Oracle® Communications Diameter Signaling Router

DSR Software Upgrade Procedure

Release 5.x

909-2277-001

March 2014

Oracle® Communications Diameter Signaling Router DSR Software Upgrade Procedure, Release 5.x

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

Contact Oracle's Tekelec 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.x, or incremental upgrade from an earlier DSR 5.x release to a later DSR 5.x release. The upgrade of both HP C-Class blades and RMS servers is covered by this document. The audience for this document includes Tekelec customers as well as following internal groups: Software Development, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document provides step-by-step instructions to execute any incremental or major software upgrade.

The DSR 5.x Software Release includes all Tekelec Platform Distribution (TPD) software. Any upgrade of TPD required to bring the DSR to release 5.x occurs automatically as part of the DSR 5.x software upgrade. The execution of this procedure assumes that the DSR 5.x 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.x software loads. Please contact Tekelec Customer Service for the same refer Appendix K.
- Initial installation of DSR software. Refer [5] and [6].

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, Tekelec*

[4] *PM&C 5.5 Incremental upgrade, 909-2281-001, Tekelec.*

[5] *DSR 4.x installation document.909-2228-001. Tekelec*

[6] *DSR 5.0 installation document. 909-2278-001, Tekelec.*

[7] *DSR 5.0 Base Hardware and Software installation document 909-2282-001, Tekelec.*

[8] *2-tier to 3-tier migration WI006897, Tekelec*

1.3 Acronyms

Table 1. Acronyms

CD-ROM	Compact Disc Read-only Media
CSV	Comma-separated Values
CPA	Charging Proxy Agent
cSBR	Charging Session Binding Repository
DA	Diameter Agent
DA MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DIH	Diameter Intelligent Hub, one kind of XIH
DR	Disaster Recovery

Table 1. Acronyms

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 Virtualization 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.x.
Incremental Upgrade	An upgrade within a given DSR release e.g. 5.0.x to 5.0.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Single Server Upgrade	The process of converting a DSR 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.x 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.x server from its current release to a prior release. This could be performed due to a misbehaving system. Once the upgrade is accepted, server can't 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	See Signaling Network Element. 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 statuses 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 E.g. changing from 1+1 (Active Standby) policy to N+0 (Multiple Active) policy.
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).
RMS Diameter site	One or two RMS geographic sites that implement a single Diameter network element. If there are two RMS geographic sites, they are always configured as a geo-redundant pair, and only one handles the signaling duties of the network element at any given time. The primary RMS Diameter site contains the NOAM pair used to manage the network element, while the geo-redundant RMS Diameter site contains a disaster recovery NOAM pair.

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 the author's intent. 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 Tekelec Customer Service (*US: 1-888-367-8552, Intl: +1-919-460-2150)* for assistance before attempting to continue.

1.5.1 Executing Procedures

The figure 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 below 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 is formatted in **`10-point bold Courier`** font.

Figure 1. Example Procedure steps used in this document

1 ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2 ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 1. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. The report opens in a new window. 4. Verify the configuration data is correct for your network. 5. Save the report and print the report. Keep these copies for future reference. 6. Close report window.

1.6 Recommendations

Here are 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, whenever possible, primary NOAM 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.

Note that GUI activities are logged in a security log, but it is also recommended to use a screen capture tool to collect a sequence of screen shots before, during, and after the upgrade. This can also be useful for later analysis.

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.x. An incremental upgrade advances the DSR from an earlier DSR 5.x source release to a more recent 5.x target release.

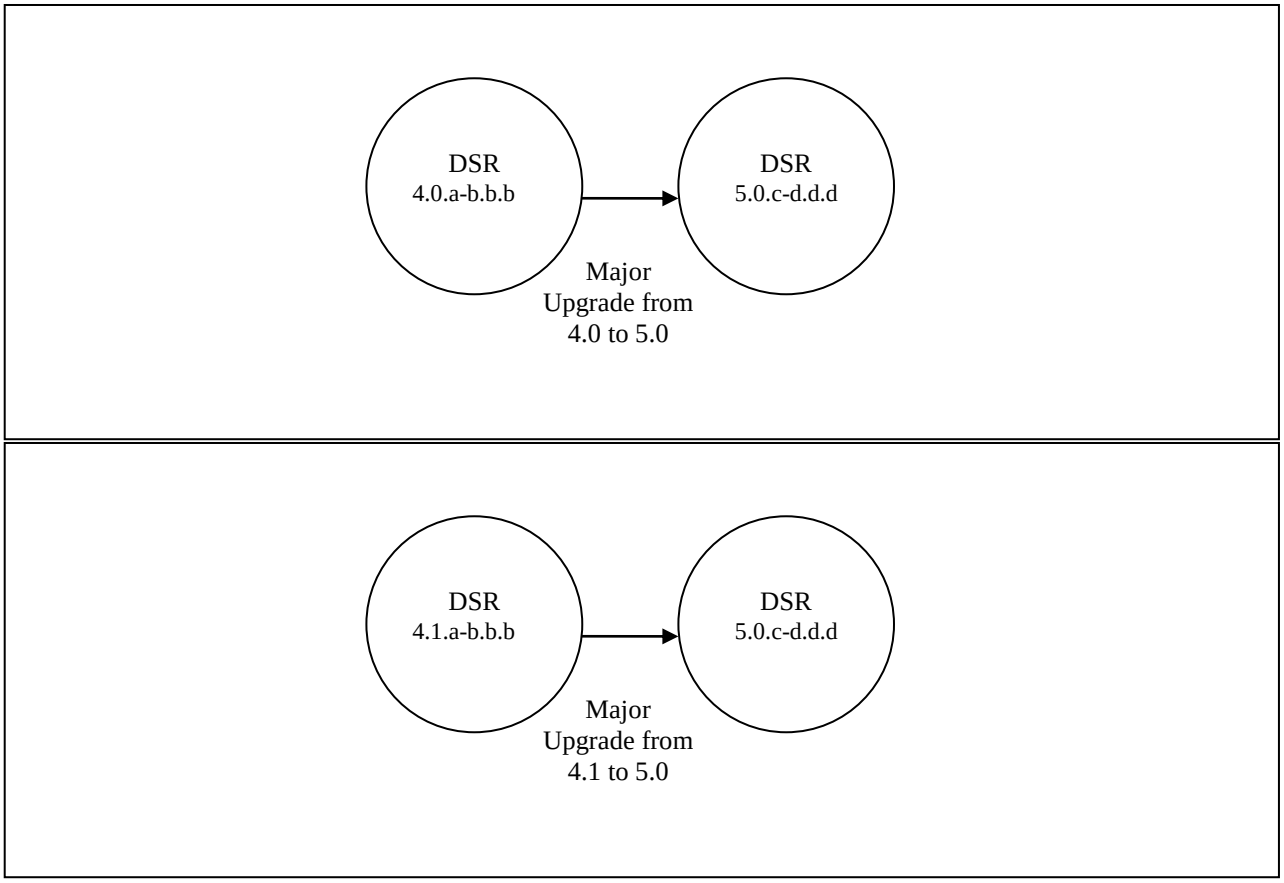
Note that for any incremental upgrade, the source and target releases must have the same value of "x". For example, advancing a DSR from 5.0.0-50.1.0 to 5.0.0-50.2.0 or to 5.0.1-50.2.0 is an incremental upgrade. But advancing a DSR running a 5.0 release to a 5.1 target release constitutes a major upgrade.

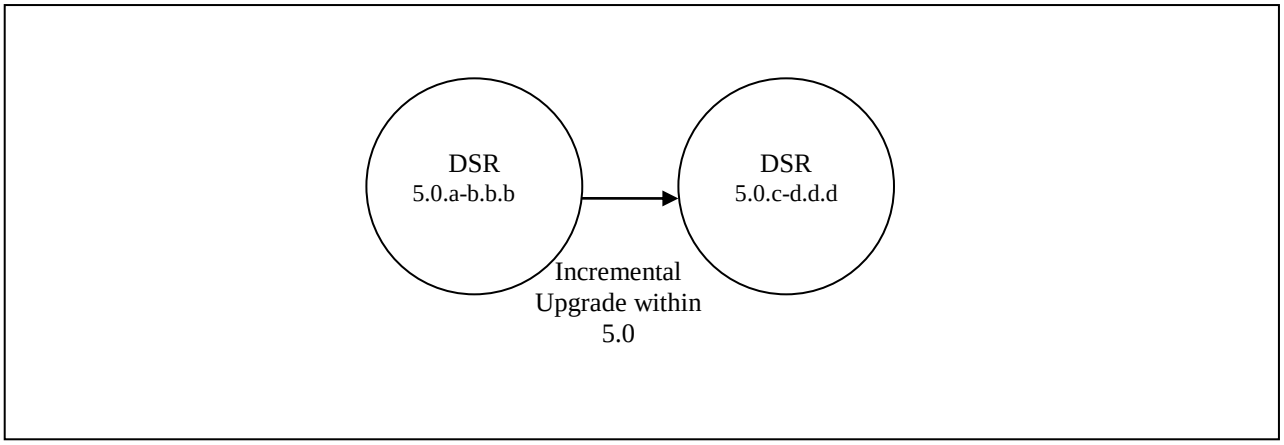
2.1 Supported Upgrade Paths

The supported paths to upgrade to a DSR 5.x 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 (Split Network Level and Site Level OAM functions) 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 5.0, while retaining the existing 2-Tier or 3-Tier configuration. For 2-Tier Upgrade, the upgrade will upgrade a site-at-a-time to DSR 5.0.

Note: A feature is provided in DSR 5.0 to allow migration from 2-Tier to 3-Tier architecture. This would be performed after the upgrade to DSR 5.0 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 SO (SOAM) – refers to the Site level OAM function in a 3-Tier deployment. This replaces the 2-Tier NO.

Assumptions:

- It is assumed that only sites with N+0 redundancy will have IPFE.
- 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 will refer 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 will be 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 with 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)

Geo-diverse 3-Tier SOAM deployments are un-common, and not considered in most of the upgrade procedures.

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

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 5.0 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 an operating system for a server, 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 NOAM and SOAM Applications

(TVOE Host servers may also be used to host other DSR functions, including MPs, 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 at 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) (Preferred)
- Options to Upgrade TVOE and Application at the same maintenance window:
    - Option B: Upgrade TVOE and Application, followed by another TVOE and Application. Example: for Standby SOAM Upgrade – stop application, upgrade TVOE, upgrade Application, start application; then repeat for Active SOAM.

- 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 also these applications will also be affected.

The procedure for Upgrading TVOE environments in advance of the application upgrades (Option A) is documented in **Section 3.3.9**.

2.8 SDS Upgrade

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

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 upgrade of the DA-MPs, it is expected that traffic connections will be disabled automatically when DSR application is disabled. So, the site being upgraded is not carrying traffic.

2.10 Optional NetBackup

There is expected change in NetBackup functionality in DSR 5.x release. Previously the backup file location path in Netbackup server for DSR 4.0 was configured as/var/TKLC/db/filemgmt/. Now for DSR 5.0 the path shall be /var/TKLC/db/filemgmt/backup/.

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

2.11 RMS Deployments

DSR 4.1 added support for Rack Mount Server (RMS) deployments of DSR. All Deployments with RMS will be 3-Tier. In these smaller deployments, the Message Processing (MP) servers may be 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 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.

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 you 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 your 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 iLO/XMI IP addresses (whichever applicable) from the workstations directly connected to the DSR servers is required.

3.1.1 Application ISO Image File / Media

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

The DSR 5.x ISO image file name will be in the following format:

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

Note: Prior to the execution of this upgrade procedure it is assumed that the DSR 5.x 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 to them before starting the upgrade procedure.

3.1.2 Logins, Passwords and Server IP Addresses

Obtain all the information in the following table. This 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	
	SO 1 XMI IP Address (Site 2)	
	SO 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)	

[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.

	P-DRA IPFE B 2 Server Group Server(Site 1)	
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 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 iLO IP Address (optional)	
	DA MP 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	

3.2 Plan Upgrade Maintenance Windows

This section provides a high-level checklist to help you keep track of individual server upgrades. The servers have been 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.
Below mentioned figure shows a recommended approach to collecting the upgrade activities into Maintenance windows. This document supports this approach.

Note that the blue arrows represent provisioned data flow between the servers. This provisioned data flow (often called Replication) must be managed during upgrade to avoid a case where an upgraded NO or SO server might be attempting to push data to a non-upgraded server. For this reason, Replication will be disabled between servers at times during the upgrade activities.

Figure 3. Upgrade Maintenance Windows for 3-Tier Upgrade

[4] As instructed by Tekelec Customer Service.

!! 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 a 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

Number of maintenance window required for DSR setup upgrade can be calculated by using the sheet attached below.

This sheet takes setup details as the input from user and accordingly calculates the number of maintenance window required for upgrade. This sheet in also specifies in detail, which all servers need to be upgraded in which maintenance window. Complete DSR upgrade MWs details and timings can be found out in the attached sheet. Please see the instructions tab of the sheet for more information and details.

DSR Upgrade Time Analysis.xlsx

3.2.3 Maintenance Window 1 (3-Tier NOAM servers)

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

This Maintenance Window will not be 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 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 you are 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 : _____ ☐ cSBR: _____ ☐ cSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ pSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____ ☐ SpareSBR: _____ ☐ DA-MP1: _____ ☐ DA-MP2: _____ ☐ DA-MP3: _____

	☐ DA-MP4: _____ ☐ DA-MP5: _____ … ☐ 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 does also apply to 2-Tier upgrade, 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 don't have any effect on the live system and can save upon maintenance window time, if executed before the start of the Maintenance Window. Note that the elapsed time is for a "Lab Environment", and that they might vary on Live Systems.

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	Backup all Global and Site Provisioning Data	None
Procedure 3	0:10-2:00	0:30-3:30	Full DB Backup	None
Procedure 4	0:10-1:15 (Depends upon number of servers)	0:40-1:45	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(Upgrade Preparation for PDRA configuration only))	None
Procedure 6	0:15-0:20	1:15-5:35	New LV for NetBackup Client	None
Procedure 7	0:02-0:10*	0:57-5:45	ISO Administration	None

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, 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.x

3.3.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the new DSR5.x 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 TEKELEC TECHNICAL SERVICES 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 Tekelec Customer Care Center	Contact the Tekelec Customer Care Center and inform them of your plans to upgrade this system. See Appendix K 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 each site-level Active NO (repeat procedure for each site level NO)

Procedure 2: Backup 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 TEKELEC TECHNICAL SERVICES 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: Log into the NOAM GUI using the VIP. 1. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
2 ☐	Verify and collect Server Group Configuration data	View the Server Group configuration data; verify the data; save and print report: From the NOAM VIP GUI 1. Select **Configuration > Server Groups** to view Server Group screen. 2. Click **Report** at the bottom of the table to generate a report for all entries.

Procedure 2: Backup Global and Site Provisioning Data

		3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	Verify and collect Servers Configuration data	View the Servers configuration data; verify the data; save and print report: From the NOAM VIP GUI 1. Select **Configuration > Servers** to view Servers 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 your 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: From the NOAM VIP GUI 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 your network. 4. Save the report and/or print the report. Keep these copies for future reference.
5 ☐	Verify and collect Signaling Network Configuration data	View the Signaling Networks configuration data; verify the data; save and print report: From the NOAM VIP GUI 1. Select **Configuration > Network** to view the Signaling Networks. 2. Click **Report** (or "**Report All**" for DSR 5.x) at the bottom of the table to generate a report **for all entries**. 3. Verify the configuration data is correct for your 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 3 through 5(not required for DSR 5.x). 6. Select **Configuration > Network > Routes** and repeat sub steps 3 through 5(not required for DSR 5.x).
6 ☐	Collect database reports	Backup the global database from the primary active NO server: From the NOAM VIP GUI 1. Select **Status & Manage > Database** to view 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.
7 ☐	Backup all global and site provisioning databases for NO (and SO's) **IMPORTANT: Required for Disaster Recovery**	Backup the global database from the primary active NO and all Active SO servers: **For the active NO server (and all active SO's for 3-Tier)** Login to NO or SO GUI 1. Select **Status & Manage > Database** to return to the Database Status screen. 2. Click to highlight the **Active NO** server (if logged into Active NOAM GUI) or **Active SO** server (if logged into Active SOAM 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. Click **Backup** and archive both **Configuration** and **Provisioning** Data**(Note**: **Provisioning check box is not selectable from the GUI)** 4. Enter **Comments** (optional) 5. Click **OK**. **Repeat substeps 1 to 5 for each Active NO and active SO server (if exists)** Note: Active NO/SO can be found out by going to Status & Manage->HA screen, and see which server is currently assigned the VIP in the "Active VIPs" field. The server having VIP

Procedure 2: Backup Global and Site Provisioning Data

		assigned will be the Active one.
8 ☐	Save database backups for NO (and SO's) **IMPORTANT: Required for Disaster Recovery**	Save database backups to your local workstation: **For the active NO server and active SO's (if exists)** Login to NO or SO GUI 1. Select **Status & Manage > Files;** the **Files** menu is displayed. 2. Click on the Active NO server tab**.** 3. Select your database backup file and click Download button. 4. A confirmation window prompts you. Click **Save**. 5. The Choose File window is displayed. Select a destination folder on your local workstation to store the backup file. Click **Save**. 6. The Download Complete confirmation displays. Click **Close**. **Repeat substeps 1 to 6 for each Active NO and Active SO server (if exists).**
9 ☐	Analyze and plan MP upgrade sequence	From collected data, Analyze system topology and plan for any MPs which will be out-of-service during upgrade sequence. 1. Analyze system topology gathered in Step 1,2 and 3. 2. Plan for any MP upgrades by consulting Tekelec to assess the impact of out-of-service MP servers 3. Determine exact sequence 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 DB Run Environment Backup

STEP #	This procedure (executed form 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 TEKELEC TECHNICAL SERVICES 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 in the Active NO: `ssh root@<NO_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

Procedure 3: Full DB Run Environment Backup

S T E P #	This procedure (executed form 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
2 ☐	**SSH to Active NO:** Execute Full Backup for all servers (managed from this NO)	Execute the **backupAllHosts** utility on '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** Following output will be generated for DSR 5.x 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 mins to 2 hrs for this command to complete, depending upon the data in the database.** **Do not proceed until 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, login to each server in the system individually, and Execute the following 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.

Procedure 3: Full DB Run Environment Backup

S T E P #	This procedure (executed form 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
3 ☐	**Active NO GUI:** Verify that backups are created for all servers	**For the active NO:** Login to Active NO or SO GUI 1. Select **Status & Manage > Files;** the **Files** menu is displayed. 2. Click on each server tab, in turn 3. 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 4: Perform Health Check (Upgrade Preparation)

1 Verify Software Versions on DSR Servers

From the Active NO GUI:

Select **Upgrade Administration** form:
(DSR 4.x: "**Administration > Upgrade**"
DSR 5.x: " **Administration -> Software Management -> Upgrade**")

The Upgrade Administration screen is displayed (example below):

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the 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

Upgrade Screen in DSR 5.x GUI

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

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

Procedure 4: Perform Health Check (Upgrade Preparation)

2 ☐	Verify Server Status is Normal	Verify Server Status is Normal: Log in to Active NOAM GUI. 1. Select **Status & Manage > Server;** the Server Status screen is displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting status, and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is not recommended to continue executing upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
3 ☐	Log all current alarms	Log all current alarms in the system: From the Active NO GUI 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view isis displayed. 2. Set collection interval as 1 Day or more if needed and click **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 substeps 3 and 4. 5. Log into Active SO (if exists) and repeat substeps 2 to 5.
4 ☐	Check if new Firmware Release may be required for the system.	Contact the Tekelec Customer Care Center by referring to Appendix K of this document to find out 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 upgrade is required, acquire the Firmware release package and follow procedures provided with this package to determine which specific system components (Switches, Servers, etc) may require upgrade. Plan for Firmware Upgrade Maintenance windows, if needed, since this activity is typically performed before the DSR Upgrade.
5 ☐	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)	1. Record the target DSR Release on which servers needs to be upgraded. (5.x.y-5x.nn.a). 2. Find out the PM&C version. 3. For upgrade to DSR 5.x minimum PM&C required is **5.5**. 4. If PM&C version is below 5.5, then identify proper PM&C upgrade document (to be used later) based on the indented DSR upgrade path. : a) For major DSR upgrade I.e. from DSR 4.x->5.x follow reference [3]. For Incremental upgrade i.e. from DSR 5.0->DSR 5.x follow reference [4]**.**

Procedure 4: Perform Health Check (Upgrade Preparation)

6 ☐	Check the TVOE Host server software version	1. Find the target DSR release from Table 3. 2. Contact the Tekelec Customer Care Center by referring to Appendix K of this document to find out 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, then need to plan for TVOE Host upgrades. See planning section of this document.
7 ☐	Check if netbackup client installed on NOAM/SOAM(if exists)	1. Check the Netbackup server version before starting with DSR upgrade. 2. Supported versions of Netbackup client and Netbackup server for DSR 5.x release are 7.1 or 7.5. 3. If Netbackup server is not on 7.1 or 7.5 then plan a Netbackup upgrade before starting with DSR upgrade.
8 ☐	Check if the setup has customer supplied apache certificate installed and protected with a passphrase.	1. Verify if the setup has customer supplied apache certificate installed and protected with passphrase. 2. If the certificate is installed then rename the certificate. (Make sure that original name is noted down for further usage in Section 4.9.1 Step 4)

3.3.6.1 Perform Health Check (Upgrade Preparation only for PDRA configuration)

Execute following procedure to take diameter configuration data backup and health check required for only PDRA specific deployments.

Procedure 5: Perform Health Check (Upgrade Preparation for PDRA configuration)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify all servers status are normal	1. Log in to GUI using NOAMP VIP 2. Select the **Status & Manage -> Server** menu item. 3. Verify all servers status are Normal (Norm). 4. Do not proceed without consent from Engineering/Customer Service to upgrade if any of the server status displayed is not **Norm**. Note: It is not recommended to continue executing 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 Active NOAMP VIP and **Active SOAM VIP on all the Sites.**	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 Alarms CSV file generated and all the current alarms in the system.

Procedure 5: Perform Health Check (Upgrade Preparation for PDRA configuration)

		4. Keep this information for future reference on client machine.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for all the sites**	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 Avaialble" 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 Avaialble" and "Available" Route Groups. Select **Maintenance->Peer Nodes** screen. 8. Filter out all the Peer Nodes with "**Peer Node Operational Status"** as **"Is Not Available"** and **"Is Available".** 9. Record the number of "**Not Available**" and "**Available**" peer nodes. 10. Select **Maintenance->Connections** screen. 11. Filter out all the Connections with "**Operational Status"** as **"Is Not Available"** and **"Is Available".** 12. Record the number of "**Not Available**" and "Available" connections. 13. Select **Maintenance->Applications** screen. 14. Filter out all the Applications with "**Operational State"** as **"Is Not Available" and "Is Available".** 15. Record the number of "**Not Available**" and "**Available**" applications. 16. Save this off to a client machine.
4 ☐	Capture the Policy SBR Status **On Active NOAMP 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 some editor. a. BindingRegion b. PDRAMatedSites 3. Save this off to a client machine.
5 ☐	Capture the IPFE Configuration Options Screens. On Active SOAM GUI on all the Sites.	1. Select Main Menu: IPFE->Configuration->Options 2. Capture and archive the screen capture of the complete screen. 3. Save this off to a client machine.
6 ☐	Capture the IPFE Configuration Target Set screens On Active SOAM GUI on all the Sites.	1. Select Main Menu: IPFE->Configuration->Target Sets 2. Capture and archive the screen capture of the complete screens. 3. Save this off to a client machine.
7 ☐	Export and archive the Diameter and P-DRA configuration data. On Active SOAM GUI on all the Sites.	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 APDE status button at the top of the screen. 4. Browse to Main Menu->Status & Manage->Files and download all the exported files to client machine or use SCP utility to download the files from Active SOAM to the client machine.
8 ☐	Data shall be captured for each PDRA Site.	Execute steps 1 to 7 for each PDRA Site.

3.3.7 Create new Logical Volume for NetBackup Client on NO/SO(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 Symantec's NetBackup utility is already installed on one or more OAM(NO or SO) servers in the DSR to be upgraded. If you know NetBackup is not installed on any of the OAM servers, you can skip this section entirely. If you are not sure if NetBackup is installed on any OAM server, the first step of Procedure 5 below gives instructions on how to check. And 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 will not be 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 needs to 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 6: New LV for NetBackup Client

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 TEKELEC TECHNICAL SERVICES 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>`
		
		(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`

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
		If this file exists then a version of the NB client has been installed on this application. If file doesn't exist then move to Step 9. `# su - platcfg` The platcfg utility menu will be displayed, Now navigate to following submenus : 1. Navigate to NetBackup configuration and select the *Verify NetBackup Client Installation* option Platform Configuration Utility 3.06 (C) 2003 - 2012 Tekelec, Inc. Hostname: N02 lqqqqu NetBackup Configuration Menu tqqqqqk x x x Enable Push of Netbackup Client x x Verify NetBackup Client Push a x x Install NetBackup Client a x x Verify NetBackup Client Installation x x Remove File Transfer User a x x Exit x x x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj 2. If NetBackup client is installed, the following screen will appear.-

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
		Platform Configuration Utility 3.06 (C) 2003 - 2012 Tekelec, Inc. Hostname: N02 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 mqqqqqqqqqqj mqqqqqqqqqqj mqqqqqj mqqqqqqqqqj mqqqqqqj Note : Following error in verify NetBackup Client Installation output is acceptable : `[ERROR] - RC script: vxpbx_exchanged` 3. Select Exit to return to previous menu. If NetBackup is installed move to Step 2, otherwise move to Step 9.

2 ☐	Check if NetBackup Logical volume already exists	Execute the following command to check if logical volume for NetBackup client already exists :
		`# df -B M`
		Following output will show that 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 NetBackup logical Volume exists then move to Step 9, otherwise move to next step 3.

STEP #	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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	

3 ☐	Mount the upgrade media	Insert Diameter Signaling Router 5.xISO into 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 to mount ISO:
		`# mount -o loop DSR_5.x.iso /media/cdrom`

4 ☐	Verify that the script is available on the media	To be sure it is available on the upgrade media, execute the "ls" command to list the relocateNetBackup script, like this: `# ls <mount point>/upgrade/bin/relocateNetBackup` Verify that the relocateNetBackup script is present, otherwise contact Tekelec.
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. 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.

STEP #	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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
7 ☐	Check if NetBackup logical volume exists.	Execute the following command to check if Logical volume for NetBackup client exists : **# df -B M** Following output will show that 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 NetBackup logical Volume exists then move to next Step,otherwise contact Tekelec customer service by referring to Appendix K 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.

3.3.8 ISO Administration

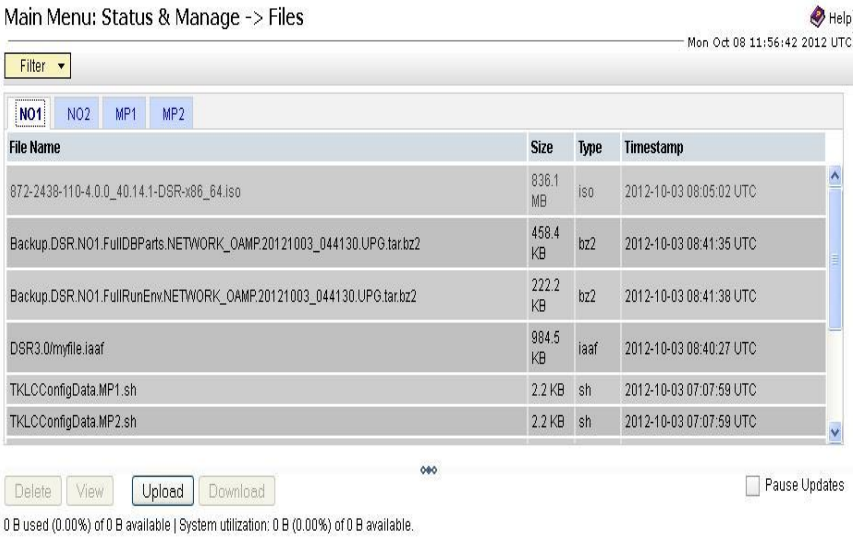
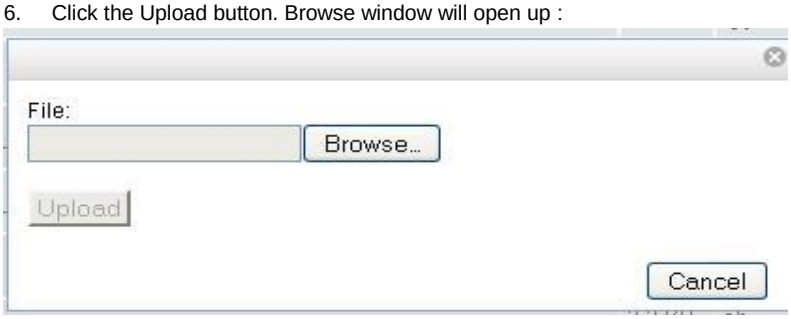
Detailed steps on ISO Administration are given in Procedure 6.

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, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 7: ISO Administration

STEP #	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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.

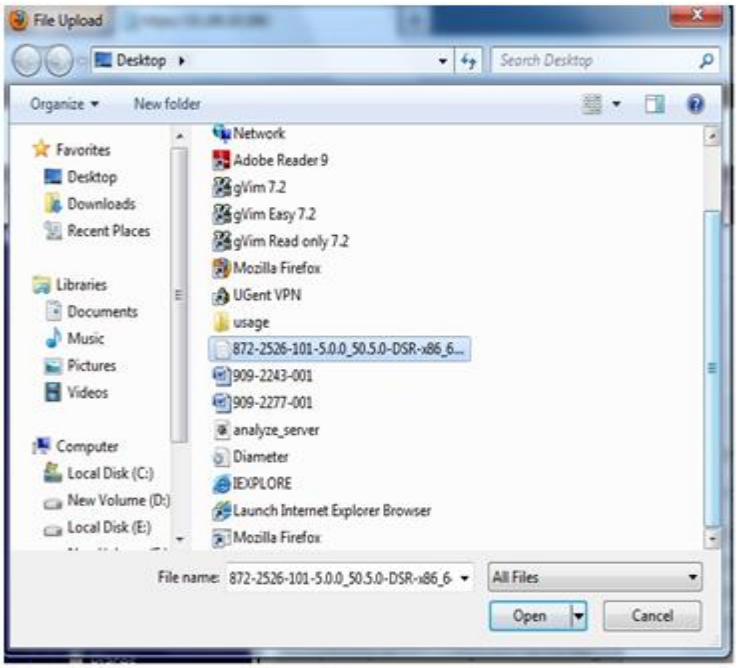
Procedure 7: ISO Administration

1 ☐	Upload ISO to Active NO server via the DSR 4.x/5.x GUI session.	There are 2 methods to upload the application ISO to the Active NO based on the type of the media: Execute either Option 1(Using NOAM GUI Upload function for ISO file transfer over the network) **OR** Option 2 (Local site media ISO transfer, using PM&C). **OPTION 1:** Using 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 in to the active NO GUI. 2. Select **Status & Manage > Files;** the Files menu is displayed  3. Click the active NO server in your 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 your 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 :  7. Click **Browse** to select the file to upload.

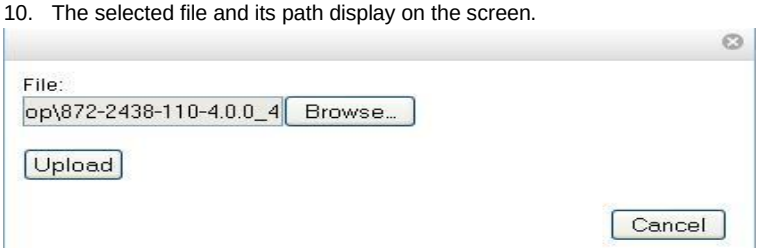
[5] The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

Procedure 7: ISO Administration

8. The Choose File window displays, allowing you to select 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.



11. Click **Upload.**
12. The ISO file begins uploading to the file management storage area.
13. Wait for 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 your network upload speed is slow. (Depending on your network speed, up to 25 minutes).
14. Backup the ISO file to the PMAC by ssh from the Active NO and executing the following command, Refer to [4] Procedure 12 for creating space on PM&C if desired space is not available on PM&C::
    a) cd into the directory on the active NOAM where your ISO image is located
    ```
    # cd /var/TKLC/db/filemgmt
    ```
    b) Using sftp, connect to the PM&C management server
    ```
    # sftp
    pmacftpusr@<pmac_management_network_ip>
    # put <image>.iso
    ```
    c) 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.

Procedure 7: ISO Administration

```
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 ISO image to 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 less than 5.0 version :

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

3. Log in to Active NO and Execute 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 following command:

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

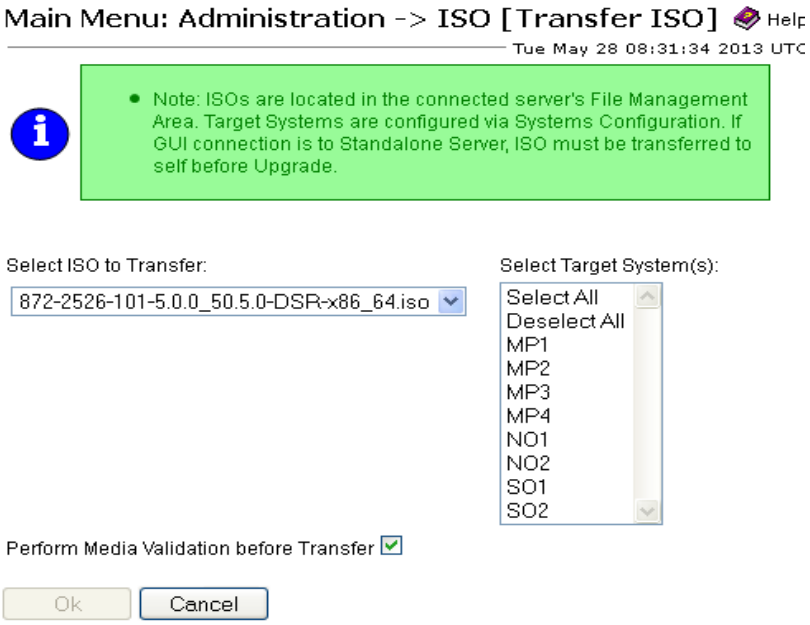
Procedure 7: ISO Administration

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 NO GUI, navigate to **Administration** -> **ISO** for DSR 4.x or navigate to **Administration->Software Management-> ISO Deployment** for DSR 5.x GUI.

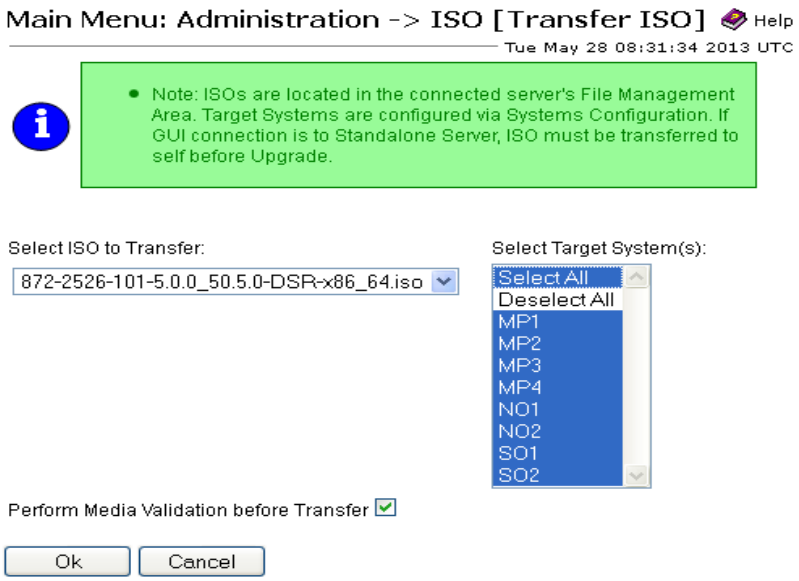
2. Click on "**Transfer ISO**"



Procedure 7: ISO Administration

3. Under the "**Select ISO to Transfer:**" drop down menu select the DSR 5.x 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. You will be returned 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 Tekelec support for assistance.

3.3.9 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 5.0 Upgrades of the NO's and other servers. Performing the TVOE upgrades BEFORE will reduce the time required for DSR Application Upgrade procedures.
[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 Upgrades for servers that are managed by this PMAC.

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

Table 5. TVOE Upgrade (multiple site servers in a MW)

Procedure	This Step	Cum.	Procedure Title	Impact
	0:01-0:05	0:01-0:05	Verify health of site	
Procedure 8	30 min per TVOE Host (see note)	0:05-3:05	Upgrade TVOE for multiple servers at a site	DSR servers running as virtual guests on the TVOE host will be stopped briefly and unable to perform their DSR role while the TVOE Host is being upgraded.
	0:01-0:05	3:05-3:10	Verify health of site	

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 8: Upgrade TVOE Hosts for a site

STEP #	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 Tekelec 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 8: Upgrade TVOE Hosts for a site

3 ☐	Determine if there are SDS Applications on the TVOE Hosts	Login to TVOE hosts and execute: `# virsh list --all` **If the application list includes SDS NOAM applications, then make this team aware of the planned 30 minute outage of the SDS NOAM applications during the TVOE Upgrade.**
4 ☐	Upgrade the TVOE hosting the DSR standby server(s)	Upgrade TVOE of a standby server: **Execute Appendix J**
5 ☐	Upgrade the TVOE hosting the DSR active server(s)	Upgrade TVOE of a 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 **Tekelec 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 Normal state, these servers should be brought to the Normal or the 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 Tekelec Customer Support to diagnose those alarms and determine whether they need to be addressed or if it is safe to proceed with the upgrade.

Please read the following notes on upgrade procedures:

- Procedure completion times shown here 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 Tekelec Technical Services 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? _____

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

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

Are there IPFE servers to upgrade? _____

Are there PDRA or SBR 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.

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

Use the answers to these questions to select the required upgrade procedure from shown in 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 will apply.

*It is recommended that the specific upgrade sections are identified **before the Maintenance window**, and sections that will not be used are "greyed 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.x upgrade for 3-tier (1+1) setup (major or incremental)	3-Tier DSR Upgrade for (1+1) DA-MP configuration.	Section 4.2
2	DSR 5.x upgrade for 3 tier (N+0) setup (major or incremental)	3-Tier DSR Upgrade for (N+0) DA-MP configuration.	Section 4.3
3	DSR 5.x upgrade for 3 tier (N+0) RMS server setup (major or incremental)	3-Tier DSR Upgrade for (N+0) DA-MP configuration on RMS servers.	Section 4.4
4	DSR 5.x upgrade for 3-tier (1+1) RMS server setup (major or incremental)	3-Tier DSR Upgrade for (1+1) DA-MP configuration on RMS servers.	Section 4.5
5	Policy DRA DSR 5.x upgrade (major or incremental)	Upgrade for Policy DRA application	Section 4.6

Table 7. 2-Tier Upgrade Path Reference

Type	Supported Configurations	Upgrade Path	Section Reference
4	DSR 5.x upgrade for 2-tier (1+1) setup (major or Incremental)	2-Tier DSR Upgrade, for (1+1) DA-MP configuration.	Section 4.7 (Each Site)
5	DSR 5.x Upgrade for 2-tier (N+0) setup (major or incremental)	2-Tier DSR Upgrade for (N+0) DA-MP configuration.	Section 4.8 (Each Site)

4.2 3-Tier DSR Upgrade for (1+1) DA-MP configuration (possibly including TVOE)

This section contains upgrade steps for DSR 5.x (3-tier setup) with (1+1) configuration (major or incremental).

4.2.1 NO Upgrade Execution for 3-Tier (1+1) setup

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), and 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 (For DSR 3-tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 9	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check	None
Procedure 10	0.05-0.10	0.06-0.15	0.06-0.15	0.06-0.15	Inhibit Replication	No Traffic Impact
Procedure 11	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade DR-NOs	Provisioning Disabled, No Traffic Impact

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 12	0:25-1:00	0:56-2:15	1:25-2:00	2:56-4:15	Upgrade NOs	Provisioning Disabled, No Traffic Impact
Procedure 13	0:05-0:10	1:01-2:25	0:05-0:10	3:01-4:25	Allow Replication between NOs and DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 14	0:01-0:05	1:02-2:30	0:01-0:05	3:02-4:30	Verify Post Upgrade Status	Provisioning to SOAM is not supported till site upgrades are also performed.

4.2.2 Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAMs)

This procedure is used to determine the health and status of the network and servers. This must be executed on the active NOAM.

Procedure 9: Perform Health Check (Pre-Upgrade of 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 TEKELEC TECHNICAL SERVICES 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.x) , 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 9: Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAM)

2 **NO GUI:** Verify NO Servers existing Application Version

For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade).

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases.

Upgrade Screen in DSR 4.x

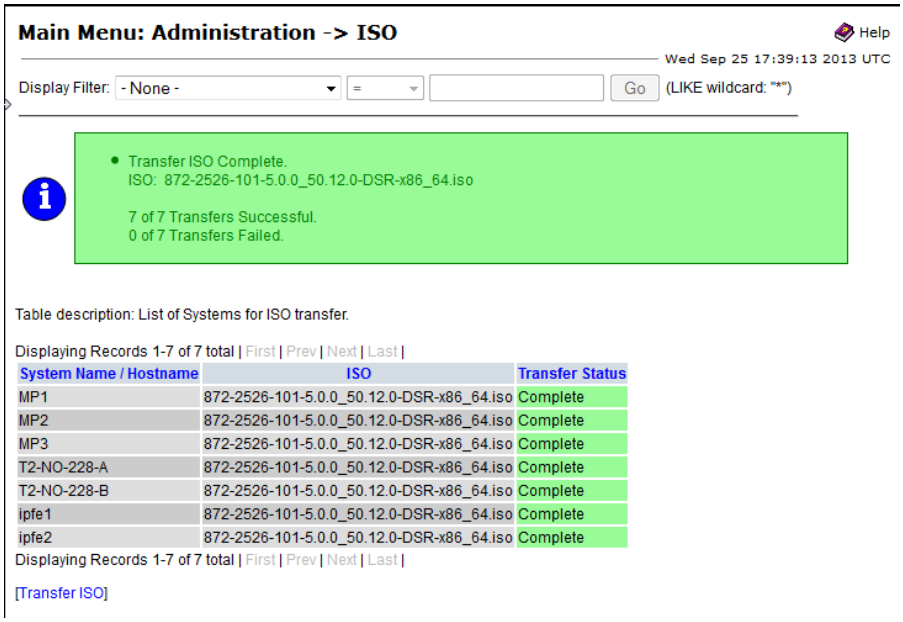
Main Menu: Administration -> Upgrade

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.x

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 9: Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAM)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify DSR ISO file has been Transferred to all servers: Example:  IF Not, see ISO Administration 3.3.8.
4 ☐	Verify Server Status is Normal	Verify Server Status is Normal: Log Into the NOAM GUI using the VIP. 1. Select **Status & Manage > Server;** the Server Status screen is displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is not recommended to continue executing 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.
5 ☐	Log all current alarms at NOAM	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
6 ☐	Repeat for active SOAMs	Log all current alarms in the SOAM: 1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

Procedure 9: Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAM)

7 ☐	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. Select **Status and Manage → Files** Check time stamp on two 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 re-perform) a full Backup, if needed.

4.2.3 Inhibit Replication for 3-tier (1+1) setup

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

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 10. Inhibit Replication for 3-Tier (1+1) setup

S T E P #	This Procedure inhibits replication 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 (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window	
1 ☐	Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. 1. Select **Status & Manage > Database;** the Database Status screen is displayed 2. Click **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] - Provisioning is manually disabled**. 5. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 10. Inhibit Replication for 3-Tier (1+1) setup

2 ☐	Inhibit SOAP replication **(This step will NOT be required for most upgrades!)**	**Record current DSR release number_____ex: 4.0.2_40.27.3** **SKIP THIS STEP if current release is DSR 4.0.0_40.19.0 or greater.** Use your SSH client to connect to the active NO server (ex. ssh, putty): **ssh <Active NO IP address>** **login as: root** **password: <enter password>** 1. Execute the following command to disable SOAP replication : **# iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"** Execute following command to verify if above command successfully updated NodeInfo records: **# iqt -E NodeInfo** Verify that **excludeTables** field shall include '**HaNodeLocPref HaVipDef**' table names **for each NodeId present on the setup** : E,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef** Note: SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO,SO or MP servers.
3 ☐	Inhibit replication to MP servers (1+1) redundancy	Inhibit database replication to MP servers in the following order: • Standby DA-MP • Active DA-MP From Active NO: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Select the appropriate **DA-MP server**. 3. Click **Inhibit Replication** button. 4. Verify the ***Inhibited*** text is displayed for server. 5. **Repeat** the **above steps for** all remaining servers in the order: standby, then active). Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. **ALL DA-MPs must be inhibited.**

Procedure 10. Inhibit Replication for 3-Tier (1+1) setup

4 ☐	Inhibit replication to SO servers at a site	Inhibit database replication to SO servers in the following order:
		• Site:
		  ○ Standby SO
		  ○ Active SO
		
		From Active NO:
		1. Select **Status & Manage > Database**
		The Database Status screen is displayed.
		2. Select the appropriate **SO server.**
		3. Click **Inhibit Replication** button.
		4. Verify the ***Inhibited*** text is displayed for server.
		5. **Repeat** the **above steps for** all remaining Site (servers) in the order: standby, then active).
		
		ALL SOAM must be inhibited.

5 ☐	Verify that MPs and SO Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all MPs and all SOs, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other MPs and SO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
6 ☐	Inhibit replication to NO servers.	Inhibit database replication to all servers in the following order: • Standby NO • Active NO • Standby DR NO(if applicable) • Active DR NO(if applicable) Select **Status & Manage > Database** The Database Status screen is displayed. 1. Select the appropriate NO or DR-NO server based on the list above. 2. Click Inhibit Replication button. 3. Verify the Inhibited text is displayed for server. 4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
7 ☐	Verify that All Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other servers must have: Alarm ID = 31113 (Replication Manually Disabled)

Procedure 10. Inhibit Replication for 3-Tier (1+1) setup

8 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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 substeps 2 through 5 for all the sites present in the setup.

4.2.4 Upgrade DR-NOs of 3-Tier (1+1) setup

Procedure 11. Upgrade DR-NO(s) 3 –Tier (1+1) configuration

S T E P #	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	*Begin Upgrade of DR-NOs*	*Next Steps will begin Upgrade of the DR-NO servers.* *SKIP this Procedure if the deployment does not include DR-NO servers.*
2 ☐	Upgrade Host TVOE for **Standby** DR-NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** DR NO
3 ☐	Upgrade **Standby** DR-NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR DR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step mentioned below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
4 ☐	Upgrade Host TVOE for **Active** DR-NO (if needed)	*Skip this step if:* • *the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** DR NO to upgrade TVOE.

5 ☐	Verify if cmha is running on upgraded DR NO	Log into the just-upgraded **standby** DR NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 11. Upgrade DR-NO(s) 3 –Tier (1+1) configuration

6 ☐	Upgrade **Active** DSR DR-NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR DR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step mentioned below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
7 ☐	Proceed to next procedure	Proceed to upgrade the NO servers, using the next procedure

4.2.5 Upgrade NOs of 3-Tier (1+1) setup

Procedure 12. Upgrade NO for 3 –Tier (1+1) configuration

S T E P #	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Upgrade Host TVOE for **Standby** NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** NO
2 ☐	Upgrade **Standby** NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step mentioned below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
3 ☐	Upgrade Host TVOE for **Active** NO (if needed)	*Skip this step if:* • *the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** NO to upgrade TVOE.

4 ☐	Verify that cmha is running on upgraded NO.	Log into the just-upgraded **standby** NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 12. Upgrade NO for 3 –Tier (1+1) configuration

5 ☐	Upgrade **Active** DSR NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
6 ☐	Verify NO GUI access via VIP Address	Close and re-open Browser using the VIP address for the NOAM. Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected. The NOAM GUI will show the new DSR 5.0 release. Expected Alarms include: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other servers must have: Alarm ID = 31113 (Replication Manually Disabled)
	Proceed to next procedure	Proceed to next procedure, to allow replication between NOs.

4.2.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier (1+1) configuration

Procedure 13. Allow Replication between NO and DR NO Servers of 3-Tier(1+1)

S T E P #	This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, and (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**

Procedure 13. Allow Replication between NO and DR NO Servers of 3-Tier(1+1)

1 ☐	Allow replication to NO and DR-NO servers only.	Allow database replication to **NO and DR-NO servers ONLY:** **Note: The NO servers intentionally have a sequence of "Allow Active, Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.** Select **Status & Manage > Database.** The Database Status screen is displayed. 1. Select the **Active NO server.** 2. Click Allow Replication button. 3. Verify the Inhibited text is not displayed for the server. After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 4. Repeat the Allow action link for **Standby NO server.** **Repeat sub-steps 1 through 4 for DR NO(s) (if applicable).** **Note: You must not allow Replication to any SOAMs or MPs. This can result in database corruption at these servers.**
2 ☐	Verify NO and DR-NO Replication	It is expected that NO and SO Provisioning is still disabled, and this will remain disabled till sites are upgraded. Verify that NO VIP GUI shows following alarms : Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and MP servers must have: Alarm ID = 31113 (Replication Manually Disabled) **IF Upgrade verification steps indicate a problem, consult with support on the best course of action. Procedures for backout of the upgrade are included in this document.**

4.2.7 Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup

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

Procedure 14: Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 14: Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		
		1. Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers :
		
		Use your SSH client to connect to the upgraded server (ex. 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 Tekelec.
		
		`# alarmMgr --alarmstatus`
		
		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 Tekelec in case above output is not generated.

2 ☐	**NO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the NOAM GUI via the VIP. 2. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is displayed. 3. Click **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) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
3 ☐	Verify Traffic status	View KPI reports to verify traffic is at the expected condition.

Procedure 14: Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup

4 ☐	Enable global provisioning and configuration(if new Network element is required to be added)	Enable provisioning and configuration updates on the entire network (if new Network element is required to be added): **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 to only upgraded SO(s).** 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the “primary” active NOAM.
End of maintenance window		

4.2.8 Site Upgrade for (1+1) 3-tier Configuration

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

- DSR 4.x->5.x Major upgrade
- DSR 5.x Incremental upgrade

[Note: For any DSR system consisting of containing 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 are running on 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-enabled at the completion of the site upgrade.

Table 9. Site Upgrade Execution Overview (For DSR (1+1) 3-tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 15	0:25-1:00	0:26-1:05	1:25-2:00	1:26-2:05	Upgrade SO(s) of (1+1) 3 – Tier configuration.	None
Procedure 16	0:25-1:00	0:51-2:05	0:25-1:00	1:51-3:05	Upgrade MP(s) of (1+1) 3-Tier configuration.	None
Procedure 17	0:01-0:05 Per MP	1:07-3:25	0:01-0:05 Per MP	2:07-4:25	Verify Post-Upgrade Status of the Site	None

4.2.9 Upgrade SO of 3-Tier (1+1) configuration

For each site in the 3-tier DSR, the SOAM(s) (Procedure 15) and associated DA-MPs (Procedure 16 & Procedure 17) should be upgraded within a single maintenance window. Additionally, Tekelec recommends that only a single site be upgraded in any particular maintenance window.

Procedure 15. Upgrade SO(s) of (1+1) 3 -Tier configuration.

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window.	
1 ☐	Verify that Site Provisioning is disabled	Verify that site provisioning is disabled. Else disable site provisioning for the site that is currently being upgraded : 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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
2 ☐	Upgrade TVOE Host for Standby Server	If the TVOE Host for the Standby SO needs to be upgraded: **Execute Appendix J** for the standby SO TVOE Host
3 ☐	Upgrade Standby SO	Upgrade 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 step 3 below.
4 ☐	Upgrade TVOE Host for Active SO Server	IF Active SO is hosted on TVOE blade, and the TVOE Host needs to be upgraded: **Execute Appendix J** to upgrade the Active SO TVOE Host

Procedure 15. Upgrade SO(s) of (1+1) 3 -Tier configuration.

5 ☐	Verify cmha process is running on upgraded SO	Execute following steps to make sure that cmha process is up on upgraded server:
		1. Log into the just-upgraded standby SO, execute the following command:
		`# ssh root@<SO XMI IP ADDRESS>`
		`login as: root`
		`password: <enter password>`
		Execute following command on SO:
		`[root@SO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58 1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

6 ☐	Upgrade Active SO	Upgrade Active DSR 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 step 6 below.
7 ☐	Allow replication to SO servers.	Allow database replication to SO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen is displayed. 3. Select the Active SO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 6. Repeat the **Allow** action link for Standby SO server. **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.**
8 ☐	Install NetBackup on NO and SO (If required)	If Netbackup is to be installed on your DSR, execute the procedure found in Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.**

4.2.10 Upgrade DA-MP(s) of 3-Tier (1+1) configuration

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

Procedure 16: Upgrade MP(s) of (1+1) 3-Tier configuration

STEP #	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 Tekelec 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 of the standby DA-MP by going to Status & Manage -> HA. Note: Active DA-MP server can be identified by looking out for the VIP. 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 Standby MP server[6] using Upgrade Single Server procedure: **Execute Appendix G –** Single Server Upgrade for Standby DA-MP After successfully completing the procedure in Appendix G, return to this point and continue with Step 3 below.
3 ☐	Upgrade the Active DA-MP server.	Upgrade active MP server using the Upgrade Single Server procedure. **Execute Appendix G –** Single Server Upgrade for Active DA-MP After successfully completing the procedure in Appendix G, return to this point and continue with Step 4 below. Note: The DA-MP server replication is enabled in Appendix G, executed above.
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 to only upgraded SO(s). 5. Log in to the active NOAM GUI using the VIP. 6. Select **Status & Manage > Database** The Database Status screen is displayed. 7. Click **Enable Provisioning** button. 8. Verify the text of the button changes to **Disable Provisioning.** Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM.
5 ☐	Enable Site Provisioning	**Enable Site provisioning :** 1. Log into the SOAM VIP GUI of the site just upgraded above. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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] The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

Procedure 16: Upgrade MP(s) of (1+1) 3-Tier configuration

6 ☐	Update Max Allowed HA Role for NO and SO.	1. While logged in to the active NOAM GUI, go to Status & Manage-> HA screen. 2. Click 'Edit' button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click 'Ok' button.

4.2.11 Verify Post-Upgrade Status (1+1 3-Tier)

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

Procedure 17: Verify Post-Upgrade Status (1+1 3 Tier)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen isis displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Execute following commands on the upgraded servers : Use your SSH client to connect to each of the upgraded DA-MP server (ex. 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 Tekelec in case of errors.** **# alarmMgr --alarmstatus** 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** Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each server.

Procedure 17: Verify Post-Upgrade Status (1+1 3 Tier)

2 ☐	Log all current alarms	Log all current alarms in the system: 1. Log in to the Active NOAM GUI VIP. 2. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. Following Alarm ID will be observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** **3.** Click **Report** button to generate an Alarms report. **4.** Save the report and print the report. Keep these copies for future reference.
3 ☐	Execute Post Upgrade Overview	Execute Procedure 77 Post-Upgrade .
End of second maintenance window		

Note: If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 15 in another maintenance window.

4.3 3-Tier DSR Upgrade for (N+0) DA-MP configuration (possibly including TVOE)

This section contains upgrade steps for DSR 5.x (3-tier setup) upgrade with (N+0) configuration (major or incremental).

4.3.1 NO Upgrade Execution for 3-Tier (N+0) setup

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), and 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 10. NO Upgrade Execution Overview (For DSR 3-tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 18	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check	None
Procedure 19	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Inhibit Replication	No Traffic Impact
Procedure 20	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 21	0:25-1:00	0:56-2:15	1:25-2:00	2:56-4:15	Upgrade NOs	Provisioning Disabled, No Traffic Impact
Procedure 22	0:05-0:10	1:01-2:25	0:05-0:10	3:01-4:25	Allow Replication between NOs and DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 23	0:01-0:05	1:02-2:30	0:01-0:05	3:02-4:30	Verify Post Upgrade Status	Provisioning to SOAM is not supported till site upgrades are also performed.

4.3.2 Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAMs)

This procedure is used to determine the health and status of the network and servers. This must be executed on the active NOAM.

Procedure 18: Perform Health Check (Pre-Upgrade of 3-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 TEKELEC TECHNICAL SERVICES 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 there are not on the required release (typically 2.5.x), 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 18: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM)

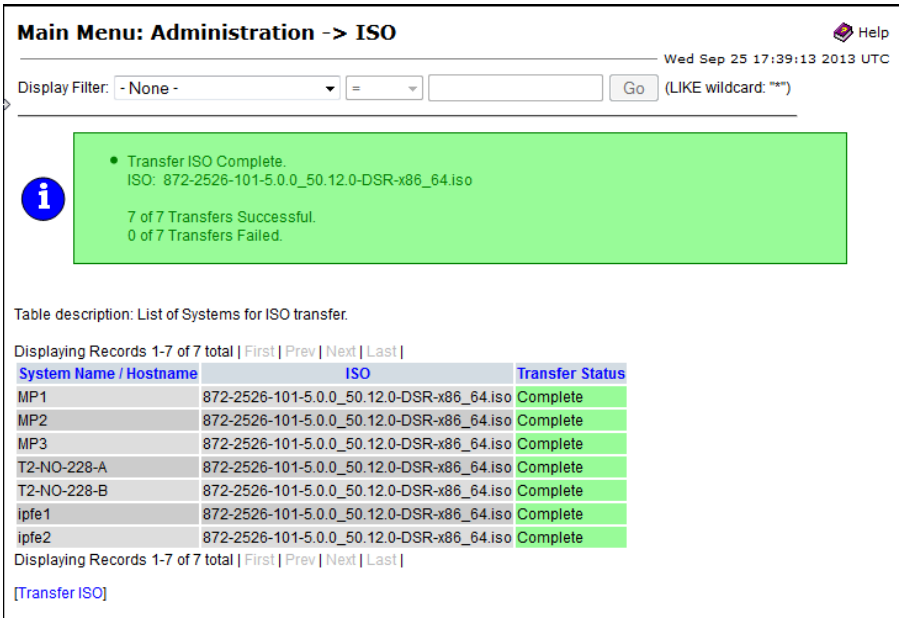
2 ☐	**NO GUI:** Verify NO Servers existing Application Version	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade). Example: **Note**: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases. **Upgrade Screen in DSR 4.x** **Main Menu: Administration -> Upgrade** (see 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)

Upgrade Screen in DSR 5.x

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 18: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify DSR ISO file has been Transferred to all servers: Example:  IF Not, see ISO Administration 3.3.8.
4 ☐	Verify Server Status is Normal	Verify Server Status is Normal: Log Into the NOAM GUI using the VIP. 1. Select **Status & Manage > Server;** the Server Status screen is displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is not recommended to continue executing 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.
5 ☐	Log all current alarms at NOAM	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
6 ☐	Repeat for active SOAMs	Log all current alarms in allSOAM(s): 1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

Procedure 18: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM)

7 ☐	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. Select **Status and Manage → Files** Check time stamp on two 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 re-perform) a full Backup, if needed.

4.3.3 Inhibit Replication for 3-tier(N+0) setup

Inhibit Replication between NOs, and replication from NOs to SOs.

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

Procedure 19. Inhibit Replication for 3-Tier(N+0) setup

S T E P #	This Procedure inhibits replication for 3-Tier NO (and DR-NO) servers, prior to upgrade. Also inhibits replication from NOs to SOs. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window	
1 ☐	Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. 1. Select **Status & Manage > Database;** the Database Status screen is displayed 2. Click **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] - Provisioning is manually disabled**. 5. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 19. Inhibit Replication for 3-Tier(N+0) setup

2 ☐	Inhibit SOAP replication **(This step will NOT be required for most upgrades!)**	**Record current DSR release number_____ex: 4.0.2_40.27.3** **SKIP THIS STEP if current release is DSR 4.0.0_40.19.0 or greater.** Use your SSH client to connect to the active NO server (ex. ssh, putty): **ssh <Active NO IP address>** **login as: root** **password: <enter password>** 1. Execute the following command to disable SOAP replication : **# iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"** Execute following command to verify if above command successfully updated NodeInfo records: **# iqt -E NodeInfo** Verify that **excludeTables** field shall include '**HaNodeLocPref HaVipDef**' table names **for each NodeId present on the setup** : E,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef** SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO,SO or MP servers.
3 ☐	Inhibit replication to MP servers (N+0)	Replication of MPs will be inhibited during site upgrade.

4 ☐	Inhibit replication to SO servers at a site	Inhibit database replication to SO servers in the following order:
		
		• Site:
		  ○ Standby SO
		  ○ Active SO
		
		From Active NO:
		1. Select **Status & Manage > Database**
		  The Database Status screen is displayed.
		2. Select the appropriate **SO server.**
		3. Click **Inhibit Replication** button.
		4. Verify the ***Inhibited*** text is displayed for server.
		5. **Repeat** the **above steps for** all remaining servers in the order: standby, then active).
		
		ALL SOAM must be inhibited.

Procedure 19. Inhibit Replication for 3-Tier(N+0) setup

5 ☐	Verify that SO Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all SOs, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) servers must have: Alarm ID = 31113 (Replication Manually Disabled)
6 ☐	Inhibit replication between NO servers.	Inhibit database replication between NO servers in the following order: • Standby NO • Active NO • Standby DR NO(if applicable) • Active DR NO(if applicable) Select **Status & Manage > Database** The Database Status screen is displayed. 1. Select the appropriate NO or DR-NO server based on the list above. 2. Click Inhibit Replication button. 3. Verify the Inhibited text is displayed for server. 4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
7 ☐	Verify that All NO and SO Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
8 ☐	Disable Site Provisioning at all SOAMs	Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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 substeps 2 through 5 for all the sites present in the setup.

4.3.4 Upgrade DR-NOs of 3-Tier (N+0) setup

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 20. Upgrade DR-NO(s) 3 -Tier configuration

S T E P #	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	*Begin Upgrade of DR-NOs*	*Next Steps will begin Upgrade of the DR-NO servers.* *SKIP this Procedure if the deployment does not include DR-NO servers.*
2 ☐	Upgrade Host TVOE for **Standby** DR-NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** DR NO
3 ☐	Upgrade **Standby** DR-NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR DR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
4 ☐	Upgrade Host TVOE for **Active** DR-NO (if needed)	*Skip this step if:* • *the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** DR NO to upgrade TVOE.

Procedure 20. Upgrade DR-NO(s) 3 -Tier configuration

5 ☐	Verify cmha process is running on upgraded DR NO	Log into the just-upgraded **standby** DR NO upgraded above, execute the following command:
		
		`ssh <NO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		`[root@NO1 ~]# pl | grep "cmha"`
		
		The following output should be generated:
		
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		
		If no output is generated then execute following command:
		
		`service start_cmha start`

6 ☐	Upgrade **Active** DSR DR-NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR DR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
7 ☐	Proceed to next procedure	Proceed to upgrade the NO servers, using the next procedure

4.3.5 Upgrade NOs for 3-Tier(N+0) setup

Procedure 21. Upgrade NO for 3 –Tier(N+0) configuration

S T E P #	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Upgrade Host TVOE for **Standby** NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** NO
2 ☐	Upgrade **Standby** NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
3 ☐	Upgrade Host TVOE for **Active** NO (if needed)	*Skip this step if:* • *the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** NO to upgrade TVOE.

4 ☐	Verify cmha process is running on upgraded NO	Log into the just-upgraded **standby** NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 21. Upgrade NO for 3 –Tier(N+0) configuration

5 ☐	Upgrade **Active** DSR NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
6 ☐	Verify NO GUI access via VIP Address	Close and re-open Browser using the VIP address for the NOAM. Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected. The NOAM GUI will show the new DSR 5.0 release. Expected Alarms include: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and MP servers must have: Alarm ID = 31113 (Replication Manually Disabled)
	Proceed to next procedure	Proceed to next procedure, to allow replication between NOs.

4.3.6 Allow Replication between NO and DR NO Servers ONLY for 3-Tier(N+0) setup

Procedure 22. Allow Replication between NO and DR NO Servers for 3-Tier (N+0) setup

S T E P #	This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.

Procedure 22. Allow Replication between NO and DR NO Servers for 3-Tier (N+0) setup

1 ☐	Allow replication to NO and DR-NO servers only.	Allow database replication to **NO and DR-NO servers ONLY:** **Note: The NO servers intentionally have a sequence of "Allow Active, Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.** Select **Status & Manage > Database.** The Database Status screen is displayed. 1. Select the **Active NO server.** 2. Click Allow Replication button. 3. Verify the Inhibited text is not displayed for the server. After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 4. Repeat the Allow action link for **Standby NO server.** **Repeat sub-steps 1 through 4 for DR NO(s) (if applicable).** **Note: You must not allow Replication to any SOAMs or MPs. This can result in database corruption at these servers.**
2 ☐	Enable global provisioning and configuration(if new Network element is required to be added)	Enable provisioning and configuration updates on the entire network (if new Network element is required to be added): **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 to only upgraded SO(s).** 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM.

4.3.7 Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)

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

Procedure 23: Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)

S T E P #	This procedure verifies Post Upgrade Status for 3-Tier(1+1) 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 23: Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)

1 ☐	**SSH:** Verify NO and DR-NO Server Status(optional)	Verify Server Status after NO servers upgraded:
		
		1. Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers :
		
		Use your SSH client to connect to the upgraded server (ex. 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 Tekelec.
		
		`# alarmMgr --alarmstatus`
		
		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 Tekelec in case above output is not generated.

2 ☐	**NO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the NOAM GUI via the VIP. 2. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is displayed. 3. Click **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) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

Procedure 23: Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)

3 ☐	**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 view is displayed. 3. Click **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) Alarm ID = **31113** (Replication Manually Disabled)
4 ☐	Verify Traffic status	Login to SOAM GUI to view KPI reports to verify traffic is at the expected condition.
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 can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.** **Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs 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 check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices** 1. Login to 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).
6 ☐	*Note on Provisioning status*	Provisioning on the SOs, and Replication from NO to the Site level SO, will typically remain disabled till further upgrades are performed on the sites. SO provisioning shall also remain disabled. NOTE: (SO replication inhibit will prevent most NO configuration changes from being propagated to the SOs.)
End of maintenance window		

4.3.8 Site Upgrade for 3-Tier (N+0) Configuration.

This section contains the steps required to upgrade a 3-tier DSR site that has a SOAM function, and 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) (i.e. site) should be upgraded in its own separate maintenance window.
Global provisioning can be re-enabled after Site upgrade(if required).

Table 11. Upgrade Execution Overview (For DSR (N+0) 3 tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 24	0:25-1:00	0:26-1:05	1:25-2:00	1:26-2:05	Upgrade SO(s) of (N+0) 3-Tier configuration	None
Procedure 25	0:25-1:00	0:51-2:05	0:25-1:00	1:51-3:05	Upgrade SBR(s) 3-Tier Configuration	None
Procedure 26	0:25-1:10	1:16-3:15	0:25-1:10	2:16-4:15	Upgrade Multiple MP(s) in 3-Tier Configuration	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 27	0:25-1:00	1:41-4:15	0:25-1:00	2:41-5:15	Upgrade IPFE(s) 3-Tier Configuration	None
Procedure 29	0:01-0:05 Per MP	1:57-5:35	0:01-0:05 Per MP	3:07-6:35 worst-case cumulative time (16 DA-MPs is considered)	Perform Health Check (Post Upgrade of MPs)	None

4.3.9 Upgrade SO of (N+0) 3-Tier configuration

Detailed steps are shown in the procedure below.

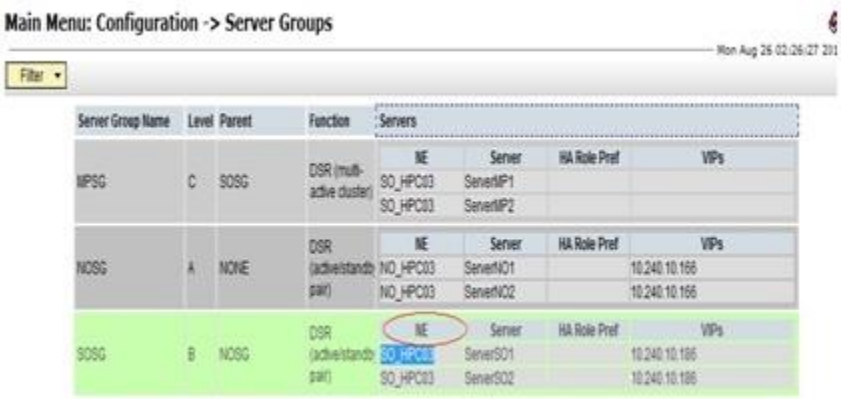
Procedure 24. Upgrade SO(s) of (N+0) 3-Tier configuration.

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window(If required)	
1 ☐	Verify Traffic status	Login to Active SOAM and verify KPI reports to verify traffic is at the expected condition.
2 ☐	Verify that site Provisioning is disabled	Verify that site provisioning for the site which is currently being upgraded is disabled. By logging into the site VIP and checking for Provisioning disabled alarm. If provisioning disabled alarm is not present then execute following steps : 1. Log into the GUI of the SOAM which needs to be upgraded, using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled.

3 ☐	Inhibit replication to MP servers (N+0)	**Record current release number _____ ex: 4.0.2_40.27.3**
		
		• **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G). In this case, SKIP THIS STEP.**
		
		[Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.]
		
		• **IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands** to inhibit A and B level replication on **all MP servers of this site**
		
		Log into Active NO(if logged out, else ignore this step) :
		
		`# ssh root@<Active NO XMI IP>`
		`login as: root`
		`password: <enter password>`
		
		Execute following command on active NO :
		
		`# for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site which is being upgraded>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done`

Procedure 24. Upgrade SO(s) of (N+0) 3-Tier configuration.

Note: NE name of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong to the site which is being upgraded then siteId will be SO_HPC03.



Note: After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B' :

```
[root@NO1 ~]# iqt NodeInfo
    nodeId          nodeName        hostName nodeCapability     inhibitRepPlans
siteId excludeTables
  A1386.099         NO1             NO1      Active
NO_HPC3
  B1754.109         SO1             SO1      Active
SO_HPC03
  C2254.131         MP2             MP2      Active             A B
SO_HPC03
  C2254.233         MP1             MP1      Active             A B
SO_HPC3
```

4 ☐	Upgrade TVOE Host for Standby SO(if needed)	IF standby SO is hosted on TVOE blade, Verify that the TVOE Host is Upgraded. **Execute Appendix J** for the standby SO TVOE Host if needed.
5 ☐	Upgrade standby SO	Upgrade 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 step 5 below.

Procedure 24. Upgrade SO(s) of (N+0) 3-Tier configuration.

6 ☐	Active SO TVOE Host Upgrade (if needed)	IF Active SO is hosted on TVOE blade, and the TVOE Host needs to be upgraded: **Execute Appendix J** to upgrade the Active SO TVOE Host Execute following commands on upgraded server:

7 ☐	Verify cmha process is running on upgraded SO	1. Log into the just-upgraded standby SO, execute the following command:
		
		`# ssh root@<SO XMI IP ADDRESS>`
		`login as: root`
		`password: <enter password>`
		
		Execute following command on SO:
		
		`[root@SO1 ~]# pl | grep "cmha"`
		
		The following output should be generated:
		
		`A 10128 cmha Up 11/20 00:15:58 1 cmha`
		
		If no output is generated then execute following command:
		
		`# service start_cmha start`

8 ☐	Upgrade Active SO.	Upgrade 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 next procedure. Note: At this point, SO replication is still inhibited (from the GUI), and the C-level servers replication is "AB Inhibitied: (INH Plans=A,B) from the iset command. However, Repl Status shows Allowed for the C Level servers (from the GUI)
9 ☐	Install NetBackup on NO and SO (If required).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document**

4.3.10 Upgrade cSBR(s)

If the DSR being upgraded is running OFCS, ensure that the cSBR(s) are upgraded on an enclosure basis: 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.
Any of the cSBR of 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 4.6.2 of this document

Procedure 25. Upgrade cSBR(s) in 3-Tier(N+0) Configuration

STEP #	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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
1 ☐	Find the enclosures in the system.	Find the enclosures in the system. Each enclosure shall contain an IPFE, Active MPs, active cSBRs and a standby cSBR.
2 ☐	Find the active cSBR(s) in the enclosure	Find and record the hostname of Active and Standby cSBR(s) in the enclosure by going to Status & Manage -> HA screen and finding the servers with role as cSBR.
3 ☐	Upgrade cSBRs in OFCS configuration	1. Upgrade each of the standby cSBR servers identified in step 2, following the Upgrade Single Server procedure. All the 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 with sub-step 2 below. 2. Upgrade each of the leftover cSBRs identified in step 2, following the Upgrade Single Server procedure. All the Leftover 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 next procedure below.

4.3.11 Upgrade All Active DA-MPs

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: 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 26 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 25 must be executed four distinct times.

Procedure 26. Upgrade All Active DA-MPs in a 3-Tier Configuration

STEP #	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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify all the DA-MPs to be upgraded together.	User can choose any number of MP(s) on which upgrade can be executed in parallel considering traffic.
2 ☐	Upgrade Active MPs	Upgrade the selected DA-MPs, executing the Upgrade Single Server procedure on all selected DA-MPs in parallel. **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G for all selected DA-MPs, return to this point and continue with next procedure.

4.3.12 Upgrade IPFE(s) in 3-Tier(N+0) configuration

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 27. Upgrade IPFE(s) in 3-Tier(N+0) Configuration

STEP #	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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify IPFE upgrade order	User can choose any number of IPFEs on which upgrade can be executed in parallel considering traffic impact. All the 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 27. Upgrade IPFE(s) in 3-Tier(N+0) Configuration

2 ☐	Upgrade IPFE servers	1. Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure. **Execute Appendix G** -- Single Server Upgrade Procedure 2. Upgrade remaining IPFEs of the current site in parallel using Appendix G

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	Execute following steps on each IPFE server just upgraded :
		
		1. Use ssh client to connect to the IPFE server :
		
		`ssh <IPFE XMI IP address>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute following command on the IPFE server :
		
		`# grep "IPV6_AUTOCONF=no" /etc/sysconfig/network`
		`# grep "IPV6FORWARDING=yes" /etc/sysconfig/network`
		
		If the outcome of any of the above command is blank then execute the steps below else skip the steps below
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# init 6`
		
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

4.3.13 Allow Replication for Upgraded Site in 3-Tier(N+0) configuration

This procedure is used to allow 'A B' level replication for MP servers (inhibited as part of Appendix G (step 4).
Also allows the replication and provisioning disabled for SO servers.
Global Provisioning can be enabled after a site upgrade if required.

Procedure 28: Allow Replication for upgraded Site in 3-Tier(N+0) configuration

S T E P #	This procedure allow replication 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	

1 ☐	Enable 'A B' level replication inhibited for MP(s)(Only if source upgrade release is earlier than 4.1.0_41.16.0)	**Note: The following steps will uninhibit replication to C level servers**
		
		Enable replication disabled previously only if **source upgrade release was earlier than 4.1.0_41.16.0** :
		
		1. Log into the standby SO using ssh client or puTTy :
		
		`ssh <standby SO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to enable replication :
		
		`# iload /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml`
		
		`# pm.set off inetrep`
		
		`# pm.set on inetrep`
		
		Execute above sub-steps 1 and 2 for the active SO as well.

2 ☐	Allow replication to SO servers.	Allow database replication to SO servers: 1. Log into the active NO GUI using the VIP. 2. Select **Status & Manage > Database** 3. The Database Status screen is displayed. 4. Select the **Active SO** server. 5. Click Allow Replication button. After the Allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. Note: "Allowed" text dialog may be hidden beneath the Provisoing disabled text dialog. 6. Verify the Inhibited text is not displayed for the server. 7. Repeat the Allow action link for Standby SO server. **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.**

Procedure 28: Allow Replication for upgraded Site in 3-Tier(N+0) configuration

3 ☐	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 to the entire network. Please note that by enabling global provisioning new data provisioned at NOAM will be replicated to only upgraded SO(s). 1. Log into the active NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.**
4 ☐	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 **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**
5 ☐	Update Max Allowed HA Role for NO and SO.	1. While logged in to the active NOAM GUI, go to the Status & Manage-> HA screen. 2. Click 'Edit' button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click 'Ok' button.

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

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

Procedure 29: Verify Post Upgrade status (N+0 3-Tier)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen is displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 4. Execute following commands on the upgraded servers : Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. 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 Tekelec in case of errors.

Procedure 29: Verify Post Upgrade status (N+0 3-Tier)

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Log in to the active NOAM GUI using VIP and select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed.
		Following Alarm ID will be observed on all 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 server, then execute following commands on that particular server to check the existence of alarm :
		
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. 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 Tekelec in case above output is not raised.
		
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each MP server.
		
		3. Click **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

3 ☐	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
End of second maintenance window.		

Note: If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 24 in another maintenance window.

4.4 3-Tier DSR Upgrade for (N+0) DA-MP configuration on RMS servers (including TVOE)

This section contains the steps required to upgrade a 3-tier DSR, deployed on RMSes, 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: - Make sure that session output should be logged for future debugging.

4.4.1 NO Upgrade Execution for RMS servers (N+0) setup

This section contains upgrade steps for DSR 5.x (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), and 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 12. NO Upgrade Execution Overview (For DSR 3-tier(N+0) RMS configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 30	0:01-0:05	0:01-	0:01-0:05	0:01-	Perform Health Check	None

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
		0:05		0:05		
Procedure 31	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Inhibit Replication	No Traffic Impact
Procedure 32	0:25-1:00	0:31-2:15	1:25-2:00	1:31-2:15	Upgrade DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 33	0:25-1:00	0:56-3:15	1:25-2:00	2:56-4:15	Upgrade NOs	Provisioning Disabled, No Traffic Impact
Procedure 34	0:05-0:10	1:01-3:25	0:05-0:10	3:01-4:25	Allow Replication between NOs and DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 35	0:01-0:05	1:02-3:30	0:01-0:05	3:02-4:30	Verify Post Upgrade Status	Provisioning to SOAM is not supported till site upgrades are also performed.

4.4.2 Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAMs on RMS blade)

This procedure is used to determine the health and status of the network and servers. This must be executed on the active NOAM.

Procedure 30: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM on RMS blade)

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 TEKELEC TECHNICAL SERVICES 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.x), 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 30: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM on RMS blade)

2 **NO GUI:** Verify NO Servers existing Application Version

For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade).

Example:

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases.

Upgrade Screen in DSR 4.x

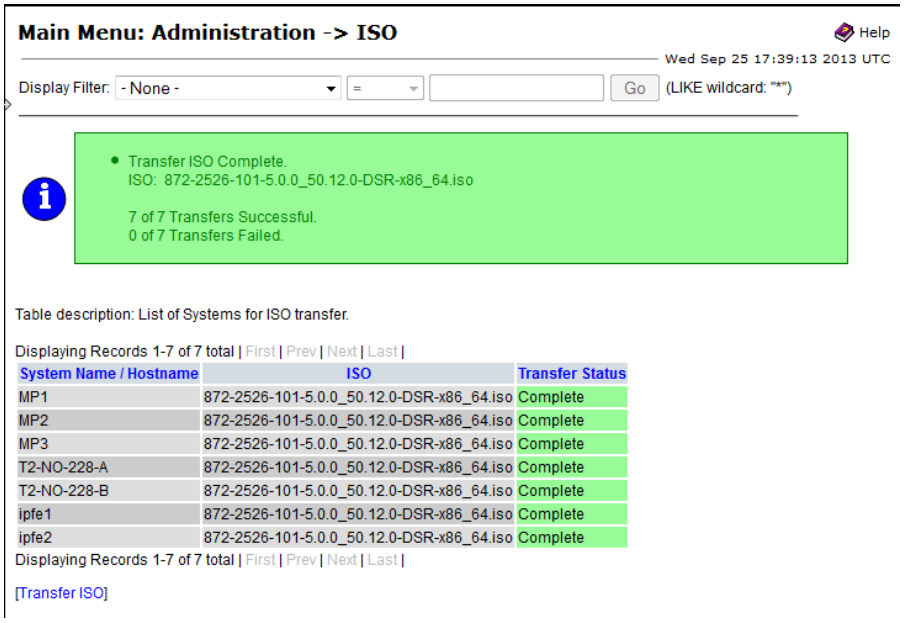
Main Menu: Administration -> Upgrade

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.x

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 30: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM on RMS blade)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify DSR ISO file has been Transferred to all servers: Example:  IF Not, see ISO Administration 3.3.8.
4 ☐	Verify Server Status is Normal	Verify Server Status is Normal: Log Into the NOAM GUI using the VIP. 1. Select **Status & Manage > Server;** the Server Status screen is displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is not recommended to continue executing 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.
5 ☐	Log all current alarms at NOAM	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
6 ☐	Repeat for active SOAMs	Log all current alarms in the SOAM: 1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

Procedure 30: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM on RMS blade)

7 ☐	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. Select **Status and Manage → Files** Check time stamp on two 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 re-perform) a full Backup, if needed.

4.4.3 Inhibit Replication for 3-tier(N+0) RMS configuration

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

Procedure 31. Inhibit Replication for 3-Tier(N+0) RMS setup

S T E P #	This Procedure inhibits replication 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 (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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window	
1 ☐	Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. 1. Select **Status & Manage > Database;** the Database Status screen is displayed 2. Click **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] - Provisioning is manually disabled**. 5. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Inhibit replication to MP servers (N+0)	Replication of MPs will be inhibited during site upgrade.

3 ☐	Inhibit replication to SO servers at a site	Inhibit database replication to SO servers in the following order:
		
		• Site:
		  ○ Standby SO
		  ○ Active SO
		
		From Active NO:
		1. Select **Status & Manage > Database**
		The Database Status screen is displayed.
		2. Select the appropriate **SO server.**
		3. Click **Inhibit Replication** button.
		4. Verify the ***Inhibited*** text is displayed for server.
		5. **Repeat** the **above steps for** all remaining servers in the order: standby, then active).
		
		ALL SOAMs must be inhibited.

Procedure 31. Inhibit Replication for 3-Tier(N+0) RMS setup

4 ☐	Verify that SO Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all SOs, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) servers must have: Alarm ID = 31113 (Replication Manually Disabled)
5 ☐	Inhibit replication between NO servers.	Inhibit database replication between NO servers in the following order: • Standby NO • Active NO • Standby DR NO(if applicable) • Active DR NO(if applicable) Select **Status & Manage > Database** The Database Status screen is displayed. 5. Select the appropriate NO or DR-NO server based on the list above. 6. Click Inhibit Replication button. 7. Verify the Inhibited text is displayed for server. 8. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
6 ☐	Verify that NOs and SOs are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
7 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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 substeps 2 through 5 for all the sites present in the setup.

4.4.4 Upgrade DR-NOs of 3-Tier(N+0) setup on RMS servers

Procedure 32. Upgrade DR-NO(s) 3 –Tier(N+0) RMS configuration

S T E P #	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	*Begin Upgrade of DR-NOs*	*Next Steps will begin Upgrade of the DR-NO servers.* *SKIP this Procedure if the deployment does not include DR-NO servers.*
2 ☐	Upgrade Host TVOE for **Standby** DR-NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** DR NO
3 ☐	Upgrade **Standby** DR-NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR DR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
4 ☐	Upgrade Host TVOE for **Active** DR-NO (if needed)	*Skip this step if:* • *the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** DR NO to upgrade TVOE.

5 ☐	Verify cmha process is running on upgraded DR NO	Log into the just-upgraded **standby** DR NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 32. Upgrade DR-NO(s) 3 –Tier(N+0) RMS configuration

6 ☐	Upgrade **Active** DSR DR-NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR DR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
7 ☐	Proceed to next procedure	Proceed to upgrade the NO servers, using the next procedure

4.4.5 Upgrade NOs for 3-Tier(N+0) RMS setup

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 33. Upgrade NO for 3 –Tier(N+0) RMS configuration

S T E P #	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Upgrade Host TVOE for **Standby** NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** NO
2 ☐	Upgrade **Standby** NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
3 ☐	Upgrade Host TVOE for **Active** NO (if needed)	*Skip this step if:* • *the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)*

4 ☐	Verify cmha process is running on upgraded NO server.	**Execute Appendix J** for the **active** NO to upgrade TVOE.
		Log into the just-upgraded **standby** NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 33. Upgrade NO for 3 –Tier(N+0) RMS configuration

5 ☐	Upgrade **Active** DSR NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
6 ☐	Verify NO GUI access via VIP Address	Close and re-open Browser using the VIP address for the NOAM. Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected. The NOAM GUI will show the new DSR 5.0 release. Expected Alarms include: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SOs and NOs servers must have: Alarm ID = 31113 (Replication Manually Disabled)
	Proceed to next procedure	Proceed to next procedure, to allow replication between NOs.

4.4.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier(N+0) RMS configuration

Procedure 34. Allow Replication between NO and DR NO Servers on RMS servers (3-tier(N+0))

S T E P #	This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, and 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.

Procedure 34. Allow Replication between NO and DR NO Servers on RMS servers (3-tier(N+0))

1 ☐	Allow replication to NO and DR-NO servers only.	Allow database replication to **NO and DR-NO servers ONLY:** **Note: The NO servers intentionally have a sequence of "Allow Active, Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.** Select **Status & Manage > Database.** The Database Status screen is displayed. 1. Select the **Active NO server.** 2. Click Allow Replication button. 3. Verify the Inhibited text is not displayed for the server. After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 4. Repeat the Allow action link for **Standby NO server.** **Repeat sub-steps 1 through 4 for DR NO(s) (if applicable).** **Note: You must not allow Replication to any SOAMs or MPs. This can result in database corruption at these servers.**
2 ☐	Verify NO and DR-NO Provisioning/replication	It is expected that NO Provisioning is still disabled, and this will remain disabled till sites are upgraded. Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) Following alarms shall not be raised for NO or DR NO servers: Alarm ID = 31113 (Replication Manually Disabled) **IF Upgrade verification steps indicate a problem, consult with support on the best course of action. Procedures for backout of the upgrade are included in this document.**

4.4.7 Verify Post Upgrade Status on RMS servers (3-tier(N+0) NO Upgrade)

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

Procedure 35: Verify Post Upgrade Status on RMS servers (3-tier(N+0) NO Upgrade)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 35: Verify Post Upgrade Status on RMS servers (3-tier(N+0) NO Upgrade)

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		
		1. Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers :
		
		Use your SSH client to connect to the upgraded server (ex. 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 Tekelec.
		
		`# alarmMgr --alarmstatus`
		
		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 Tekelec in case above output is not generated.

2 ☐	**NO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the NOAM GUI via the VIP. 2. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is displayed. 3. Click **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) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

Procedure 35: Verify Post Upgrade Status on RMS servers (3-tier(N+0) NO Upgrade)

3 ☐	**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 view is displayed. 3. Click **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) Alarm ID = **31113** (Replication Manually Disabled)
4 ☐	Verify Traffic status	Login to SOAM GUI to view KPI reports to verify traffic is at the expected condition.
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 can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.** **Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs 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 check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices** 1. Login to Active NO console and execute the following command **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh** NOTE: This command may execute without any output when no changes are required (no devices were found to update).
6 ☐	*Note on Provisioning status*	Provisioning on the NO and SOs, and Replication from NO to the Site level SO, will typically remain disabled till further upgrades are performed on the sites. SO provisioning shall also remain disabled. NOTE: (SO replication inhibit will prevent most NO configuration changes from being propagated to the SOs.)
End of maintenance window		

4.4.8 Site Upgrade for (N+0) 3-Tier RMS Configuration.

This section contains the steps required to upgrade a 3-tier DSR site that has a 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 site has been upgraded.

Table 13. Upgrade Execution Overview (For DSR (N+0) 3 tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 37	0:26-1:05	0:26-1:05	0:26-1:05	0:26-1:05	Upgrade SO(s) of (N+0) 3-Tier configuration	None
Procedure 38	0:20-1:10	0:46-2:15	0:20-1:10	0:46-2:15	Upgrade Multiple MP(s) in 3-Tier Configuration	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 39	0:10-1:00	1:56-3:15	0:10-1:00	1:56-3:15	Upgrade IPFE(s) 3-Tier Configuration	None
Procedure 41	0:01-0:05 Per MP	1:57-4:35	0:01-0:05 Per MP	1:57-4:35 worst-case cumulative time (16 DA-MPs is considered)	Perform Health Check (Post Upgrade of MPs)	None

4.4.9 Perform Health Check for 3-Tier(N+0) RMS configuration

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

Procedure 36: Perform Health Check for Site Upgrade (3-Tier (N+0) RMS blade)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status	Verify Server Status after NO servers upgraded: 1. Execute following commands on both the active and standby NOAM servers: Use your SSH client to connect to the upgraded server (ex. 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. Contact Tekelec if any errors are observed. 2. Log in to Active NOAM VIP GUI and select Alarms & Events-> View Active screen to verify Servers alarms. Servers have following expected alarms: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) 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 server, then execute following commands on that server to check the existence of 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 Tekelec in case above output is not raised.** 3. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each server.

Procedure 36: Perform Health Check for Site Upgrade (3-Tier (N+0) RMS blade)

2 ☐	Log all current alarms	Log all current alarms in the system from the already logged in Active NOAM VIP : 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view isis displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.

4.4.10 Upgrade SO (3-Tier(N+0) RMS configuration)

Detailed steps are shown in the procedure below.

Procedure 37. Upgrade SO(s) of (N+0) 3-Tier RMS configuration.

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window(If required)	
1 ☐	Verify Traffic status	Login to Active SOAM and verify KPI reports to verify traffic is at the expected condition.
2 ☐	Verify that site Provisioning is disabled	Verify that site provisioning for the site which is currently being upgraded is disabled. By logging into the site VIP and checking for Provisioning disabled alarm. If provisioning disabled alarm is not present then execute following steps : 1. Log into the GUI of the SOAM which needs to be upgraded, using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled.

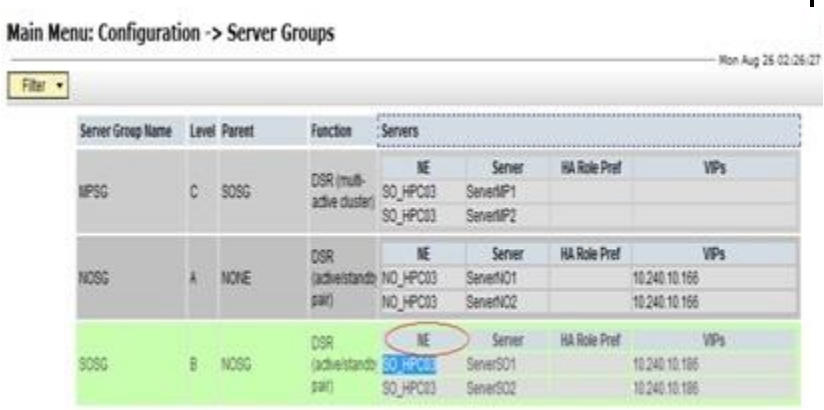
3 ☐	Inhibit replication to MP servers (N+0)	**Record current release number___ex: 4.0.2_40.27.3_____**
		• **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G). In this case, SKIP THIS STEP.**
		[Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.]
		• **IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the commands** to inhibit A and B level replication on **all MP servers of this site** :
		Log into Active NO(if logged out, else ignore this step) :
		`# ssh root@<Active NO XMI IP>`
		`login as: root`
		`password: <enter password>`

Procedure 37. Upgrade SO(s) of (N+0) 3-Tier RMS configuration.

Execute following command on active NO :

```
# for i in $(iqt -p -z -h -fhostName NodeInfo
where "nodeId like 'C*' and siteId='<NE name of
the site which is being upgraded>'"); do iset -
finhibitRepPlans='A B' NodeInfo where
"nodeName='$i'"; done
```

Note: NE name of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong to the site which is being upgraded then siteId will be SO_HPC03.



Note: After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B' :

```
[root@NO1 ~]# iqt NodeInfo
    nodeId          nodeName        hostName nodeCapability    inhibitRepPlans
siteId excludeTables
  A1386.099         NO1             NO1      Active
NO_HPC3
  B1754.109         SO1             SO1      Active
SO_HPC03
  C2254.131         MP2             MP2      Active            A B
SO_HPC03
  C2254.233         MP1             MP1      Active            A B
SO_HPC3
```

3	Upgrade standby SO	Upgrade 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 step 4 below. **Note: In an RMS-based DSR the SOAM is a guest on a TVOE host that has already been upgraded as part of the NOAM upgrade.**

Procedure 37. Upgrade SO(s) of (N+0) 3-Tier RMS configuration.

4 ☐	Upgrade Active SO.	Upgrade 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 next procedure. **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.** Note: At this point, SO replication is still inhibited (from the GUI), and the C-level servers replication is "AB Inhibitied: (INH Plans=A,B) from the iset command. However, Repl Status shows Allowed for the C Level servers (from the GUI)
5 ☐	Install NetBackup on NO and SO (If required).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.**

4.4.11 Upgrade All Active DA-MPs of 3-Tier(N+0) RMS configuration

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

Procedure 26 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 26 must be executed four distinct times.

Procedure 38. Upgrade All Active DA-MPs in a 3-Tier(N+0) RMS Configuration

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
1 ☐	Identify all the DA-MPs to be upgraded together.	User can choose any number of MP(s) on which upgrade can be executed in parallel considering traffic.
2 ☐	Upgrade Active MPs	Upgrade the selected DA-MPs, executing the Upgrade Single Server procedure on all selected DA-MPs in parallel. **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G for all selected DA-MPs, return to this point and continue with Step 3 below.

4.4.12 Upgrade IPFE(s) in 3-Tier(N+0) RMS Configuration

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 39. Upgrade IPFE(s) in 3-Tier(N+0) RMS Configuration

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
1 ☐	Identify IPFE upgrade order	User can choose any number of IPFEs on which upgrade can be executed 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.
2 ☐	Upgrade IPFE servers	1. Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure. **Execute Appendix G** -- Single Server Upgrade Procedure 2. Upgrade remaining IPFEs of the current site in parallel using Appendix G

Procedure 39. Upgrade IPFE(s) in 3-Tier(N+0) RMS Configuration

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	Execute following steps on each IPFE server just upgraded :
		
		1. Use ssh client to connect to the IPFE server :
		
		`ssh <IPFE XMI IP address>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute following command on the IPFE server :
		
		`# grep "IPV6_AUTOCONF=no" /etc/sysconfig/network`
		`# grep "IPV6FORWARDING=yes" /etc/sysconfig/network`
		
		`If the outcome of any of the above command is blank then execute the steps below else skip the steps below`
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# init 6`
		
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

4.4.13 Allow Replication for Upgraded Site(N+0) configuration of RMS blade

This procedure is used to allow 'A B' level replication for MP servers (inhibited as part of Appendix G (step 4). Also allows the replication inhibited for SO servers.

Procedure 40: Allow Replication for upgraded Site(N+0) configuration of RMS blade

S T E P #	This procedure allow replication for SO and MP servers of 3-Tier(N+0) RMS 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Enable 'A B' level replication inhibited for MP(s)	Enable replication disabled previously only if **source upgrade release was earlier than 4.1.0_41.16.0** : 1. Log into the standby SO using ssh client or puTTy : **ssh <standby SO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable replication : **# iload /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml** **# pm.set off inetrep** **# pm.set on inetrep** **Execute above sub-steps 1 and 2 for the active SO as well.**
2 ☐	Allow replication to SO servers.	Allow database replication to SO servers: 1. Log into the active NO GUI using the VIP. 2. Select **Status & Manage > Database** 3. The Database Status screen is displayed. 4. Select the Active SO server. 5. Click Allow Replication button. After the Allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. Note: "Allowed" text dialog may be hidden beneath the Provisoing disabled text dialog. 6. Verify the Inhibited text is not displayed for the server. 7. Repeat the Allow action link for Standby SO server. **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.**

Procedure 40: Allow Replication for upgraded Site(N+0) configuration of RMS blade

3 ☐	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 to only upgraded SO(s). 1. Log into the active NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen isis displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.**
4 ☐	Enable site provisioning.	**Enable Site provisioning :** 1. Log into the SOAM VIP GUI of the site just upgraded above. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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.**
5 ☐	Update Max Allowed HA Role for NO and SO.	1. While logged in to the active NOAM GUI, go to the Status & Manage-> HA screen. 2. Click 'Edit' button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click 'Ok' button.

4.4.14 Verify Post Upgrade status on RMS servers (N+0 3-Tier)

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

Procedure 41: Verify Post Upgrade status on RMS servers (N+0 3-Tier)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen isis displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 4. Execute following commands on the upgraded servers : Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. 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 Tekelec in case of errors.

Procedure 41: Verify Post Upgrade status on RMS servers (N+0 3-Tier)

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Log in to the active NOAM GUI using VIP and select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed.
		Following Alarm ID will be observed on all 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 server, then execute following commands on that particular server to check the existence of alarm :
		
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. 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 Tekelec in case above output is not raised.
		
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each MP server.
		
		3. Click **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

3 ☐	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
End of second maintenance window.		

Note: If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 37 in another maintenance window.

4.5 3-Tier DSR Upgrade for (1+1) DA-MP configuration on RMS servers (including TVOE)

This section contains the steps required to upgrade a 3-tier DSR, deployed on RMSes, 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: - Make sure that session output should be logged for future debugging.

4.5.1 NO Upgrade Execution for RMS servers (1+1) setup

This section contains upgrade steps for DSR 5.x (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), and 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 14. NO Upgrade Execution Overview (For DSR 3-Tier(1+1) RMS configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 42	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check	None
Procedure 43	0:05-0:10	0:06-0:15	0:05-0:10	0:06-0:15	Inhibit Replication	No Traffic Impact
Procedure 44	0:25-1:00	0:31-1:15	1:25-2:00	1:31-2:15	Upgrade DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 45	0:25-1:00	0:56-2:15	1:25-2:00	2:56-4:15	Upgrade NOs	Provisioning Disabled, No Traffic Impact
Procedure 46	0:05-0:10	1:01-2:25	0:05-0:10	3:01-4:25	Allow Replication between NOs and DR-NOs	Provisioning Disabled, No Traffic Impact
Procedure 47	0:01-0:05	1:02-2:30	0:01-0:05	3:02-4:30	Verify Post Upgrade Status	Provisioning to SOAM is not supported till site upgrades are also performed.

4.5.2 Perform Health Check on RMS servers (Pre-Upgrade of 3-Tier(1+1) NOAMs)

This procedure is used to determine the health and status of the network and servers. This must be executed on the active NOAM.

Procedure 42: Perform Health Check on RMS servers (Pre-Upgrade of 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 TEKELEC TECHNICAL SERVICES 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.x) , 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 42: Perform Health Check on RMS servers (Pre-Upgrade of 3-Tier(1+1) NOAM)

2 **NO GUI:** Verify NO Servers existing Application Version

For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade).

Example:

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases.

Upgrade Screen in DSR 4.x

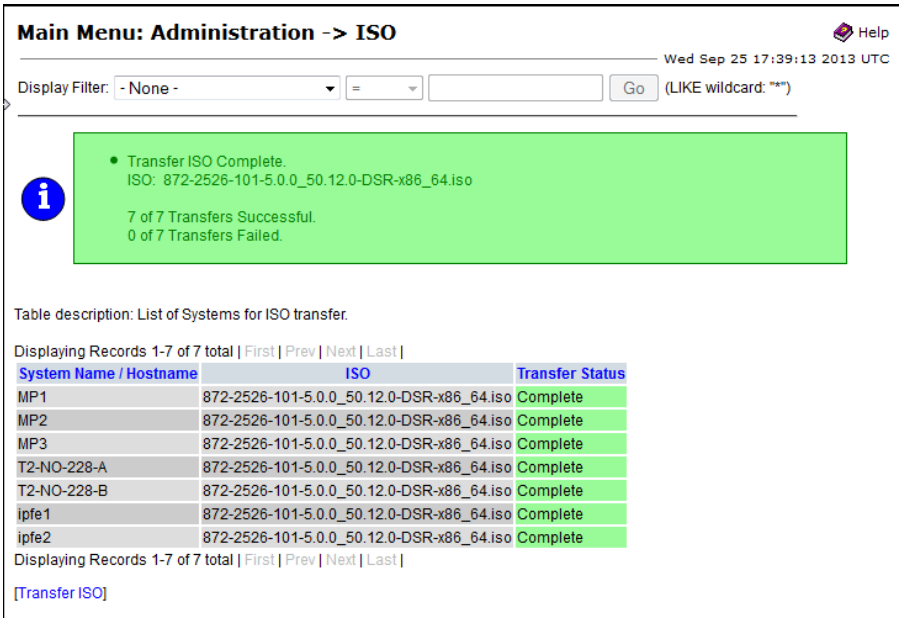
Main Menu: Administration -> Upgrade

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.x

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 42: Perform Health Check on RMS servers (Pre-Upgrade of 3-Tier(1+1) NOAM)

3 ☐	**NO GUI:** Verify ISO for Upgrade has been Deployed	Verify DSR ISO file has been Transferred to all servers: Example:  IF Not, see ISO Administration 3.3.8.
4 ☐	Verify Server Status is Normal	Verify Server Status is Normal: Log Into the NOAM GUI using the VIP. 1. Select **Status & Manage > Server;** the Server Status screen is displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is not recommended to continue executing 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.
5 ☐	Log all current alarms at NOAM	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
6 ☐	Repeat for active SOAMs	Log all current alarms in the SOAM: 1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

Procedure 42: Perform Health Check on RMS servers (Pre-Upgrade of 3-Tier(1+1) NOAM)

7 ☐	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. Select **Status and Manage → Files** Check time stamp on two 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 re-perform) a full Backup, if needed.

4.5.3 Inhibit Replication for 3-tier(1+1) setup on RMS servers

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

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 43. Inhibit Replication for 3-Tier(1+1) setup on RMS servers

S T E P #	This Procedure inhibits replication 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
	Start of next maintenance window	
1 ☐	Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. 1. Select **Status & Manage > Database;** the Database Status screen is displayed 2. Click **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] - Provisioning is manually disabled**. 5. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Inhibit replication to MP servers (1+1)	Inhibit database replication to MP servers in the following order: • Standby DA-MP • Active DA-MP From Active NO: 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Select the appropriate **DA-MP server**. 3. Click **Inhibit Replication** button. 4. Verify the ***Inhibited*** text is displayed for server. 5. **Repeat** the **above steps for** all remaining servers in the order: standby, then active). Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. **ALL DA-MPs must be inhibited.**

Procedure 43. Inhibit Replication for 3-Tier(1+1) setup on RMS servers

3 ☐	Inhibit replication to SO servers at a site	Inhibit database replication to SO servers in the following order:
		• Site:
		  ○ Standby SO
		  ○ Active SO
		
		From Active NO:
		1. Select **Status & Manage > Database**
		The Database Status screen is displayed.
		2. Select the appropriate **SO server.**
		3. Click **Inhibit Replication** button.
		4. Verify the ***Inhibited*** text is displayed for server.
		5. **Repeat** the **above steps for** all remaining servers in the order: standby, then active).
		
		ALL SOAM must be inhibited.

4 ☐	Verify that MPs and SO Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all MPs and all SOs, at all sites. The following alarms are expected: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other MP(s) and SO(s) servers should have: Alarm ID = **31113** (Replication Manually Disabled)
5 ☐	Inhibit replication to NO servers.	Inhibit database replication to all servers in the following order: • Standby NO • Active NO • Standby DR NO(if applicable) • Active DR NO(if applicable) Select **Status & Manage > Database** The Database Status screen is displayed. 1. Select the appropriate NO or DR-NO server based on the list above. 2. Click Inhibit Replication button. 3. Verify the Inhibited text is displayed for server. 4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**

Procedure 43. Inhibit Replication for 3-Tier(1+1) setup on RMS servers

6 ☐	Verify that All Servers are Inhibited	Select **Status & Manage > Database** Verify that the Replication status is Inhibited for all servers, and all sites. The following alarms are expected: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other MP(s)/SO(s) and NO servers should have: Alarm ID = **31113** (Replication Manually Disabled)
7 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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 substeps 2 through 5 for all the sites present in the setup.

4.5.4 Upgrade DR-NOs of 3-Tier(1+1) RMS servers setup

Procedure 44. Upgrade DR-NO(s) 3 –Tier(1+1) RMS configuration

S T E P #	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (1+1) 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	*Begin Upgrade of DR-NOs*	*Next Steps will begin Upgrade of the DR-NO servers.* *SKIP this Procedure if the deployment does not include DR-NO servers.*
2 ☐	Upgrade Host TVOE for **Standby** DR-NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** DR NO
3 ☐	Upgrade **Standby** DR-NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR DR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
4 ☐	Upgrade Host TVOE for **Active** DR-NO (if needed)	*Skip this step if:* • *the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** DR NO to upgrade TVOE.

5 ☐	Verify cmha process is running on upgraded DR NO	Log into the just-upgraded **standby** DR NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 44. Upgrade DR-NO(s) 3 –Tier(1+1) RMS configuration

6 ☐	Upgrade **Active** DSR DR-NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR DR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
7 ☐	Proceed to next procedure	Proceed to upgrade the NO servers, using the next procedure

4.5.5 Upgrade NOs for 3-Tier(1+1) RMS configuration

Procedure 45. Upgrade NO for 3 –Tier(1+1) RMS configuration

S T E P #	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (1+1) 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Upgrade Host TVOE for **Standby** NO (if needed)	*Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **standby** NO
2 ☐	Upgrade **Standby** NO server (using Upgrade Single Server procedure)	Upgrade the **standby** DSR NO: **Execute Appendix G.** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
3 ☐	Upgrade Host TVOE for **Active** NO (if needed)	*Skip this step if:* • *the deployment does not have a NO site* • *the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)* **Execute Appendix J** for the **active** NO to upgrade TVOE.

4 ☐	Verify cmha process is running on upgraded NO.	Log into the just-upgraded **standby** NO upgraded above, execute the following command:
		`ssh <NO XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58`
		`1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

Procedure 45. Upgrade NO for 3 –Tier(1+1) RMS configuration

5 ☐	Upgrade **Active** DSR NO server (using Upgrade Single Server procedure).	Upgrade the **active** DSR NO: **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. **IF Upgrade fails – do not proceed. Consult with support on the best course of action.**
6 ☐	Verify NO GUI access via VIP Address	Close and re-open Browser using the VIP address for the NOAM. Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected. The NOAM GUI will show the new DSR 5.0 release. Expected Alarms include: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other MP(s)/SO(s) and NO servers should have: Alarm ID = **31113** (Replication Manually Disabled)
	Proceed to next procedure	Proceed to next procedure, to allow replication between NOs.

4.5.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier(1+1) RMS configuration

Procedure 46. Allow Replication between NO and DR NO Servers on RMS servers(3-tier(1+1))

S T E P #	This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, (1+1) 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**

Procedure 46. Allow Replication between NO and DR NO Servers on RMS servers(3-tier(1+1))

1 ☐	Allow replication to NO and DR-NO servers only.	Allow database replication to **NO and DR-NO servers ONLY:** **Note: The NO servers intentionally have a sequence of "Allow Active, Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.** Select **Status & Manage > Database.** The Database Status screen is displayed. 1. Select the **Active NO server.** 2. Click Allow Replication button. 3. Verify the Inhibited text is not displayed for the server. After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 4. Repeat the Allow action link for **Standby NO server.** **Repeat sub-steps 1 through 4 for DR NO(s) (if applicable).** **Note: You must not allow Replication to any SOAMs or MPs. This can result in database corruption at these servers.**
2 ☐	Verify NO and DR-NO Replication	It is expected that NO and SO Provisioning is still disabled, and this will remain disabled till sites are upgraded. Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other MP(s) and SO(s) servers but not NO(s) should have: Alarm ID = **31113** (Replication Manually Disabled) **IF Upgrade verification steps indicate a problem, consult with support on the best course of action. Procedures for backout of the upgrade are included in this document.**

4.5.7 Verify Post Upgrade Status (3-tier(1+1) RMS NO Upgrade)

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

Procedure 47: Verify Post Upgrade Status (3-tier(1+1) RMS NO Upgrade)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 47: Verify Post Upgrade Status (3-tier(1+1) RMS NO Upgrade)

1 ☐	**SSH:** Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:
		
		1. Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers :
		
		Use your SSH client to connect to the upgraded server (ex. 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 Tekelec.
		
		`# alarmMgr --alarmstatus`
		
		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 Tekelec in case above output is not generated.

2 ☐	**NO GUI:** Verify Alarm status	Log all current alarms in the system: 1. Log into the NOAM GUI via the VIP. 2. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is displayed. 3. Click **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) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
3 ☐	Verify Traffic status	View KPI reports to verify traffic is at the expected condition.
4 ☐	*Note on Provisioning status ….*	Provisioning on the NO and SOs, and Replication from NO to the Site level SO and MPs, will typically remain disabled till further upgrades are performed on the sites.
End of maintenance window		

4.5.8 Site Upgrade for (1+1) 3-Tier RMS Configuration.

This section contains the steps required to upgrade a 3-tier DSR site that has a SOAM function, and 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 between after one of the site is completely upgraded.

Table 15. Upgrade Execution Overview (For DSR (1+1) 3 tier RMS configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 48	0:26-1:05	0:26-1:05	0:26-1:05	0:26-1:05	Upgrade SO(s) of (1+1) 3-Tier configuration	None
Procedure 49	0:20-1:10	0:46-2:15	0:20-1:10	0:46-2:15	Upgrade Active/Standby MP(s) in 3-Tier Configuration	None
Procedure 50	0:01-0:05 Per MP	0:47-3:35	0:01-0:05 Per MP	0:47-3:35 worst-case cumulative time (16 DA-MPs is considered)	Perform Health Check (Post Upgrade of MPs)	None

4.5.9 Upgrade SO of RMS configuration(3-tier (1+1))

Detailed steps are shown in the procedure below.

Procedure 48. Upgrade SO(s) of (1+1) 3-Tier configuration.

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of next maintenance window(If required)	
1 ☐	Verify site provisioning is disabled.	Verify site provisioning is disabled. Else execute following steps : 1. Log into the GUI of the SOAM which needs to be upgraded, using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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.
2 ☐	Upgrade standby SO	Upgrade 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 step 3 below. **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 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 next procedure. **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).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.**

4.5.10 Upgrade DA-MP(s) of 3-Tier (1+1) configuration on RMS servers

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

Procedure 49: Upgrade MP(s) of (1+1) 3-Tier configuration on RMS servers

STEP #	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 Tekelec 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 of the standby DA-MP by going to Status & Manage -> HA. Note: Active DA-MP server can be identified by looking out for the VIP. 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 Standby MP server[7] using Upgrade Single Server procedure: **Execute Appendix G** – Single Server Upgrade for Standby DA-MP After successfully completing the procedure in Appendix G, return to this point and continue with Step 3 below.
3 ☐	Upgrade the Active DA-MP server.	Upgrade active MP server using the Upgrade Single Server procedure. **Execute Appendix G** – Single Server Upgrade for Active DA-MP After successfully completing the procedure in Appendix G, return to this point and continue with Step 4 below. Note: The DA-MP server replication is enabled in Appendix G, executed above.
4 ☐	Allow replication to SO servers.	Allow database replication to SO servers: 1. Log into the active NO GUI using the VIP. 2. Select **Status & Manage > Database** 3. The Database Status screen is displayed. 4. Select the Active SO server. 5. Click Allow Replication button. After the Allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. 6. Verify the Inhibited text is not displayed for the server. 7. Repeat the Allow action link for Standby SO server. **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.**

[7] The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

Procedure 49: Upgrade MP(s) of (1+1) 3-Tier configuration on RMS servers

5 ☐	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 to only upgraded SO(s). 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen isis displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM.
6 ☐	Enable site provisioning.	**Enable Site provisioning :** 1. Log into the SOAM VIP GUI of the site just upgraded above. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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**
7 ☐	Update Max Allowed HA Role for NO and SO.	1. While logged in to the active NOAM GUI, go to Status & Manage-> HA screen. 2. Click 'Edit' button. 3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 4. Click 'Ok' button.

4.5.11 Verify Post Upgrade status of RMS servers(3-Tier(1+1))

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

Procedure 50: Verify Post Upgrade status of RMS servers(3-Tier(1+1))

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen isis displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 4. Execute following commands on the upgraded servers : Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. 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 Tekelec in case of errors.

Procedure 50: Verify Post Upgrade status of RMS servers(3-Tier(1+1))

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Log in to the active NOAM GUI using VIP and select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed.
		Following Alarm ID will be observed on all 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 server, then execute following commands on that particular server to check the existence of alarm :
		
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. 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 Tekelec in case above output is not raised.
		
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each MP server.
		
		3. Click **Report** button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.

3 ☐	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
End of second maintenance window.		

Note: If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 48 in another maintenance window.

4.6 Policy DRA Upgrade for 3-tier Configuration

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

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

As with other DSR 5.0 Major upgrades, the TVOE Host environments may optionally be planned and executed before executing these procedures, in separate Maintenance window(s).

Table 16. Upgrade Execution Overview for PDRA (Site 1)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 52	1:10-1:20	1:10-1:20	2:10-2:20	2:10-2:20	TVOE upgrade and NO Servers Upgrade	TVOE upgrade will stop all the applications running on it.
Procedure 53	1:00-1:10	2:10-1:30	2:00-2:10	4:10-4:30	TVOE upgrade and SO server upgrade– Site 1	TVOE upgrade will stop all the applications running on it.
Procedure 54	1:00-1:20	3:10-3:50	1:00-1:20	5:10-5:50	Policy SBR Upgrade – Site 1	
Procedure 55	1:00-2:00	4:10-5:50	1:00-2:00	6:10-7:20	Policy DRA Upgrade – Site 1	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 56	0:30-1:00	4:40-6:50	0:30-1:00	6:40-8:20	IPFE Server Upgrade – Site 1	None
Procedure 57	0:01-0:05	4:41-6:55	0:01-0:05	6:41-8:25	Post Upgrade Steps	None
Procedure 58	0:10-0:15	4:51-7:10	0:10-0:15	6:51-8:35	Perform Health Check (Upgrade Preparation)	None

Table 17 Upgrade Execution Overview for PDRA (Site 2)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 59	1:10-1:20	1:10-1:20	2:10-2:20	2:10-2:20	TVOE upgrade and NO Servers Upgrade	TVOE upgrade will stop all the applications running on it.
Procedure 60	1:00-1:10	2:10-1:30	2:00-2:10	4:10-4:30	TVOE upgrade and SO server upgrade– Site 2	TVOE upgrade will stop all the applications running on it.
Procedure 61	1:00-1:20	3:10-3:50	1:00-1:20	5:10-5:50	Policy SBR Upgrade – Site 2	
Procedure 62	1:00-2:00	4:10-5:50	1:00-2:00	6:10-7:20	Policy DRA Upgrade – Site 2	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 63	0:30-1:00	4:40-6:50	0:30-1:00	6:40-8:20	IPFE Server Upgrade – Site 2	None
Procedure 64	0:01-0:05	4:41-6:55	0:01-0:05	6:41-8:25	Post Upgrade Steps	None
Procedure 65	0:10-0:15	4:51-7:10	0:10-0:15	6:51-8:35	Perform Health Check (Upgrade Preparation)	None

4.6.1 Perform Health Check (Pre-Upgrade of NOAM)

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

Procedure 51: Perform Health Check (Pre-Upgrade of 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: **1.** Log into the NOAM GUI using the VIP. **2.** Select **Status & Manage > Server;** the Server Status screen isis displayed. **3.** Verify all 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 executing 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 the above steps for SO VIP GUI.
2 ☐	Log all current alarms	Log all current alarms in the system: **1.** Select **Alarms & Events > View Active**; the Alarms & Events > View Active view isis displayed. **2.** Click **Report** button to generate an Alarms report. **3.** Save the report and/or print the report. Keep these copies for future reference. Repeat the steps for SO VIP GUI.

4.6.2 Upgrade NOs

Procedure 52. TVOE Upgrade and NO Servers Upgrade

S T E P #	This procedure upgrades the TVOE of NOAM servers and upgrades NOAM servers of the setup. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of maintenance window 1	
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 **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. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)
2 ☐	Inhibit replication to PDRA and pSBR MP servers.	**Replication of C level MP servers will be inhibited during site upgrade.**
3 ☐	Inhibit replication to NO and SO servers	**Inhibit database replication to all the NO/SO servers in the following order:** • All the Spare SO(s) (For each site) • All the Standby SO(s) (For each site) • All the Active SO(s) (For each site) • Standby DR NOAM(if applicable) • Active DR NOAM(if applicable) • Standby NO • Active NO a) Select **Status & Manage > Database** The Database Status screen is displayed. b) Select the appropriate server based on the list above. c) Click **Inhibit Replication** button. d) Verify the ***Inhibited*** text is displayed for server. e) Repeat the **Inhibit** sub-step actions, steps a through e, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
4 ☐	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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 substeps 2 through 5 for all the sites present in the setup.

Procedure 52. TVOE Upgrade and NO Servers Upgrade

5 ☐	Upgrade standby DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby DR NO and Standby DSR NO if Standby DR NO and Standby DSR NO are hosted on TVOE blade before proceeding with below mentioned steps. Upgrade standby DSR NO server and standby DSR 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 Step 6 below.
6 ☐	Upgrade 2nd NO server. (NOTE: If logged out of Active NOAMP VIP, Log back into Active NOAMP VIP again.)	Note: - Execute Appendix J for 2nd DR NO(mate) and 2nd DSR NO(mate) if DR NO and DSR NO are hosted on TVOE blade before proceeding with below mentioned steps. Upgrade the 2nd NO server (the mate) and 2nd 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 sub-step 2 below. 2. Clear the browser cache after upgrade is completed.
7 ☐	Allow replication to NO and DR NO(if exists) servers.	Allow database replication to all upgraded NO servers in the following order: • Active NO • Standby NO • Active DR NOAM (if applicable) • Standby DR NOAM(if applicable) 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Select the appropriate server based on the list above. 3. Click **Allow Replication** button. 4. Verify the ***Allowed*** text is displayed for server. 5. Repeat the **Allow** sub-step actions, steps 2 through 4, for all remaining NO servers in the order shown above. **Note: Replication to any SOAMs or MPs must not be allowed in this step.** **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
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 can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.** **Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs 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 check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices** 1. Login to Active NO console and execute the following command **/usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh**
End of maintenance window 1		

4.6.2.1 Maintenance Window 2 – Site 1

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

Note: - Make sure that session output should be logged for future debugging.

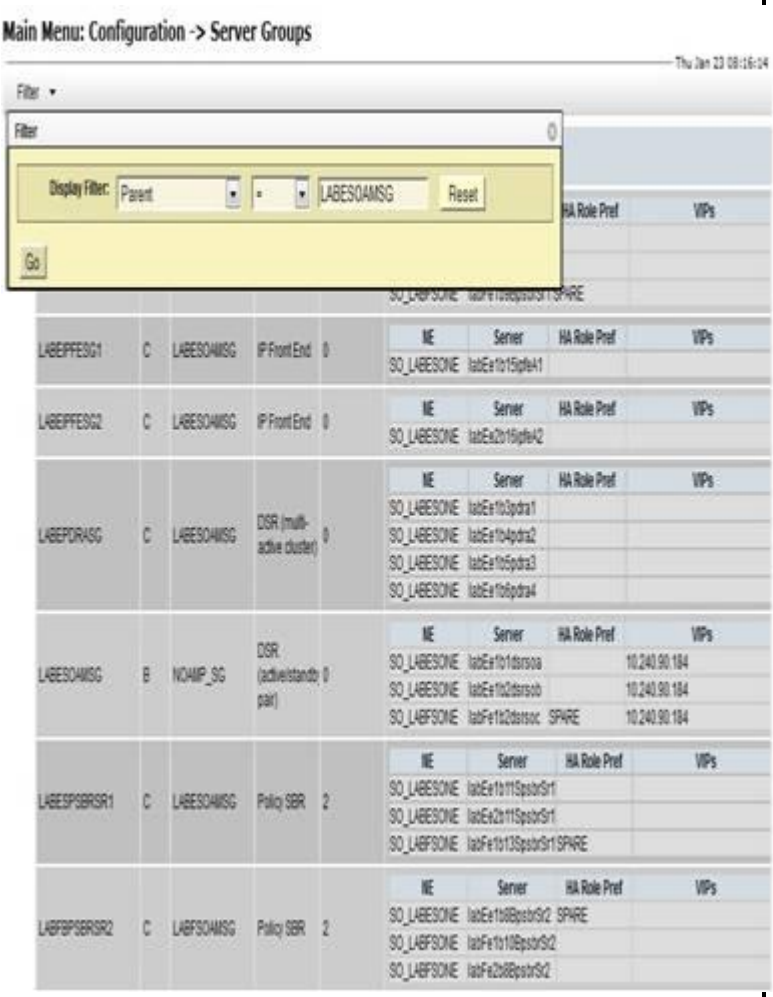
Procedure 53. TVOE Upgrade and SO Servers Upgrade

S T E P #	This procedure upgrade the TVOE 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
	Start of maintenance window 2	
1 ☐	Verify site provisioning is disabled	Verify site provisioning is disabled. Else execute following steps : 1. Log into the GUI of the SOAM which needs to b upgraded using the VIP. 2. Select **Status & Manage > Database** the Database Status screen isis displayed 3. Click **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

2 ☐	Inhibit replication to PDRA and pSBR MP servers.	**Record current release number___ex: 4.0.2_40.27.3_____**
		
		• **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G Step 13). In this case, SKIP THIS STEP.**
		
		[Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.]
		
		• **IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands** to inhibit replication A and B level replication on **all MP servers of this site**:
		
		Log into Active NO(if logged out, else ignore this step) :
		
		`# ssh root@<Active NO XMI IP>`
		`login as: root`
		`password: <enter password>`
		
		Execute following command on active NO for each of the C level server groups present in this Site(which needs to be upgraded) :
		
		`# srvrGrps="'<servergroup1>','<servergroup2>','<servergroup3>'……..<servergroupn>";for i in $(iqt -p -z -h -fclusterId ServerGroup where "ServerGroupName in ($srvrGrps)");do iset -finhibitRepPlans='AB' NodeInfo where "nodeId like '$i*'"; done`
		
		NOTE
		Server Group names of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen. Filter out the server groups on the basis of Parent. Here parent is the site which

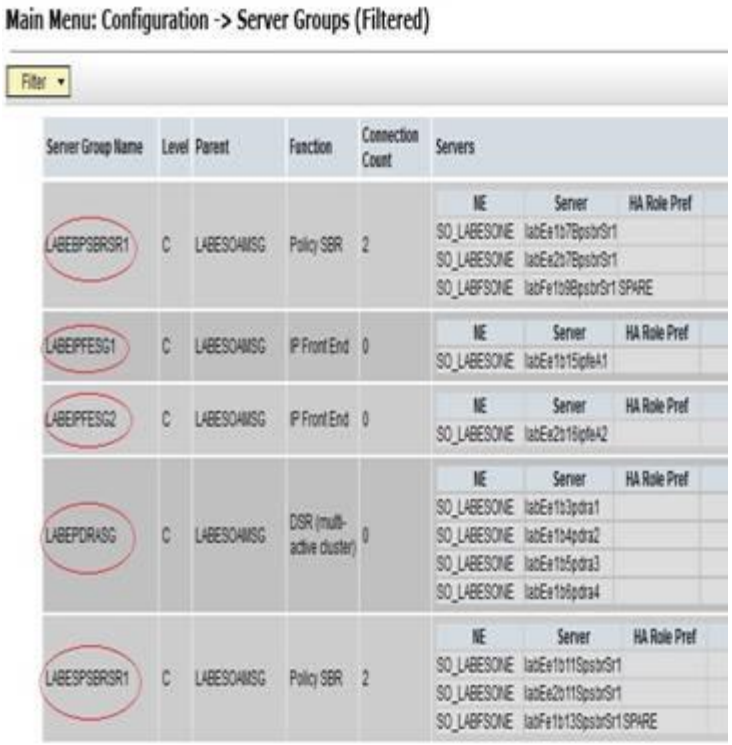
Procedure 53. TVOE Upgrade and SO Servers Upgrade

needs to be upgraded. Please see the snapshot below for more details.(here Site which needs to be upgraded is LABESOAMSG, hence parent is LABESOAMSG)



For e.g. Filtered output will look like :

Procedure 53. TVOE Upgrade and SO Servers Upgrade

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


Execute the above mentioned command for each of the filtered out Servergroups.

<u>An e.g:</u>

```
#srvrGrps="'LABEPDRASG','LABEBPSBRSR1','LABE
SPSBRSR1','LABEIPFESG1','LABEIPFESG2'";for i
in $(iqt -p -z -h -fclusterId ServerGroup
where "ServerGroupName in ($srvrGrps)");do
iset -finhibitRepPlans='A B'  NodeInfo where
"nodeId like '$i*'"; done
```
</td></tr>
<tr><td>3 ☐</td><td>Upgrade standby SO and **spare SO** in parallel</td><td>

Note: - Execute Appendix J for Standby DSR SO and Spare DSR SO if Standby DSR SO and Spare DSR SO are hosted on TVOE blade before proceeding with below mentioned steps.

1. Upgrade Standby DSR SO server and spare SO in parallel using Upgrade Single Server procedure :

Execute Appendix G -- Single Server Upgrade Procedure

Note: Spare server is located at the mated site of the site being upgraded

After successfully completing the procedure in Appendix G, return to this point and continue with next step.

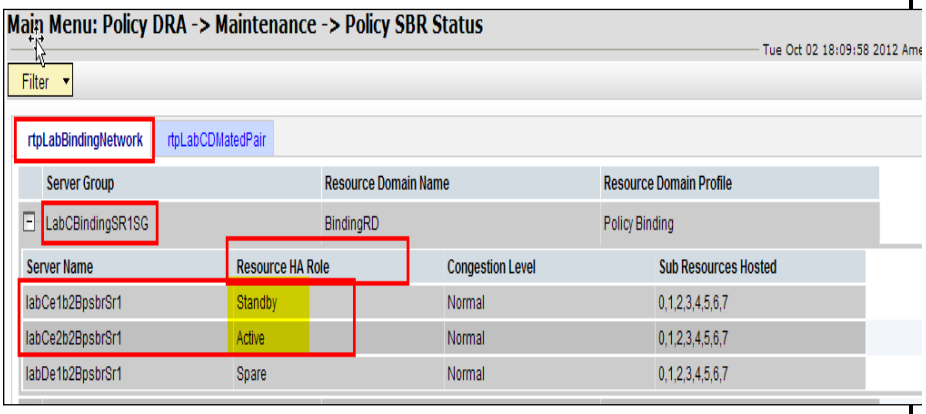
</td></tr>
</table>

Procedure 53. TVOE Upgrade and SO Servers Upgrade

4 ☐	Upgrade active DSR SO.	Note: - Execute Appendix J for Active DSR SO if Active DSR SO is hosted on TVOE blade before proceeding with below mentioned steps. 1. Upgrade active DSR 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 next step.
5 ☐	Allow replication to SO servers of the upgraded site ONLY (**upgraded site only)**.	Allow database replication to SO servers of the currently upgraded site only: 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** 3. The Database Status screen is displayed. 4. Select the Active SO server recently upgraded. 5. Click **Allow Replication** button**.** 6. Verify the ***Inhibited*** text is not displayed for the server**.**After the Allow action, server HA requires time to recover(up to 3 minutes) before 'Allowed' text is displayed. 7. Repeat the Allow action for Standby SO server recently upgraded. 8. Repeat the Allow action for Spare SO server recently upgraded (This is the spare which is located at the other mated site). **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby-Allow Spare". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.** 9. While server HA is recovering, monitor Server Status for recovery. 10. Select **Status & Manage >** HA The HA Status screen isis displayed. 11. Wait for "OAM Max HA Role" field to display **"Active","Standby" or "Spare"**. It may take up to 3 minutes for server HA to recover and for Server Status HA field to display the current operational status of "Active","Standby" or "Spare". **Note: SOAM server replication shall be allowed only for the currently upgraded site. For the leftover sites which are not yet upgraded, replication for each SOAMs of that sites shall remain inhibited else DB corruption can occur.**
		THIS PROCEDURE HAS BEEN COMPLETED

4.6.3 Policy SBR MP Server Upgrade

Procedure 54. Policy SBR Upgrade – Site 1

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify the pSBR Server Group(s) to Upgrade	From the data captured from 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 the servers in server group(s) selected for upgrade in sub-step 1. 3. Log into the NOAMP GUI using the VIP 4. Select the "Main Menu: Policy DRA->Maintenance->Policy SBR Status", and open each server group chosen in sub-step 1, Note which server is active, standby and spare(the Resource HA Role) for each server group chosen for upgrade. The following figure provides an example: **labCe2b2BpsbrSr1 - Active** **labCe1b2BpsbrSr1 – Standby** **labDe1b2BpsbrSr1 - Spare** 
2 ☐	Upgrade standby and spare Policy SBR Servers as identified in Step 1 in this procedure.	**Note: Spare P-SBR of this triplet will be present in the different site.** 1. Upgrade Standby Policy SBR server and spare Policy SBR 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 next step.

Procedure 54. Policy SBR Upgrade – Site 1

3 ☐	Upgrade Active Policy SBR Server as identified in Step 1 in this procedure	1. Upgrade Active Policy SBR 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 next step.
4 ☐	Repeat steps 1 through 4 for all the Binding and Session Server Groups with Active, Standby in Site 1 and Spare in Site 2	Repeat the steps 1-4 for all remaining binding and session server groups that need to be upgraded.

4.6.4 Upgrade Multiple DA-MPs in 3-tier DSR running PDRA-Site 1

Procedure 55. Upgrade Multiple DA-MPs of PDRA setup – Site 1

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify the "**DSR (multi-active cluster)**" to Upgrade in Site 1	From the data captured from Table 3, 1. Pick the "DSR (multi-active cluster)" Server Group in Site 1 2. Identify the servers in Server Group **identified in sub-step1** .
2 ☐	Upgrade Policy DRA Server as identified in Step 1	1. Upgrade half of the Policy DRA (DA-MP) servers in parallel l 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 next step.
3 ☐	Repeat steps 2 for all the server identified in Step 1 in this procedure.	Repeat the steps in step 2 in this procedure for rest of the Policy DRA (DA-MP) servers.

4.6.5 Upgrade IPFE

Procedure 56. IPFE Server Upgrade – Site 1

S T E P #	IPFE 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 Tekelec 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 Server Group identified in sub-step 1 above
2 ☐	Upgrade IPFE Server as identified in Step 1 in this procedure	Step 1: Upgrade IP Front End 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 next step.

3 ☐	Execute the following steps on the IPFE.	Execute following steps on each IPFE server just upgraded :
		1. Use ssh client to connect to the IPFE server :
		`ssh <IPFE XMI IP address>`
		`login as: root`
		`password: <enter password>`
		2. Execute following command on the IPFE server :
		`# grep "IPV6_AUTOCONF=no" /etc/sysconfig/network`
		`# grep "IPV6FORWARDING=yes" /etc/sysconfig/network`
		If the outcome of any of the above command is blank then execute the steps below else skip the steps below
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# init 6`
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

5 ☐	Repeat steps 1 through 4 for all the "**IP Front End**"	Repeat the steps in step 1-4 in this procedure.

4.6.6 Post Upgrade Execution – Site 1

Execute this procedure after the site has been upgraded.

Procedure 57. Site 1: Post Upgrade Steps

STEP #	**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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Enable 'A B' level replication inhibited for MP(s)(**only if source upgrade release was less than 4.1.0_41.16.0)** **NOTE: Do not use VIP address when doing ssh to the servers for this step**	**Note: The following steps will uninhibit replication to C level servers** Enable replication disabled previously only if **source upgrade release was less than 4.1.0_41.16.0** : 1. Log into Standby SO command prompt upgraded in Site 1 : Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <SO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable replication : **# iload /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml** **# pm.set off inetrep** **# pm.set on inetrep** **Execute above Steps 1 and 2 for upgraded Active SO of Site 1 as well.**
2 ☐	Enable global provisioning and configuration.	Enable global provisioning and configuration updates on the entire network: 1. Select Status & Manage > Database The Database Status screen isis displayed. 2. Click Enable Provisioning button. 3. Verify the button text changes to Disable Provisioning.
3 ☐	Enable global provisioning and configuration.	Enable Site provisioning after upgrade is completed: 1. Log into the SOAM VIP GUI for the upgraded site. 2. Select **Status & Manage > Database;** The Database Status screen isis displayed 3. Click **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. Verify the button text changes to **Disable Site Provisioning**
4 ☐	Execute FQDN – NE ID Mapping script	**NOTE: Execute this step if upgrading from a release < 4.0.5_41.6.0 to a later release.** 1. Ssh into Active NOAMP using the XMI VIP IP Address: 2. Execute this step **#/var/TKLC/appworks/library/Pdra/scripts/syncFqdnReferences.sh**

Procedure 57. Site 1: Post Upgrade Steps

5 ☐	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 later release. This procedure needs to be executed after each site has been upgraded.** 1. Download the script truncateLocalTable.sh. 2. Transfer the truncateLocalTable.sh file to **/root** of the Active SOAM Server. 3. Log into Active SO command prompt upgraded in Site 1 : Use your SSH client to connect to the upgraded server (ex. 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**

4.6.7 Site 1 – Verify Post Upgrade Status

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

Procedure 58: Verify Post Upgrade Status

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify all servers status are normal	1. Log in to GUI using NOAMP VIP 2. Select the **Status & Manage -> Server** menu item. 3. Verify all servers status are Normal (Norm). 4. Do not proceed without consent from Engineering/Customer Service to upgrade if any of the server's status displayed is not **Norm**. 5. Do not proceed without consent from Engineering/Customer Service if there are any unexpected Major or Critical alarms. Note: It is not recommended to continue executing 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 Active NOAMP VIP and **Active SOAM VIP on site 1.**	**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 Alarms CSV file generated and all the current alarms in the system. 4. Keep this information for future reference on client machine.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP for site 1.**	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 Avaialble" 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 Avaialble" 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.
4	Capture the Policy SBR Status	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

Procedure 58: Verify Post Upgrade Status

☐	**On Active NOAMP GUI**	by either taking screen captures or documenting it in some editor. a. Binding Region b. PDRAMatedSites Save this off to a client machine.
5 ☐	Capture the IPFE Configuration Options Screens. On Active SOAM GUI on Site 1	1. Select Main Menu: IPFE->Configuration->Options 2. Capture and archive the screen capture of the complete screen. 3. Save this off to a client machine
6 ☐	Capture the IPFE Configuration Target Set screens On Active SOAM GUI on Site 1	1. Select Main Menu: IPFE->Configuration->Target Sets 2. Capture and archive the screen capture of the complete screens. 3. Save this off to a client machine. 4.
7 ☐	Export and archive the Diameter and P-DRA configuration data. On Active SOAM GUI on Site 1	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 APDE status button at the top of the screen. 4. Browse to Main Menu->Status & Manage->Files and download all the exported files to client machine or use SCP utility to download the files from Active SOAM to the client machine.
8 ☐	Compare this data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Please verify if the health check status of the upgraded site 1 is same as pre-upgrade health check taken in Procedure 5. If it is any worse, report it toTekelec Customer service.
End of maintenance window 2		

4.6.8 SOAM Upgrade – Site 2

Following procedure deals with Site 2 SOAM servers and TVOE upgrade - but only if a Site 2 SOAM is hosted on a blade who's TVOE has not already been upgraded as part ofProcedure 53.

Procedure 59. SOAM Servers Upgrade

S T E P #	This procedure verifies that the SOAM server with TVOE platform upgrade steps have been completed and upgrade 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**
Start of maintenance window 3	
1 ☐	Verify site provisioning is disabled	Verify site provisioning is disabled. Else execute following steps: 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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
2	Inhibit replication to PDRA and pSBR MP servers.	**Record current release number___ex: 4.0.2_40.27.3_____**

Procedure 59. SOAM Servers Upgrade

- **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G Step 13). In this case, SKIP THIS STEP.**

  [Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.]

- **IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands** to inhibit replication A and B level replication on **all MP servers of this site**:

  Log into Active NO(if logged out, else ignore this step) :

```
# ssh root@<Active NO XMI IP>
login as:  root
password:  <enter password>
```

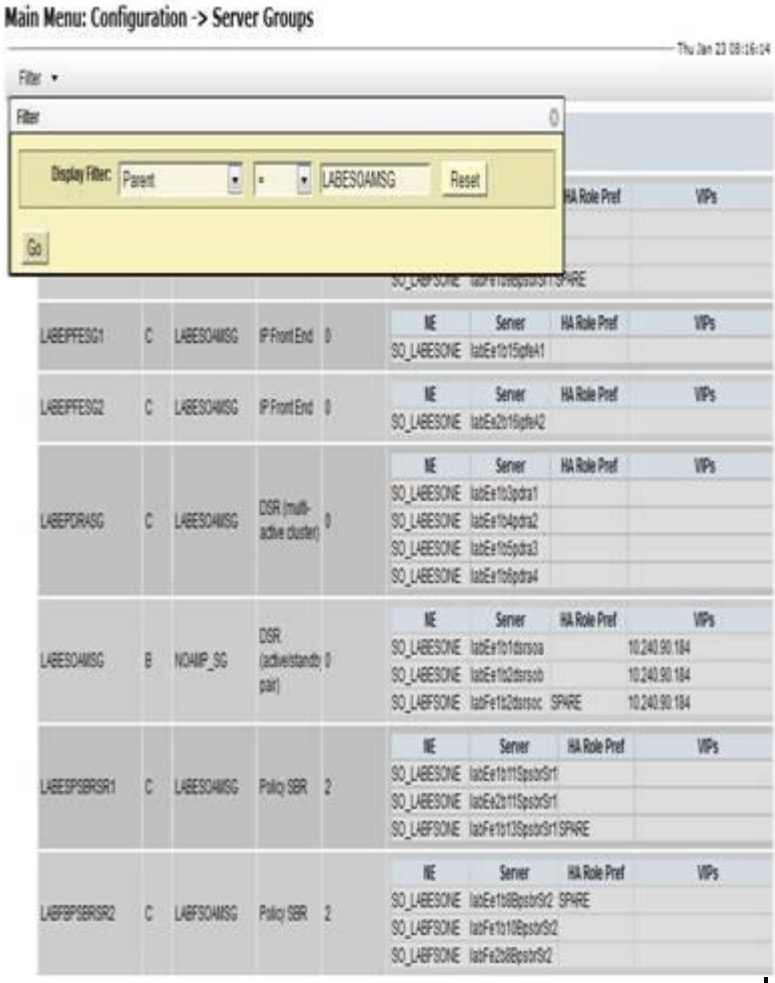
  Execute following command on active NO for each of the C level server groups present in this Site(which needs to be upgraded) :

```
# srvrGrps="
'<servergroup1>','<servergroup2>','<servergroup
3>'……..<servergroupn>";for i in $(iqt -p -z -h
-fclusterId ServerGroup where "ServerGroupName
in ($srvrGrps)");do iset -finhibitRepPlans='A
B'  NodeInfo where "nodeId like '$i*'"; done
```

  NOTE

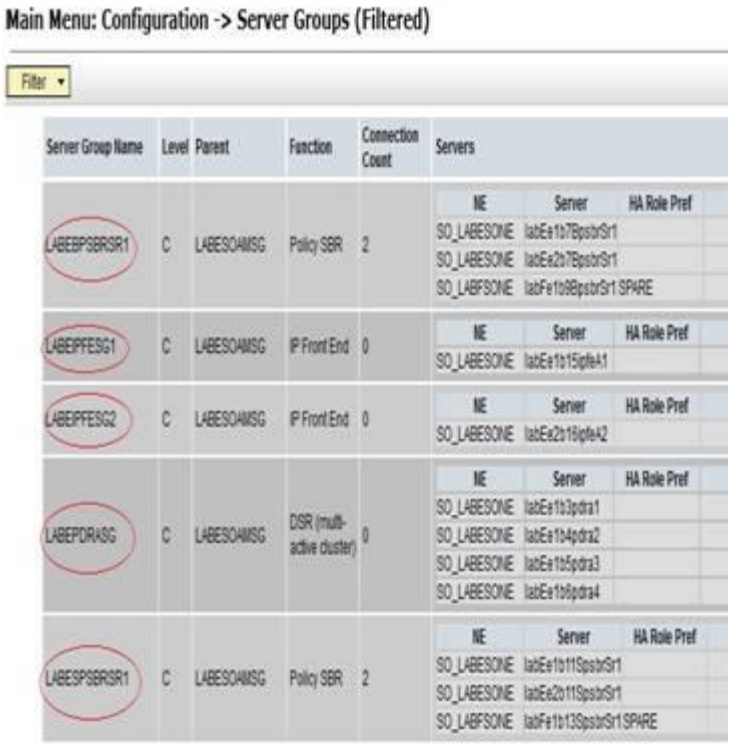
  Server Group names of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen. Filter out the server groups on the basis of Parent. Here parent is the site which needs to be upgraded. Please see the snapshot below for more details.(here Site which needs to be upgraded is LABESOAMSG, hence parent is LABESOAMSG)

Procedure 59. SOAM Servers Upgrade



For e.g. Filtered output will look like :

Procedure 59. SOAM Servers Upgrade

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


Execute the above mentioned command for each of the filtered out Servergroups.

<u>An e.g:</u>

```
#srvrGrps="'LABEPDRASG','LABEBPSBRSR1','LABE
SPSBRSR1','LABEIPFESG1','LABEIPFESG2'";for i
in $(iqt -p -z -h -fclusterId ServerGroup
where "ServerGroupName in ($srvrGrps)");do
iset -finhibitRepPlans='A B'  NodeInfo where
"nodeId like '$i*'"; done
```
</td></tr>
<tr><td>3</td><td>Upgrade TVOE platform on SOAM blades</td><td>1. Upgrade TVOE platform for blades hosting SO (See Appendix E6.Appendix D). If upgrade is required, follow Appendix J Upgrade TVOE platform. is displayed</td></tr>
<tr><td>4</td><td>Upgrade standby SO and spare SO in parallel.</td><td>Note: - Execute Appendix J for Standby DSR SO and Spare DSR SO if Standby DSR SO and Spare DSR SO are hosted on TVOE blade before proceeding with below mentioned steps.

Note: Spare SO of this triplet will be present in the different site.

1. Upgrade standby SO and spare 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 next step.</td></tr>
</table>

Procedure 59. SOAM Servers Upgrade

5 ☐	Upgrade active DSR SO.	Note: - Execute Appendix J for Active DSR SO if Active DSR SO is hosted on TVOE blade before proceeding with below mentioned steps. 1. Upgrade active DSR 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 next step.
6 ☐	Allow replication to SO servers of the upgraded site ONLY (**This site – e.g. Site2**).	Allow database replication to SO servers of the currently upgraded site only: 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** 3. The Database Status screen gets displayed. 4. Select the Active SO server recently upgraded. 5. Click **Allow Replication** button**.** 6. Verify the ***Inhibited*** text is not displayed for the server**.** 7. Repeat the Allow action for Standby SO server recently upgraded. 8. Repeat the Allow action for Spare SO server recently upgraded (This is the spare which is located at the other mated site). **Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby-Allow Spare". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.** After the Allow action, server HA requires time to recover (up to 3 minutes). 9. While server HA is recovering, monitor Server Status for recovery. 10. Select **Status & Manage >** HA The HA Status screen gets displayed. 11. Wait for "OAM Max HA Role" field to display **"Active","Standby" or "Spare"**. It may take up to 3 minutes for server HA to recover and for Server Status HA field to display the current operational status of "Active","Standby" or "Spare". **Note: SOAM server replication shall be allowed only for the currently upgraded site. For the leftover sites which are not yet upgraded, replication for each SOAMs of that sites shall remain inhibited else DB corruption can occur.**

4.6.9 Policy SBR MP Server Upgrade

Procedure 60. Policy SBR Upgrade – Site 2

STEP #	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 Tekelec 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 servers in Server Group in site 2 or multiple server groups in site 2. 3. Login into NOAMP VIP 4. Go to "Main Menu: Policy DRA->Maintenance->Policy SBR Status", NOTE down the Resource HA Role LabDBindingSR2SG BindingRD Server Name | Resource HA Role labCe1b7BpsbrSr2 | Spare labDe1b7BpsbrSr2 | Active labDe2b2BpsbrSr2 | Standby
2 ☐	Upgrade standby and spare Policy SBR Servers as identified in Step 1 in this procedure.	**Note: Spare P-SBR of this triplet will be present in the different site.** Step 1: Upgrade standby Policy SBR server and spare Policy SBR 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 next step.
3 ☐	Upgrade active Policy SBR Server as identified in Step 1 in this procedure	Step 1: Upgrade active Policy SBR 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 next step.
4 ☐	Repeat steps 1 through 4 for all the Binding and Session Server Groups with Active, Standby in Site 2) and Spare in Site 1.	Repeat the steps 1-4 for all remaining binding and session server groups that need to be upgraded.

4.6.10 Upgrade Multiple DA-MPs in 3-tier DSR running PDRA-Site 2

Procedure 61: Upgrade Multiple DA-MPs of PDRA setup – Site 2

STEP #	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 Tekelec 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-step1.
2 ☐	Upgrade Policy DRA Server as identified in Step 1	1. Upgrade Policy DRA (DA-MP) 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 next step.
3 ☐	Repeat steps 2 for all the servers identified in Step 1 in this procedure.	Repeat the steps in step 2 in this procedure for rest of the Policy DRA (DA-MP) servers.

4.6.11 IPFE Server Upgrade

Procedure 62. IPFE Server Upgrade – Site 2

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify the **IP Front End** Server Group to Upgrade in Site 1(LabC)	From the data captured in Table 3, 1. Pick one "**IP Front End**" Server Group in Site 2. 2. Identify the servers in Server Group identified in sub-step 1 above
2 ☐	Upgrade IPFE Server as identified in Step 1 in this procedure	Step 1: Upgrade IP Front End 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 next step.

3 ☐	Execute the following steps on the IPFE.	Execute following steps on each IPFE server just upgraded :
		
		1. Use ssh client to connect to the IPFE server :
		
		`ssh <IPFE XMI IP address>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute following command on the IPFE server :
		
		`# grep "IPV6_AUTOCONF=no" /etc/sysconfig/network`
		`# grep "IPV6FORWARDING=yes" /etc/sysconfig/network`
		
		If the outcome of any of the above command is blank then execute the steps below else skip the steps below
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# init 6`
		
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

5 ☐	Repeat steps 1 through 4 for all the "**IP Front End**"	Repeat the steps in step 1-4 in this procedure.

4.6.12 Post Upgrade Execution – Site 2

Procedure 63. Site 2: Post Upgrade Steps

STEP #	NOTE: Execute this step after site has been 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Enable 'A B' level replication inhibited for MP(s)(**only if source upgrade release was less than 4.1.0_41.16.0)** **NOTE: Do not use VIP address when doing ssh to the servers for this step**	**Note: The following steps will uninhibit replication to C level servers** Enable replication disabled previously only if **source upgrade release was less than 4.1.0_41.16.0** : 1. Log into Standby SO command prompt upgraded in Site 2 : Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <SO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable replication : **# iload /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml** **# pm.set off inetrep** **# pm.set on inetrep** **Execute above Steps 1 and 2 for upgraded Active SO of Site 2 as well.**
2 ☐	Enable global provisioning and configuration.	Enable global provisioning and configuration updates on the entire network: 1. Select Status & Manage > Database The Database Status screen isis displayed. 2. Click Enable Provisioning button. 3. Verify the button text changes to Disable Provisioning. Enable Site provisioning after upgrade is completed: 4. Log into the SOAM VIP GUI for the site upgrade above. 5. Select **Status & Manage > Database** the Database Status screen isis displayed 6. Click **Enable Site Provisioning** button. 7. Confirm the operation by clicking **Ok** in the popup dialog box. Verify the button text changes to **Disable Site Provisioning**

Procedure 63. Site 2: Post Upgrade Steps

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 NOAMP Server : a) Login (SSH) to the Active NOAMP Server b) Move into directory using 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 later release. This procedure needs to be executed after each site has been upgraded.** 1. Download the script truncateLocalTable.sh. 2. Transfer the truncateLocalTable.sh file to **/root** of the Active SOAM Server. 3. Log into Active SO command prompt upgraded in Site 1 : Use your SSH client to connect to the upgraded server (ex. 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**

4.6.13 Site 2– Verify Post Upgrade Status

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

Procedure 64: Verify Post Upgrade Status

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify all servers status are normal	1. Log in to GUI using NOAMP VIP 2. Select the **Status & Manage -> Server** menu item. 3. Verify all server status are Normal (Norm). 4. Do not proceed without consent from Engineering/Customer Service (refer Appendix K) to upgrade if any of the server's status displayed is not **Norm**. 5. Do not proceed without consent from Engineering/Customer Service (refer Appendix K) if there are any unexpected Major or Critical alarms. Note: It is not recommended to continue executing 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 Active NOAMP VIP and **Active SOAM 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 Alarms CSV file generated and all the current alarms in the system. 4. Keep this information for future reference on client machine.
3 ☐	Capture the Diameter Maintenance Status **On Active SOAM VIP of site 2).**	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 Avaialble**" 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.
4	Capture the Policy SBR Status	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

Procedure 64: Verify Post Upgrade Status

☐	**On Active NOAMP GUI**	by either taking screen captures or documenting it in some editor. a. BindingRegion b. PDRAMatedSites 3. Save this off to a client machine.
5 ☐	Capture the IPFE Configuration Options Screens. On Active SOAM GUI on Site 2.	1. Select Main Menu: IPFE->Configuration->Options 2. Capture and archive the screen capture of the complete screen. 3. Save this off to a client machine.
6 ☐	Capture the IPFE Configuration Target Set screens On Active SOAM GUI on Site 2	1. Select Main Menu: IPFE->Configuration->Target Sets 2. Capture and archive the screen capture of the complete screens. 3. Save this off to a client machine.
7 ☐	Export and archive the Diameter and P-DRA configuration data. On Active SOAM GUI on Site 2	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 APDE status button at the top of the screen. 4. Browse to Main Menu->Status & Manage->Files and download all the exported files to client machine or use SCP utility to download the files from Active SOAM to the client machine.
8 ☐	Compare this data to the Pre-Upgrade health check to verify if the system has degraded after the third Maintenance window.	Please verify if the health check status of the upgraded site is same as pre-upgrade health check taken in Procedure 5. If it is any worse, report it to Tekelec Customer service by referring to Appendix K of this document.
End of maintenance window 3		

4.7 Site Upgrade for (1+1) 2-Tier Configuration

This section contains major upgrade steps for DSR 4.x->5.x (2-tier setup) upgrade with (1+1) i.e. active-standby configuration and DSR 5.x incremental upgrade for (1+1) 2-tier configuration.

The Elapsed Time mentioned in table below specifies the time with TVOE upgrade and without TVOE upgrade. In some of the setups NO(s) are hosted on TVOE blades. TVOE applications also sometimes need to be upgraded. Hence TVOE upgrade estimates are included in separate column.

Table 18. Upgrade Execution Overview (For DSR (1+1) 2-tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 65Procedure 61	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check	None
Procedure 66Procedure 62	0:30-1:00	0:31-1:05	1:30-2:00	1:31-2:05	Upgrade NO(s) of (1+1) 2-Tier configuration	None
Procedure 63	0:01-0:05	0:32-1:10	0:01-0:05	1:32-2:10	Perform Health Check	None
Procedure 68Procedure 64	0:30-1:00	1:02-2:10	0:30-1:00	2:02-3:10	Upgrade MP(s) of (1+1) 2-Tier configuration	None
Procedure 69	0:01-0:05 Per MP	1:04-2:20	0:01-0:05	2:04-3:20	Perform Health Check (Post Upgrade of MPs)	None

4.7.1 Perform Health Check (Pre-Upgrade of 2-tier NOAM)

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

Procedure 65: Perform Health Check

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log Into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen is displayed. 3. Verify all 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 executing 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 view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.

4.7.2 Upgrade 2-Tier NOAM(s)

Detailed steps are shown in the procedure below.

Procedure 66: Upgrade NO(s) of (1+1) 2-Tier configuration

S T E P #	This procedure verifies that the NOAM upgrade steps have been completed. This procedure is specific to 2-tier DSR OAM deployment. 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
	Start of maintenance window	
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 **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] - Provisioning is manually disabled**. 6. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

2 ☐	Inhibit SOAP replication
	
	(This step will NOT be required for most upgrades)
		Record current DSR release number___ex: 4.0.2_40.27.3_____
		
		SKIP THIS STEP
		if current release is 4.0.0_40.19.0 or greater
		
		1. Log into the Active NO command prompt :
		
		Use your SSH client to connect to the Active NO server (ex. ssh, putty):
		`ssh <server address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to disable SOAP replication :
		
		`# iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"`
		
		Execute following command to verify if above command successfully updated NodeInfo records:
		
		`# iqt -E NodeInfo`
		
		Verify that **excludeTables** field shall include '**`HaNodeLocPref HaVipDef`**' table names **for each NodeId present on the setup** :
		
		e,g,
		
		`nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef`
		
		SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO or MP servers.

Procedure 66: Upgrade NO(s) of (1+1) 2-Tier configuration

3 ☐	Inhibit replication to all servers.	Inhibit database replication to all servers in the following order: • Standby DA-MP • Active DA-MP • Standby NO • Active NO 1. Select **Status & Manage > Database** The Database Status screen is displayed. 2. Select the appropriate server based on the list above. 3. Click **Inhibit Replication** button. 4. Verify the ***Inhibited*** text is displayed for server. 5. Repeat the **Inhibit** sub step actions, steps 2 through 4, for all remaining servers in the order shown above. **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.**
4 ☐	Upgrade TVOE Host (if needed)	If TVOE Host for the Standby NO needs to be upgraded. **Execute Appendix J** for the standby NO TVOE Host
4 ☐	Upgrade Standby NO server (using Upgrade Single Server procedure).	**Execute Appendix G** –Single Server Upgrade for standby NO After successfully completing the procedure in Appendix G, return to this point and continue with step 5 below.
5 ☐	Upgrade TVOE Host (if needed) .	If TVOE Host for the Active NO needs to be upgraded. **Execute Appendix J for the active NO TVOE Host**

6 ☐	Verify cmha process is running on upgraded NO server	Log into the just-upgraded standby NO, execute the following command to make the NO Active again.
		
		`# ssh root@<NO XMI IP>`
		`login as: root`
		`password: <enter password>`
		
		Execute following command on NO:
		
		`[root@NO1 ~]# pl | grep "cmha"`
		
		The following output should be generated:
		
		`A 10128 cmha Up 11/20 00:15:58 1 cmha`
		
		If no output is generated then execute following command:
		
		`service start_cmha start`

Procedure 66: Upgrade NO(s) of (1+1) 2-Tier configuration

7 ☐	Upgrade 2nd NO server.	**For Active NO,** **Execute Appendix G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with sub-step 1 below. 1. Clear the browser cache after upgrade is completed. Close and re-open Browser using the VIP address for the NOAM and clear the browser cache. Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected. The NOAM GUI will show the new DSR 5.0 release. Expected Alarms include: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other servers must have: Alarm ID = 31113 (Replication Manually Disabled)
8 ☐	Allow replication between NO servers.	Allow database replication between NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen is displayed. 3. Select the **Active NO** server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**. After** the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server 6. Repeat the **Allow** action link for Standby NO server. **Note: Replication to any of the MPs must not be allowed in this step.** **Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.** Expected Alarms include: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other MP servers(excluding NOs) must have: Alarm ID = 31113 (Replication Manually Disabled)
9 ☐	Install NetBackup on NO (If required)	If Netbackup is to be installed on your DSR, execute the procedure found in Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.**

4.7.3 Perform Health Check

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

Procedure 67: Perform Health Check (Post-Upgrade of 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status	Execute the following commands on both the active and standby NOAM servers: 1. Use your SSH client to connect to the upgraded server (ex. 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. Note: It is safe to ignore this error if it appears after upgrade from DSR 4.x to 5.x: 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 expected alarms: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) 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 server, then execute following commands on that server to check the existence of 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 78 is executed to accept the upgrade on each server

Procedure 67: Perform Health Check (Post-Upgrade of NOAM)

2 ☐	Log all current alarms	Log all current alarms in the system: 1. Log into NOAM GUI via the VIP. 2. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is is displayed. 3. Click **Report** button to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference.

4.7.4 2-Tier Upgrade DA-MP(s)

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

Procedure 68: Upgrade MP(s) of (1+1) 2-Tier configuration

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
1 ☐	Verify and Record the status of the MP before upgrade	Verify and record the status of each DA-MP Server by going to Status & Manage -> HA and record the hostname of active DA-MP server and standby DA-MP server. Note: Active DA-MP server can be identified by looking out for the VIP. 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 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 Step 3 below.
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 Step 4 below.
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 **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.**
5 ☐	Update Max Allowed HA Role for NO	1. While logged in to the active NOAM GUI, 2. Go to **Status & Manage-> HA** screen. 3. Click 'Edit' button. 4. Check the 'Max Allowed HA Role' for the NO. By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 5. Click 'Ok' button.

4.7.5 Verify Post Upgrade Status (1+1 2-Tier)

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

Procedure 69: Verify Post Upgrade Status (1+1 2-Tier)

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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	Verify Server Status is Normal	Verify Server Status is Normal:
		1. Log in to the active NOAM GUI using the VIP.
		2. Select **Status & Manage > Server;** the Server Status screen is displayed.
		3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc).
		3. Execute following commands on all of the upgraded DA-MP servers :
		Use your SSH client to connect to the upgraded DA-MP server (ex. ssh, putty):
		`ssh <DA-MP server XMI IP address>`
		`login as: root`
		`password: <enter password>`
		`# verifyUpgrade`
		Examine the output of the above command, and determine if any errors were reported. Contact Tekelec in case of errors.

2 ☐	Log all current alarms	Log all current alarms in the system:
		1. Log in to the Active NOAM GUI VIP.
		2. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed.
		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 server, then execute following commands on that server to check the existence of alarm :
		`# alarmMgr --alarmstatus`
		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`
		3. Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server
		4. Click **Report** button to generate an Alarms report.
		5. Save the report and print the report. Keep these copies for future reference.

3 ☐	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade

Procedure 69: Verify Post Upgrade Status (1+1 2-Tier)

End of maintenance window.

4.8 Site Upgrade for (N+0) 2-Tier configuration

This section contains major upgrade steps for DSR 4.x->5.x (2-tier setup) upgrade with (N+0) configuration and for DSR 5.x incremental upgrade for 2-tier (N+0) configuration.

The Elapsed Time mentioned in the table below specifies the time with TVOE upgrade and without TVOE upgrade. In some of the setups NO(s) are hosted on TVOE blades. TVOE applications also sometimes need to be upgraded. Hence TVOE upgrade estimates are included in separate column.

Table 19. Upgrade Execution Overview (For (N+0) 2-tier configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 70	0:01 - 0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check (Pre-Upgrade of NOAM)	None
Procedure 71	0:25 - 1:00	0:26-1:05	1:25-2:00	1:26-2:05	Upgrade 2-Tier NO(s)	The Active NO is the only server available in the pair while its mate is being upgraded. Provisioning and Configuration are disabled. Updates are not allowed.
Procedure 72	0:02 - 0:05	0:28-1:10	0:02-0:05	1:28-2:10	Perform Health Check (Post Upgrade of NOAM)	None
Procedure 73	0:20 - 1:00	0:48-2:10	0:20-1:00	1:48-3:15	Upgrade Multiple MP(s) in 2-Tier Configuration	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 74	0:20 - 1:00	1:08-3:10	0:20-1:00	2:08-4:15	Upgrade IPFE(s) in 2-Tier Configuration	None
Procedure 74	0:01 - 0:05 Per MP	1:09-4:30 (The worst-case cumulative time for 16 DA-MPs is considered	0:01-0:05 Per MP	2:09-5:35 (The worst-case cumulative time for 16 DA-MPs is considered)	Perform Health Check (Post Upgrade of MPs)	None

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
		)				

4.8.1 Perform Health Check (Pre-Upgrade of NOAM)

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

Procedure 70: Perform Health Check (Pre-Upgrade of NOAM)

STEP #	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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen isis displayed. 3. Verify all 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 executing 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 view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	Verify that a recent version of the Full DB backup has been performed	Verify that a fresh version of the Full DB backup has been performed. Status and Manage → Files Check time stamp on two 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 full Backup, if needed.

4.8.2 Upgrade 2-Tier NOAM

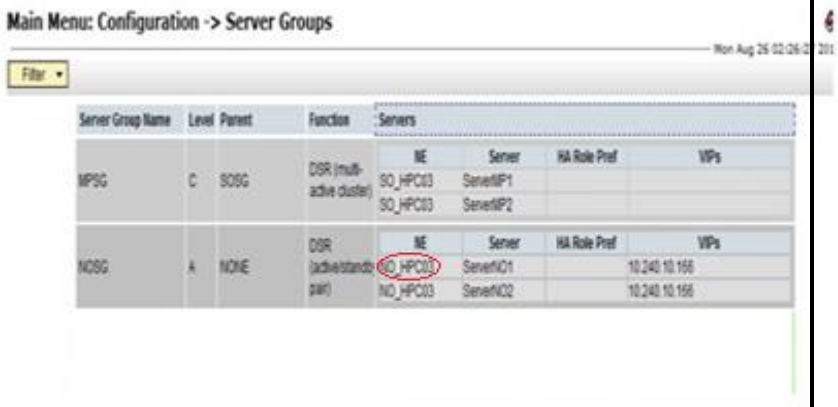
Detailed steps are shown in the procedure below.

Procedure 71. Upgrade NO(s) of (N+0) 2-Tier configuration

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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
	Start of maintenance window	
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 **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] - Provisioning is manually disabled**. 5. Active NO server will have the following expected alarm: - Alarm ID = **10008** (Provisioning Manually Disabled)

2 ☐	Inhibit SOAP replication (this is typically not required)	**Record current DSR release number___ex: 4.0.2_40.27.3_____**
		
		ONLY EXECUTE THIS STEP IF upgrading from a release less than DSR 4.0.0_40.19.0 (most upgrades will not use this step!)
		
		1. Log into the active NO command prompt :
		
		Use your SSH client to connect to theActive NO server (ex. ssh, putty):
		`ssh <Active NO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to disable SOAP replication :
		
		`# iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"`
		
		Execute following command to verify if above command successfully updated NodeInfo records:
		
		`# iqt -E NodeInfo`
		
		Verify that **excludeTables** field shall include '**`HaNodeLocPref HaVipDef`**' table names **for each NodeId present on the setup** :
		
		E,g,
		
		`nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef`
		
		SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO or SO(s)/DA-MP servers.

Procedure 71. Upgrade NO(s) of (N+0) 2-Tier configuration

3 ☐	Inhibit replication to MP servers (depending on upgrade release)	**Record current release number___ex: 4.0.2_40.27.3_____**
		
		• **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G). In this case, SKIP THIS STEP.**
		
		[Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.]
		
		• **IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands** to inhibit A and B level replication on **all MP servers of this site:** .
		
		Log into Active NO(if logged out, else ignore this step) :
		
		`# ssh root@<Active NO XMI IP>`
		`login as: root`
		`password: <enter password>`
		
		Execute following command on active NO :
		
		`# for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site which is being upgraded>'"); do iset -finhibitRepPlans='A' NodeInfo where "nodeName='$i'"; done`
		
		Note: NE name of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen.
		
		Please see the snapshot below for more details.
		
		 
		
		E.g. if Server NO1 belong to the site which is being upgraded then siteId will be NO_HPC03.
		Note: After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B' :

Procedure 71. Upgrade NO(s) of (N+0) 2-Tier configuration

		[root@NO1 ~]# iqt NodeInfo nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A1386.099 NO1 NO1 Active NO_HPC3 B1754.109 SO1 SO1 Active SO_HPC03 C2254.131 MP2 MP2 Active A B SO_HPC03 C2254.233 MP1 MP1 Active A B SO_HPC3
4 ☐	Inhibit replication to NO servers.	**Inhibit database replication to the NO servers in the following order:** **Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.** o Standby NO o Active NO **a)** Select **Status & Manage > Database** b) The Database Status screen isis displayed. **c)** Select the appropriate server based on the list above. **d)** Click **Inhibit Replication** button. **e)** Verify the ***Inhibited*** text is displayed for server. **f)** Repeat the **Inhibit** substep actions, steps a through f, for all remaining servers in the order shown above.
5 ☐	Upgrade standby NO server (using Upgrade Single Server procedure).	1. **If the TVOE Host needs to be upgraded, Execute Appendix J** Upgrade TVOE, for the standby NO, before proceeding with the following steps. See 6.Appendix D to check TVOE version, if needed. **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 step 6 below.
6 ☐	Upgrade 2nd NO TVOE server.	1. Execute Appendix J again for the active NO if 2nd NO is on different TVOE blade before proceeding with the following steps.

Procedure 71. Upgrade NO(s) of (N+0) 2-Tier configuration

7 ☐	Verify cmha process is running.	1. Log into the just-upgraded standby NO, execute the following command:
		`# ssh root@<NO IP>`
		`login as: root`
		`password: <enter password>`
		Execute following command on NO:
		`[root@NO1 ~]# pl | grep "cmha"`
		The following output should be generated:
		`A 10128 cmha Up 11/20 00:15:58 1 cmha`
		If no output is generated then execute following command:
		`service start_cmha start`

8 ☐	Upgrade 2nd NO server.	1. Upgrade the 2nd 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 sub-step 4 below. *Before login to the Upgrade GUI, clear your browser cache. (Note: some gui forms may appear incomplete, or may have incorrect* behaviors, if the browser cache is not cleared.)
9 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen isis displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server. 6. Repeat the **Allow** action link for Standby NO server. **Note: Replication to any of the MPs must not be allowed in this step.** **Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps.**
10 ☐	Install NetBackup 7.5 on NO (If required).	Please refer to Appendix I. **Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.**

4.8.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 72: Perform Health Check (Post-Upgrade of 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify Server Status	Verify Server Status after NO servers upgraded: 1. Execute following commands on both the active and standby NOAM servers: Use your SSH client to connect to the upgraded NO server (ex. 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. Contact Tekelec if any errors are observed. 2. Log in to Active NOAM VIP GUI and select Alarms & Events-> View Active screen to verify alarms. Servers have following expected alarms: Active NO server has: Alarm ID = **10008** (Provisioning Manually Disabled) All other servers might have: Alarm ID = **31113** (Replication Manually Disabled) 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 server, then execute following commands on that server to check the existence of 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 Tekelec in case above output is not raised. 3. Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server.

Procedure 72: Perform Health Check (Post-Upgrade of NOAM)

2 ☐	Log all current alarms	Log all current alarms in the system from the already logged in Active NOAM VIP : 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view isis displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	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 can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.** **Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs 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 check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices** 1. Login to 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).

4.8.4 Upgrade All Active DA-MPs

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: successfully upgrade the DA-MPs in one enclosure first. Then upgrade the DA-MPs in the second enclosure. This approach will ensure that service is not affected. This approach will ensure service is not affected.

Procedure 73 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 21 must be executed four distinct times.

Procedure 73. Upgrade Multiple DA-MPs in 2-Tier Configuration

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 Tekelec 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: User can choose any number of MP(s) on which upgrade can be executed 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 G** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix G for all selected DA-MPs, return to this point and continue with Step 3 below.
3 ☐	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 'Edit' button. 4. Check the 'Max Allowed HA Role' for all the NO(s) . By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 5. Click 'Ok' button.

4.8.5 Upgrade IPFE(s)

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 74. Upgrade IPFE(s) in 2-Tier Configuration

STEP #	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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.	
1 ☐	Identify IPFE upgrade order	User can choose any number of IPFEs on which upgrade can be executed in parallel depending upon traffic conditions. All the IPFE should belong to same enclosure and only after the first enclosure has been successfully upgraded should the IPFE(s) in the second enclosure be upgraded.
2 ☐	Upgrade IPFE servers (if exists)	Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure. **1. Execute Appendix G** -- Single Server Upgrade Procedure 2. Upgrade leftover IPFEs of the current site in parallel using Appendix G.

3 ☐	Execute ipfeNetUpdate on each upgraded IPFE server	Execute following steps on each IPFE server just upgraded :
		
		1. Use ssh client to connect to the IPFE server :
		
		`ssh <IPFE XMI IP address>`
		`login as: root`
		`password: <enter password>`
		
		2. Execute following command on the IPFE server :
		
		`# grep "IPV6_AUTOCONF=no" /etc/sysconfig/network`
		`# grep "IPV6FORWARDING=yes" /etc/sysconfig/network`
		
		`If the outcome of any of the above command is blank then execute the steps below else skip the steps below`
		
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		`# init 6`
		
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

4	Enable global provisioning and configuration.	Enable provisioning and configuration updates on the entire network: 1. Log into the Active Network OAM NE using the VIP. 2. Select Status & Manage > Database The Database Status screen is displayed. 3. Click Enable Provisioning button. 4. Verify the text of the button changes to Disable Provisioning.

4.8.6 Allow Replication for upgraded 2 tier (N+0) Setup

This procedure is used to allow 'A' level replication for MP servers (inhibited as part of Appendix G (step 12).

Procedure 75: Allow Replication for Upgraded Site

S T E P #	This procedure allow replication for 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**SSH**:
	Enable 'A' level replication inhibited for MP(s).
		Note: The following steps will uninhibit replication to C level servers
		
		Enable replication disabled previously only if **source upgrade release was earlier than 4.1.0_41.16.0** :
		
		1. Log into the standby NO using ssh client or puTTy :
		
		`ssh <standby NO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to enable replication :
		
		`# iload /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml`
		
		`# pm.set off inetrep`
		
		Note: This command will cause a failover, if performed on the Active server.
		
		`# pm.set on inetrep`
		
		Execute above sub-steps 1 and 2 for the active NO as well.

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

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

This includes all DA-MPs and IPFE servers.

Procedure 76: Verify Post Upgrade Status (N+0 2-Tier)

S T E P	This procedure verify 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**

Procedure 76: Verify Post Upgrade Status (N+0 2-Tier)

#		

1 ☐	**SSH MP Server:**
	Verify Server Status is Normal
		Verify Server Status is Normal:
		
		1. Log in to the active NOAM GUI using the VIP.
		2. Select **Status & Manage > Server;** the Server Status screen is displayed.
		3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc).
		3. Execute following commands on the upgraded MP servers(both IPFE and DA-MPs) :
		
		Use your SSH client to connect to the upgraded server (ex. 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 Tekelec 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:** Log all current alarms	Log all current alarms in the system: 1. Log in to the Active NOAM GUI VIP and select **Alarms & Events > View Active**; the Alarms & Events > View Active view is displayed. Following Alarm ID will be observed for all the upgraded servers(DA-MPs and IPFE) : Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** 2. Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server. 3. Click **Report** button to generate an Alarms report. 4. Save the report and print the report. Keep these copies for future reference.
3 ☐	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
End of maintenance window.		

4.9 Post-Upgrade Procedures

The procedures shown in the following table are executed inside a maintenance window. Note that the elapsed time is for a "Lab Environment", and that they might vary on Live Systems.

Table 20. Post-Upgrade Procedures Overview

Procedure	Elapsed Time (Hours: Minutes)		Procedure Title	Impact
	This Step	Cum.		
Procedure 77	0:05-0:10	0:05-0:10	Perform Health Check (Software Upgrade Completion)	Software is upgraded with target release software.

4.9.1 Perform Post-Upgrade

Procedure 77: Perform Post Upgrade Health Check

STEP #	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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	
1 ☐	Verify Server Status is Normal	Verify Server Status is Normal: **1.** Log in to the active NOAM GUI using the VIP. 2. Select **Status & Manage > Server;** the Server Status screen is displayed. 3. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), 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 view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.

Procedure 77: Perform Post Upgrade Health Check

3 ☐	Allow SOAP replication previously inhibited. **(If upgrading from DSR release < 40.19.0 and upgrade is already accepted)**	If the upgrade has already been accepted, and the DSR was running a source release older than 4.0.0_40.19.0 prior to the upgrade, execute the following steps, else ignore below mentioned steps :
		
		1. Log into the Active NO command prompt :
		
		Use your SSH client to connect to the upgraded server (ex. ssh, putty):
		`ssh <NOAM VIP>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute the following command to enable SOAP replication :
		
		`# iset -fexcludeTables='' NodeInfo where "1=1"`
		
		Note: This step needs to be executed only if upgraded from any DSR release before 4.0.0_40.19.0.

4 ☐	Check if the setup previously have customer supplied apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	1. Verify if the setup had customer supplied apache certificate installed and protected with passphrase before start of upgrade (refer Procedure 4 Step 11) 2. If the certificate was installed and renamed as part of Procedure 4 Step 11 then rename the certificate back to original.

4.9.2 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 previous release from which upgrade was done.

Procedure 78: Accept Upgrade (Post-Upgrade of full system)

STEP #	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 TEKELEC TECHNICAL SERVICES 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.]

Procedure 78: Accept Upgrade (Post-Upgrade of full system)

2 Accept upgrade for a single server

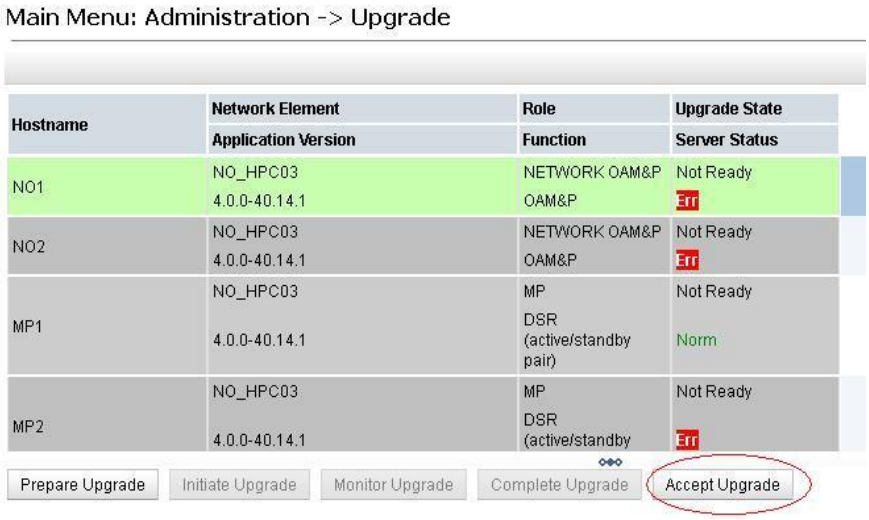
Accept upgrade of a single server

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases.

1. Select **Administration->Software Management->Upgrade. T**he Upgrade Administration screen displays.
2. Select the first server record in the table.

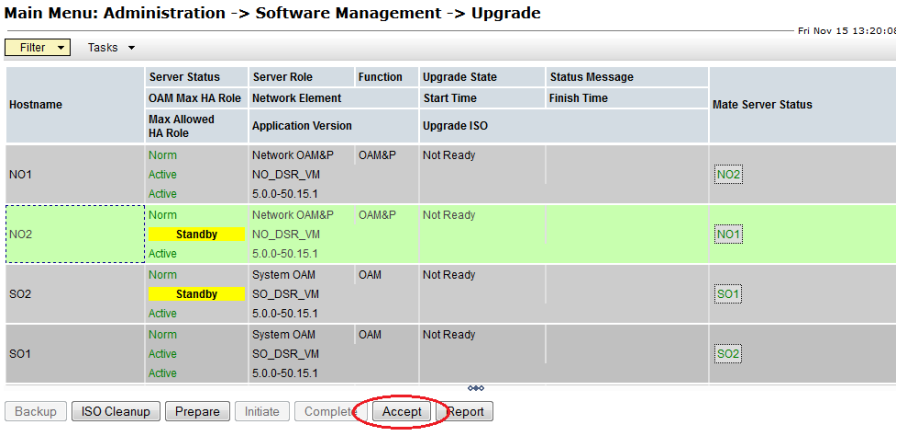
Upgrade screen in DSR 4.x

3. Click the "Accept Upgrade" button



Upgrade screen in DSR 5.x

3. Click the "Accept" button



4. A confirmation dialog will warn that once accepted the server will not be able to revert back to the previous image state.
5. Click "OK"
6. The Upgrade Administration screen re-displays.
7. Select **Alarms & Events > View** Active; the Alarms & Events > View Active view displays.
8. As upgraded is accepted on each server the corresponding Alarm ID **32532 (Server Upgrade Pending Accept/Reject)** should automatically clear.

Procedure 78: Accept Upgrade (Post-Upgrade of full system)

3 ☐	Accept upgrade of the rest of the system	Accept Upgrade all Servers in the system: 1. Repeat step 1 of this procedure until the upgrade of all Servers within the system have been accepted.

5. BACKOUT PROCEDURE OVERVIEW

The procedures shown in the following table 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. Note that the elapsed time are for a "Lab Environment", and they might vary on Live Systems.

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 79	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.
	0:01-0:05	Varies	Perform Health Check (Post-Backout)	None

5.1 Recovery Procedures

Upgrade procedure recovery issues should be directed to the Tekelec Customer Care Center by referring to Appendix K of this document. Before executing any of these procedures, contact the Tekelec 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 Tekelec 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 needed to be backout.

1. Select Administration->Software Management->Upgrade
2. Based on the "Application Version" column, identify all the hostnames that need to be back 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. Backout procedure **WILL** cause traffic loss. Since all possible reasons cannot be predicted ahead of time, contact the Tekelec 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 3.3.5are present on every server that is to be backout.** 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 Tekelec Customer Care Center by referring to Appendix K 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 79: Back Out Entire Network

S T E P #	This procedure is used to back out and 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: 1. Select Administration->Software Management->Upgrade The Upgrade Administration screen is displayed. 2. Identify the servers with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 3. Make note of these servers. They have been identified for Backout.
2 ☐	Disable global provisioning and configuration.	Disable provisioning and configuration updates on the entire network: 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 to disable Provisioning: 1. Log into the NOAM VIP GUI. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click **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] - Provisioning is manually disabled**. 6. Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled)

Procedure 79: Back Out Entire Network

3 ☐	Inhibit replication to all servers	Inhibit database replication to all servers(leaving PSBR servers): First, inhibit the non-active servers: 1. Select **Status & Manage > Database** The Database Status screen gets displayed. 2. Select a non-active server to inhibit. (Don't inhibit replication for PSBR servers) 3. Click **Inhibit Replication** button**.** 4. Verify the ***Inhibited text*** is displayed for server**.** Repeat the **Inhibit** action link for all non-active servers. Next, inhibit the active servers: 5. Select **Status & Manage > Database** The Database Status screen gets displayed. 6. Select an active server to inhibit. (Don't inhibit replication for PSBR servers). 7. Click **Inhibit Replication** button**.** 8. Verify the ***Inhibited text*** is displayed for server**.** Repeat the **Inhibit** action link for all active servers(leaving PSBR servers replication in allowed state).
4 ☐	Inhibit replication for PSBR servers.	Log into the Active NO and Execute following commands to inhibit replication A and B level replication on all PSBR servers of this site which needs to be backed out. **# iset -finhibitRepPlans='A B' NodeInfo where "nodeName='<PSBR server Nodename>'"** Note: Execute above command for each of the PSBR server which needs to be backed out.
5 ☐	Backout Standby DA-MP Servers, Standby cSBR(s) and Standby pSBR(s) ,as applicable	Back out **Standby MP** servers. 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 80, Backout Single Server, for each standby/spare C-level server identified above. Note: There will be no standby DA-MPs for (N+0) DA-MP configurations.
6 ☐	Back out DA-MPs, IPFEs, cSBRs, pSBRs, as applicable" or "Back out remaining C-level servers, as applicable	Back out **MP server** (the mate, if dealing with a server pair),Else backout all the leftover IPFE(s),SBR(s), pSBR(s) and DA MP(s) in parallel Execute Section 5.3.2 Back Out Single Server.
7 ☐	Back out Spare DA-MP Server(s).(as applicable)	Back out the spare **DA-MP server** , if one exists: Execute Section 5.3.2 Back Out Single Server..
8 ☐	Back out the standby SOAM server (as applicable).	Back out standby **DSR SO** server: Execute Section 5.3.2 Back Out Single Server..
9 ☐	Back out active SO Server (as applicable).	Back out active **SO** server: Execute Section 5.3.2 Back Out Single Server..

Procedure 79: Back Out Entire Network

10 ☐	Back out spare SO Server (as applicable).	Back out spare **SO** server: Execute Section 5.3.2 Back Out Single Server..
11 ☐	Back out standby DR NO server (as applicable).	Back out **primary standby DR NO** server: Execute Section 5.3.2 Back Out Single Server.
12 ☐	Back out 2nd DR NO server (as applicable).	Back out **2nd primary DR NO server** (the mate): Execute Section 5.3.2 Back Out Single Server.
13 ☐	Back out standby NO server.	Back out **primary standby NO** server: Execute Section 5.3.2 Back Out Single Server.
14 ☐	Back out 2nd NO server.	Back out 2nd primary NO server (the mate): Execute Section 5.3.2 Back Out Single Server.
15 ☐	Backout PM&C if upgraded previously	For PM&C backout follow reference [3].

Procedure 79: Back Out Entire Network

16 ☐	Back out TVOE if upgraded previously	**If the NO/SO server hosts the TVOE software, check if TVOE backout is required (If upgraded previously). If backout is not required then skip to next step.**
		
		Execute following steps for each TVOE blade upgraded previously :
		
		1. Disable all the applications running on TVOE blade:
		a) Log into the NOAM GUI using VIP.
		b) Select **Status & Manage > Server;** the Server Status screen is displayed
		c) Select all the applications running on 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 the selected servers is changed to 'Disabled'.
		
		2. Find out the guests running on 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 the guests running on TVOE host.
		
		3. Execute the following command for each guest from Step 2 :
		
		`# virsh shutdown <guestname>`
		
		Note: Shutting down of applications may lead to lost VIP. Wait till all the TVOE blades on which NO(s) are hosted are successfully backed out.
		
		4. Periodically execute 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 79: Back Out Entire Network

17 ☐	Enable virtual guest watchdogs if disabled previously	1. If virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [6] Otherwise execute following sub-steps:
		a) Log into TVOE host by using following command :
		`# ssh root@<TVOE IP>`
		`login as: root`
		`password: <enter password>`
		b) Execute following command to start the TVOE guests shutdown in step 13 sub-step 3 above (if not already started).
		`# virsh start <guestname>`
		c) Periodically execute following command until the command displays all the VM guests running.
		`# virsh list`
		
		2. Enable all the applications running on 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 the applications running on 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 the selected servers is changed to 'Enabled'.
		
		Note: This step shall be executed only if TVOE is backed out in Step 13.
		
		Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable).

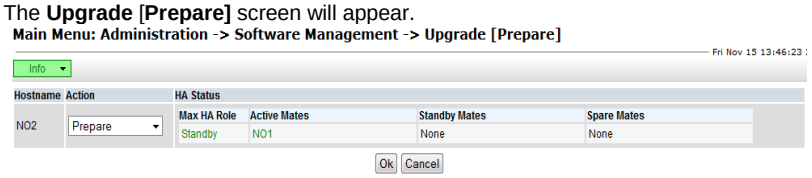
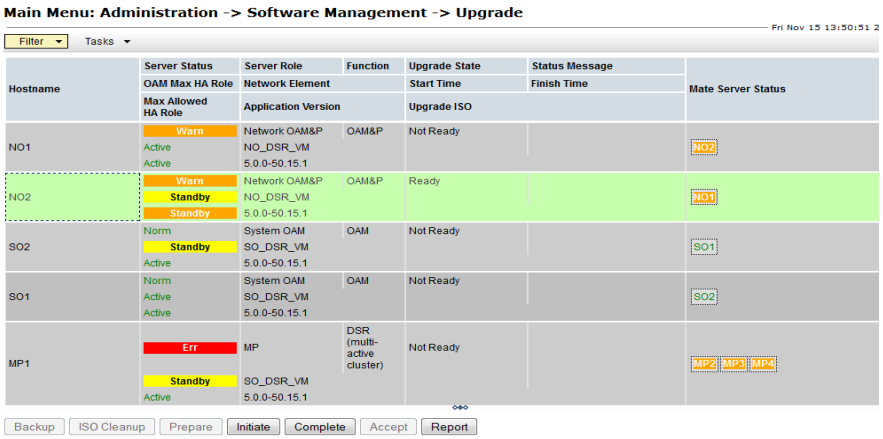
18 ☐	Allow replication to NO servers.	**Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps.** Allow database replication to NO servers: 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Select the active NO server. 3. Click **Allow Replication** button. 4. Verify the ***Inhibited*** text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. 5. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. .
19 ☐	Allow replication to SO servers.	Allow database replication to SO servers: The following steps are to be executed for all SO servers in all Signaling NEs. 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Select the Active SO server. **3.** Click **Allow Replication** button**.**. **4.** Verify the ***Inhibited*** text is not displayed for the server**.** After the allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed 5. Repeat the **Allow** action for Standby SO server. 6. Repeat 1) to 5) for all remaining SO servers in all Signaling NEs.

Procedure 79: Back Out Entire Network

20 ☐	Allow replication to C-level servers.	Allow database replication to all C-level servers: The following steps are to be executed for all C-level servers in all Signaling NEs. 1. Select **Status & Manage > Database** the Database Status screen is displayed. 2. Select the Active MP server. 3. Click **Allow Replication** button. 4. Verify the ***Inhibited text*** is not displayed for the server. After the allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. 5. Repeat the **Allow** action for Standby MP server (if dealing with a server pair). 6. While server HA is recovering, monitor Server Status for recovery. Select **Status & Manage > Servers** The Server Status screen is displayed. 7. Wait for the screen to refresh and show the Server Status fields for the server. 8. Wait for HA field to display **Norm**. It may take up to 3 minutes for server HA to recover and for Server Status HA field to change to **Norm**. 9. Repeat sub steps 1) to 9) for all remaining C-level servers in all Signaling NEs.
21 ☐	Allow replication for PSBR servers.	Log into the Active NO server and execute following command to allow replication for backed out PSBR servers :- **# iset -finhibitRepPlans='' NodeInfo where "nodeName='<PSBR server Nodename>'"** Note: Execute above command for each of the PSBR server which is currently backed out.
22 ☐	Enable Site Provisioning	**<u>Enable Site provisioning</u> :** 1. Log into the SOAM VIP GUI of the site. 2. Select **Status & Manage > Database** the Database Status screen is displayed 3. Click **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**
23 ☐	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 **Enable Provisioning** button. 3. Verify the button text changes to **Disable Provisioning.**
24 ☐	Remove 'Ready' state (if exists) for any backed out server	From Active NO GUI : 1. Select **Status & Manage > Servers**; the Server Status screen is displayed. 2. If the any of the backed-out server's 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 of the backed-out servers shows an Upgrade State of "Ready" or "Success", then select that backed-out 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.

5.3.2 Back Out Single Server

Procedure 80: Back out Single Server

S T E P #	This procedure will back out the upgrade of DSR 5.x 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. Select **Administration->Software Management->Upgrade.** The Upgrade Administration screen is displayed 2. Select the server to backout and check its upgrade state : a) If the upgrade state is "Ready" then press "**Complete**" button. b) Else, select the server to be downgraded and press the "**Prepare"** button. The **Upgrade** [**Prepare]** screen will appear.  3. 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.** 4. Click **OK.** This starts the Make Ready action on the server. You will be returned to the Upgrade Administration screen. 5. Wait for the screen to refresh and show both the Upgrade Ready State as **Ready** and the **Upgrade** action link to be enabled for the server that was to be upgraded. It may take up to a minute for the Upgrade Ready State to change to **Ready**.  ***Note: If this is the Active server in an Active-Standby pair, the Make Ready action WILL cause an HA switchover. The HA switchover is an expected outcome from the Make Ready action.*** ***Note: The preparation steps required to upgrade a server are also required when preparing to back out a server.***

Procedure 80: Back out Single Server

2 ☐	SSH to server	Use your SSH client to connect to the server (ex. ssh, putty): Note: You must consult your own software client's documentation to learn how to launch a connection. For example: `ssh <server address>` Note: If you do not have direct access to the IMI or if TVOE is installed on blade, then you must access the target server via a connection through the active NO. SSH to the active NO XMI first. Once you are logged into the NO; from there, SSH to the target server's IMI address.

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

4 ☐	Execute the backout	Find out the state of the server which is going to be backed out. Server shall be in Standby/Spare. Execute following command to find the state :-
		
		`# ha.mystate`
		
		If the state of the server is Active then move to step 1 mentioned above.
		
		Execute the backout using the ugwrap script:
		
		`# screen`
		`# /var/TKLC/backout/reject`
		
		NOTE: If backout asks if you would like to continue backout, answer "**y**".

5 ☐	Backout proceeds	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot.
6 ☐	SSH to server	Use your SSH client to connect to the server (ex. ssh, putty): Note: You must consult your own software client's documentation to learn how to launch a connection. For example: `ssh <server address>` Note: If you do not have direct access to the IMI or if TVOE is installed on blade, then you must access the target server via a connection through the active NO. SSH to the active NO XMI first. Once you are logged into the NO; 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 80: 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 you would like 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 work with Tekelec Customer Care Center by referring to Appendix K of this document for further instructions.

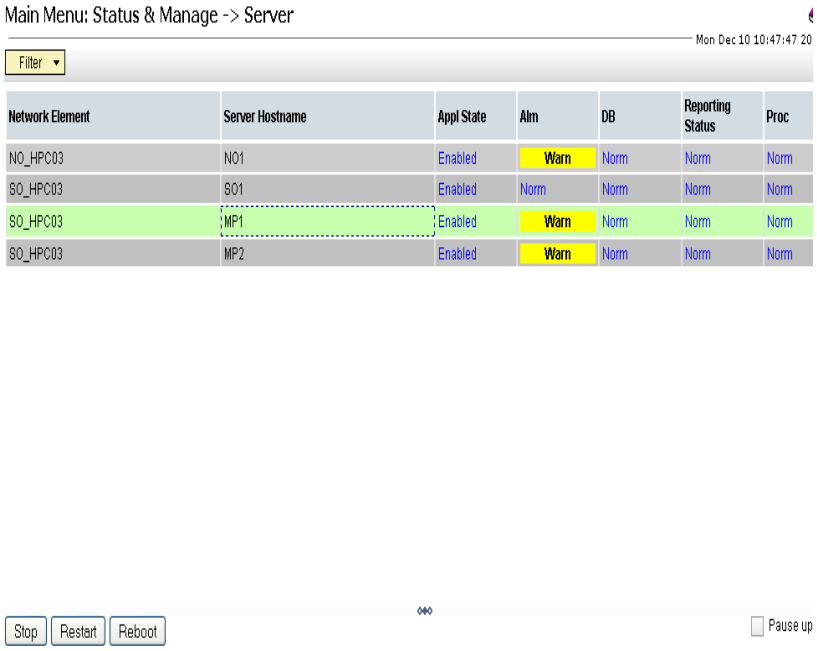
9 ☐	Verify the backout	1. Examine the output of the following commands to determine if any errors were reported:
		`# verifyUpgrade`
		
		This command will show the current rev on the server:
		
		`# appRev`
		
		2. If the backout was not successful because other errors were recorded in the logs, then contact Tekelec Customer Care Center by referring to Appendix K 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.

11 ☐	Verify services restart	Verify services have restarted:
		
		1. You must wait several (approx. 6 minutes) minutes for a reboot to complete before being able to log back into the server.
		2. SSH and log back into the server as root. The method is the same as Steps 2 and 3 of Section 5.3.1(this procedure).
		3. If this is an NO or SO, verify httpd service is running. Execute the command:
		
		`# service httpd status`
		
		4. Verify 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 Tekelec Customer Care Center by referring to Appendix K of this document for further instructions.

Procedure 80: Back out Single Server

12 ☐	Workaround for major backout (DSR 5.x -> DSR 4.x)	If the backed out server is Standby NO
		1. Log into Active NO :
		`login as: root`
		`password: <enter password>`
		
		2. Execute following commands on command line :
		`# ivi NodeInfo`
		
		Change the NodeCapability of Active NO to 'Stby'.
		Change the NodeCapability of Standby NO to 'Active'.
		Save the table.
		
		Note: This will cause switchover, so if logged in VIP then it will be logged out. Login back to VIP and proceed forward.

13 ☐	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 Application Status Enabled, then select the server row and press the Stop button.  3. Select **Administration > Upgrade (on DSR 4.x GUI) or Administration >Software Management >Upgrade(on DSR 5.x GUI);** the Upgrade Administration screen is displayed. 4. 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.x GUI)** button. Otherwise, skip to sub-step 6 below. **Note**: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases

Procedure 80: Back out Single Server

Upgrade Screen in DSR 4.x

Main Menu: Administration -> Upgrade

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)	Success Warn
	NO_HPC03	MP	Not Ready

Prepare Upgrade | Initiate Upgrade | Monitor Upgrade | Complete Upgrade | Accept Upgrade

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

Main Menu: Administration -> Upgrade [Remove Ready]

Mon Oct 08 12:34:

- Selecting 'Ok' will result in the selected server's application being enabled and the Max HA Capability of 'Active' set. 'Observer' is set for query servers.

Selected Server: MP1

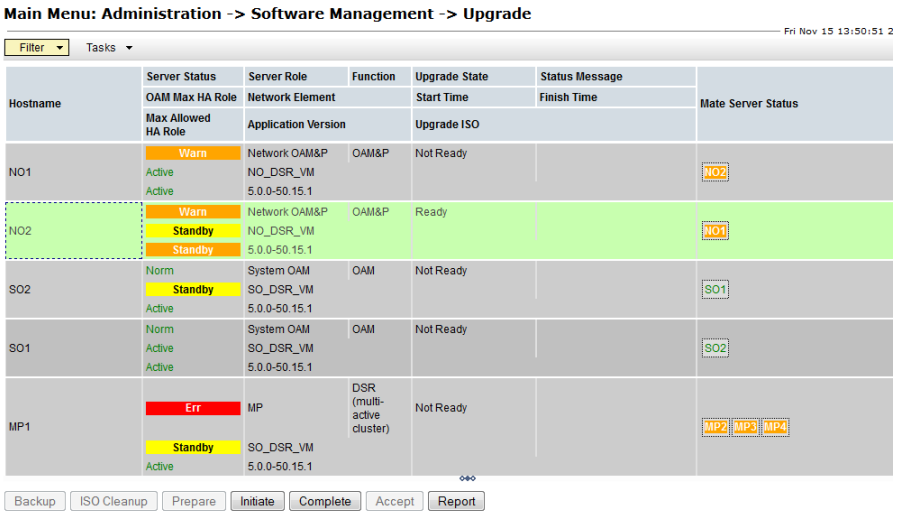
Ok | Cancel

Upgrade Ready Criteria	Selected Server Status	Mate Status
Max HA Role	Standby	Active
Critical Alarms	0	0
Major Alarms	0	1
Minor Alarms	2	4
Database Server Status	Norm	Warn
HA Server Status	Norm	Norm
Process Server Status	Man	Err
Application State	Disabled	Enabled

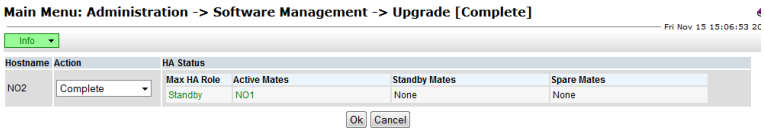
Ok | Cancel

Procedure 80: Back out Single Server

Upgrade Screen in DSR 5.x



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



5. Click **OK.** This will now remove the Forced Standby designation for the backed-out server.

   Note: Due to backout being initiated from the command line instead of through the GUI, 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.

6. Verify the **Application Version** value for this server has been downgraded to the original release version.

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 81: 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 TEKELEC TECHNICAL SERVICES 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 isis displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Do not proceed to upgrade if any of the server statuses displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms. Note: It is recommended to troubleshoot 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 view is displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.

3 ☐	Execute optimization script only if backout is done to DSR release less than 4.1.0-41.19.0	**Note: Don't execute following steps for PSBR/PDRA servers.**
		Use your SSH client to connect to the upgraded server (ex. ssh, putty):
		`ssh <server address>`
		`login as: root`
		`password: <enter password>`
		Execute following commands :-
		`# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force`
		`# sleep 20`
		`# prod.start`
		`# pm.sanity`
		Note: Execute optimization script for all the servers backed out to DSR release less than 4.1.0-41.19.0 in the setup.

6. APPENDIXES

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 Tekelec, 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 Tekelec 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.

Tekelec Signature: _____ Date: _____

Customer Signature: _____ Date: _____

APPENDIX D. SECTION DELETED

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, and 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 (RMSes), 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 82: 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 TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE**.	

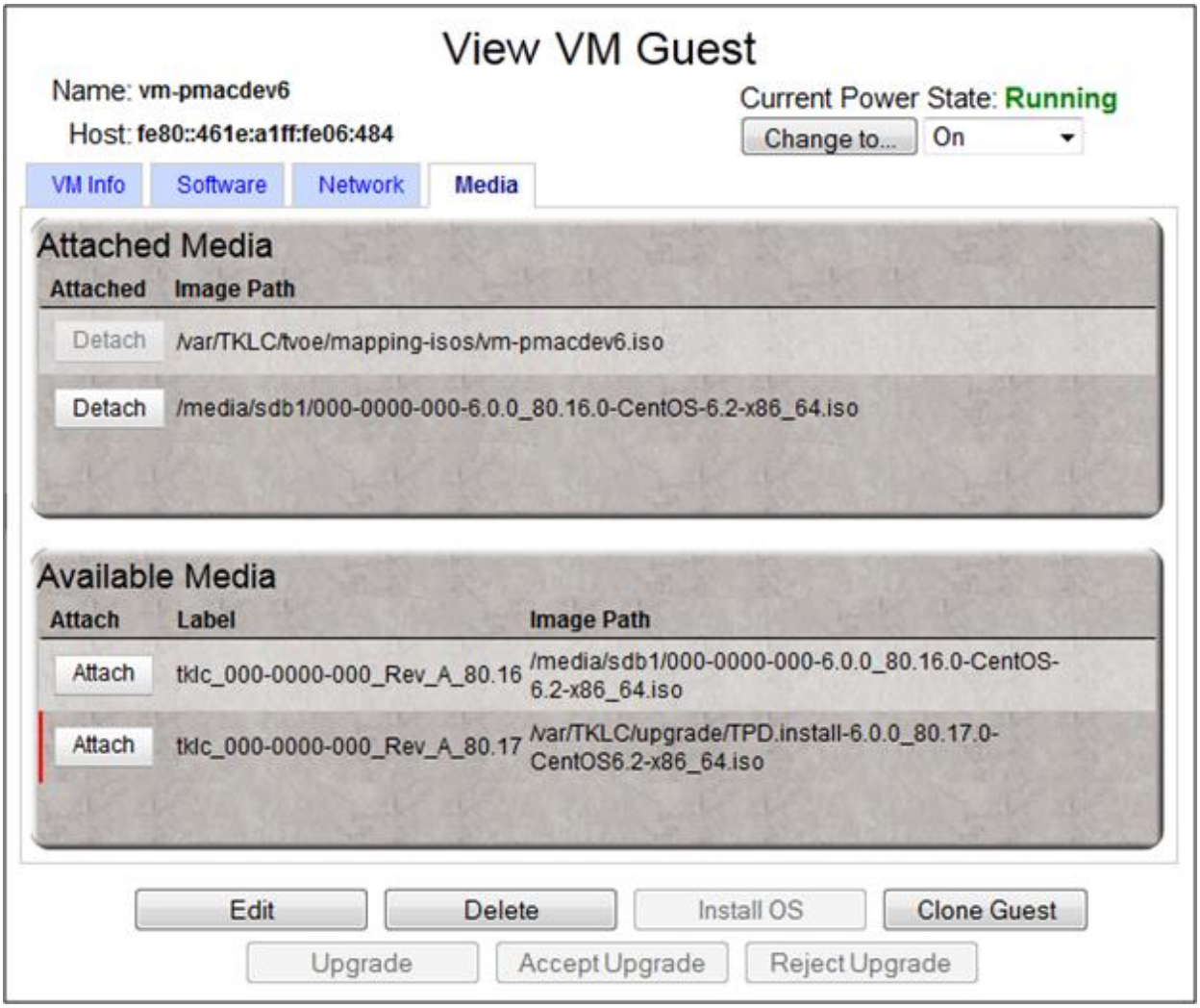
1 ☐	Determine the version of TVOE already running on the bare-metal server that hosts the virtual guest you are currently upgrading.	1. Log into the host server on which TVOE is installed.
		2. Execute the following command to get the current TVOE installed version :
		`[root@dsrTVOEblade2 ~]# appRev`
		`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	Please contact Tekelec customer by referring to Appendix K of this document to get support for the same.
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 given in Appendix J.

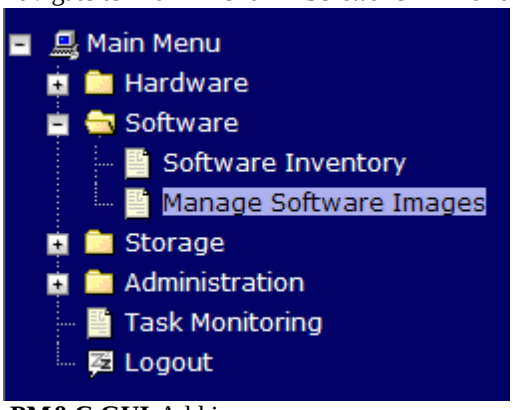
APPENDIX F. ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY

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.

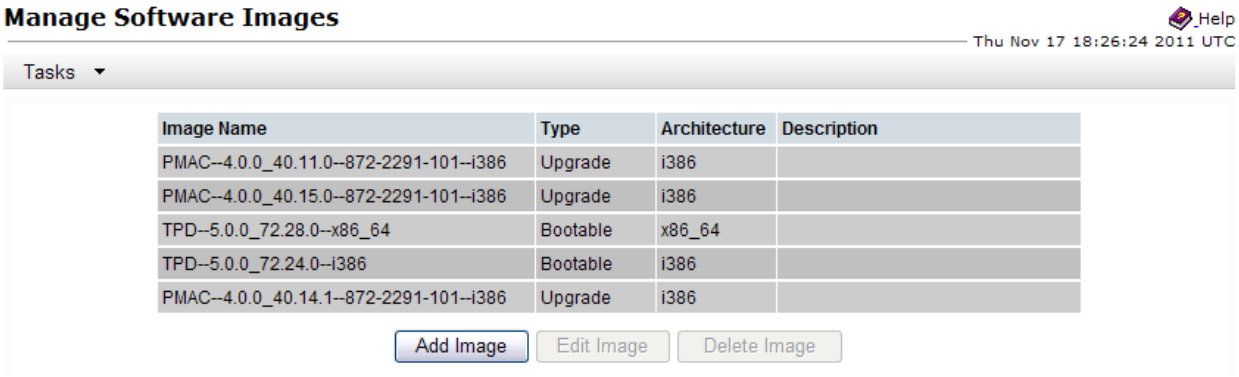
1. In the PM&C GUI, navigate to **Main Menu ➢ VM Management.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.
2. Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button.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

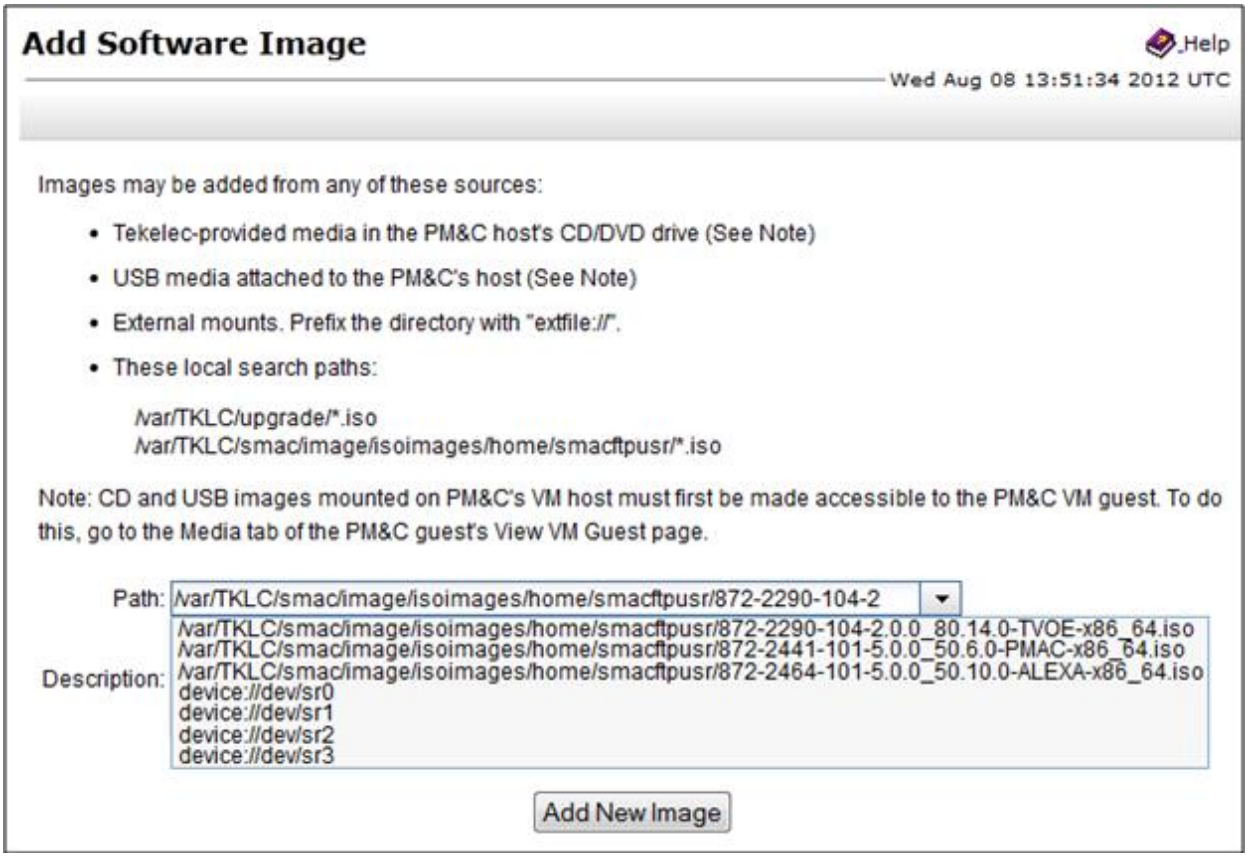


4. **PM&C GUI:**Add image
   Press the **Add Image** button .



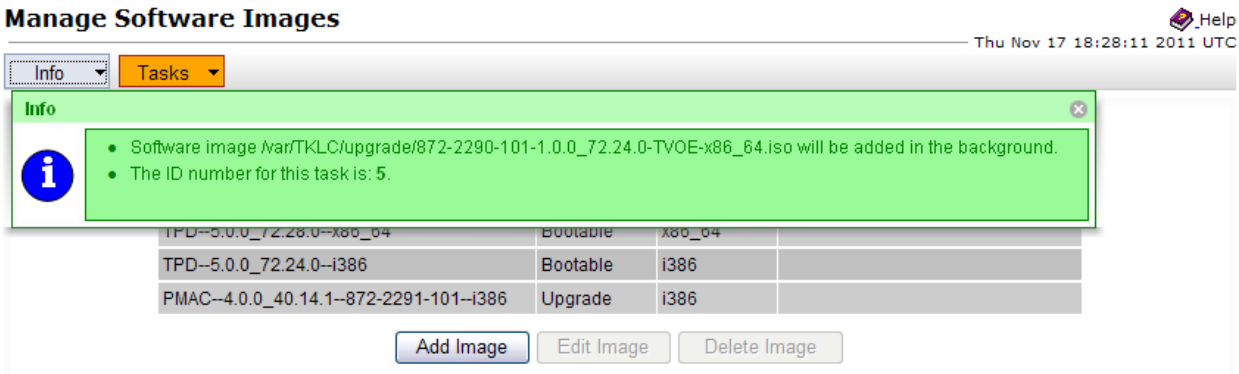
5. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:
   - If the image was transferred to PM&C via sftp it will appear in the list as a local file"/var/TKLC/...".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…").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

   Enter an appropriate image description and press the **Add New Image** button.



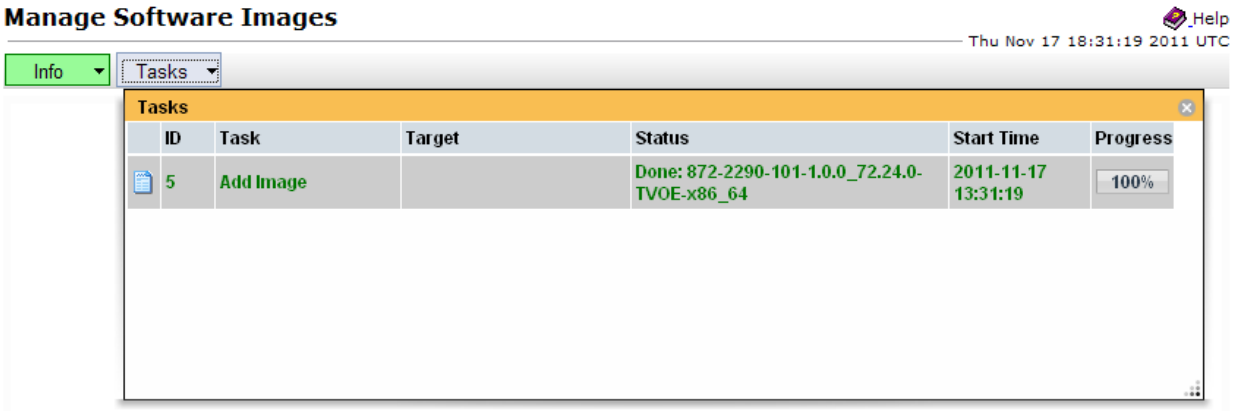
6. **PM&C GUI** Monitor the Add Image status

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 your DSR. Make multiple copies of Appendix G to mark up, or keep another form of written record of the steps performed.

Procedure 83: 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 Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.

Procedure 83: Upgrade Single Server – Upgrade Administration

1

NO GUI – Upgrade Administration:
View the pre-upgrade status of Servers

From the Active NO GUI:

Select **Upgrade Administration** form
(DSR 4.x: "**Administration > Upgrade**"
DSR 5.x: " **Administration -> Software Management -> Upgrade**")

The Upgrade Administration screen is displayed (example below):

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the 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

Upgrade Screen in DSR 5.x

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

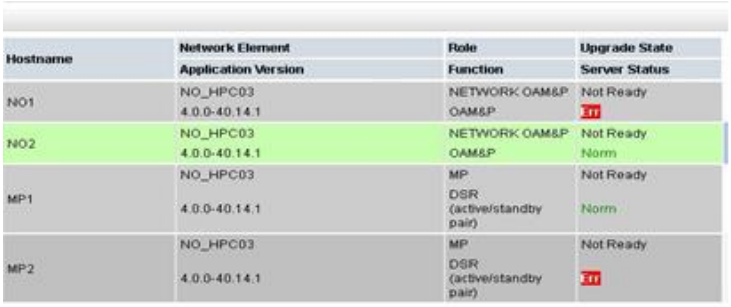
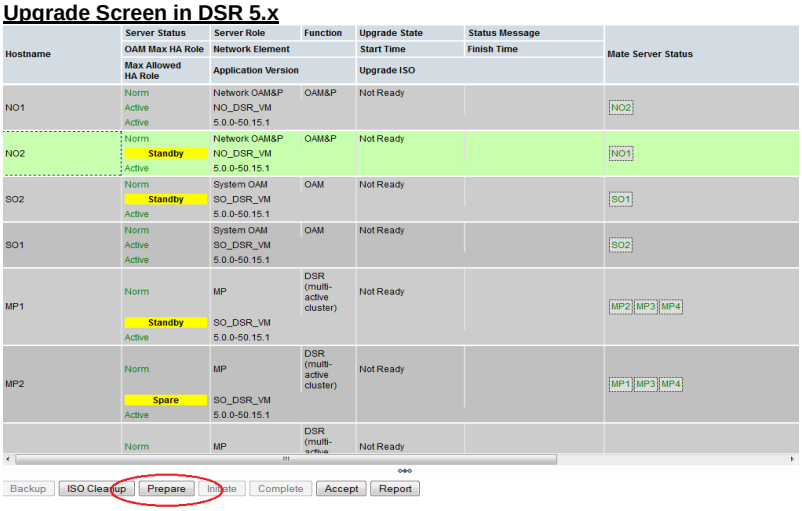
The following status may be expected:
Active NO server will have the following expected alarm:
Alarm ID = **10008** (Provisioning Manually Disabled)

Servers with replication disabled may have the following expected alarms:
Alarm ID = **31113** (Replication Manually Disabled)
Alarm ID = **10075** (The server is no longer providing services because application processes have been manually stopped (result of make ready)
Alarm ID = **31228** (High Availability Server failed to receive mate heartbeats)

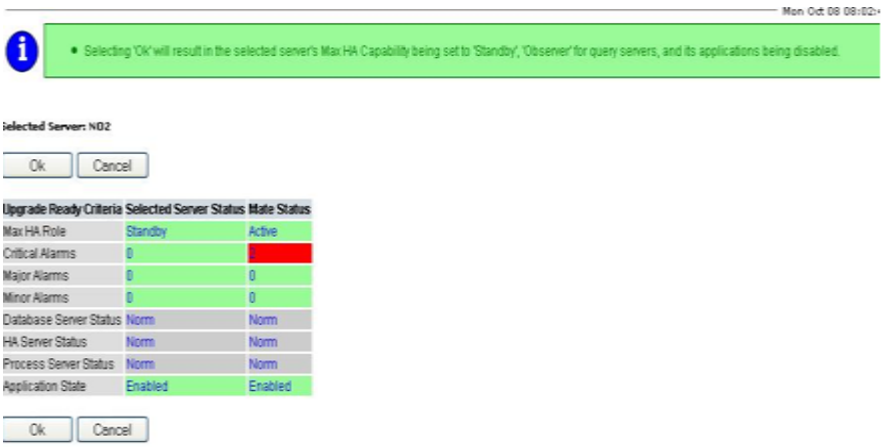
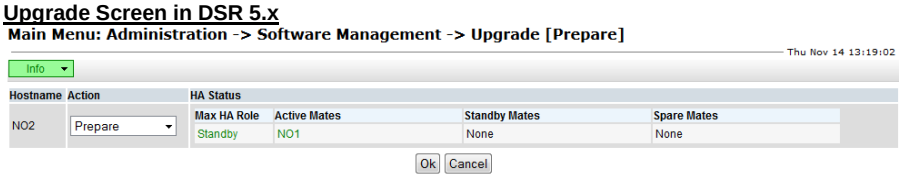
Procedure 83: Upgrade Single Server – Upgrade Administration

2 ☐	**NO GUI – Upgrade Administration:** Verify status of Server to be upgraded	For the server to be upgraded: 1. Identify 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**. If the server is in 'Ready' state then skip the "Prepare Upgrade" steps and Start Upgrade at Step 7
3 ☐	**Identify key info for the server to be upgraded**	Before executing this procedure, document the following information for this server upgrade: For the site: Is the source upgrade release {less than, greater than or equal to} **DSR 4.1.0_41.16.0?** ____ Is the DA-MP redundancy for this site {(1+1), (N+0)}? _____ Is the site 3-Tier or 2-Tier OAM? _____ For this server: Is the server {3-tier NO, 2-Tier NO, SO, MP or other C level server} ?_____ Is the server {Standby, Active}? _____ You must have clear answers to these questions to proceed. *NOTE: if the server is part of an Active/Standby pair, the following Make Ready step will cause a failover, and the server will become Standby.*

Procedure 83: Upgrade Single Server – Upgrade Administration

4 ☐	**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.x)** (In this example, NO with name "NO2" will be made ready for Upgrade) **Note:** Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases. **Upgrade Screen in DSR 4.x**   **Upgrade Screen in DSR 5.x**  The Upgrade "Make Ready" form will be displayed. (see next step)

Procedure 83: Upgrade Single Server – Upgrade Administration

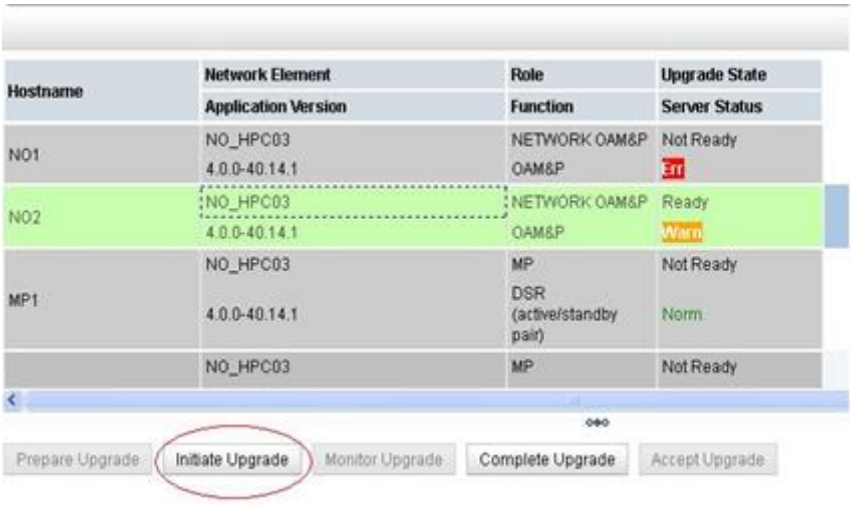
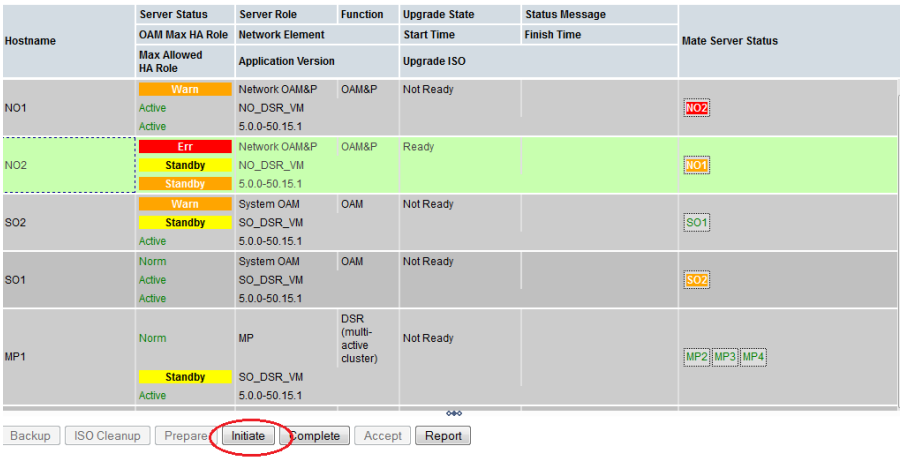
5 ☐	**NO GUI – Upgrade Administration:** Prepare Upgrade (step 2)	**Upgrade** form is displayed (see example below) **Note:** Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases. For the Max Ha Role: 1. 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** **Upgrade Screen in DSR 4.x**  **Upgrade Screen in DSR 5.x**  ***Note: If this is the active server in an active/standby pair, the Make Ready action WILL cause an HA switchover.*** ***If the server being upgraded is the active NOAM, the HA switchover will cause the GUI session to be automatically logged out. You can log back into the GUI using the NOAM VIP.*** ***For 2 tier Active-Standby Setup, the Make Ready action on DA-MP server MAY cause the value in the HA Status field under the Selected Server Status be shown as 'Active' for both the DA-MP(s). This is OK. Please proceed with upgrade.***

Procedure 83: Upgrade Single Server – Upgrade Administration

6 ☐	**NO GUI – Upgrade Administration:** Verify Upgrade Status is "Ready"	Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute) Depending on the server being upgraded, new alarms may occur. 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 = **32515** (Server HA Failover Inhibited) Alarm ID = **31228** (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)

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	Ready Warn
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 83: Upgrade Single Server – Upgrade Administration

7 ☐	**NO GUI – Upgrade Administration** : Initiate Upgrade (initiate) (part 1)	Initiate Upgrade on the server: **Note:** Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases **<u>Upgrade Screen in DSR 4.x</u>** 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 "**Initiate Upgrade"** button.  **<u>Upgrade Screen in DSR 5.x</u>** 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 "**Initiate"** button. 

Procedure 83: Upgrade Single Server – Upgrade Administration

8 ☐	**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 you will be returned to the Upgrade **Administration** screen. 

9 View In-Progress Status (monitor)

View Upgrade Administration form:

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases.

Upgrade Screen in DSR 4.x

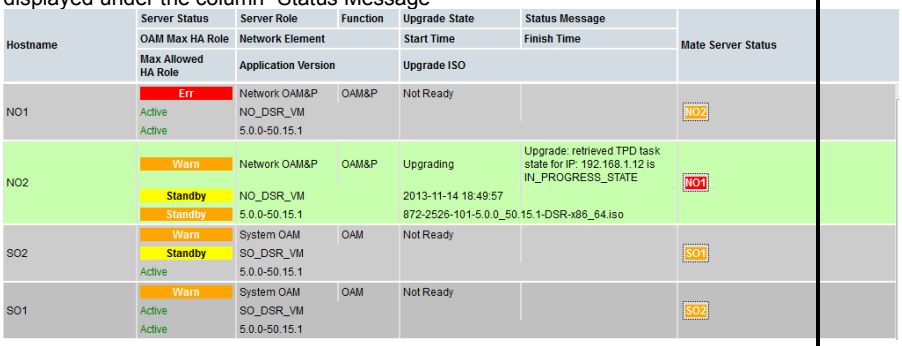
1. Observe the **Upgrade State** of the server of interest.
2. For more detailed status of the upgrade for a given server select the server, and click the **Monitor Upgrade** button

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.x

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



Wait for the upgrade to complete. The "**Upgrade State**" column will show "**Success**". This step will take around 15-20 minutes.

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.

10 ☐	**Optional :** View In-Progress Status from command line of server	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: 5.0.0_50.12.5`
		`  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`

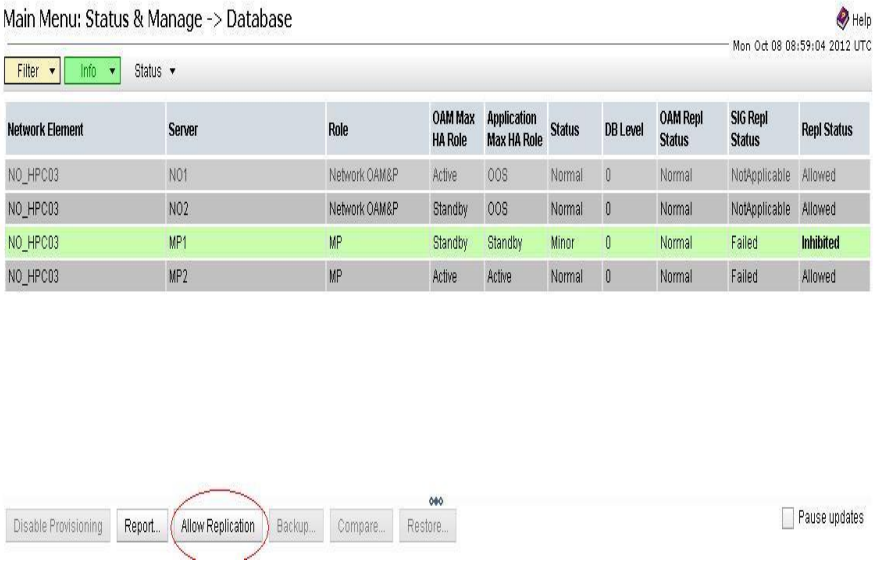
11 ☐	**IF Upgrade Fails:**	Access the server command line (via ssh or Console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		
		Contact Tekelec Customer Care by referring to Appendix K of this document and provide these files.

12 ☐	If upgraded server is: **2-Tier NO Server**, and (N+0) DA MP configuration	Execute following commands IF: • Server is 2-Tier NO Server, and (N+0) DA-MP configuration -- AND -- • SOURCE UPGRADE RELEASE is **less than DSR 4.1.0_41.16.0** **Note: The following steps will inhibit replication to C level servers** Log into upgraded **NO server**: **`# ssh root@<Standby NO IP>`** **`login as:  root`** **`password:  <enter password>`** **Note: Take the backup of TableDef table. We will be requiring this data to enable the replication once this site is successfully upgraded** Execute following commands:: **`# iqt -Iarchiver -N TableDef  > /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml`** **Note: Re-verify if the backup file gets created in the /var/TKLC/db/filemgmt directory by executing the following command.** **`# ls -ltr /var/TKLC/db/filemgmt/$(hostname).TableDef.backup`** Inhibit the A to C level replication

		# iset -frepPlanId=Off TableDef where "repPlanId='A'"# iset -frepPlanId=A TableDef where "name='DoubleParam'" Look for the output similar to **" === changed <Number of Records> records ==="** to ensure that the above commands gets executed successfully. Restart inetrep process **# pm.set off inetrep** **# pm.set on inetrep** **Note: Re-verify if the replication gets inhibited successfully by executing the following command** **# iqt -ph TableDef where "repPlanId='A'"** Only Records for table DoubleParam shall be displayed as the output of the above command. Example output from this command: `185 -45 DoubleParam 0xa38f0dde ComcolConfigPart -1 -1 1 286 6 72 82 2 82 2 32 0 1 -1 A Uc 0x483a49da comcol.schema 2086 IdbCore.h`
13	If upgraded server is: **3-Tier SO Server,** and (N+0) DA-MP configuration	Execute following commands IF: • Server is 3-Tier SO Server, and (N+0) DA-MP configuration -- AND -- • SOURCE UPGRADE RELEASE is **less than DSR 4.1.0_41.16.0** **Note: The following steps will inhibit replication to C level servers** Log into upgraded **SO server**: **# ssh root@<Stanby SO IP>** **login as: root** **password: <enter password>** **Note: Take the backup of TableDef table. We will be requiring this data to enable the replication once this site is successfully upgraded** Execute following commands on the upgraded SO server :- **# iqt -Iarchiver -N TableDef > /var/TKLC/db/filemgmt/$(hostname).TableDef_backup.xml** **Note: Re-verify if the backup file gets created in the /var/TKLC/db/filemgmt directory by executing the following command** **# ls -ltr /var/TKLC/db/filemgmt/$(hostname).TableDef.backup** Inhibit the A and B level replication to C level **# iset -frepPlanId=Off TableDef where "repPlanId='A' or**

		repPlanId='B'" **# iset -frepPlanId=A TableDef where "name='DoubleParam'"** Look for the output similar to **" === changed < Number of Records > records ==="** to ensure that above commands gets executed successfully Restart inetrep process **# pm.set off inetrep** Note: This command will cause a failover, if performed on the Active server. **# pm.set on inetrep** Note: Re-verify if the replication gets inhibited successfully by executing the following command **# iqt -ph TableDef where "repPlanId='A' or repPlanId='B'"** Only Records for table DoubleParam shall be displayed as the output of the above command Example output from this command: `185 -45 DoubleParam 0xa38f0dde ComcolConfigPart -1 -1 1 286 6 72 82 2 82 2 32 0 1 -1 A Uc 0x483a49da comcol.schema 2086 IdbCore.h` Skip steps 14 and 15. Move to Step 16.

14 ☐	If upgraded server is: MP Server (or any C level server)	**SKIP THIS STEP IF SOURCE UPGRADE RELEASE is less than DSR 4.1.0_41.16.0** Execute following commands IF: • Server is MP or other C level server -- AND -- • SOURCE UPGRADE RELEASE is **greater than or equal to DSR 4.1.0_41.16.0** **Note: The following steps will allow 'A and B' level replication to upgraded C level servers** Log into **Active NO (either 2-tier or 3-tier)**: **# ssh root@<*Active NO IP*>** **login as: root** **password: <enter password>** Execute following command , where the ***<server name>*** is the name of the upgraded MP (or other C level server: **# iset -finhibitRepPlans=' ' NodeInfo where "nodeName='<*server name*>'"** **Note: After executing above steps to enable replication on MP(s) no indication on GUI would be raised. Verification of replication enabling on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers shall be empty:** **[root@NO1 ~]# iqt NodeInfo** nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A1386.099 NO1 NO1 Active NO_HPC3 B1754.109 SO1 SO1 Active SO_HPC03 C2254.131 MP2 MP2 Active SO_HPC03 C2254.233 MP1 MP1 Active SO_HPC3 Note: This allows AB Replication for the upgraded C level server, which was inhibited during the upgrade of the NOAM .
15 ☐	If upgraded server is: **MP** server (or any C lever server) Allow replication	**IF the server being upgraded is a MP (any C level server), the following steps must be executed once the Upgrade State is "Success" :** From the active NO GUI: 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Select the MP server that was just upgraded. 3. Click **Allow Replication** button **only if replication is Inhibited**, Else move to next step.



Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status
NO_HPC03	NO1	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicable	Allowed
NO_HPC03	NO2	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicable	Allowed
NO_HPC03	MP1	MP	Standby	Standby	Minor	0	Normal	Failed	**Inhibited**
NO_HPC03	MP2	MP	Active	Active	Normal	0	Normal	Failed	Allowed

4. Verify the ***Inhibited*** text is not displayed for server.
5. Wait for the screen to refresh and show the Replication Status field as ***Allowed*** for the server.

16 Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 1)

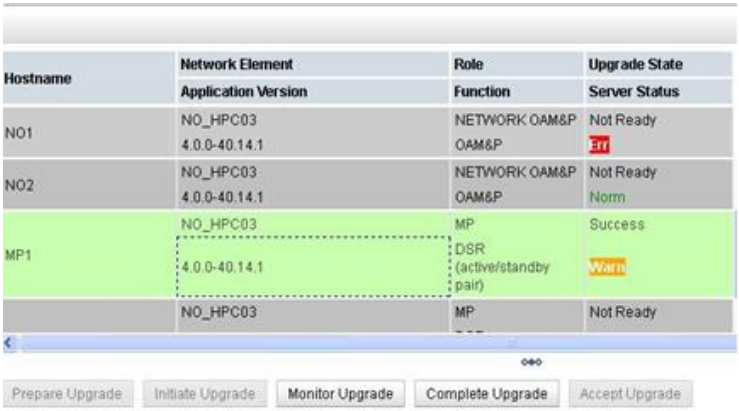
Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type.

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases

1. Select Upgrade Administration screen
   (DSR4.x: "Administration > Upgrade"
   DSR5.x: " 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**.

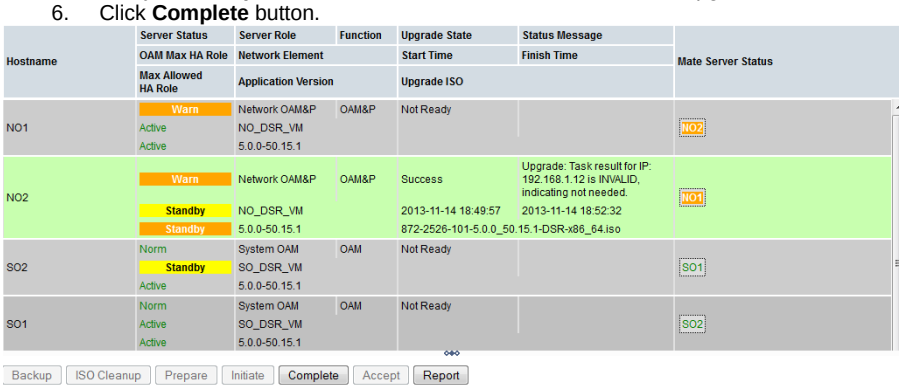
Upgrade Screen in DSR 4.x

5. Verify the **Complete Upgrade** button is enabled for the server that was upgraded
6. Click **Complete Upgrade** button.



Upgrade Screen in DSR 5.x

5. Verify the **Complete** button is enabled for the server that was upgraded
6. Click **Complete** button.

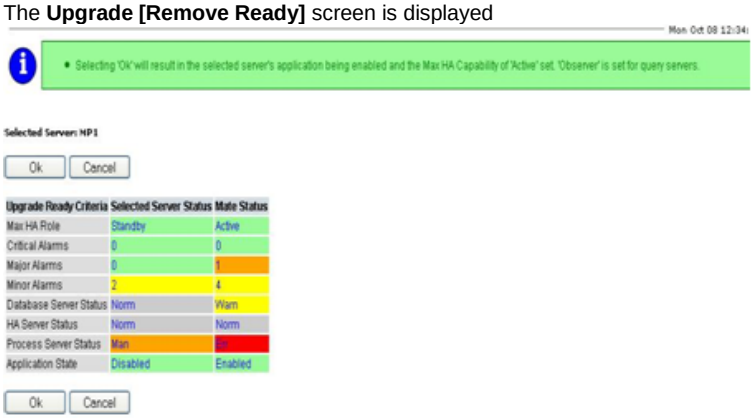


17 Take the upgraded server out of the upgrade ***SUCCESS sta***te. (part 2)

Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases

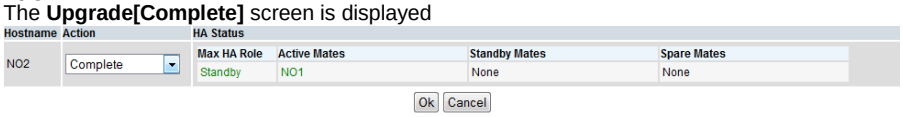
Upgrade Screen in DSR 4.x

The **Upgrade [Remove Ready]** screen is displayed



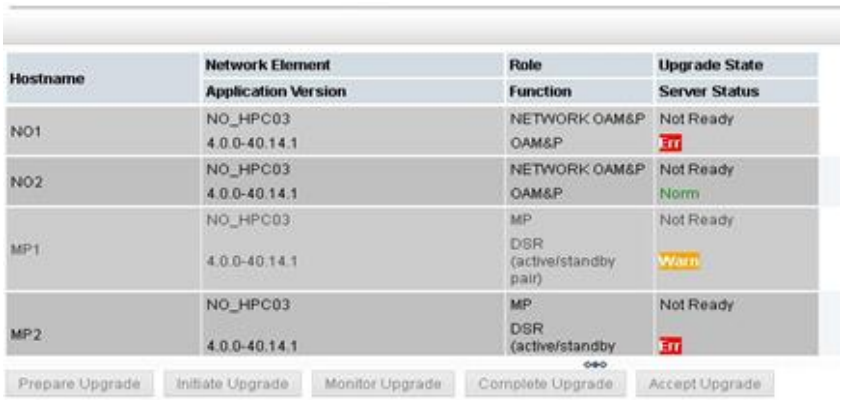
Upgrade Screen in DSR 5.x

The **Upgrade[Complete]** screen is displayed

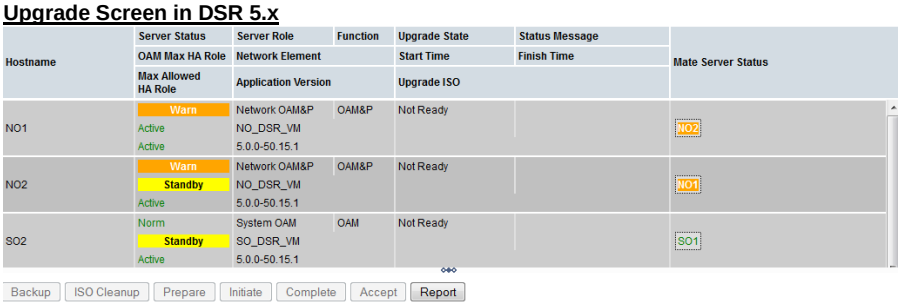


1. Record all the **Upgrade Ready Criteria** and Selected **Server Status** values for this server. Keep this information for future reference.
2. Click **OK**. This completes the Remove Ready action on the server.
3. The Upgrade Administration screen is displayed.
4. Wait for the screen to refresh and show the Upgrade Ready State is **Not Ready** and the **Upgrade** action link is disabled for the 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 4.x



Upgrade Screen in DSR 5.x



18 ☐	View Post-Upgrade Status.	View Post-Upgrade Status of the server: 1. Active NO(or SO for 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) NOTE: Do Not Accept upgrade at this time. This alarm is OK. Servers that still have replication disabled will have the following expected alarm: Alarm ID = **31113** (Replication Manually Disabled)
19 ☐	Procedure Complete.	The single server upgrade is now complete. Return BACK to the overall DSR upgrade procedure step that directed you to execute Appendix G.

APPENDIX H. UPGRADE FIRMWARE

Firmware Upgrade procedures are not included in this document. See Tekelec Customer Care by referring to Appendix K of this document for the latest info 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.
• Filesystem for Netbackup client software has been created (Create LV and Filesystem for Netbackup Client Software)
• Contact Tekelec to determine if the version of Netbackup Client being installed requires workarounds.

1. Follow Tekelec Provided Workarounds
   Follow tekelec 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 gives the procedure for upgrading TVOE on a host server that supports one or more DSR virtual guests.

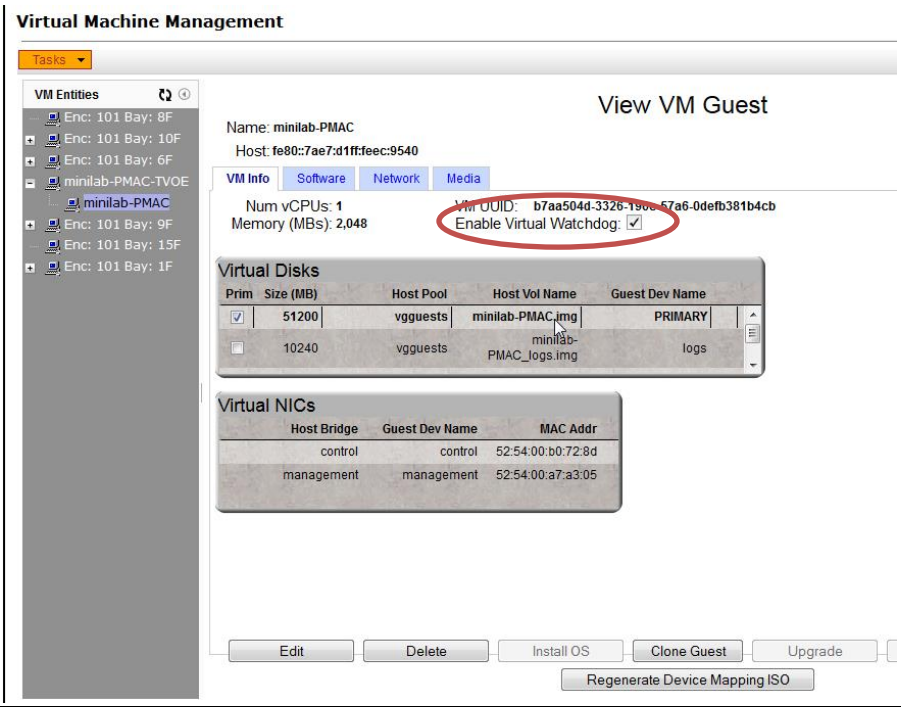
If you are upgrading a DSR server that is deployed as a virtual guest on a bare-metal server running the TVOE host software, then TVOE itself may have to be upgraded first. Refer to Appendix D to determine if a TVOE upgrade is required.

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

Procedure 84: Upgrade TVOE

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 TEKELEC TECHNICAL SERVICES 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 isis 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. Find out the guests running on 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 till TVOE is successfully upgraded.**
5 ☐	After completed …	After TVOE upgrade is completed on the Host Server, the Application(s) may not be started automatically. Proceed as below to restore service.

Procedure 84: Upgrade TVOE

6 ☐	Verify Enable Virtual Guest Watchdog is set for VM	From PMAC VM Management form, verify that the "Enable Virtual Watchdog" is checked. 

6 ☐	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 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 7.
		`# virsh start <guestname>`
		
		c) Periodically execute following command until the command displays all the VM guests running.
		`# virsh list`

7 ☐	Enable all the applications disabled in step1	Enable all the applications running on current TVOE blade: Log into the NOAM VIP GUI a) Select **Status & Manage > Server;** the Server Status screen isis displayed b) Select all the applications (NO(s)/SO(s)) running on current TVOE blade, excluding the server which is in upgrade 'Ready' state. Upgrade State can be verified from Administration->Upgrade screen. c) Click the 'Restart' button. d) Confirm the operation by clicking **Ok** in the popup dialog box. Verify that the 'Appl State' for all the selected servers is changed to 'Enabled'.

APPENDIX K. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A Representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your 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.

Tekelec TAC Engineers are available to provide solutions to your 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.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec – Global

Email (All Regions): support@tekelec.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

• **Mexico**
Phone:
001-888-367-8552

• **Peru**
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