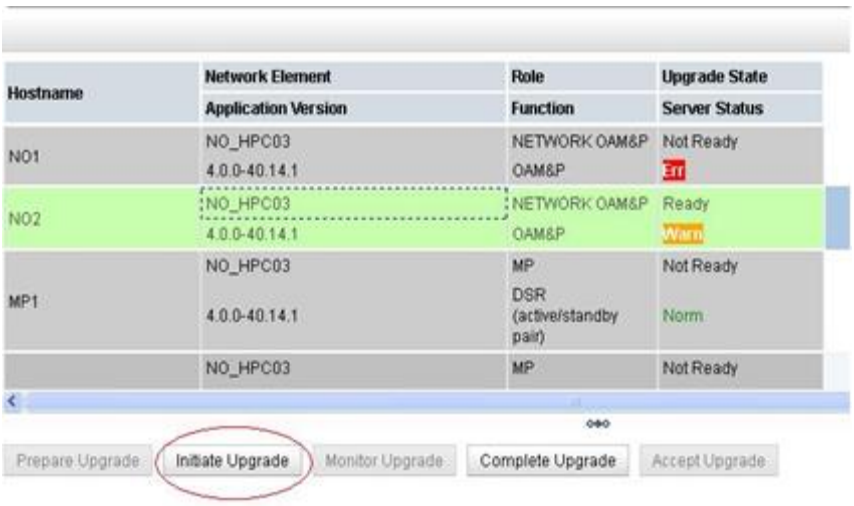
Procedure 96: Upgrade Single Server – Upgrade Administration

		 **Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up**  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 = **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)
6	**NO GUI – Upgrade Administration** : Initiate Upgrade (initiate) (part 1)	Initiate the upgrade on the server: **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases.

Procedure 96: Upgrade Single Server – Upgrade Administration

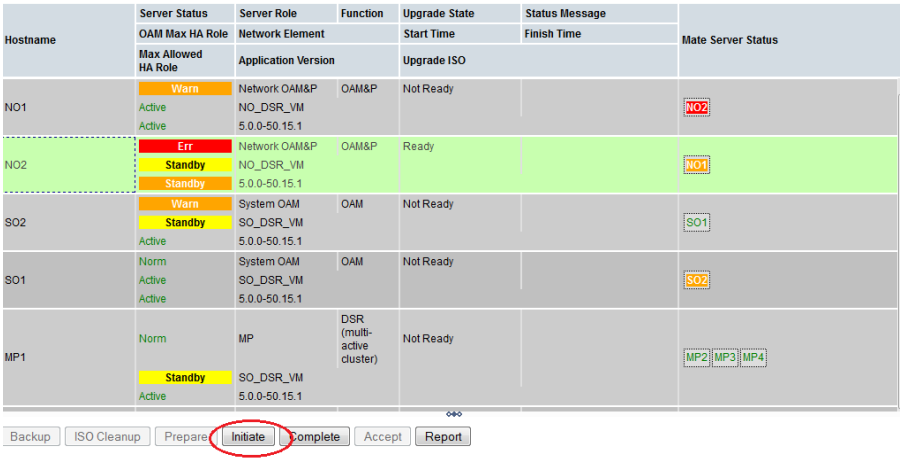
Upgrade Screen in DSR 4.x

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



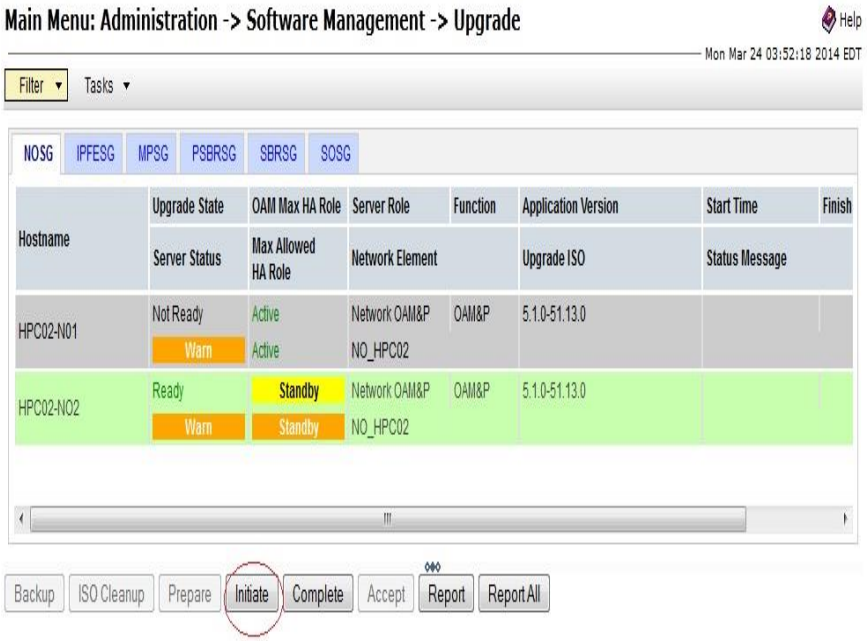
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

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

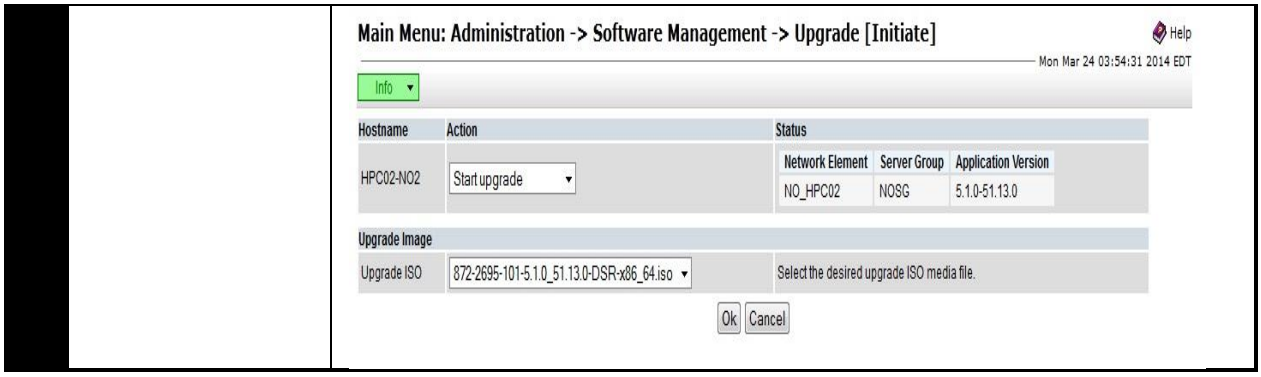


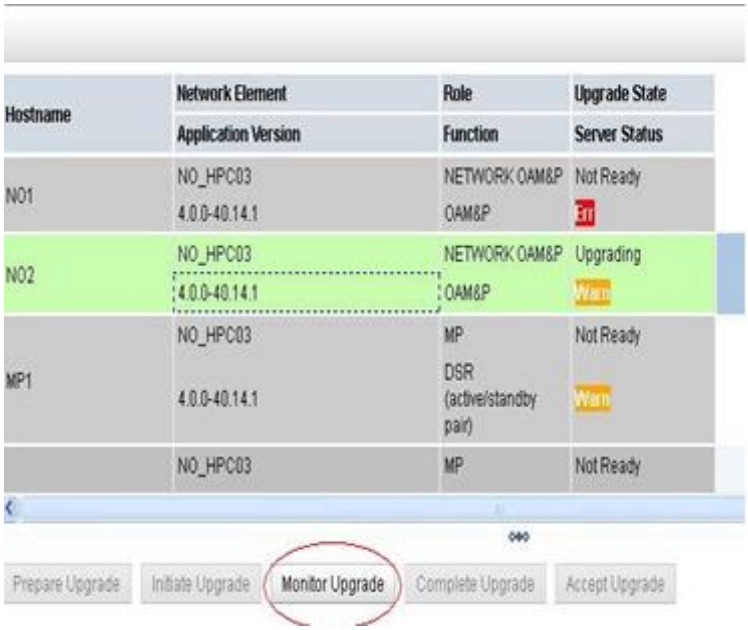
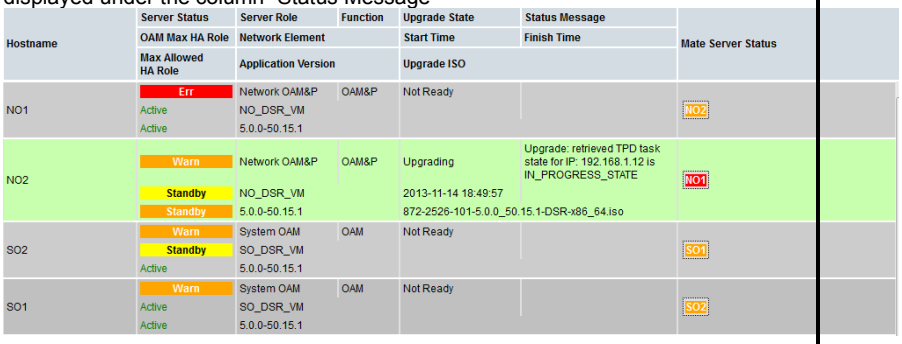
Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

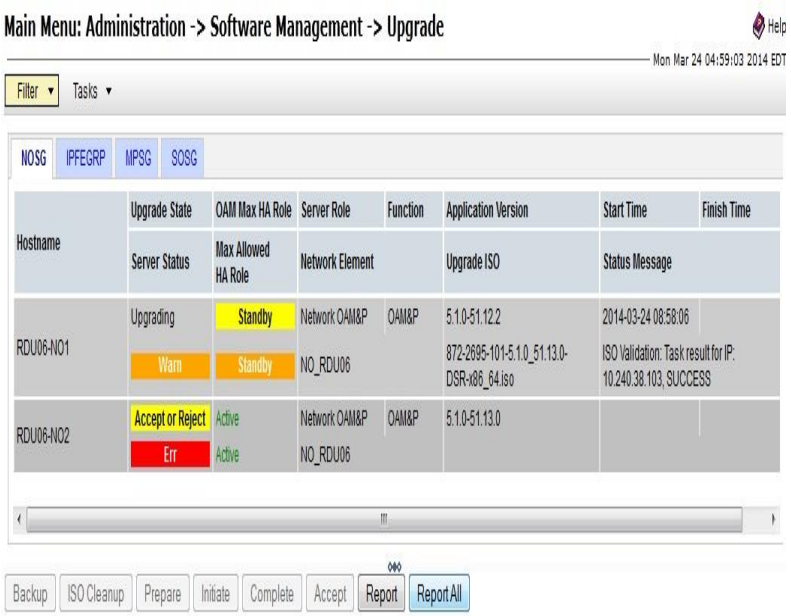
Procedure 96: Upgrade Single Server – Upgrade Administration

		
7	**NO GUI – Upgrade Administration** : Initiate Upgrade (part 2) – Select ISO form	The Initial Upgrade form will be displayed: **[DSR 4.x: Administration > Upgrade [Initiate],** **DSR 5.x: 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 be returned to the Upgrade **Administration** screen. **Upgrade initiate screen in DSR 4.x,5.0 and DSR 5.1 releases up to 5.1.0-51.12.2**  **Upgrade initiate screen in DSR 5.1 releases 5.1.0-51.13.0 and up**

Procedure 96: Upgrade Single Server – Upgrade Administration



8 ☐	View In-Progress Status (monitor)	View the Upgrade Administration form: **Note:** The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. **Upgrade Screen in DSR 4.x** 1. Observe the **Upgrade State** of the server of interest. 2. For more detailed status of the upgrade for a given server, select the server, and click the **Monitor Upgrade** button  The **Administration > Monitor** Upgrade screen is displayed, and upgrade progress data is presented. 3. Wait for the upgrade to complete. The "**Upgrade State**" under the "**Server Status**" column will show "**Success**". This step will take around 15-20 minutes. **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"  **Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up** 1. Observe the **Upgrade State** of the server of interest. Upgrade status will be displayed under the column "Status Message"



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

Alarm ID = **10008** (Provisioning Manually Disabled)
Alarm ID = **10075** (The server is no longer providing services because application processes have been manually stopped)
Alarm ID = **10073** (Server Group Max Allowed HA Role Warning)
Alarm ID = **32515** (Server HA Failover Inhibited)
Alarm ID = **31228** (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)
Alarm ID = **31283** (Highly available server failed to receive mate heartbeats)
Alarm ID = **31106** (DB Merge To Parent Failure)
Alarm ID = **31107** (DB Merge From Child Failure)
Alarm ID = **31233** (HA Secondary Path Down)
Alarm ID = **31101** (DB Replication To Slave Failure)

Wait for the upgrade to complete. The "**Upgrade State**" column will show "**Success**". This step will take around 15-20 minutes.

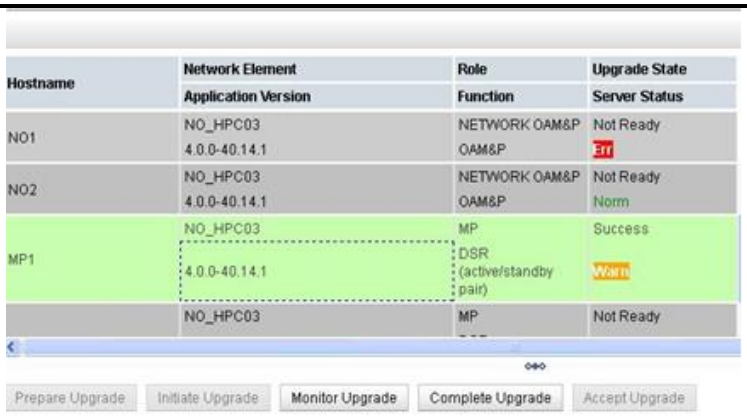
See step 9 below for instructions if the Upgrade fails, or execution time exceeds 30 minutes.

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.

9 ☐	**Optional :** View In-Progress Status from command line of server	An optional method to view Upgrade progress from a command line:
		
		In case the user wants 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 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: 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`

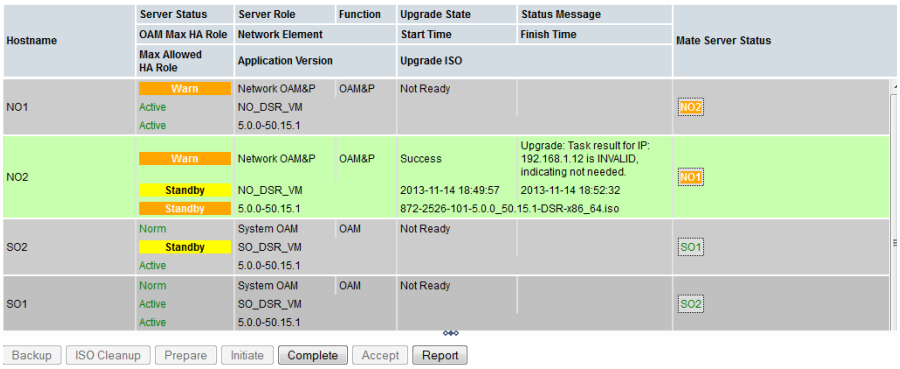
10 ☐	**IF Upgrade Fails:**	Access the server command line (via ssh or Console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		
		Contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document and provide these files.

11 ☐	**Workaround to be applied on upgraded server.**	Login to the successfully upgraded server from command line : **`# ssh root@<XMI of upgraded server>`** **`login as:  root`** **`password:  <enter password>`** Execute following command : **`# edd.op --load-all`**
12 ☐	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 DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases. 1. Select the Upgrade Administration screen (DSR4.x: "**Administration > Upgrade**" DSR5.1: " **Administration -> Software Management -> Upgrade**") 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 4.x</u>** 5. Verify the **Complete Upgrade** button is enabled for the server that was upgraded 6. Click the **Complete Upgrade** button.



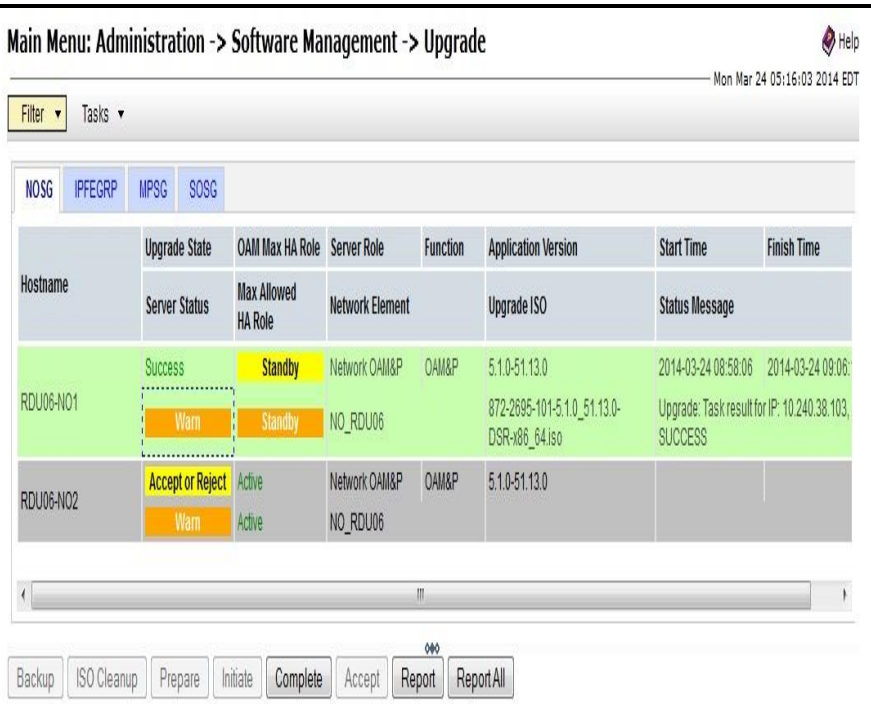
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

5. Verify the **Complete** button is enabled for the server that was upgraded
6. Click the **Complete** button.



Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

5. Verify the **Complete** button is enabled for the server that was upgraded
6. Click the **Complete** button.

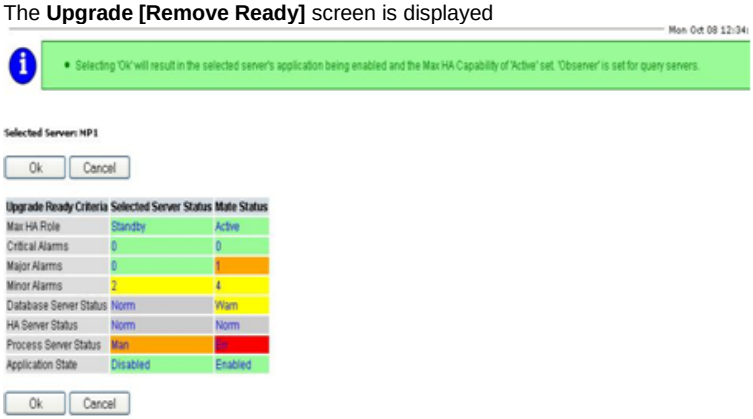


13 Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 2)

Note: The look and feel of the Upgrade screen has changed between the DSR 4.x and DSR 5.1 releases. The example below provides a snapshot from both releases.

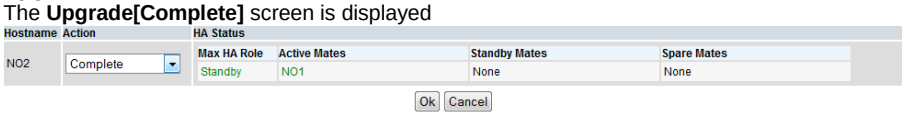
Upgrade Screen in DSR 4.x

The **Upgrade [Remove Ready]** screen is displayed



Upgrade Screen in DSR 5.1

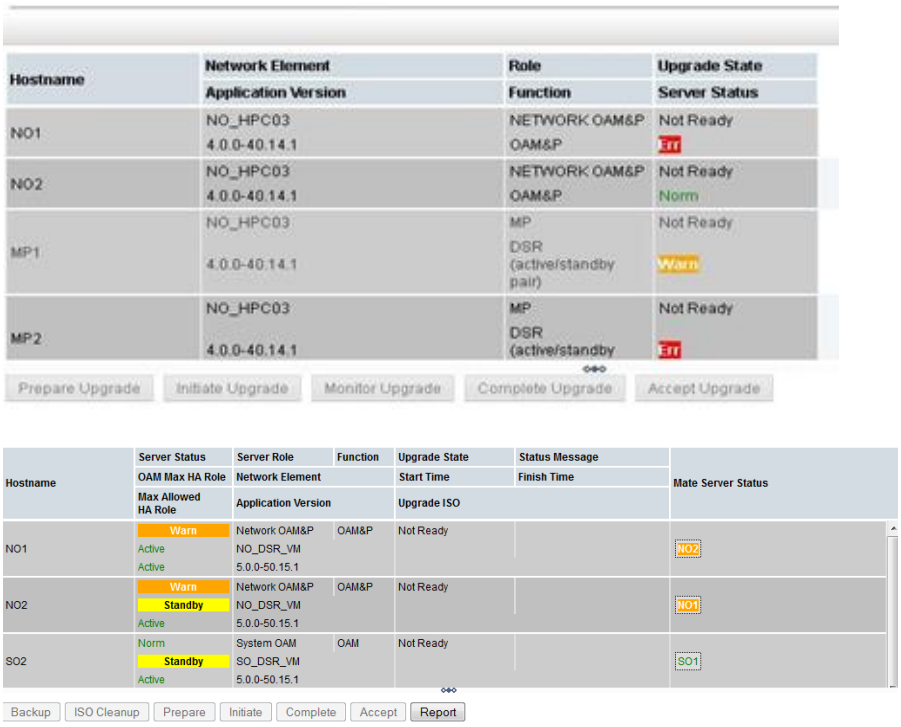
The **Upgrade[Complete]** screen is displayed



1. Record the **Upgrade Ready Criteria** and selected **Server Status** values for this server. Keep this information for future reference.
2. Click **OK**. This completes the Remove Ready action on the server. The Upgrade Administration screen is displayed.

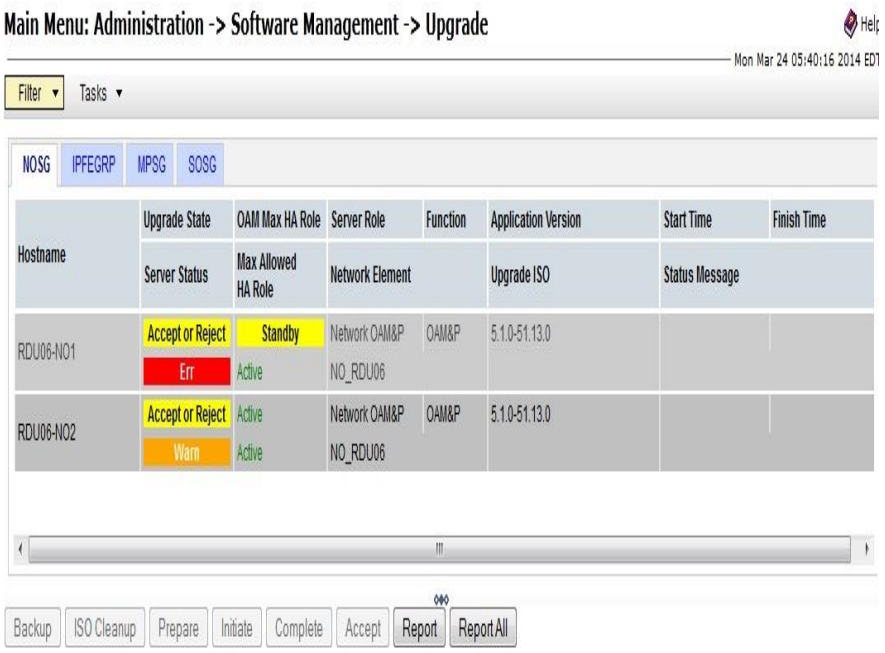
Upgrade Screen in DSR 4.x

3. Wait for **the scree**n to refresh and show the Upgrade Ready State is **Not Ready** 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 **Not Ready**.



Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

4. 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**.



14 ☐	View Post-Upgrade Status.	View the Post-Upgrade Status of the server: 1. The Active NO (or SO for a 3 –Tier setup) server **will have some or all the following expected alarm(s):** 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 = **10008** (Provisioning Manually Disabled) Alarm ID = **10010** (Stateful database not yet synchronized with mate database) Alarm ID = **32532** (Server Upgrade Pending Accept/Reject) Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault) Alarm ID = 31000 (Program impaired by s/w fault) NOTE: Do Not Accept upgrade at this time. This alarm is OK.
15 ☐	Procedure Complete.	The single server upgrade is now complete. Return to the overall DSR upgrade procedure step that directed the execution of Appendix G.

APPENDIX H. UPGRADE FIRMWARE

Firmware Upgrade procedures are not included in this document. Contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document for the latest information on Firmware upgrades.

APPENDIX I. NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

NOTE: Execute the following procedure to switch/migrate to having NetBackup installed via NBAutoInstall (Push Configuration) instead of manual installation using platcfg

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed, and then complete TPD-related tasks that are needed for effective Netbackup Client operation.
With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *Netbackup Client Install/Upgrade with platcfg*.
Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

Prerequisites:
• Application server platform installation has been completed.
• Site survey has been performed to determine the network requirements for the application server and interfaces have been configured.
• NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server.
• The filesystem for Netbackup client software has been created (Create LV and Filesystem for Netbackup Client Software)
• Contact the Oracle CGBU Customer Care Center to determine if the version of Netbackup Client being installed requires workarounds.

1. Follow Oracle CGBU Provided Workarounds
   Follow Oracle CGBU provided procedures to prepare the server for Netbackup Client install using nbAutoInstall.

2. **Application server iLO:** Login and launch the integrated remote console
   SSH to the application Server (PM&C or NOAM) as root using the management network for the PM&C or XMI network for the NOAM.

3. Enable nbAutoInstall:
   Execute the following command:
   ```
   # /usr/TKLC/plat/bin/nbAutoInstall --enable
   ```
   The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly.
   At any time, the customer may now push and install a new version of Netbackup Client.

4. Return to calling procedure if applicable.

APPENDIX J. 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.

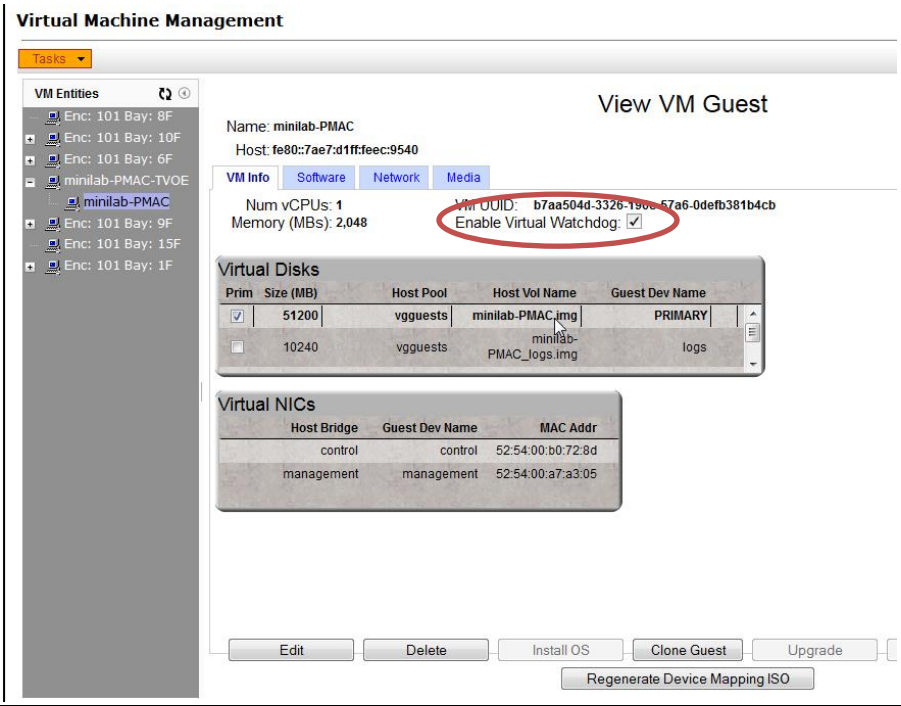
Procedure 97: Upgrade TVOE Platform

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Disable all the applications running on current TVOE blade.	1. Log into the NOAM VIP GUI 2. Select **Status & Manage > Server.** The Server Status screen is displayed 3. Identify the NO or SO (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 ☐	Find out the guests running on TVOE host.	1. List the guests running on the TVOE Host by using following command :
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		`# virsh list --all`
		Note: the output of above command will list all the guests running on current TVOE host.

3 ☐	Shutdown each guest running on TVOE host.	1. Execute the following command for each guest identified in Step 2 : `# virsh shutdown <guestname>`
4 ☐	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` 2. Once all VMs have been properly shut down: **Upgrade TVOE** using "PMAC Aided TVOE Upgrade Procedure" from Reference [2] *TVOE 2.5 upgrade Document. 909-2276-001. V 1.0 or greater.*. [If the "PMAC Aided TVOE Upgrade" procedure is not possible, it is also possible to upgrade TVOE using the alternate procedure provided in Reference [2].] **Note: If Active NO is hosted on the TVOE blade which is being upgraded, then VIP may be lost until TVOE is successfully upgraded.**

Procedure 97: Upgrade TVOE Platform

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.
6	Verify Enable Virtual Guest Watchdog is set for VM	From the PMAC VM Management form, verify that the "Enable Virtual Watchdog" is checked. 

7	Start guests on TVOE host.	Execute following steps :
		a) Log into upgraded TVOE Host by using following command :
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		b) 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>`
		c) Periodically execute the following command until the command displays all the VM guests running.
		`# virsh list`

Procedure 97: Upgrade TVOE Platform

8 ☐	Enable all the applications disabled in step1	Enable all applications running on current TVOE blade: Log into the NOAM VIP GUI a) Select **Status & Manage > Server.** The Server Status screen is displayed b) Select all the applications (NO(s)/SO(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. c) Click the '**Restart**' button. d) Confirm the operation by clicking **Ok** in the popup dialog box. e) Verify that the 'Appl State' for all the selected servers is changed to '**Enabled**'.

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

Procedure 98: 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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**NO GUI – Upgrade Administration:** View the pre-upgrade status of Servers	From the Active NOAM GUI: Select **Upgrade Administration** form DSR 5.x: " **Administration -> Software Management -> Upgrade**") The Upgrade Administration screen is displayed (example below): **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2** **The following status may be expected:** Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	**NO GUI – Upgrade Administration:** 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", 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 Policy 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.

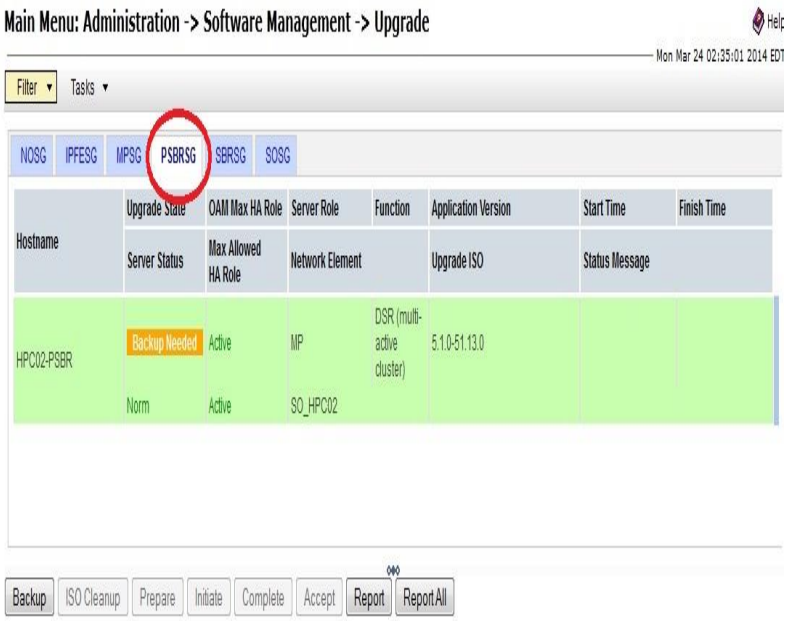
Hostname	Server Status OAM Max HA Role Max Allowed HA Role	Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO2
Viper-NO2	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 98: Upgrade Multiple Servers – Upgrade Administration

3. Verify the Upgrade State is **Not Ready** for each MP server to be upgraded.

Only Required for DSR 5.1 releases 5.1.0-51.13.0 and up:

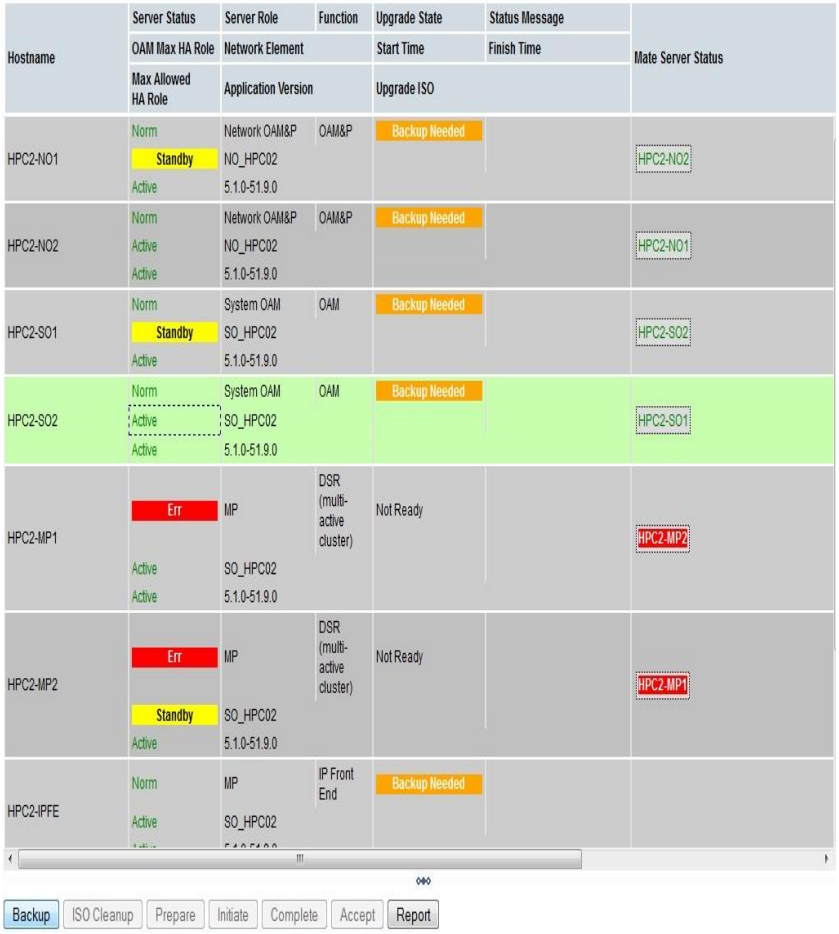
- From the Administration -> Software Management -> Upgrade screen, select the Server Group of the server which needs to be upgraded.



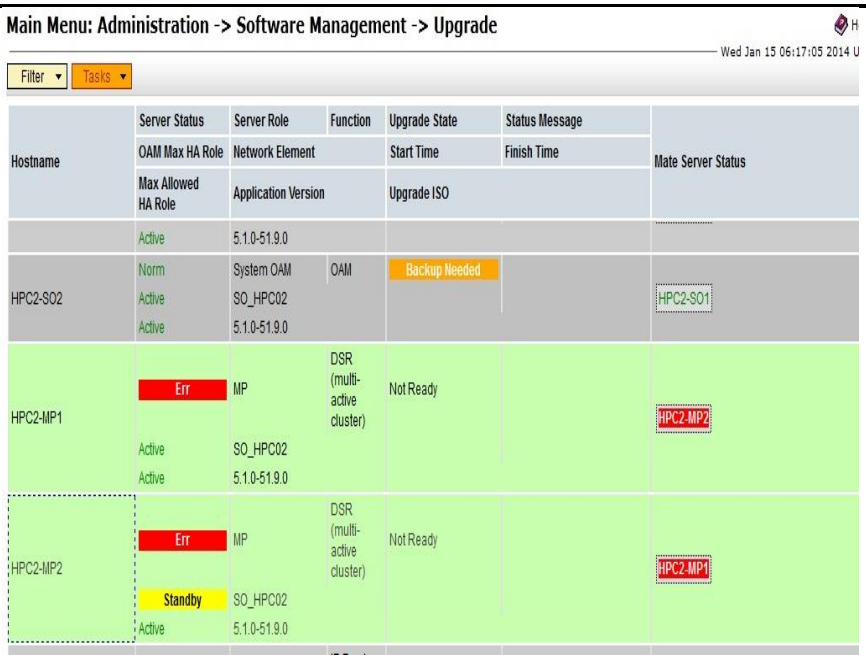
Required for all DSR releases :

- If the servers are in 'Ready' state then skip the "Prepare Upgrade" steps and start the upgrade at Step 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.

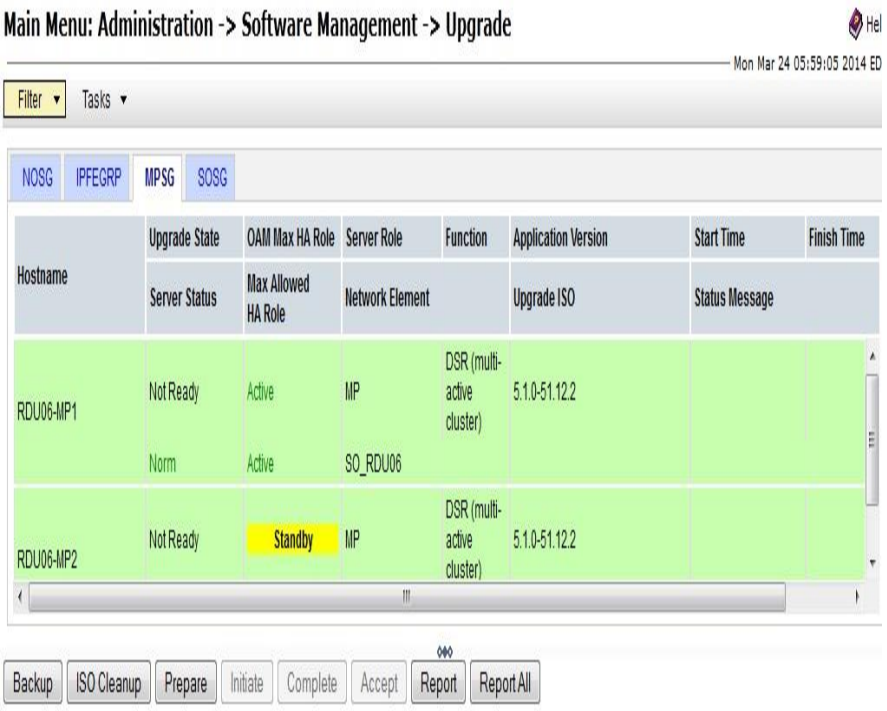
Procedure 98: Upgrade Multiple Servers – Upgrade Administration

		
3	**NO GUI – Upgrade Administration:** Prepare Upgrade (step 1)	For the server s to be upgraded: On the Upgrade form, make the server 'Upgrade Ready', by selecting the servers to be upgraded (using Ctrl button) and, Select: **Prepare** (In this example, MP1 and MP2 will be made ready for Upgrade) **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2**

Procedure 98: Upgrade Multiple Servers – Upgrade Administration

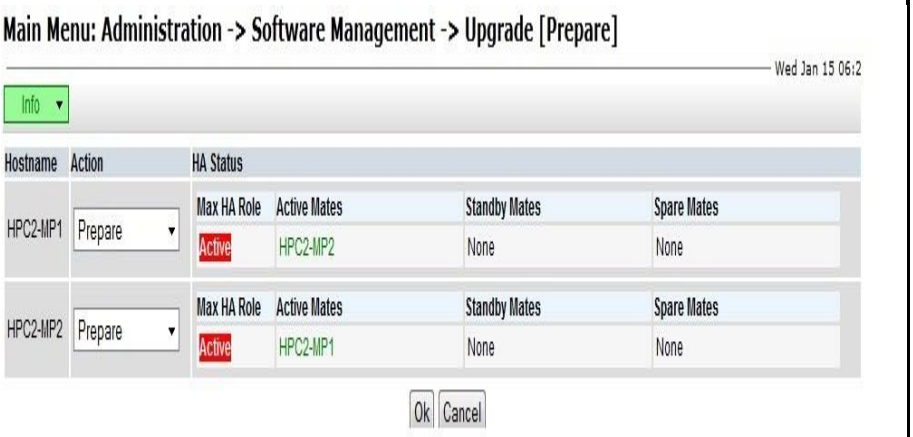


Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

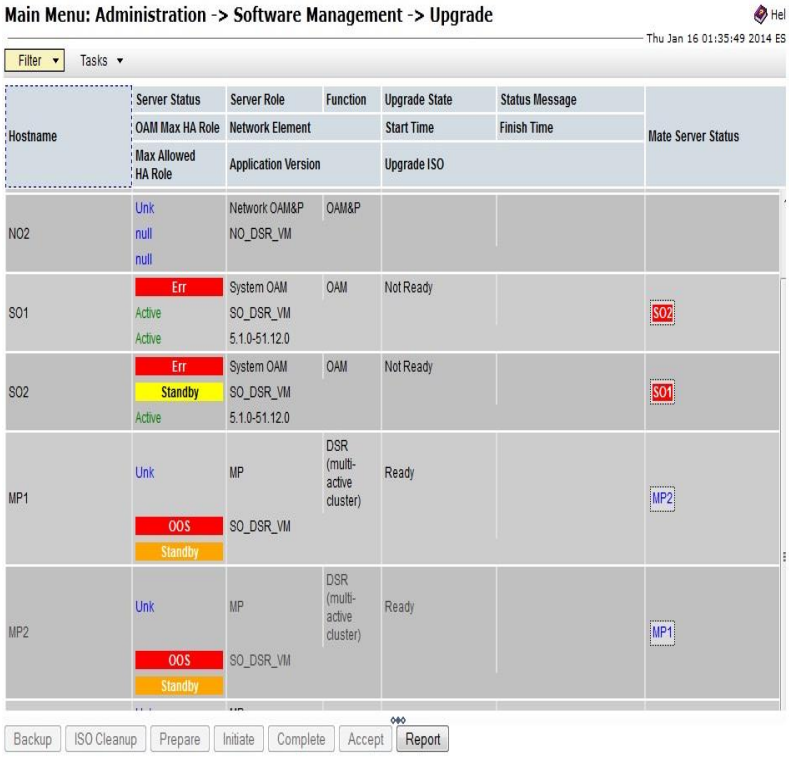


The Upgrade “Make Ready” form will be displayed. (see next step)

Procedure 98: Upgrade Multiple Servers – Upgrade Administration

4 ☐	**NO GUI – Upgrade Administration:** 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", you MUST use the "Resource HA Role" value from the Policy 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 Policy SBR Status screen.** 2. If the condition of the Server to be upgraded is as expected, then: Select: **OK** **Upgrade screen in DSR 5.x**  ***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.*** ***For a 2-tier Active-Standby Setup, the Make Ready action on a DA-MP server MAY cause the value in the HA Status field under the Selected Server Status be shown as 'Active' for both DA-MP(s). This is OK. Please proceed with upgrade.***
5 ☐	**NO GUI – Upgrade Administration:** 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**

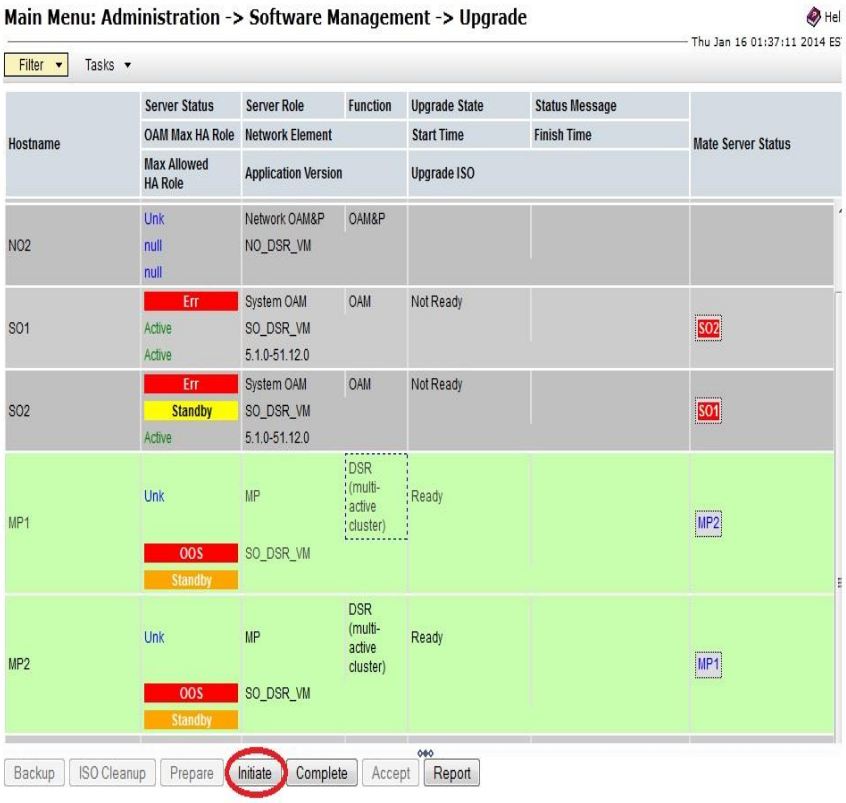
Procedure 98: Upgrade Multiple Servers – Upgrade Administration



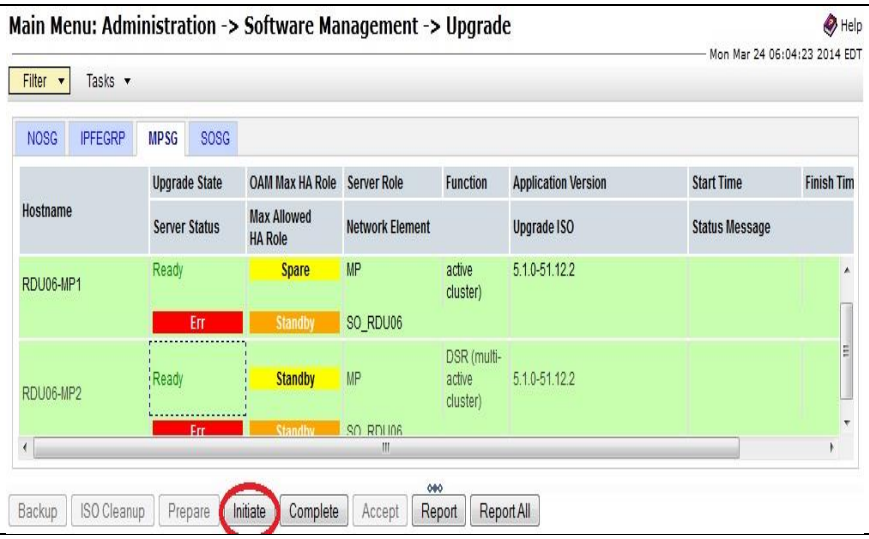
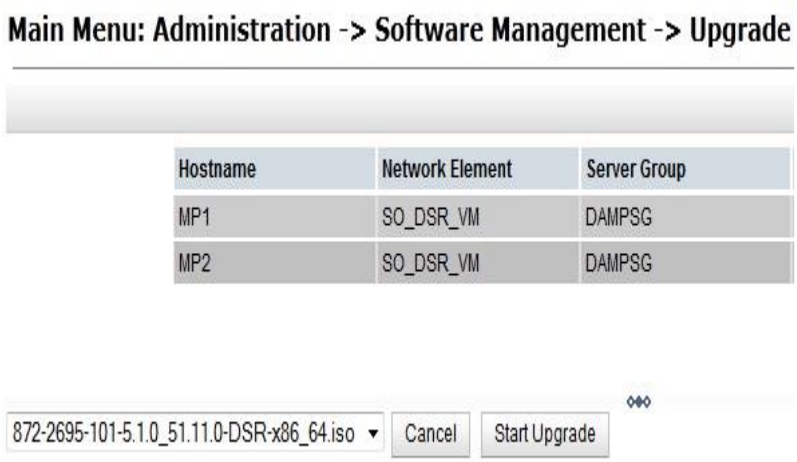
Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

Depending on the server being upgraded, new alarms may occur.

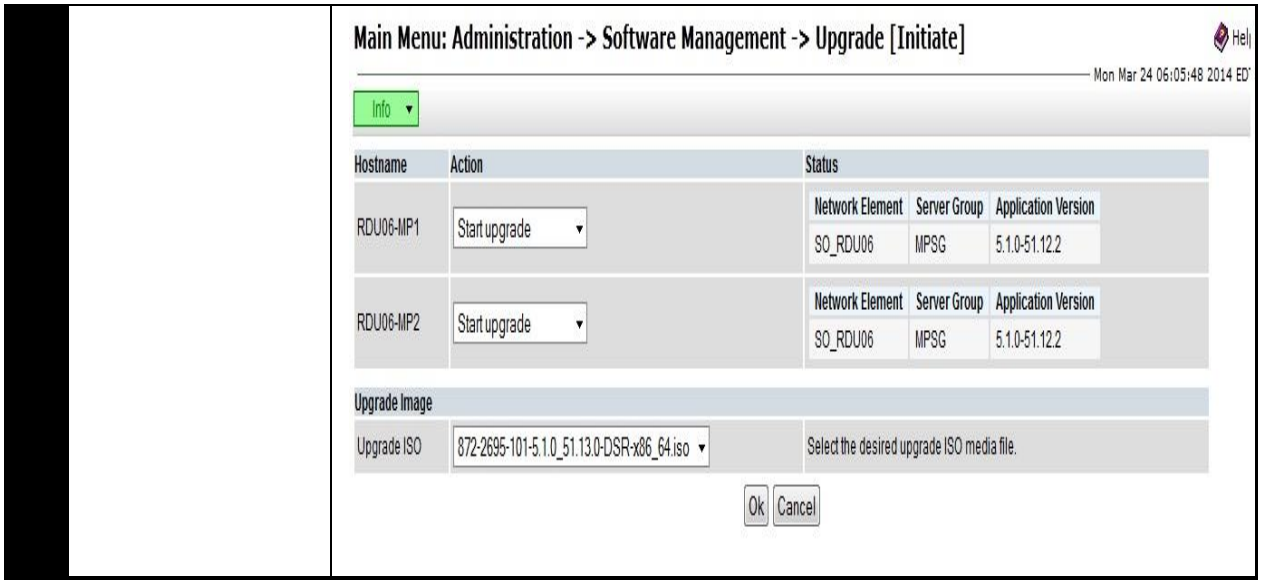
Procedure 98: Upgrade Multiple Servers – Upgrade Administration

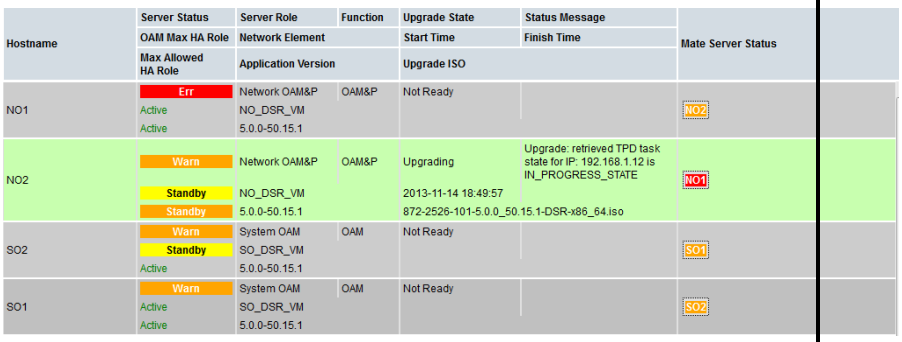
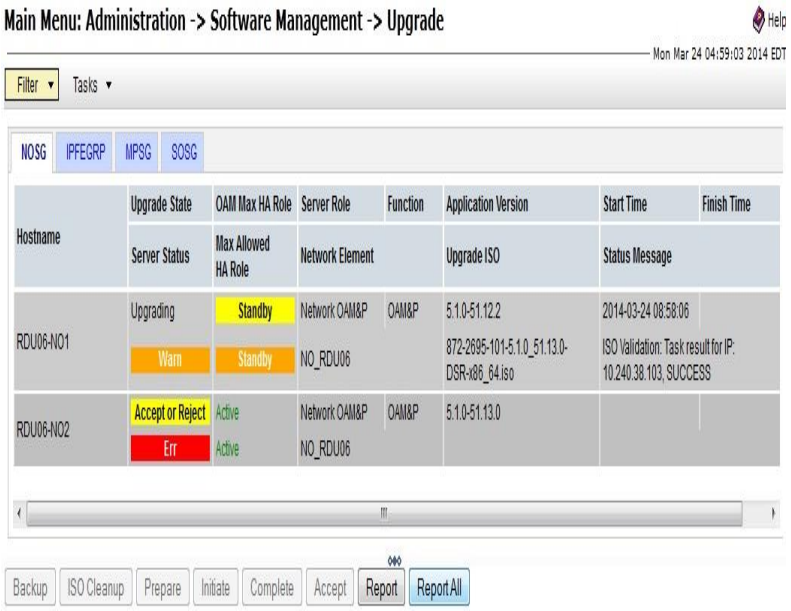
		Servers may have a combination of the following expected alarms. Note: Not all servers have all alarms: Alarm ID = **10008** (Provisioning Manually Disabled) Alarm ID = **10075** (The server is no longer providing services because application processes have been manually stopped) Alarm ID = 10073 (Server Group Max Allowed HA Role Warning) Alarm ID = **32515** (Server HA Failover Inhibited) Alarm ID = **31228** (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)
6	**NO GUI – Upgrade Administration** : Initiate Upgrade (initiate) (part 1)	Initiate Upgrade on the servers: **<u>Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2</u>** 1. While viewing the Upgrade Administration screen, select the servers to be upgraded 2. Ensure that the "**Initiate"** button is enabled for the servers to be upgraded. 3. Click the "**Initiate"** button.  **<u>Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up</u>**

Procedure 98: Upgrade Multiple Servers – Upgrade Administration

		
7	**NO GUI – Upgrade Administration** : Initiate Upgrade (part 2) – Select ISO form	The Initial Upgrade form will be displayed: **DSR 5.x: 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. **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2**  **Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up**

Procedure 98: Upgrade Multiple Servers – Upgrade Administration



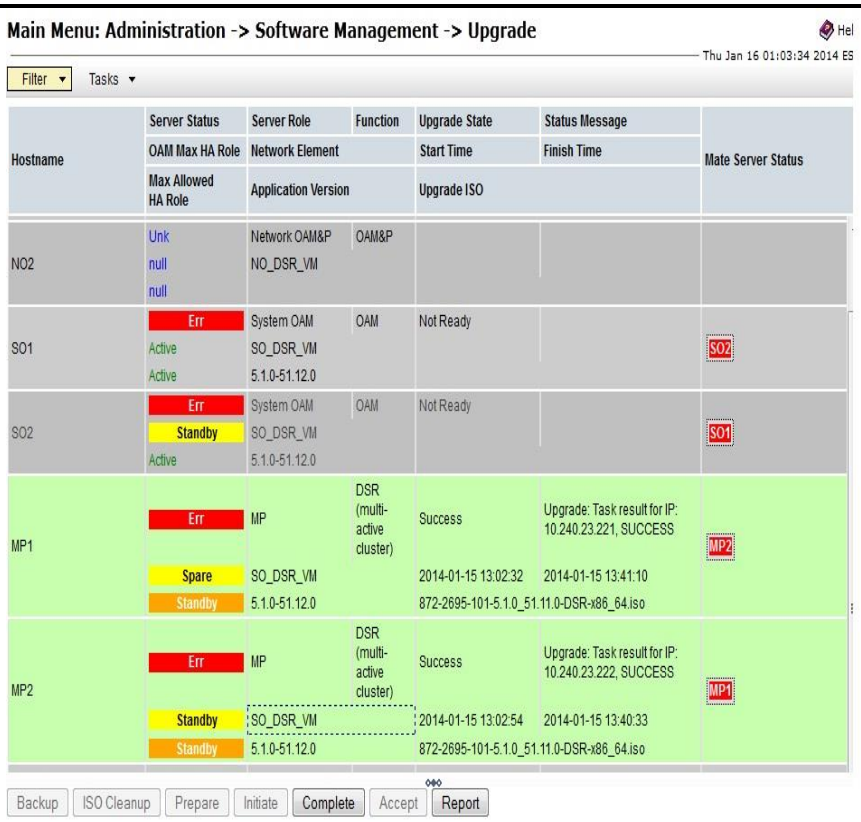
8	View In-Progress Status (monitor)	The View Upgrade Administration form: **Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2** 1. Observe the **Upgrade State** of the servers of interest. The upgrade status will be displayed under the column "Status Message"  **Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up**  Wait for the upgrade to complete. The "**Upgrade State**" column will show "**Success**". This step will take around 15-20 minutes. Servers may have a combination of the following expected alarms. Note: Not all servers have all alarms: Alarm ID = **10008** (Provisioning Manually Disabled) Alarm ID = **10075** (The server is no longer providing services because application processes have been manually stopped) Alarm ID = **10073** (Server Group Max Allowed HA Role Warning) Alarm ID = **32515** (Server HA Failover Inhibited) Alarm ID = **31228** (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server) Alarm ID = **31283** (Highly available server failed to receive mate heartbeats) Alarm ID = **31106** (DB Merge To Parent Failure) Alarm ID = **31107** (DB Merge From Child Failure) Alarm ID = **31233** (HA Secondary Path Down) Alarm ID = **31101** (DB Replication To Slave Failure)

		See step below for instructions if the Upgrade fails, or execution time exceeds 30 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.*

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`

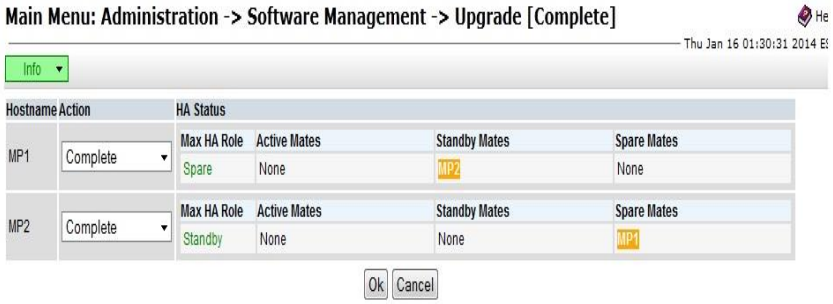
10 ☐	**IF Upgrade Fails:**	Access the server command line (via ssh or Console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		
		Contact the Oracle CGBU Customer Care Center by referring to Appendix O of this document and provide these files.

11 ☐	**Workaround to be applied on upgraded servers.**	Login to each of the successfully upgraded servers from command line : **`# ssh root@<XMI of upgraded server(s)>`** **`login as: root`** **`password: <enter password>`** Execute following command on each upgraded server: **`# edd.op --load-all`**
12 ☐	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 status: 4. Verify the **Upgrade State** of the servers that was upgraded is **Success**. **Upgrade Screen in DSR 5.x** 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.



13 Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 2)

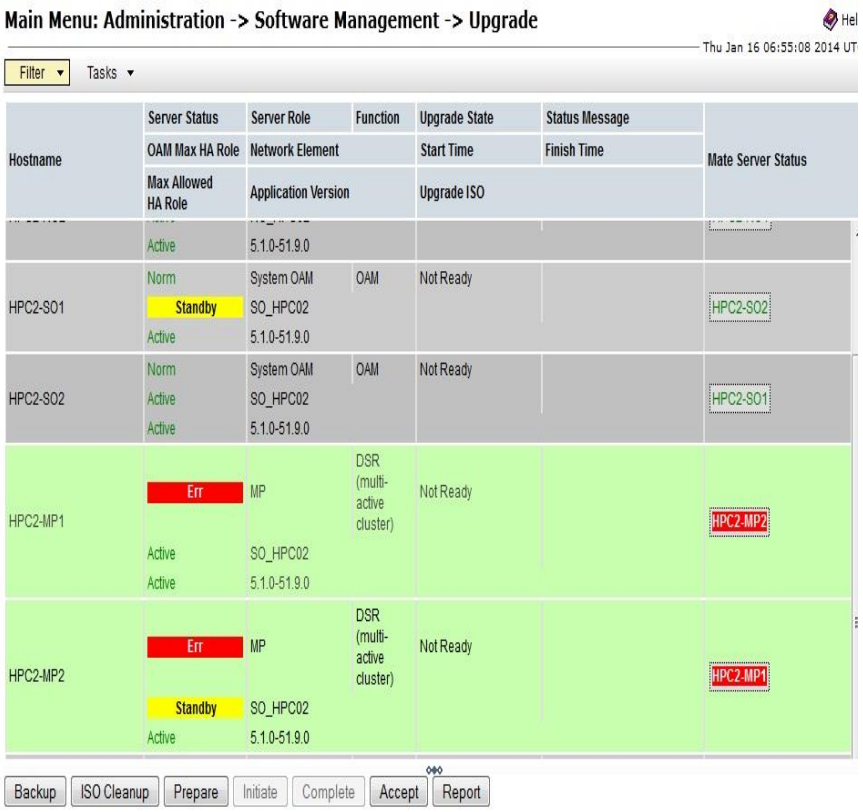
The **Upgrade[Complete]** screen is displayed



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.

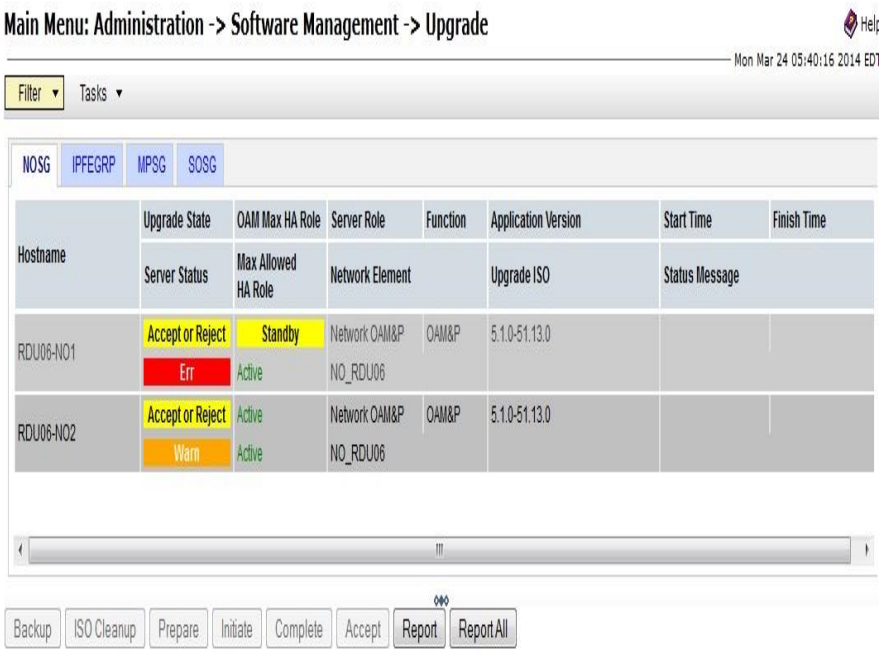
Upgrade screen in DSR 5.0 and DSR 5.1 releases up to 5.1.0-51.12.2

4. Wait for the screen to refresh and show the Upgrade Ready State is **Not Ready** 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 **Not Ready**.



Upgrade screen in DSR 5.1 releases 5.1.0-51.13.0 and up

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**.



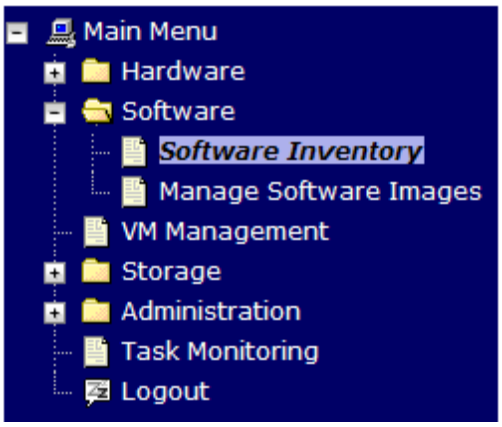
14 ☐	View Post-Upgrade Status.	View Post-Upgrade Status of the server: 1. The Active NO (or SO for a 3 –Tier setup) **server will have some or all the following expected alarm(s):** Alarm ID = **10075** (The server is no longer providing services because application processes have been manually stopped) Or Alarm ID = **31000** (Program impaired by S/W Fault) Alarm ID = **10008** (Provisioning Manually Disabled) Alarm ID = **10010** (Stateful database not yet synchronized with mate database) Alarm ID = **32532** (Server Upgrade Pending Accept/Reject) Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault) Alarm ID = 31000 (Program impaired by s/w fault) NOTE: Do Not Accept upgrade at this time. This alarm is OK.
15 ☐	Procedure Complete.	The multiple servers upgrade is now complete. Return to the overall DSR upgrade procedure step that directed the execution of Appendix K.

APPENDIX L. ALTERNATE SERVER UPGRADE USING PM&C

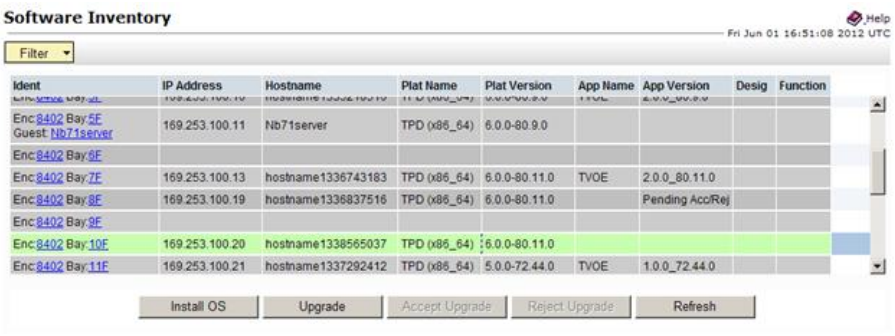
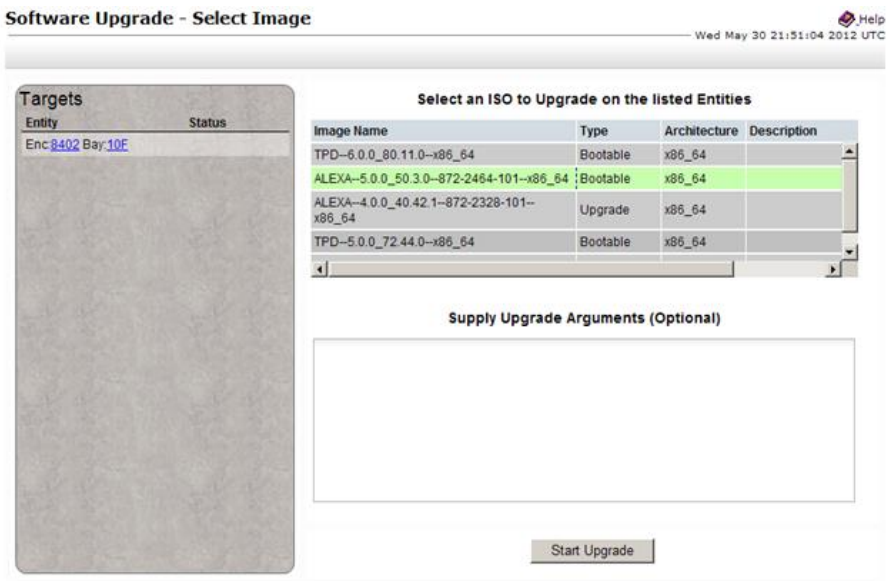
This appendix provides the procedure for upgrading the Standby NO and DR-NO using the PM&C interface. This upgrade method is an alternative to using the NOAM Upgrade GUI, and is used only when the NOAM Upgrade GUI refresh is sluggish due to the large number of C-level servers.

Note: Before executing this procedure, download the target release ISO to the PM&C image repository in accordance with Appendix F, Adding ISO Images to PM&C Image Repository.

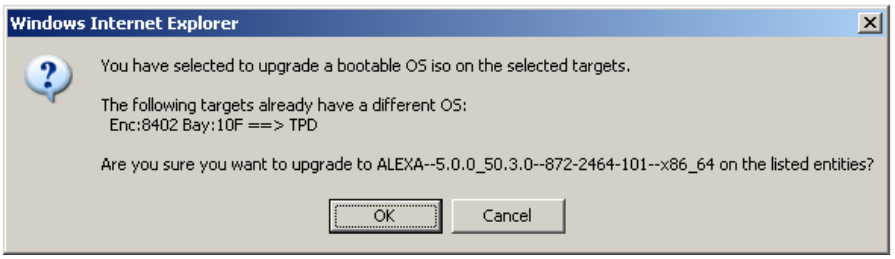
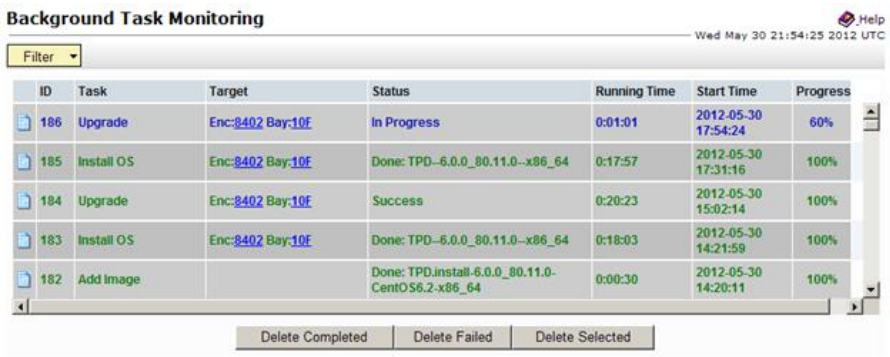
Procedure 99: Alternate Server Upgrade using PM&C

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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 99: 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. 

Procedure 99: Alternate Server Upgrade using PM&C

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

APPENDIX M. EXPIRED PASSWORD WORKAROUND PROCEDURE

This appendix provides the procedures to handle a password expiration during upgrade. Procedure 100 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 101 after the site is upgraded. Failure to remove the workaround will inhibit password aging on the server.

Appendix M.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 100: Inhibit Password Aging

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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:
		`ssh root@<server_ip>`
		(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`

Procedure 100: Inhibit Password Aging

		5. 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.

Appendix M.2. Enable Password Aging

This procedure removes the password expiration workaround that is enabled by Procedure 100.

Procedure 101: Enable Password Aging

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, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER 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:
		
		`ssh root@<server_ip>`
		
		(Answer 'yes' if prompted to confirm the identity of the server.)
		
		2. Delete the pw.ini file:
		
		`# rm /var/TKLC/appworks/ini/pw.ini`
		
		3. Execute the following command:
		
		`# clearCache`
		
		4. Repeat sub-steps 1 through 4 for the Standby SOAM

2 ☐	Repeat for other upgraded sites	Repeat step 1 for other upgraded sites.

APPENDIX N. POLICY DRA APN TABLE VALIDATION PROCEDURE

This section defines the procedures that are executed to validate the Access Point Names (APN) database table on a DSR system with release 4.1.5 or 5.0. When upgrading from DSR 4.1.5 or 5.0 to a later release, the APN table potentially may have conflicting database entries. These procedures contain the steps to detect and resolve these conflicts.

Appendix N.1. APN Table Validation Preparation

This procedure is part of P-DRA APN conflict resolution preparation. It is used to obtain the Conflict Resolution Tool, and determine the health and status of the DSR system network and servers.

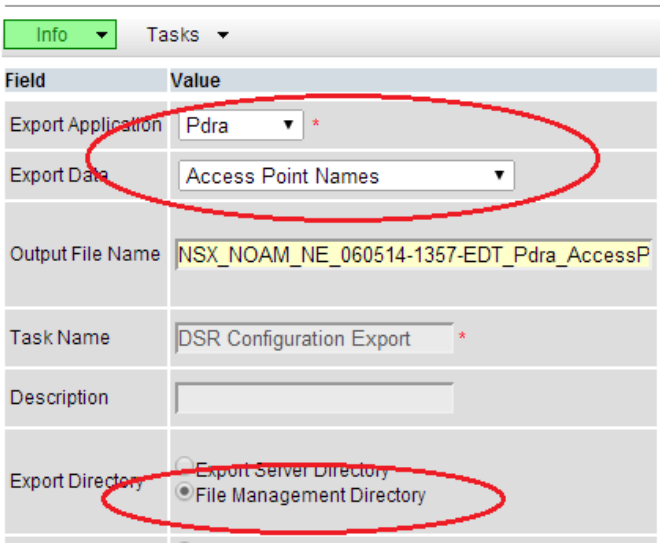
Procedure 102: APN Table Validation Preparation

S T E P #	This procedure performs a health check of the PDRA system prior to checking the APN table for conflicts. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify DSR Release	Verify the DSR Release supports the P-DRA Application: 1. Log into the NOAM VIP GUI. 2. Select **Administration > Software Versions** The DSR Software Versions Report screen is shown. 3. Verify the Eagle XG DSR RPM Version shows version 5.0.x or less.
2 ☐	Verify Server status	Verify Server status: From the Active NOAM GUI: 1. Select **Status & Manage > Server** The Server Status screen is shown. 2. Verify Server Status is Normal (Norm) for Replication (Repl), Collection (Coll), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed if any of the following is not **Norm: Alm, DB, Reporting Status, Proc**. If any of these is not Norm, corrective action should be taken to restore the status to Norm before proceeding with the APN conflict resolution. Contact the Oracle CGBU Customer Care Center for assistance as necessary. 4. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the APN conflict resolution. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the resolution. The resolution may be able to proceed in the presence of certain Major or Critical alarms. Contact the Oracle CGBU Customer Care Center for assistance as necessary.
3 ☐	Log all current alarms	Log all current alarms in the system: From the Active NOAM GUI: 1. Select **Alarms & Events > View Active** **T**he Alarms & Events > View Active view is shown. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference. 4. Select **Alarms & Events > View History** and repeat steps 2 and 3.

Procedure 102: APN Table Validation Preparation

<table>
<tr><td>4 ☐</td><td>Export APN data</td><td>Export the APN table data to the local workstation.

From the Active NOAM GUI:
1. Select Diameter > Configuration > Export.
The Export form is displayed.
2. Complete the form as shown in the figure below. For Output File Name, accept the default filename, or enter a custom filename.
3. Click Ok.

4. Browse to Main Menu >Status & Manage >Files and download the exported file to the client machine. The exported APN data is to be used for data recovery in the event that the wrong APN is deleted in Procedure 104.</td></tr>
<tr><td>5 ☐</td><td>Proceed to next procedure</td><td>Proceed to Procedure 103, APN Conflict Detection.</td></tr>
</table>

Appendix N.2. APN Conflict Detection

This section provides the detailed procedure steps of the APN Conflict Detection.

!! WARNING!! This and the subsequent procedures require replication to be working throughout the DSR system. Please do not proceed further if any replication Alarm (e.g. 31101) is present on the system. Please contact the Oracle CGBU Customer Care Center for assistance.

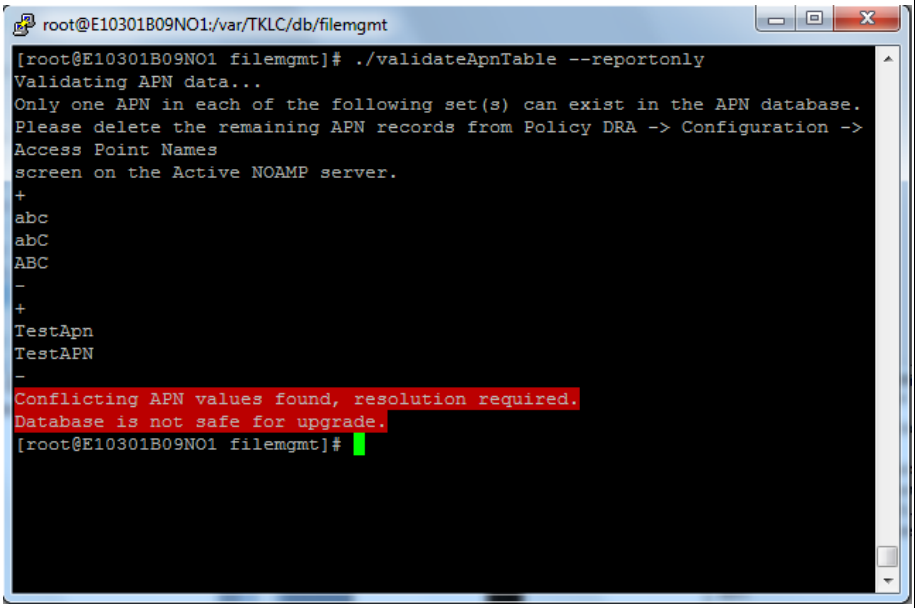
Procedure 103:

APN Conflict **Detection**

S T E P #		
	This procedure detects the presence of APN conflicts in the database. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Conflict Resolution tool is accessible.	1. Download the Conflict Resolution Tool from the following link, which will open the file in the default web browser. http://twiki.ssz.tekelec.com/bin/viewfile/Engineering/Nextgen/Pdra51ApnResolution?rev=3;filename=validateApnTable 2. Use the browser's "Save As" feature to save the downloaded file on the local workstation as a text file with the filename "validateApnTable" (with no file type suffix).
2 ☐	Upload the Resolution Tool to the Active NOAM server File Management Area	From the Active NOAM GUI: 1. Navigate to **Main Menu > Status & Manage > Files.** 2. Click Upload, Browse and locate the file downloaded in step 1 and click Upload again. Please wait for the upload to complete. If the upload was successful, the file will appear in the list on the Files screen. **3.** Confirm that the file size displayed matches what was downloaded earlier.
3 ☐	Establish a secure shell session on the Active NOAM	1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM: `ssh root@<server_ip>` (Answer 'yes' if prompted to confirm the identity of the server.) Note: Using the NOAM VIP address will automatically connect to the active NOAM.
4 ☐	Change directory to the File Management Area.	Change to the File Management Area `# cd /var/TKLC/db/filemgmt`

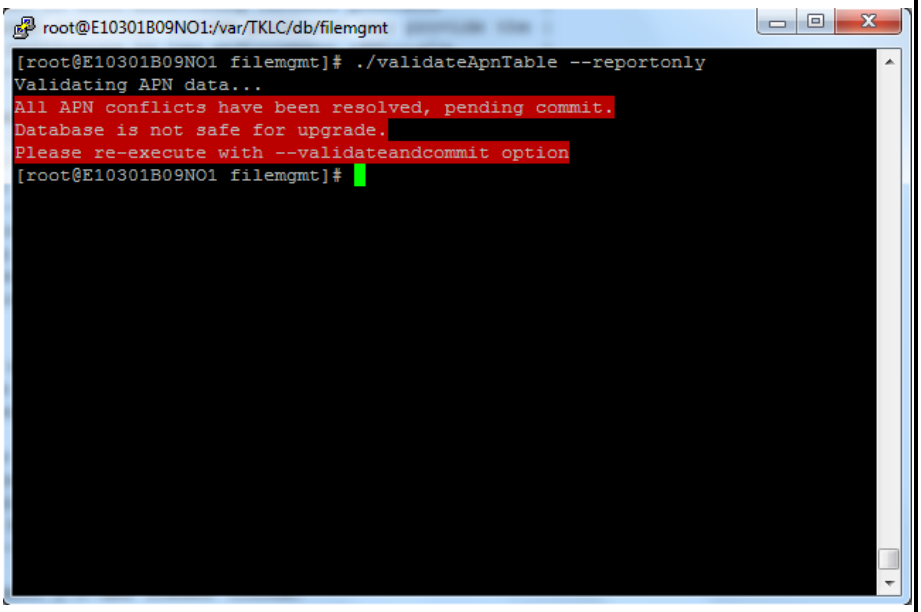
Procedure 103:

APN Conflict **Detection**

5 ☐	Convert to Unix format	Convert the script to Unix format: `# dos2unix validateApnTable`
6 ☐	Set required permissions	Set required permissions on the file: `# chmod +x validateApnTable`
7 ☐	Run the Conflict Resolution Tool in report only mode	The following command will run the conflict resolution tool in detection mode, i.e. the command will not resolve any conflicts or alter the database in any way. It will only present a report of the conflicting APN values, if any. `# ./validateApnTable --reportonly` The next course of action depends on the output of the tool. Various possible outputs are detailed in steps 7 (a) through 7(c). Please follow the "**Next Action**" mentioned in the step that matches the output.
7(a) ☐	Conflicts found	If the tool finds any conflicting APN records present in the database, it will display those records in a format as shown below with the following message: **"Conflicting APN values found, resolution required. Database is not safe for upgrade."** **Next Action:** Follow Procedure 104, APN Conflict Resolution to resolve the conflicts. Sample: 

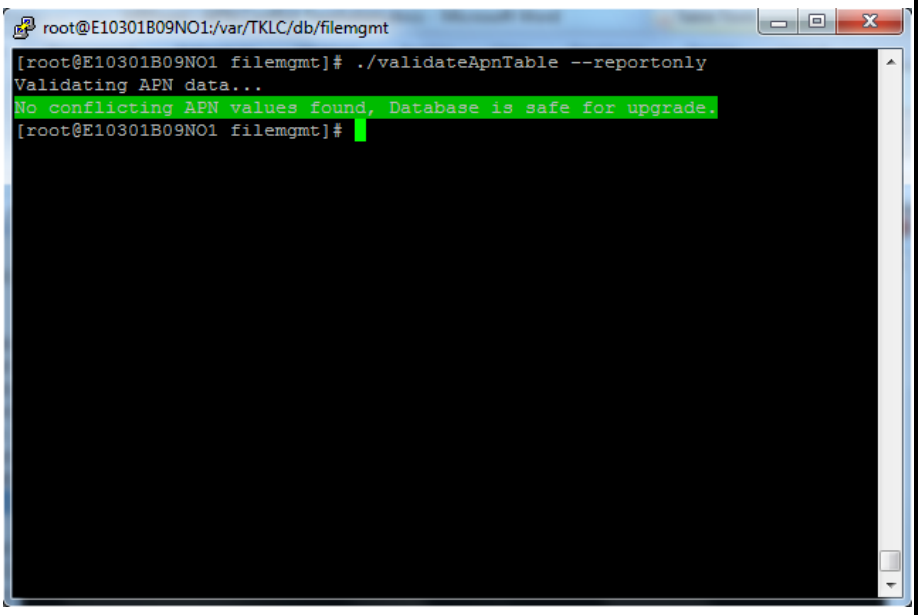
Procedure 103:

APN Conflict **Detection**

7(b) ☐	No conflicts found, commit required	If the tool does not find any conflicts in the database, however it detects that a commit is required, then it will report this as: **"All APN conflicts have been resolved, pending commit.** **Database is not safe for upgrade.** **Please re-execute with --validateandcommit option"** **Next Action:** Follow Procedure 105, DB Validate and Commit to execute the database commit. Sample: 

Procedure 103:

APN Conflict **Detection**

7(c) ☐	No conflicts found, commit not required.	If the tool does not find any conflicting APNs, and no database commit is required, then it will report this as: **"No conflicting APN values found, Database is safe for upgrade."** **Next Action:** No Action Required. Continue with PDRA upgrade. Sample: 

Appendix N.3. APN Conflict Resolution

This procedure resolves the conflicts found in the APN database.

NOTE:- This procedure needs to be executed only if the APN Conflict Resolution Tool reported conflicts in the database. If unsure, please refer to Procedure 103 **Step 7.**

Procedure 104: APN Conflict Resolution

S T E P #	This procedure resolves the conflicts reported by the preceding procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 104: APN Conflict Resolution

1 ☐	Identify the APN records that are valid and being used by message processing servers	The report of the tool groups the conflicting records into sets of APN values that are different only by case. The goal here is to reduce each such set to have at most one APN.
		
		In each set, identify one name and designate it as "Valid". This might need consultation with the Network Operator/Administrator. Call all the other names in the set as "Invalid". Note down all such "Invalid" AP names. All APN records in all sets other than the ones designated as "Valid" will be considered as obsolete and safe for removal.
		
		Consideration for selection of a valid APN:
		
		The technician (in consultation with the network administrator) must gather information about the (case of the) Access Point Names configured in the Policy Client nodes that are connected to the DSR system, and from which the DSR expects to receive messages on the Gx/Rx/GxPrime or other supported interfaces. Such AP names are the ones that are to be chosen as valid.
		
		NOTE: The APN is contained in the "Called-Station-Id" AVP of Diameter Messages such as CCR, AAR etc.
		
		NOTE: In case different Policy Client nodes have different cases of the same APN configured, the technician needs to pick one of them. In such scenarios, APN values contained in the messages coming from the other nodes (i.e. the nodes having the APN case that were not picked) will be ignored. See the paragraph below for expected behavior.
		
		Please take extreme care to select the correctly cased APN records as "Valid" records as otherwise the APN received in incoming messages will be ignored until the system is upgraded to release 5.1 or later. Alarm 22730 is expected to be raised with minor severity.
		
		Sample output of validateApnTable executed in Procedure 103 Step 7.
		
		`Validating APN data...`
		`Only one APN in each of the following set(s) can exist in the APN database.`
		`Please delete the remaining APN records from Policy DRA -> Configuration -> Access Point Names`
		`screen on the Active NOAMP server.`
		`+`
		`abc`
		`abC`
		`ABC`
		`-`
		`+`
		`TestApn`
		`TestAPN`
		`-`
		`Conflicting APN values found, resolution required.`
		`Database is not safe for upgrade.`
		
		For the first set in the example above, the technician performing this procedure needs to select one value among "abc", "abC" and "ABC" and designate it as valid. Let us say "abc" is valid.
		
		For the second set, select one value between "TestApn" and TestAPN" and designate it as valid. Let us say "TestApn" is valid.

2 ☐	Navigate to Access Point Names screen	From the Active NOAM GUI: Navigate to **Main Menu: Policy DRA -> Configuration -> Access Point Names**
3 ☐	Delete the Invalid APN records	One-by-one, select and delete all records that were identified as "Invalid" APN records in step 1. Example: Following the above example, select and delete "abC", "ABC" and "TestAPN".

Procedure 104: APN Conflict Resolution

4 ☐	Go back to Conflict detection	Repeat Procedure 103 Step 7 to ensure that all conflicts have been resolved.

Appendix N.4. DB Validate and Commit

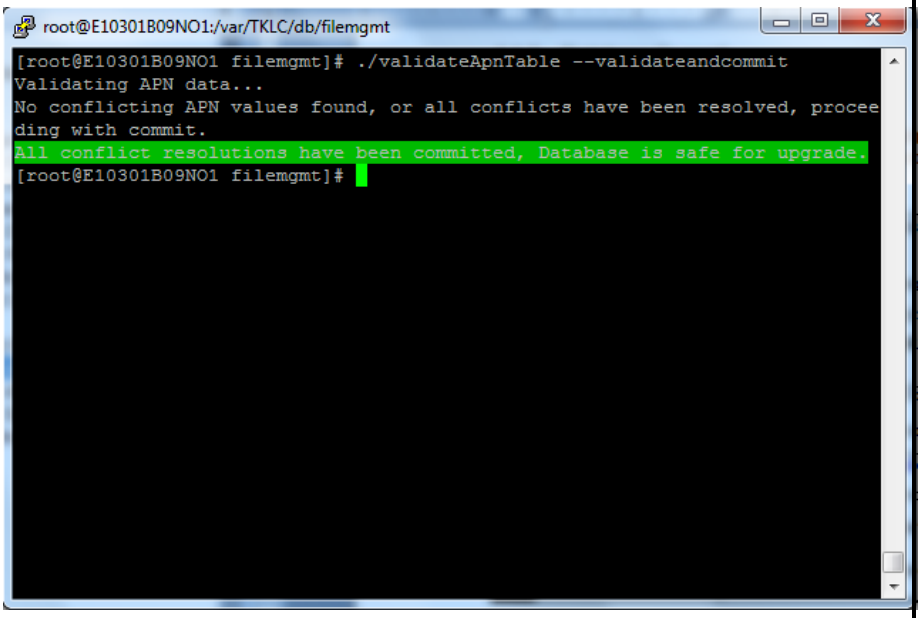
This procedure commits the conflict resolution changes to the database.

NOTE:- This procedure needs to be executed only if the APN conflict resolution tool reported that commit is pending. If unsure, please refer to Procedure 103 **Step 7.**

Procedure 105: DB Validate and Commit

S T E P #	This procedure commits the resolutions to the database. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT THE ORACLE CGBU CUSTOMER CARE CENTER AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Return to the secure shell session on the Active NOAM	Return to the secure shell console of Procedure 103 Step 7. If that console has been closed, please follow Procedure 103 steps 3 and 4.

Procedure 105: DB Validate and Commit

1 ☐	Run the Conflict Resolution Tool in validate and commit mode.	Execute the following command: **# ./validateApnTable --validateandcommit** This will validate and commit the conflict resolutions and confirm the same with the following message: **"All conflict resolutions have been committed, Database is safe for upgrade."** Sample: 

APPENDIX O. ACCESSING ORACLE CGBU'S CUSTOMER SUPPORT SITE

The Oracle CGBU Customer Care Center is the initial point of contact for all product support needs. A Representative takes the call or email, creates a Consulting Services Request (CSR) and directs the requests to the Oracle CGBU Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will resolve the request.
The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Oracle CGBU TAC Engineers are available to provide solutions to technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Oracle CGBU Technical Assistance Centers are located around the globe in the following locations:

Oracle CGBU – Global

Email (All Regions): support@Oracle CGBU.com

- **USA and Canada**
  Phone:
  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)
  1-919-460-2150 (outside continental USA and Canada)
  TAC Regional Support Office Hours:
  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**
  Phone:
  +1-919-460-2150
  TAC Regional Support Office Hours (except Brazil):
  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays
- **Argentina**
  Phone:
  0-800-555-5246 (toll-free)
- **Brazil**
  Phone: 0-800-891-4341 (toll-free)
  TAC Regional Support Office Hours:
  8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays
- **Chile**
  Phone:
  1230-020-555-5468
- **Colombia**
  Phone:
  01-800-912-0537
- **Dominican Republic**
  Phone:
  1-888-367-8552
- **México**
  Phone:
  001-888-367-8552
- **Perú**
  Phone:
  0800-53-087

- **Puerto Rico**
  Phone:
  1-888-367-8552 (1-888-FOR-TKLC)
- **Venezuela**
  Phone:
  0800-176-6497
- **Europe, Middle East, and Africa**
  Regional Office Hours:
  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays
- **Signaling**
  Phone:
  +44 1784 467 804 (within UK)
- **Software Solutions**
  Phone:
  +33 3 89 33 54 00**Asia**
- **India**
  Phone:
  +91-124-465-5098 or +1-919-460-2150
  TAC Regional Support Office Hours:
  10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays.
- **Singapore**
  Phone:
  +65 6796 2288
  TAC Regional Support Office Hours:
  9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays