Oracle® Diameter Signaling Router

DSR Software Upgrade Procedure

Release 4.x

909-2243-001

December 2013

Oracle Diameter Signaling Router DSR Software Upgrade Procedure, Release 4.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

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform a software upgrade on DSR 3.x and DSR 4.x servers running on HP C-Class Blades or RMS servers. The audience for this document includes Tekelec customers as well as these DSR 4.x BNS 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 software upgrade.

The DSR 4.x Software Release includes all Tekelec Platform Distribution (TPD) software. Any TPD upgrade necessary is included automatically as part of the DSR 4.x software upgrade. The execution of this procedure assumes that the DSR 4.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. The distribution of the DSR 4.x software load is outside the scope of this procedure.

1.2 References

*[1] HP Solutions Firmware Upgrade Pack Release Notes, 795-0000-0xx,*v2.1.1 (or latest 2.1 version)

[2] Platform 5.x HP G6/G7 Configuration Procedure, 909-1620-001, latest release

[3] TVOE upgrade Document. 909-2211-001. V 1.0 or greater.

[4] Diameter Signaling Router 3.0 on HP C-Class Networking Interconnect Technical Reference, TR006999, v. 1.0 or greater, Williams et al., 2011

[5] Migration Document number WI006848,Tekelec

[6] DSR 4.0 HP C-Class Installation Document, 909-2228-001, latest release,P. Mouallem et al,. 2012

[7] PM&C 4.x to 5.x Migration procedure, 909-2208-001, Tekelec

[8] PM&C 5.x Incremental upgrade, 909-2207-001, Tekelec.

[9] Platform 6.x Configuration Procedure Reference, 909-2209-001, latest release.

[10] Formal Peer Review Process, PD001866, v9.0, Jan 2011

[10].3 Software Release Numbering

Refer to Engineering Release Notes or other appropriate document with the most recent build numbers in order to identify the proper components that comprise the product's software release.

[10].4 Acronyms

Table 1. Acronyms

CD-ROM	Compact Disc Read-only Media
CSV	Comma-separated Values
CPA	Charging Proxy Agent
DA	Diameter Agent
DA MP	Diameter Agent Message Processor
DB	Database

DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
DSR DR NO	Disaster Recovery DSR NO
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
NE	Network Element
NO	Network OAM
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
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
XMI	External Management Interface
XSI	External Signaling Interface

[10].5 Terminology

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

Table 2. Terminology

Upgrade	The process of converting an Appworks based application from its current release on a System to a newer release.
Major Upgrade	An Upgrade from one DSR release to another DSR release. For e.g. DSR 3.x to DSR 4.x
Incremental Upgrade	An Upgrade within a given DSR release for e.g. within 4.0.x to 4.0.y
Software Only Upgrade	An Upgrade that does not require a Database Schema change. Only the software is changed.
DB Conversion Upgrade	An Upgrade that requires a Database Schema change performed during Upgrade that is necessitated by new feature content or bug fixes.
Single Server Upgrade	The process of converting a DSR 3.x/4.x server from its current release on a single server 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.
Standalone Server Upgrade	Single Server Upgrade performed on a Standalone Server. This Upgrade requires the use of the platcfg UI.
Backout	The process of converting a single DSR 4.x server to a prior version. This could be performed due to failure in Single Server Upgrade.
Downgrade	The process of converting a DSR 4.x server from its current release to a prior release. This could be performed due to a misbehaving System.
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.
Target release	Software release to upgrade to.
Health Check	Procedure used to determine the health and status of the AppWorks network. This includes status displayed from the AppWorks 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	HP ProLiant DL 380 G6 server deployed with HP c-class 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 HP G6 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 MP
N+0	Setup with N Active MP(s) but no standby MP
NO	Network OAM for DSR unless and otherwise stated.
SO	System OAM for DSR unless and otherwise stated.
Migration	Changing policy and resources after upgrade. For e.g. changing from 1+1(Active Standby) policy to N+0(Multiple Active) Policy.

[10]6 How to use this Document

When executing this document, there are a few key points which help to ensure that the user understands the author's intent. These points are as follows;

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.

3)6.1 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.

3)7 Recommendations

This section is used to outline optional recommended processes, procedures, and methods used to determine additional information during and after a successful upgrade execution.

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.

3)7.1 Large Installation Support

For large systems containing multiple Signaling Network Elements, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. However, whenever possible, Primary NOAMP Network Element servers should be upgraded within the same maintenance window. When multiple maintenance windows are required, replication may be allowed and provisioning re-enabled between scheduled maintenance windows.

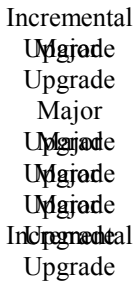
2. GENERAL DESCRIPTION

This document defines the step-by-step actions performed to execute a software upgrade of an in-service DSR 3.x/4.0 from the source release to the target release.

2.1 Supported Upgrade Paths

The supported DSR 4.x upgrade paths 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 Path



Note: The initial installation is not within the scope of this upgrade document.

3. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute an upgrade. It also provides a brief timing overview of the activities needed to upgrade source release software that is installed and running on a DSR 3.x/4.x server to the Target Release software. The approximate time required is outlined in Table 4 through Table 14, with the backout procedure overview shown in Table 15. These tables are used to plan and estimate the time necessary to complete your upgrade. Timing values are estimates only. They estimate the completion of a step or group of steps. Use the tables to plan the timing of the upgrade. Do not use the tables to execute the procedure. The actual procedures' detailed steps begin 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 3.x/4.x Network OAM servers with Administrator privileges. Note: All logins into the DSR 3.x/4.x NO servers are made via the External Management VIP unless otherwise stated.
- User logins, passwords, IP addresses and other administration information. See Section3.1.2.
- 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 IP addresses from the user's local workstation is required in the case of a Backout.

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 4.x ISO image file will be in the following format:

872-xxxx-102-4.x.z-4x.w.z-DSRx86_64.iso

Note: Prior to the execution of this upgrade procedure it is assumed that the DSR 4.x ISO image file has already been delivered to the customer's premises. This includes delivery of the ISO image file to the local workstation being used to perform this 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. The distribution of the DSR 4.x software load is outside the scope of this 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	Example
Credentials	GUI Admin Username		
	GUI Admin Password		
	Root Password		
	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		
	NO 1 XMI IP Address		labCe1b14dsrnoa
	NO 2 XMI IP Address		labCe2b14dsrnob
SO	XMI VIP address		
	SO 1 XMI IP Address (Site 1)		labCe1b14dsrsoa
	SO 2 XMI IP Address (Site 1)		labCe2b14dsrsob
	Policy DRA (DSR) Spare System OAM&P server – Site 1 Spare in Site 2, XMI IP Address		labCe1b14dsrsoc
	SO 1 XMI IP Address (Site 2)		labDe1b14soa
	SO 2 XMI IP Address (Site 2)		labDe2b14sob
	Policy DRA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address		labDe1b14soc
Binding pSBR Server Groups	Binding pSBR SR1 Server Group Servers (Site 1)		labCe2b2BpsbrSr1 labCe1b2BpsbrSr1
	Binding pSBR SR2 Server Group Servers (Site 1)		labCe1b7BpsbrSr2
	Binding pSBR SR3 Server Group Servers (Site 1)		labCe2b7BpsbrSr3 labCe1b10BpsbrSr3
	Binding pSBR SR4 Server Group Servers (Site 1)		LabDBindingSR4SG
Session pSBR Server Groups	Session pSBR SR1 Server Group Servers (Site 1)		labCe2b3SpsbrSr1 labCe1b8SpsbrSr1
	Session pSBR SR2 Server Group Servers (Site 1)		labCe1b9SpsbrSr2
	Session pSBR SR3 Server Group Servers (Site 1)		labCe2b8SpsbrSr3 labCe1b11SpsbrSr3
	Session pSBR SR4 Server Group Servers (Site 1)		labCe2b11SpsbrSr4
P-DRA MP Server Group	LabCPDRASG		

	Policy DRA MP Server Group Servers (Site 1)		labCe1b4pdra1 labCe1b5pdra2 labCe1b12pdra3 labCe1b13pdra4 labCe2b4pdra5 labCe2b5pdra6 labCe2b10pdra7 labCe2b12pdra8 labCe2b13pdra9
IPFE Server Groups	P-DRA IPFE A1 Server Group Server(Site 1)		labCe1b1ipfeA1
	P-DRA IPFE A 2 Server Group Server(Site 1)		labCe2b6ipfeA2
	P-DRA IPFE B 1 Server Group Server(Site 1)		labCe2b1ipfeB1
	P-DRA IPFE B 2 Server Group Server(Site 1)		labCe1b6ipfeB2
Binding PSBR Server Groups	Binding pSBR SR1 Server Group Servers (Site 2)		labDe1b2BpsbrSr1
	Binding pSBR SR2 Server Group Servers (Site 2)		labDe2b2BpsbrSr2 labDe1b7BpsbrSr2
	Binding pSBR SR3 Server Group Servers (Site 2)		labDe2b10BpsbrSr3
	Binding pSBR SR4 Server Group Servers (Site 2)		labDe2b7BpsbrSr4 labDe1b3BpsbrSr4
Session PSBR Server Groups	Session pSBR SR1 Server Group Servers (Site 2)		labDe1b8SpsbrSr1
	Session pSBR SR2 Server Group Servers (Site 2)		labDe1b9SpsbrSr2 labDe2b3SpsbrSr2
	Session pSBR SR3 Server Group Servers (Site 2)		labDe2b16SpsbrSr3
	Session pSBR SR4 Server Group Servers (Site 2)		labDe2b7BpsbrSr4 labDe1b3BpsbrSr4
P-DRA MP Server Group	Policy DRA MP Server Group Servers (Site 2)		labDe1b4pdra1 labDe1b5pdra2 labDe1b12pdra3 labDe1b13pdra4 labDe2b4pdra5 labDe2b5pdra6 labDe2b10pdra7 labDe2b12pdra8 labDe2b13pdra9
IPFE Server Groups	P-DRA IPFE A1 Server Group Server(Site 2)		labDe2b6ipfeA1
	P-DRA IPFE A 2 Server Group Server(Site 2)		labDe2b1ipfeB1
	P-DRA IPFE B 1 Server Group Server(Site 2)		labDe1b1ipfeA2
	P-DRA IPFE B 2 Server Group Server(Site 2)		labDe1b6ipfeB2
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		
Software	Target Release Number		
	ISO Image (.iso) file name		
Misc.	Miscellaneous additional data		

3.2 Upgrade Maintenance Windows

!! WARNING!! **IT IS RECOMENDED THAT MATED SITES BE UPGRADED IN SEPARATE MAINTENANCE WINDOWS IF AT ALL POSSIBLE.**

Note: - For 2 tier setup just refer Maintenance window 2 form specified below.

Maintenance Window 1 **Date: _____** **NOTE:** *The **NE Name** may be viewed from the DSR*	• 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 **site**. PM&C : _____

NOAM GUI under **[Main Menu → Configuration → Network Elements].**	TVOE for DR NOAM: _____ TVOE for Standby NOAM: _____ TVOE for Active NOAM: _____ DSR NOAM: _____ DR 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 **site**. TVOE for Standby SOAM: _____ TVOE for Active SOAM: _____ TVOE for Spare SOAM: _____ SOAM Site1: _____ IPFE1: _____ IPFE2 : _____ cSBR: _____ cSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ SpareSBR: _____ SpareSBR: _____ SpareSBR: _____ MP1: _____ MP2: _____ MP3: _____ MP4: _____ MP5: _____

	. . . MP64: _____
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 **site**. TVOE for Standby SOAM: _____ TVOE for Active SOAM: _____ TVOE for Spare SOAM: _____ SOAM Site2: _____ IPFE1: _____ IPFE2 : _____ cSBR: _____ cSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ pSBR: _____ SpareSBR: _____ SpareSBR: _____ SpareSBR: _____ MP1: _____ MP2: _____ MP3: _____ MP4: _____ MP5: _____ . . . MP64: _____

Note: The above Maintenance windows will upgrade only 2 site setup. If more sites are present then more maintenance windows will be required to upgrade SOAMP and MP(s). Please check the Maintenance Window 3 above.

3.3 Pre-Upgrade Overview

The pre-upgrade procedures shown in the following table may be executed outside a maintenance window if desired. 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	System Topology Check	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.

* On slow networks, the ISO transfer might take a long period of time, up to several hours

3.3.1 Pre-Upgrade Overview (Upgrade Preparation)

This section provides detailed procedures to prepare a system for upgrade execution. These procedures are executed outside a maintenance window.

3.3.2 Hardware Upgrade Preparation

There is no hardware upgrade necessary for this software upgrade.

3.3.3 Software Upgrade Preparation

This section provides the detailed procedure steps of the Upgrade Preparation. Before starting the upgrade, Review the Release Notes for the new DSR 3.x/4.x release to understand the functional differences and possible traffic impacts of the upgrade. Determine the strategy to be used to upgrade multiple sites safely.

3.3.3.1 Required Materials Check

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

Procedure 1: Required Materials Check

S T E P #	This procedure verifies that all required materials are present. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, 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 D. Note that obtaining a new online support account can take up to 48 hours.

3.3.3.2 System Topology Check

This procedure is part of Software Upgrade Preparation and is used to verify system topology of the DSR 3.x/4.x network and servers.

Procedure 2: System Topology Check

S T E P #	This procedure verifies System Topology. 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 Network Element Configuration data	View the Network Elements configuration data; verify the data; save and print report: 1. Log into the NOAM VIP GUI 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 3. Click **Report** at the bottom of the table to generate a report for all entries. 4. Verify the configuration data is correct for your network. 5. Save the report and/or print the report. Keep these copies for future reference.
2 ☐	Verify Server Group Configuration data	View the Server Group configuration data; verify the data; save and print report: 1. Select **Configuration > Server Group** to view Server Group screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
3 ☐	Verify Servers Configuration data	View the Servers configuration data; verify the data; save and print report: 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 Services Configuration data	View the Services configuration data; verify the data; save and print report: 1. Select **Configuration > Services** to view Services screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
5 ☐	Verify Signaling Network Configuration data	View the Signaling Networks configuration data; verify the data; save and print report: 1. Select **Configuration > Network** to view the Signaling Networks. 2. Click **Report** at the bottom of the table to generate a report **for all entries**. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference. 5. Select **Configuration > Network > Devices** and repeat steps 2 through 4. 6. Select **Configuration > Network > Routes** and repeat steps 2 through 4.
6	Backup all global and site provisioning	Backup the global database from the primary active NO server:

☐	databases	1. Login to the GUI for the active server to be backed-up (using the VIP.) 2. Select **Status & Manage > Database** to view Database Status screen. 3. Click to highlight the Active NO server to be backed up, and click **Report**. 4. Save the report and print the report. Keep these copies for future reference. 5. Click to highlight the Active SO (if exists) server to be backed up, and click **Report**. 6. Save the report and print the report. Keep these copies for future reference. 7. Select **Status & Manage > Database** to return to the Database Status screen. 8. Click to highlight the Active NO server (if logged into Active NOAM GUI (Note: the **Backup** button will only be enabled when the active server is selected.) 9. Click **Backup** and archive both **Configuration** and **Provisioning** (if selectable) Data 10. Enter **Comments** (optional) 11. Click **OK**. 12. Login to the Active SO GUI (using VIP) 13. Select Status & Manage-> Database screen, Select Active SO server and click **Backup**; the Backup and Archive screen is displayed. (Note: the **Backup** button will only be enabled when the active server is selected.) 14. Click **Backup** and archive both **Configuration** and **Provisioning** (if selectable) Data 15. Enter **Comments** (optional) 16. Click **OK**. 17. Repeat sub steps 12 to 16 for each site. Save database backups to your local workstation: 18. Login to the GUI for the active NO server using the NOAM VIP. **19. For the active NO/active SO(if exists) servers:** a) Select **Status & Manage > Files;** the **Files** menu gets displayed. b) Click on the Active NO server**.** c) Select **List Files**, all files stored in the file management storage area of this server will be displayed on the screen. d) Select your database backup file and click Download button. e) A confirmation window prompts you. Click **Save**. f) The Choose File window gets displayed. Select a destination folder on your local workstation to store the backup file. Click **Save**. g) The Download Complete confirmation displays. Click **Close**. h) Repeat steps c to g for Active SO server (if exists).
7 ☐	Analyze and plan MP upgrade sequence	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 and 2. 2. Plan for any MP upgrades which will cause out-of-service MP servers. 3. Determine exact sequence which MP servers will be upgraded.

3.h).3.3 Full Backup of DB

This procedure is part of Software Upgrade Preparation and is used to conduct a full backup of the COMCOL run environment on every server, to be used in the event of a backout/rollback of the new software release.

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

Procedure 3: Full DB Backup

S T E P #	This procedure conducts a full backup of the COMCOL run environment on every server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify procedure is run on every server	The full backup of the COMCOL run environment must be completed on every server in every Network Element in the system.
2 ☐	Log in to the Active NO	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.)
3 ☐	Change excluded parts	**If this is a major upgrade (from DSR 3.x->DSR 4.x)ONLY**: Execute the command: **`vi /usr/TKLC/appworks/etc/exclude_parts.d/Appworks.db_parts`** to open the Appworks.db_parts file for editing. Delete all lines from the file. the key-pair "**dd**" will delete a single line. Save the file and exit the editor with the command "**:wq!**"

4 ☐	Backup the COMCOL run environment	Execute the full_backup utility on 'Active NO':
		
		`/usr/TKLC/dpi/bin/backupAllHosts`
		
		Output similar to the following will indicate successful completion:
		
		Script Completed. Status:
		
		HOSTNAME | STATUS
		
		---------- ----------
		
		HPC3blade02 | PASS
		
		HPC3blade01 | PASS
		
		HPC3blade03 | PASS
		
		HPC3blade04 | PASS
		
		NOTE:
		
		If full_backup utility is not used then for manually taking backup on each server execute following steps :-
		
		Execute the following to manually execute the full_backup utility on each 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.`
		
		Note:- Full backup is time consuming process it will take from 10 mins to 2 hrs to complete depending upon the data in the database. Do not proceed until backup on each server is completed.
		
		(Errors will also report back to the command line.)

3.h).3.4 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 3.x/4.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.

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

Procedure 4: Perform Health Check (Upgrade Preparation)

S	This procedure performs a Health Check.

T E P #	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 gets 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's statusdisplayed 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.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Login to Active NO 2. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed. 3. Set the collection interval as 1 Day or more (if needed) and click **Report** button to generate an Alarms report. 4. Save the report and print the report. Keep these copies for future reference. 5. Select **Alarms & Events > View History** and repeat steps 3 and 4. 6. Login to Active SO (if exists) and repeat steps 2 to 5 .
3 ☐	Verify "/var/TKLC/upgrade" is empty	Execute the following command on each server: `# ls /var/TKLC/upgrade` Note: if it is found that the directory contains any files (i.e. ISOs that may not have been removed from previous upgrades), these files should be removed.

4 ☐	Perform syscheck	Execute the following command on each server: **# syscheck** Output similar to the following will indicate successful completion: Running modules in class disk... OK Running modules in class proc... OK Running modules in class system... OK Running modules in class net... OK Running modules in class hardware... OK Do not proceed if there are any errors in the Output. If NetBackup is installed then following errors are acceptable. Please check steps 1-3 of Procedure 6to find if NetBackup is installed or not :- Running modules in class net... OK Running modules in class system... OK Running modules in class proc... OK Running modules in class disk... * fs: FAILURE:: MINOR::5000000000000001 -- Server Disk Space Shortage Warning * fs: FAILURE:: Space used in "/usr" exceeds the recommended limit 80%. 81% used. One or more module in class "disk" FAILED Running modules in class hardware... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log

5 ☐	Check for the existence of the .ugwrap_pid file	1. Execute the following command on each server to determine the existence of the .ugwrap_pid file :- **# ls -la /tmp/.ugwrap_pid** If the .ugwrap_pid file ***does not*** exist there will be no output from the above command. If the .ugwrap_pid file ***does*** exist then the following output will be observed. **-rw-r--r-- 1 root root 4 Jul 24 09:11 .ugwrap_pid** If the file does not exist then you have completed this procedure Otherwise, continue to step 2. 2. Execute the following command to determine if the ugwrap process is currently running. # **ps -ef | grep ugwrap | grep -v grep** **WARNING** If there is output to the following command indicating that an ugwrap process is running than an upgrade is in progress and you should cease all command execution and contact Tekelec Customer Service immediately. If there is no output to the above command than a ugwrap process is not running, proceed to step 3. 3. Execute the following command to remove the .ugwrap_pid file, type "y" when prompted. **# rm –f /tmp/.ugwrap_pid**
6 ☐	Check for the existence of the S99TKLCsnmp_notify_runlevel_transition_complete file.	Execute the following steps on each server to determine the existence of the S99TKLCsnmp_notify_runlevel_transition_complete file :- 1. Go to the server and check /etc/rc3.d folder for S99TKLCsnmp_notify_runlevel_transition_complete file. 2. If the file exists then execute the following command to remove that file :- **# rm –f /etc/rc3.d/S99TKLCsnmp_notify_runlevel_transition_complete** 3. If in the middle of upgrade then go to **Administration > Upgrade screen** and click 'Complete Upgrade' Button. 4. Initiate Upgrade.

7 ☐	Check the firmware version of all the blades before upgrade.	1. Record the target DSR release(4.x.y-4x.nn.a) 2. Contact Tekelec Customer Service to find out the minimum supported firmware version required for the target DSR release. Follow Appendix H for the procedure to check and upgrade the current firmware.
8 ☐	Check the existing PMAC version before upgrade	1. Record the target DSR Release on which the blades need to be upgraded. (4.x.y-4x.nn.a). 2. For upgrade to DSR 4.x minimum PMAC required is **5.0**. 3. If PMAC version is below 5.0 use the following document depending upon the upgrade path :- a) For major DSR upgrade I.e. from DSR 3.x->4.x Follow [7]. b) For Incremental upgrade i.e. from DSR 4.0->DSR 4.x. Follow [8].
9 ☐	Check if netbackup client is installed on NOAMP and SOAM.	Execute following commands on both NO(s) and SO(s) to check if NetBackup is installed or not :- 1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute following command :- **# cat /usr/openv/netbackup/bin/version** 3. If file doesn't exist then don't execute steps 4 and 5 mentioned below. If this file exists then a version of the NB client has been installed on this server, Execute below mentioned steps 4 and 5. 4. Execute below mentioned command :- **# cat /usr/openv/pdde/pdag/pd.conf** 5. If pd.conf file mentioned in step 4 doesn't exist then execute below mentioned command to copy the pd.conf file. **# cp /usr/openv/lib/ost-plugins/pd.conf /usr/openv/pdde/pdag/pd.conf** **Repeat steps 1 to 5 for all the NO(s) and SO(s).**

10 ☐	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 4.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.
11 ☐	Check if the setup have customer supplied apache certificate installed and protected with a passphrase.	1. Verify if the setup have 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 3.6.1 Step 6)

2.b).3.5 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. 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.

4.b).3.6 Create new Logical Volume for NetBackup Client

This procedure is used to create a new logical volume to contain the NetBackup client software.

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.

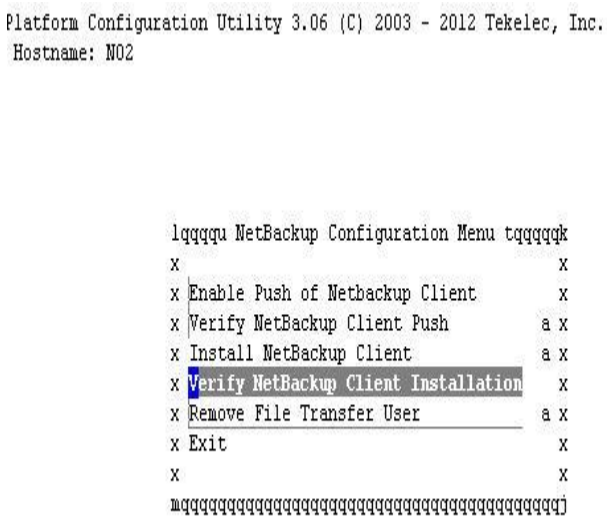
NOTE: This procedure is only required for NOAMP and SOAM servers that have the NetBackup client software installed and do not have a logical volume for NetBackup already created.

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

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	Execute the following commands to check if NetBackup is installed or not :- `# cat /usr/openv/netbackup/bin/version` 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 10. **# su – platcfg** Menu will be displayed, Now navigate to following submenus :- 1. Navigate to NetBackup configuration. Platform Configuration Utility 3.06 (C) 2003 - 2012 Tekelec, Inc. Hostname: NO2 lqqqqu NetBackup Configuration Menu tqqqqqk x x x Enable Push of Netbackup Client x x Verify NetBackup Client Push x x Install NetBackup Client a x x Verify NetBackup Client Installation a x x Remove File Transfer User a x x Exit x x x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

2. Navigate NetBackup Client Installation.



3. If NetBackup client is installed. Following screen will appear.-

Note :- Following error in verify NetBackup Client Installation output is acceptable :-
`[ERROR] - RC script: vxpbx_exchanged`

4. Select Exit to return back.

If NetBackup is installed move to Step 2, Else move to Step 10.

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 10, Else move to next step 3.

3 ☐	Log in to the server	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.)

4 ☐	Mount the upgrade media	Insert Diameter Signaling Router 4.x application media into drive of the application server. Login 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 FILENAME.iso** /media/cdrom

5 ☐	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 indeed there.
6 ☐	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.
7 ☐	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** NOTE: It has been observed that the service restart of NetBackup may return a warning. This is a function of the NetBackup client software.

8 ☐	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. Else report an error to Tekelec customer service.

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

4.b).3.7 ISO Administration

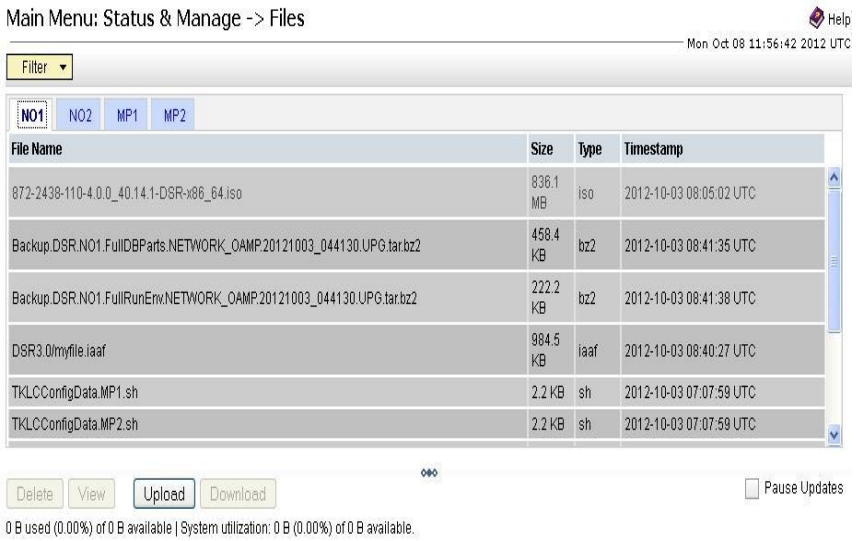
Detailed steps on ISO Administration are shown in the procedure below.

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

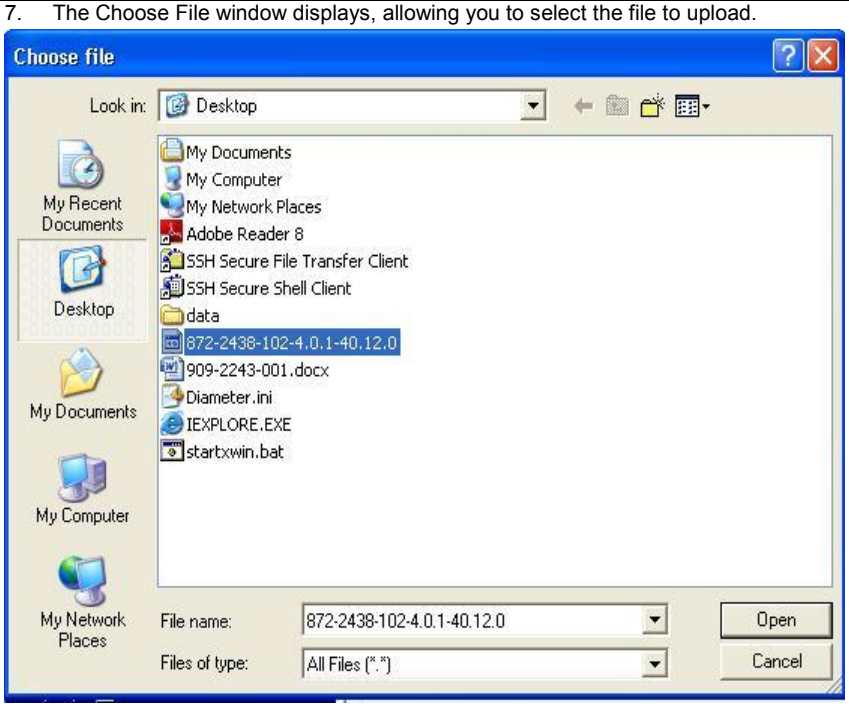
scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 7. ISO Administration

S T E P #	This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**

1 ☐	Upload ISO to Active NO server via the DSR 3.x/4.x GUI session to the Active NO.	There are 2 methods to upload the application ISO to the Active NO based on the type of the media: Execute either Option 1 **OR** Option 2. **OPTION 1:** Using an ISO Image File Upload the target release ISO image file to the File Management Area of the active NO server: 1. Select **Status & Manage > Files;** the Files menu gets displayed  2. Click the active NO server in your network. 3. All files stored in the file management storage area of this server display on the screen. 4. 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. 5. Click the Upload button. Browse window will open up :-  6. Click **Browse** to select the file to upload.

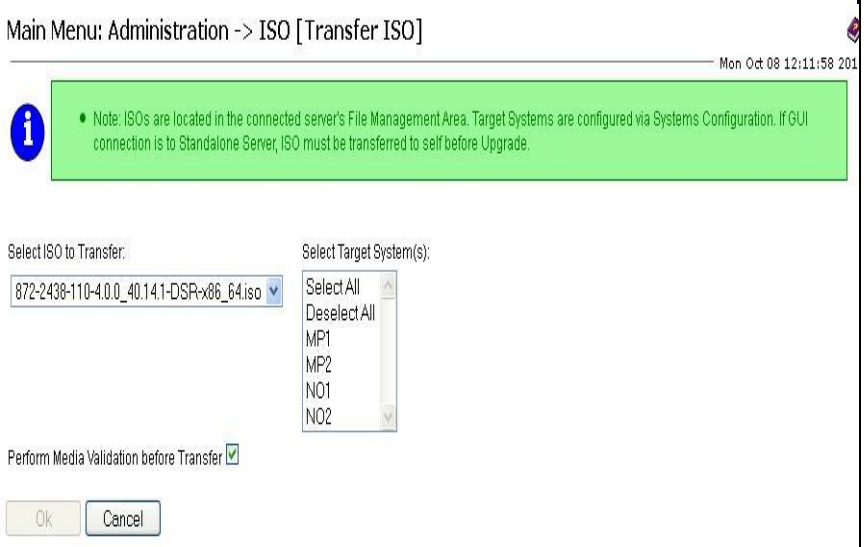
7. The Choose File window displays, allowing you to select the file to upload.



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

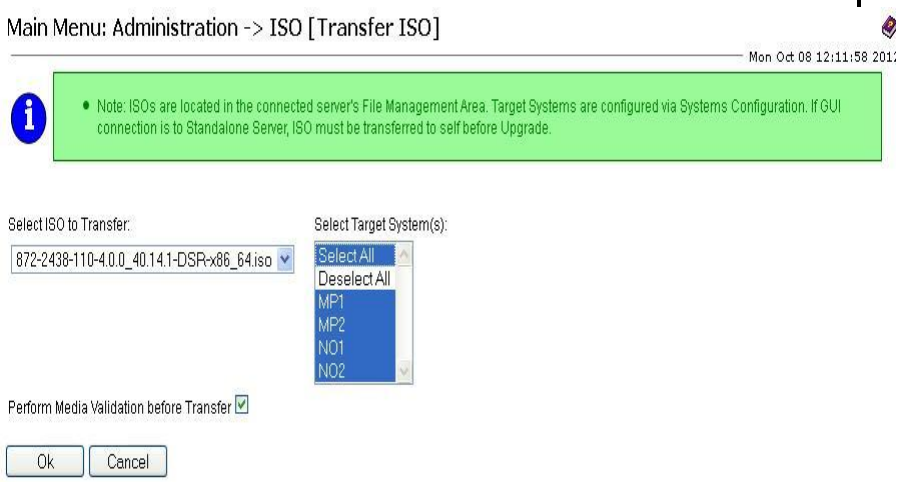
10. Click **Upload.**
11. The ISO file begins uploading to the file management storage area.
12. Wait for screen to refresh and display the uploaded ISO filename in the files list. This will usually take between 2 to 10 minutes, but more if your network upload speed is slow. (Depending on your network speed, up to 25 minutes).
13. Backup the ISO file to the pmac by ssh from the Active NO and executing the following command:
    a) cd into the directory where your ISO image is located (not on the PM&C server)
    ```
    # 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 will be provided by Tekelec.

		14. Scp the ISO file to the Standby NO using the following command: from the Active NO. **scp /var/TKLC/db/filemgmt/<DSR_ISO_Filename> root@<Standby_NO_IP>:/var/TKLC/db/filemgmt** Execute Steps 3 to 7 of **Appendix F** to add ISO image to PMAC repository **OPTION 2:** Using a Media containing the application (recommended for slow network connections between the client computer and the DSR frame – Applicable for DSR 4.x (PMAC 5.0)) 1. Execute Appendix F. 2. SSH into the pmac 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_Filename> 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. Execute following command :- **chmod 644 /var/TKLC/db/filemgmt/<DSR_ISO_Filename>** 4. SSH into the Active NO server and execute the following command: **scp /var/TKLC/db/filemgmt/<DSR_ISO_Filename> root@<Standby_NO_IP>:/var/TKLC/db/filemgmt** Now Refer **Appendix F** to add ISO image to PMAC repository

2 ☐	Transfer ISO to all DSR 3.x/4.x Servers to be upgraded.	Transfer the target release ISO image file from the active NO to all other DSR 3.x/4.x servers. 1. From the Active NO GUI, navigate to **Administration** -> **ISO**  2. Click on "**Transfer ISO"** 

3. Under the "**Select ISO to Transfer:**" drop down menu select the DSR 4.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.

6.4 Software Upgrade Procedure

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 Section3.3.3. 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.
- Command steps that require user entry are indicated with **white-on-black step numbers**.
- 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 should be 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.

6.5 Software Upgrade Execution

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

The procedures shown in the following table are executed across multiple maintenance windows depending upon the type of setup as mentioned in Section 3.2 This table covers all the supported upgrade paths followed by this document and the correct section reference which needs to be followed for each upgrade path.

Table 5. Upgrade Path Reference

	Supported Configurations	Upgrade Path	Section Reference
1	1. DSR 3.x->4.0 major upgrade 2. DSR 3.x->4.1 major upgrade (Legacy, RBAR or FABR) **Note: For DSR 3.x only 2 Tier upgrade is supported.**	DSR 3.x to DSR 4.x Major Upgrade	Section 3.5.5
2	1. DSR 4.x incremental upgrade (1+1) 2-tier configuration. 2. DSR 4.0 -> DSR 4.1 major upgrade (1+1) 2-tier configuration. (Legacy, RBAR and FABR)	DSR 4.x upgrade (1+1) 2 - tier configuration.	Section 3.5.1
3	1. DSR 4.x incremental upgrade (1+1) 3-tier configuration. 2. DSR 4.0 -> DSR 4.1 major upgrade (1+1) 3-tier configuration. (Legacy, RBAR and FABR)	DSR 4.x upgrade (1+1) 3-tier configuration.	Section 3.5.2
4	1. DSR 4.x incremental upgrade (N+0) 2-tier configuration 2. DSR 4.0 -> DSR 4.1 major upgrade (N+0) 2-tier configuration (Legacy, RBAR and FABR)	DSR 4.x upgrade (N+0) 2 - tier configuration.	Section 3.5.3
5	1. DSR 4.x incremental upgrade (N+0) 3-tier configuration. 2. DSR 4.0 -> DSR 4.1 major upgrade (N+0) 3-tier configuration (Legacy, RBAR and FABR)	DSR 4.x upgrade (N+0) 3-tier configuration.	Section 3.5.4
6	1. DSR 4.x incremental upgrade on (N+0) configuration RMS servers with DIH. DSR 4.x incremental upgrade on RMS servers without DIH	Incremental upgrade for 3 tier RMS configuration(N+0)	Section3.5.6

7	1. DSR 4.x incremental upgrade on (1+1) configuration RMS servers with DIH. DSR 4.x incremental upgrade on RMS servers without DIH	Incremental upgrade for 3 tier RMS configuration(1+1)	Section3.5.7
8	1. Policy DRA 4.x incremental upgrade.	Incremental upgrade for 3 tier Policy DRA configuration	Section3.5.8

1.5.1 DSR 4.x upgrade (1+1) 2 - tier configuration

This section contains upgrade steps for DSR 4.x (2-tier setup) upgrade with (1+1) i.e. Active-Standby configuration.

Table 6. Upgrade Execution Overview (For DSR 4.x (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 8	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 9	0:25-0:30	0:26-0:35	1:25-1:30	1:26-1:35	Upgrade NO(s) of (1+1) 2-Tier configuration	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 10	0:01-0:05	0:27-0:40	0:01-0:05	1:27-1:40	Perform Health Check(Post Upgrade of NOAM)	None
Procedure 11	0:25-0:30	0:52-1:10	0:25-0:30	1:52-2:10	Upgrade MP(s) of (1+1) 2-Tier configuration	None
Procedure 12	0:01-0:05	1:03-1:30	0:01-0:05	1:53-2:15	Perform Health Check(Post Upgrade of MPs)	None

	Per MP					

1.5.1.1 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.

Procedure 8: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 4. Do not proceed to upgrade if any of the server's statusdisplayed 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 gets 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.

3.5.1.2 Upgrade NOAM

Detailed steps are shown in the procedure below.

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

Procedure 9. 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 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.

2 ☐	Inhibit SOAP replication (If upgrading from DSR release < 40.19.0)	1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded 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** :- For e,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef** **Note: - This step needs to be executed only if upgrading from any release before 40.19.0.**
3 ☐	Inhibit replication to all servers.	Inhibit database replication to all servers in the following order: • Standby MP's • Active MP's • Standby NO • Active NO 1. Select **Status & Manage > Database** The Database Status screen gets 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 active servers last to prevent unwanted HA switchovers.**

4 ☐	Upgrade Standby NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby NO if standby NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby NO server using Upgrade Single Server procedure: 1. Execute Appendix G (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the standby NO upgraded above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

5 ☐	Upgrade 2nd NO server.	Note: - Execute Appendix J again for Active NO if Active NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above . **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade the 2nd NO server (the mate) using the Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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** 4. Clear the browser cache after upgrade is completed.

6 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server.

6.5.1.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 10: 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/SO servers upgraded:
		1. Execute following commands on the upgraded servers :-
		
		Use your SSH client to connect to the upgraded server (ex. ssh, putty):
		ssh <server address>
		
		login as: root
		password: <enter password>
		
		# verifyUpgrade
		
		Examine the output of the above command to determine if any errors were reported.
		
		Note: The following error is an expected failure for upgrade to DSR 4.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 32532 AlarmId 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
		
		Follow Procedure 69 to suppress 32532 alarmId for all the servers.

2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
4 ☐	Fix up the measurement retention for DSR 4.0 servers.	**Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1.** Execute following steps on each of the upgraded NOAMs :- 1. Use your ssh client to connect to NOAM server. **ssh <NO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute following commands: **# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd** **# cd /usr/TKLC/dsr/bin** **# ./idb.initdd** **# init 6**

2.5.1.4 Upgrade MP(s)

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

Following Procedure is used to upgrade legacy Active-Standby MP Pair.

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

Procedure 11: Upgrade MP(s) of (1+1) 2-Tier configuration

S T E P #	This procedure upgrades the 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 MP Server by going to Status & Manage -> HA and record which MP server is Active and which is Standby.
2 ☐	Upgrade a Standby MP server (using Upgrade Single Server procedure)	Upgrade Standby MP server using Upgrade Single Server procedure: 1. Execute Section Appendix G (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
3 ☐	Upgrade leftover MP server.	Upgrade Leftover MP server using the Upgrade Single Server procedure. 1. Execute Appendix G (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets 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 and SO.	1. Login into DSR GUI. 2. Go to Status & Manage-> HA screen. 3. Click 'Edit' button. 4. 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. 5. Click 'Ok' button.

6 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the Active DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- 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** Repeat Steps 1 and 2 for Standby DA MP. Note: Above steps may lead to MP switchover.
7 ☐	Install NetBackup 7.1 or 7.5 on NO(If required)	Please refer to Appendix I.

1.5.1.5 Perform Health Check (Post-Upgrade of MPs)

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

Procedure 12: Perform Health Check (Post-Upgrade of MPs)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on all of the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command, and determine if any errors were reported.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed. Following Alarm ID will be observed on all the upgraded servers :- Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Note :- If 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers. 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 Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview
End of first maintenance window.		

3.5.2 DSR 4.x upgrade (1+1) 3 – tier configuration

This section contains upgrade steps for DSR 4.x (3-tier setup) upgrade with (1+1) i.e. Active-Standby configuration.

For large systems containing multiple Signaling Network Elements or multiple sites, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. Therefore all the Primary NOAMP and DR NOAMP Network Element servers should be upgraded within the same maintenance window. Followed by upgrade of SO(s) and MP(s) in separate maintenance window. Provisioning can be re-enabled (if required) after first maintenance window i.e. after both DR NOAMP(s) and primary NOAMP(s) are upgraded successfully.

Table 7. Upgrade Execution Overview (For DSR 4.x (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 13	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 14	0:25-0:30	0:26-0:35	1:25-1:30	1:26-1:35	Upgrade NO(s) of (1+1) 3 -Tier configuration.	TVOE upgrade will stop all the applications running under it.
Procedure 15	0:01-0:05	0:27-0:40	0:01-0:05	1:27-1:40	Perform Health Check (Post Upgrade of NOAM)	None
Procedure 16	0:25-0:30	0:52-1:10	0:25-0:30	1:52-2:10	Upgrade SO(s) of (1+1) 3 – Tier configuration.	TVOE upgrade will stop all the applications running under it.
Procedure 17	0:25-0:30	1:17-1:40	0:25-0:30	2:17-2:40	Upgrade MP(s) of (1+1) 3-Tier configuration.	None
Procedure 18	0:01-0:05 Per MP	1:18-1:45	0:01-0:05 Per MP	2:18-2:45	Perform Health Check(Post Upgrade of MPs)	None

3.5.2.1 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 at NO and SO.

Procedure 13: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets 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's status 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 gets 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 above two steps for SO VIP GUI.

3.5.2.2 Upgrade NO (3-tier)

WARNING! **IT IS RECOMENDED THAT ONLY NOAMP(s) BE UPGRADED IN SINGLE MAINTENENCE WINDOW. SEPARATE MAINTENANCE WINDOWS WILL BE REQUIRED FOR EACH SOAMP SITES.**

Detailed steps are shown in the procedure below.

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

Procedure 14. Upgrade NO(s) of (1+1) 3 -Tier configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.
2 ☐	Inhibit SOAP replication (If upgrading from DSR release < 40.19.0)	1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded 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** :- For e,g, **`nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef`** **Note: - This step needs to be executed only if upgrading from any release before 40.19.0.**

3 ☐	Inhibit replication to all servers.	Inhibit database replication to all servers in the following order: • Standby MP's • Active MP's • Standby SO's • Active SO's • Standby NO • Active NO • Standby DR NO • Active DR NO 1. Select **Status & Manage > Database** The Database Status screen gets 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** 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 active servers last to prevent unwanted HA switchovers.**

4 ☐	Upgrade Standby DSR DR NO server (using Upgrade Single Server procedure).	**Note: - Execute Appendix J for Standby DR NO if Standby DR NO is hosted on TVOE blade before proceeding with below mentioned steps.**
		
		Upgrade Standby DSR DR NO (if exists) using Upgrade Single Server procedure:
		
		1. Execute Appendix G.
		(Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
		
		2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0 :-
		
		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`

5 ☐	Upgrade Active DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J again for Active DR NO if 2nd DR NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby DR NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR DR NO (if exists) using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

6 ☐	Upgrade Standby DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for standby NO if Standby NO is running on TVOE blade. Upgrade Standby DSR NO using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

7 ☐	Upgrade Active DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J again for Active NO if Active NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR NO using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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** 4. Clear the browser cache after upgrade is completed.

8 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** 6. Repeat the **Allow** action link for Standby NO server. **Repeat steps 1 to 6 for DR NO(s) as well (if exists).** **Note: Replication to any SOAMs or 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.** After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server.

6.4..2.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 15: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
4 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1. Execute following steps on each of the upgraded NOAMs :- 3. Use your ssh client to connect to NOAM server. **ssh <NO XMI IP address>** **login as: root** **password: <enter password>** 4. Execute following commands: **# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd** **# cd /usr/TKLC/dsr/bin** **# ./idb.initdd** **# init 6**
End of first maintenance window		
Provisioning can be re-enabled between maintenance windows ((If required).		

4.4..2.4 Upgrade SO (3-tier)

SOAMP servers of each site shall be upgraded in different maintenance window.
Detailed steps are shown in the procedure below.

Procedure 16. Upgrade SO(s) of (1+1) 3 -Tier configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 2nd Maintenance Window.		
1 ☐	Disable Site Provisioning	Disable Site provisioning before starting with upgrade :- 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen gets 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 DSR SO	Note: - Execute Appendix J for Standby SO if Standby SO is hosted on TVOE blade before proceeding with below mentioned steps.
		Upgrade Standby DSR SO server using Upgrade Single Server procedure :-
		1. Execute Appendix G.
		(Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
		2. Log into the Standby SO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:-
		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`

3 ☐	Upgrade Active DSR SO.	Note: - Execute Appendix J again for Active SO if Active SO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby SO server upgraded above. **# ssh root@<SO IP>** **login as: root** **password: <enter password>** Execute following command on SO:- **[root@SO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR SO server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the SO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

4 ☐	Allow replication to SO servers.	Allow database replication to upgraded SO servers : 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active SO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that server.

5 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1.
		
		Execute following steps on both upgraded active and standby SOAMs :-
		
		1. Use your ssh client to connect to SOAM server.
		`ssh <SO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute following commands:
		
		`# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd`
		
		`# cd /usr/TKLC/dsr/bin`
		
		`# ./idb.initdd`
		
		`# init 6`
		
		Execute sub-steps 1 and 2 for second SO.

2.4..2.5 Upgrade MP(s)

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

Following Procedure is used to upgrade legacy Active-Standby MP Pair.

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

Procedure 17: Upgrade MP(s) of (1+1) 3-Tier configuration

S T E P #	This procedure upgrades the 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 MP Server by going to Status & Manage -> HA and record which MP server is Active and which is Standby.
2 ☐	Upgrade a Standby MP server (using Upgrade Single Server procedure)	Upgrade Standby MP server using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
3 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the Active MP to be upgraded :- 1. Log into the Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
4 ☐	Upgrade Active MP servers	Upgrade active MP server using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
5 ☐	Enable all the comagent connections disabled.	Enable all the comagent connections disabled :- 1. Log into the Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**

6 ☐	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. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** **Enable Site provisioning :-** 1. Log into the SOAM VIP GUI upgraded above. 2. Select **Status & Manage > Database** the Database Status screen gets 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. Login into DSR GUI. 2. Go to Status & Manage-> HA screen. 3. Click 'Edit' button. 4. 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. 5. Click 'Ok' button.
8 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the Active DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- 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** Repeat Steps 1 and 2 for Standby DA MP. Note :- Above steps will lead to MP switchover.
9 ☐	Install NetBackup 7.1 or 7.5 on NO and SO(If required)	Please refer to Appendix I.

1.4..2.6 Perform Health Check (Post-Upgrade of MPs)

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

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

Procedure 18: Perform Health Check (Post-Upgrade of MPs)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command, and determine if any errors were reported.

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed.
		Following Alarm ID will be observed on all the upgraded servers :-
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :-
		
		Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty):
		`ssh <server address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# 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`
		
		Follow Procedure 69 to suppress 32532 alarmId for all the servers.
		
		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 Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview.
End of second maintenance window		

Note: - If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 16 in another maintenance window.

3.4..3 DSR 4.x upgrade (N+0) 2 - tier configuration.

This section contains upgrade steps for DSR 4.x (2-tier setup) upgrade with (N+0) i.e. multiple Active configuration.

Table 8. Upgrade Execution Overview (For DSR 4.x (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 19	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 20	0:25-0:30	0:26-0:35	1:26-1:35	1:27-1:40	Upgrade NO(s) of (N+0) 2-Tier configuration.	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 21	0:02-0:05	0:28-0:40	0:02-0:05	1:29-1:45	Perform Health Check(Post Upgrade of NOAM)	None
Procedure 22	0:20-0:40	0:48-1:20	0:20-0:40	1:49-2:25	Upgrade Multiple MP(s) in 2-Tier Configuration	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 23	0:20-0:40	1:08-2:00	0:20-0:40	2:57-3:25	Upgrade IPFE(s) in 2-Tier Configuration	Traffic will not be handled by the MP(s) which is being upgraded.
Procedure 24	0:01-0:05 Per MP	1:09-2:05	0:01-0:05 Per MP	2:58-3:30	Perform Health Check(Post Upgrade of MPs)	None

3.4..3.1 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.

Procedure 19: Perform Health Check (Pre-Upgrade of NOAM)

S T E	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.

P #	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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets 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's status 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 gets 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.

3.4..3.2 Upgrade NOAM

Detailed steps are shown in the procedure below.

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

Procedure 20. Upgrade NO(s) of (N+0) 2-Tier configuration

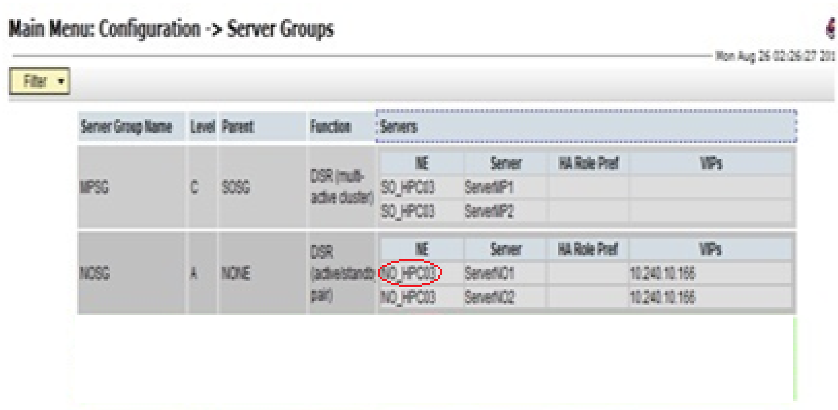
S T E P #	This procedure is used to perform NOAM upgrade successfully. This procedure is specific to 2-tier DSR OAM deployment. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**	
Start of 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.

2 ☐	Inhibit SOAP replication (If upgrading from DSR release < 40.19.0)	1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded 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** :- For e,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef** **Note: - This step needs to be executed only if upgrading from any release before 40.19.0.**
3 ☐	Inhibit replication to all 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). 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 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 the above steps to inhibit replication on MP(s), no alarms are raised on the GUI, indicating that replication on the MP is disabled. Replication inhibit on the MPs can be verified by analyzing NodeInfo output. The InhibitRepPlans field for all MP servers for the selected site (e.g. Site SO_HPC03) shall be set as 'A' :

```
[root@NO1 ~]# iqt NodeInfo
    nodeId          nodeName          hostName nodeCapability      inhibitRepPlans
                                                siteId excludeTables
  A1386.099            NO1             NO1       Active
                                   NO_HPC3
  B1754.109            SO1             SO1       Active
                                  NO_HPC03
  C2254.131            MP2             MP2       Active              A
                                  NO_HPC03
  C2254.233            MP1             MP1       Active              A
                                  NO_HPC3
```

Step	Description	Action
4 ☐	Inhibit replication to NO servers	**Inhibit database replication to the NO servers in the following order:** • Standby NO • Active NO 1. Select **Status & Manage > Database** The Database Status screen gets 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** 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 active servers last to prevent unwanted HA switchovers.**

4 ☐	Upgrade Standby NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby NO if Standby NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby NO server using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

5 ☐	Upgrade 2nd NO server.	Note: - Execute Appendix J again for Active NO if 2nd NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade the 2nd NO server (the mate) using the Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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** 4. Clear the browser cache after upgrade is completed.

6 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).

6.4..3.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 21: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
4 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1. Execute following steps on each of the upgraded NOAMs :- 1. Use your ssh client to connect to NOAM server. **ssh <NO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute following commands: **# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd** **# cd /usr/TKLC/dsr/bin** **# ./idb.initdd** **# init 6**

2.4..3.4 Upgrade Multiple MP(s)

Following Procedure is used to upgrade multiple MP(s) enclosure wise. This is used for OFCS also in this mate DSR is not present.

Procedure 22. Upgrade Multiple MP(s) in 2-Tier Configuration

S T E P #	This procedure upgrades the 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the MP(s) to be upgraded :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
2 ☐	Upgrade Active MPs	Upgrade all the MPs using the Upgrade Single Server procedure in parallel. Note: - User can choose any number of MP(s) on which upgrade can be executed in parallel. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
3 ☐	Enable all the comagent connections disabled in Step 1	Enable all the comagent connections disabled :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**
4 ☐	Update Max Allowed HA Role for NO.	1. Login into DSR GUI. 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.

5 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- 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** Repeat Steps 1 and 2 for each upgraded DA MP(s).
6 ☐	Install NetBackup 7.5 on NO (If required).	Please refer to Appendix I.

1.4..3.5 Upgrade IPFE(s)

Following Procedure is used to upgrade IPFE(s).

Procedure 23. Upgrade IPFE(s) in 2-Tier 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the IPFE(s) to be upgraded :- 1. Log into each Active IPFE command prompt :- Use your SSH client to connect to the server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**

2 ☐	Upgrade IPFE servers (if exists)	Upgrade IPFEs serially of both the enclosures using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Execute following steps :- a) Use ssh client to connect to each of the upgraded IPFE server :- **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** b) Execute following command on each upgraded IPFE server :- **# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh** c) Reboot each IPFE upgraded server using following command :- **# init 6**
3 ☐	IPFE: Edit the /etc/sysconfig/network file	Edit the /etc/sysconfig/network file: 1. Connect to each of the upgraded IPFE server. **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** 2. Check out /etc/sysconfig/network using rcstool for version control: **# rcstool co /etc/sysconfig/network** 3. Open /etc/sysconfig/network in a text editor (for example, vi) and append the following lines: **IPV6FORWARDING=yes** **IPV6_AUTOCONF=no** 4. Save your changes. 5. Check in your changes with a log message: **# rcstool ci /etc/sysconfig/network "909-2243-001 upgrade IPFE procedure"** 6. Type at the prompt of each upgraded IPFE server:- **#init 6** **Repeat Steps 1 to 6 for each upgraded IPFE server.**

4 ☐	Enable all the comagent connections disabled in Step 4	Enable all the comagent connections disabled :- 1. Log into each IPFE upgraded server, command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**
5 ☐	Enable 'A' level replication inhibited for MP(s)(**only if source upgrade release was less than 41.16.0)** **NOTE: Do not use VIP address when doing ssh to the servers for this step**	Enable A level replication disabled previously only if **source upgrade release was less than 41.16.0** :- 1. Log into Standby NO command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <NO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable A level replication :- **# ia.load /var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **# pm.set off inetrep** **# pm.set on inetrep** **Note: Re-verify if the replication inhibition gets removed successfully by executing the following command** **# iqt -h TableDef where "repPlanId='A'"** Records with Replication Plan set to A shall be displayed as the output of the above command. **Execute above Steps 1 and 2 for mated NO as well.**
6 ☐	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. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.**

4.4..3.6 Perform Health Check (Post-Upgrade of MPs)

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

Procedure 24: Perform Health Check (Post-Upgrade of MPs)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command, and determine if any errors were reported.

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed.
		Following Alarm ID will be observed on all the upgraded servers :-
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :-
		
		Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty):
		`ssh <server address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# 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`
		
		Follow Procedure 69 to suppress 32532 alarmId for all the servers.
		
		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 Post Upgrade Overview.	Execute Section Section 3.6 Post-Upgrade Overview
End of first maintenance window.		

3.4..4 DSR 4.x upgrade (N+0) 3 - tier configuration.

This section contains upgrade steps for DSR 4.x (3-tier setup) upgrade with (N+0) i.e. multiple Active configuration.

For large systems containing multiple Signaling Network Elements or multiple sites, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. Therefore all the Primary NOAMP and DR NOAMP Network Element servers should be upgraded within the same maintenance window. Followed by upgrade of SO(s) and MP(s) in separate maintenance window. Provisioning can be re-enabled (if required) after first maintenance window i.e. after both DR NOAMP(s) and primary NOAMP(s) are upgraded successfully.

Table 9. Upgrade Execution Overview (For DSR 4.x (N+0) 3 tier configuration)

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

			(with TVOE upgrade)	**(with TVOE upgrade)**		
Procedure 25	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 26	0:25-0:30	0:26-0:35	1:25-1:30	1:26-1:35	Upgrade NO(s) of (N+0) 3-Tier configuration	TVOE upgrade will stop all the applications running on it.
Procedure 27	0:02-0:05	0:28-0:40	0:02-0:05	1:28-1:40	Perform Health Check(Post Upgrade of NOAM)	None
Procedure 28	0:25-0:30	0:53-1:10	0:25-0:30	1:53-2:10	Upgrade SO(s) of (N+0) 3-Tier configuration	TVOE upgrade will stop all the applications running on it.
Procedure 29	0:10-0:30	1:03-1:40	0:10-0:30	2:03-2:40	Upgrade SBR(s) 3-Tier Configuration	None
Procedure 30	0:20-1:00	1:23-2:40	0:20-1:00	2:23-3:40	Upgrade Multiple MP(s) in 3-Tier Configuration	Traffic will not be handled by the MP(s) which are being upgraded.
Procedure 31	0:10-0:30	1:33-2:10	0:10-0:30	2:13-4:10	Upgrade IPFE(s) 3-Tier Configuration	None
Procedure 32	0:01-0:05 Per MP	1:34-3:15	0:01-0:05 Per MP	2:34-4:15	Perform Health Check(Post Upgrade of MPs)	None

3.4..4.1 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 NO and SO.

Procedure 25: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 4. Do not proceed to upgrade if any of the server's status 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 gets 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 above two steps for SO VIP GUI.

3.4..4.2 Upgrade NO (3-tier)

Detailed steps are shown in the procedure below.

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

WARNING! **IT IS RECOMENDED THAT ONLY NOAMP(s) BE UPGRADED IN SINGLE MAINTENENCE WINDOW. SEPARATE MAINTENANCE WINDOWS WILL BE REQUIRED FOR EACH SOAMP SITES.**

Procedure 26. Upgrade NO(s) of (N+0) 3-Tier configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.

2 ☐	Inhibit SOAP replication
	(If upgrading from DSR release < 40.19.0)
		1. Log into the Active NO command prompt :-
		
		Use your SSH client to connect to the upgraded 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** :-
		
		For e,g,
		
		`nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef`
		
		Note: - This step needs to be executed only if upgrading from any release before 40.19.0.

3 ☐	Inhibit replication toNO and SO servers.	Inhibit database replication to NO and SO servers in the following order: • All the Standby SO's(For each site) • All the Active SO's(For each site) • Standby NO • Active NO • Standby DR NO • Active DR NO 1. Select **Status & Manage > Database** The Database Status screen gets 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** 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 active servers last to prevent unwanted HA switchovers.**
4 ☐	Upgrade Standby DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby DR NO if DR NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR DR NO (if exists) using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

5 ☐	Upgrade Active DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active DR NO if Active DR NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby DR NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR DR NO (if exists) using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

6 ☐	Upgrade Standby DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby NO if standby NO is running on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR NO using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the NO server upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

7 ☐	Upgrade Active DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active NO if NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR NO using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0 :- 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** 4. Clear the browser cache after upgrade is completed.

8 ☐	Allow replication NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** 6. Repeat the **Allow** action link for Standby NO server. **Repeat steps 1 to 6 for DR NO(s) as well (if exists).** **Note: Replication to any SOAMs or 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).

6.4..4.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 27: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
4 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1. Execute following steps on each of the upgraded NOAMs :- 1. Use your ssh client to connect to NOAM server. **ssh <NO XMI IP address>** **login as: root** **password: <enter password>** 2. Execute following commands: **# sed -i 's/set -e/#set -e/'** **/usr/TKLC/dsr/bin/idb.initdd** **# cd /usr/TKLC/dsr/bin** **# ./idb.initdd** **# init 6**
End of first maintenance window.		
Provisioning can be re-enabled between maintenance windows.		

2.4..4.4 Upgrade SO (3-tier)

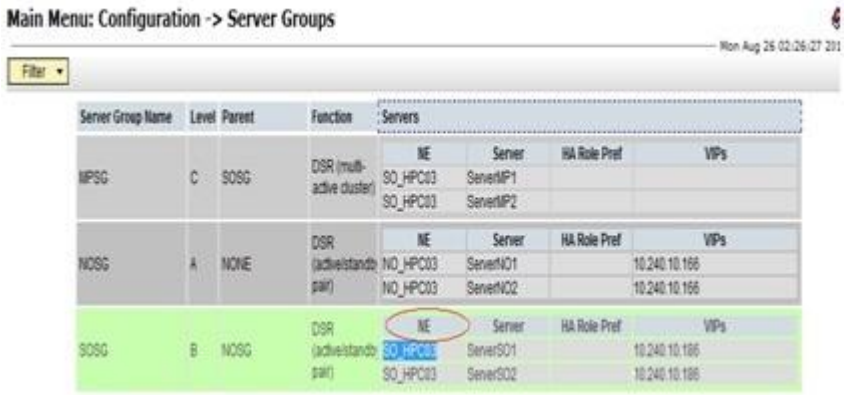
Detailed steps are shown in the procedure below.

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

Procedure 28. Upgrade SO(s) of (N+0) 3-Tier configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment 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 2nd Maintenance Window(If required)	
1 ☐	Disable Site Provisioning	Disable Site provisioning before starting with upgrade :- 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen gets 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 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`
		
		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 the above steps to inhibit replication on MP(s), no alarms are raised on the GUI, indicating that replication on the MP is disabled. Replication inhibit on the MPs can be verified by analyzing NodeInfo output. The InhibitRepPlans field for all 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 DSR SO	Note: - Execute Appendix J for Standby SO if standby SO is running on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR SO server using Upgrade Single Server procedure :- 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby SO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

4 ☐	Upgrade Active DSR SO.	Note: - Execute Appendix J for Active SO if SO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby SO server upgraded above. **# ssh root@<SO IP>** **login as: root** **password: <enter password>** Execute following command on SO:- **[root@SO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR SO server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the SO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0 :- 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**

5 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1. Execute following steps on both upgraded active and standby SOAMs :- 1. Use your ssh client to connect to SOAM server. **ssh <SOAM XMI IP address>** **login as: root** **password: <enter password>** 2. Execute following commands: **# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd** **# cd /usr/TKLC/dsr/bin** **# ./idb.initdd** **# init 6**

2.4..4.5 Upgrade SBR(s)

Following Procedure is used to upgrade SBR(s) enclosure wise.

Procedure 29. Upgrade SBR(s) in 3-Tier Configuration

S T E P #	This procedure upgrades the SBR(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, SBRs (both active and standby).
2 ☐	Find the active SBR(s) in the enclosure	Find and record Active and Standby SBR(s) in the enclosure by going to Status & Manage -> HA screen.

3 ☐	Upgrade SBRs in OFCS configuration (If exists)	1. Upgrade all the Standby cSBRs using the Upgrade Single Server procedure in parallel. – Execute Appendix G. – (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Upgrade all the New Standby cSBRs using the Upgrade Single Server procedure in parallel. – Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

2.4..4.6 Upgrade Multiple MP(s)

Following Procedure is used to upgrade multiple MP(s) enclosure wise. This is used for OFCS also in this mate DSR is not present.

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

Procedure 30. Upgrade Multiple MP(s) in 3-Tier Configuration

S T E P #	This procedure upgrades the 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the MP(s) to be upgraded :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
2 ☐	Upgrade Active MPs	Upgrade all the MPs using the Upgrade Single Server procedure in parallel. Note: - User can choose any number of MP(s) on which upgrade can be executed in parallel. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

3 ☐	Enable all the comagent connections disabled in Step 1	Enable all the comagent connections disabled :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**
4 ☐	Allow replication to SO servers.	Allow database replication to upgraded SO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active SO server. 4. Click Allow Replication button. 5. Verify the Inhibited text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).
5 ☐	Update Max Allowed HA Role for NO and SO.	1. Login into DSR GUI. 2. Go to Status & Manage-> HA screen. 3. Click 'Edit' button. 4. 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. 5. Click 'Ok' button.

6 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute following commands :- **# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force** **# sleep 20** **# prod.start** **# pm.sanity** Repeat Steps 1 and 2 for each upgraded DA MP(s).
7 ☐	Install NetBackup 7.5 on NO and SO (If required).	Please refer to Appendix I.

2.4..4.7 Upgrade IPFE(s)

Following Procedure is used to upgrade IPFE(s) enclosure wise.

Procedure 31. Upgrade IPFE(s) in 3-Tier 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the IPFE(s) to be upgraded :- 1. Log into each Active IPFE command prompt :- Use your SSH client to connect to the server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**

2 ☐	Upgrade IPFE servers (if exists)	Upgrade IPFEs serially of both the enclosures using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Execute following steps :- a) Use ssh client to connect to each of the upgraded IPFE server :- **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** b) Execute following command on each upgraded IPFE server :- **# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh** c) Reboot each IPFE upgraded server using following command :- **# init 6**
3 ☐	IPFE: Edit the /etc/sysconfig/network file	Edit the /etc/sysconfig/network file: 1. Connect to each of the upgraded IPFE server. **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** 2. Check out /etc/sysconfig/network using rcstool for version control: **# rcstool co /etc/sysconfig/network** 3. Open /etc/sysconfig/network in a text editor (for example, vi) and append the following lines: **IPV6FORWARDING=yes** **IPV6_AUTOCONF=no** 4. Save your changes. 5. Check in your changes with a log message: **# rcstool ci /etc/sysconfig/network "909-2243-001 upgrade IPFE procedure"** 6. Type at the prompt of each upgraded IPFE server:- **#init 6** **Repeat Steps 1 to 6 for each upgraded IPFE server.**

4 ☐	Enable all the comagent connections disabled in Step 4	Enable all the comagent connections disabled :- 1. Log into each IPFE upgraded server, command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**
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. 1. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** **Enable Site provisioning after upgrade is completed:-** 1. Log into the SOAM VIP GUI upgraded above. 2. Select **Status & Manage > Database** the Database Status screen gets 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**

4.4..4.8 Perform Health Check (Post-Upgrade of MPs)

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

.

Procedure 32: Perform Health Check (Post-Upgrade of MPs)

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 ☐	Allow replication disabled previously if **source upgrade release was less than 41.16.0** **NOTE: Do not use VIP address when doing ssh to the servers for this step**	Execute following command for both SO(s) only if **source upgrade release was less than 41.16.0** :- 1. Log into Active SO command prompt :- 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 following command on command prompt :- **# ia.load** **/var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **# pm.set off inetrep** **# pm.set on inetrep** **Note: Re-verify if the replication inhibition gets removed successfully by executing the following command** **# iqt -h TableDef where "repPlanId='A' or repPlanId='B'"** Records with Replication Plan set to A or B shall be displayed as the output of the above command. **Execute above Steps 1 and 2 for the mated SO as well.**
2 ☐	Verify Server Status is Normal	Verify Server Status is Normal: 1. Select **Status & Manage > Server;** the Server Status screen gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported.

3 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed.
		Following Alarm ID will be observed on all the upgraded servers :-
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :-
		
		Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty):
		`ssh <server address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# 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`
		
		Follow Procedure 69 to suppress 32532 alarmId for all the servers.
		
		2. Click **Report** button to generate an Alarms report.
		3. Save the report and print the report. Keep these copies for future reference.

4 ☐	Execute Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview
End of second maintenance window.		

Note: - If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 28 in another maintenance window.

3.4..5 DSR 3.x to DSR 4.x Major Upgrade ☐

For DSR 3.x major upgrade following are the upgrade steps.

Table 10. Upgrade Execution Overview(For DSR 3.x->4.x)

Procedure	Elapsed Time (Hours: Minutes)				Procedure title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 33	0:01-0:05	0:01-0:05	0:01-0:05	0:01-0:05	Perform Health Check(Pre-Upgrade of	None

					NOAM)	
Procedure 34	1:40-2:05	1.41-2.10	2:57-3:25	2:58-3:30	2 Tier DSR 3.x->4.x upgrade	Traffic will not be handled by the MP which is being upgraded.
Procedure 35	0:16-0:25	1:57-2:35	0:16-0:25	3:14-3:55	Perform Health Check(Post Upgrade of NOAM)	None
Procedure 36	0:08-0:15 Per MP	2:13-3:05	0:08-0:15 Per MP	3:30-4:20	Perform Health Check(Post Upgrade of MPs)	None

3.4..5.1 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.

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

Procedure 33: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 4. Do not proceed to upgrade if any of the server's status 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 gets 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.

3.4..5.2 DSR 3.x -> 4.x Upgrade Procedure

This procedure is used to upgrade DSR 3.x to DSR 4.x. For all the following DSR configurations this procedure can be followed:-

1. Legacy DSR 3.x upgrade
2. FABR DSR 3.x upgrade

Note: - Only 2 tier configuration is present in DSR 3.x.

Procedure 34. 2-Tier DSR 3.x->4.x upgrade

S T E P #	This procedure is specific to 2-tier DSR 3.x->4.x OAM upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE**.
Start of 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.
2 ☐	Disable all the connections configured.	NOTE: - Execute this step **ONLY** if mated site is present. Login to Active/Standby NO and check for the existence of **CONN_STATE_FILE** :- 1. 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 on Active NO :- **# ls /var/TKLC/db/filemgmt/CONN_STATE_FILE** 3. If the **CONN_STATE_FILE** already exists delete that file. Execute the following command:- **# rm -f /var/TKLC/db/filemgmt/CONN_STATE_FILE** Repeat Steps 1 and 3 for Standby NO. To automatically disable all the connections currently enabled, run following commands on command line :- **# cd /usr/TKLC/dpi/bin** **# ./connAdmDisableAll** **# scp /var/TKLC/db/filemgmt/CONN_STATE_FILE root@<STANDBY_NO_IP>:/var/TKLC/db/filemgmt** To manually disable all the connections currently enabled :- 1. Login into DSR GUI. 2. Go to Connections maintenance screen. 3. Disable all the enabled connections. 4. Make note of all the connections that were disabled in this step.

3 ☐	Inhibit SOAP replication	1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded 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** :- For e,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef**
4 ☐	Inhibit replication to all servers.	Inhibit database replication to all servers in the following order: • Standby MP's • Active MP's • Standby NO • Active NO 1. Select **Status & Manage > Database** The Database Status screen gets 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 active servers last to prevent unwanted HA switchovers.**
5 ☐	Upgrade Standby NO Server.	Note: - Execute Appendix J for Standby NO if Standby NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby NO server using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
6 ☐	Upgrade 2nd NO server.	1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root**

```
password:  <enter password>
```

Execute following command on NO:-

```
[root@NO1 ~]# pl | grep "cmha"
```

Following output shall 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
```

Note: Please continue with sub step 2. Start_cmha will start cmha process once Active Node moves to Force Standby.

2. Make Active NO upgrade 'Ready', if TVOE needs to be upgraded using following steps:-
   a) Select Administration > Upgrade; the Upgrade Administration screen gets displayed.
   b) Select the Active NO.
   c) Click the "Prepare Upgrade" button; the Upgrade [Make Ready] screen gets displayed.
   d) Click OK; this starts the Make Ready action on the server. The Upgrade Administration screen gets displayed.

   Note: The Make Ready action WILL cause an HA switchover. The HA switchover is an expected outcome from the Make Ready action. The HA switchover will cause the session to be logged out. If Logged out then Log in back into the DSR 3.x/4.x GUI.

3. Execute Appendix J again for Active NO if 2nd NO is on different TVOE blade before proceeding with below mentioned steps.

4. Upgrade the 2nd NO server (the mate) using the Upgrade Single Server procedure:

Execute Appendix G.
(Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

5. Clear the browser cache after upgrade is completed.
6. Login to Active NO and execute following command :-

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

# cd /usr/TKLC/dsr/prod/maint/loaders/upgrade

# ./load.dsr.upgrade.4.0.10+HaVipDefUpdates
```

7 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).

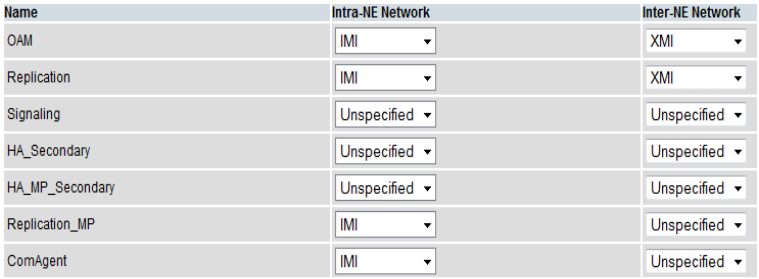
8 ☐	Fix up the measurement retention for DSR 4.0 servers.	Note: Execute following steps only if target upgrade release is 4.0. Following steps are not required for DSR 4.1.
		
		Execute following steps on each of the upgraded NOAMs :-
		
		1. Use your ssh client to connect to NOAM server.
		`ssh <NO XMI IP address>`
		
		`login as: root`
		`password: <enter password>`
		
		2. Execute following commands:
		
		`# sed -i 's/set -e/#set -e/' /usr/TKLC/dsr/bin/idb.initdd`
		
		`# cd /usr/TKLC/dsr/bin`
		
		`# ./idb.initdd`
		
		`# init 6`

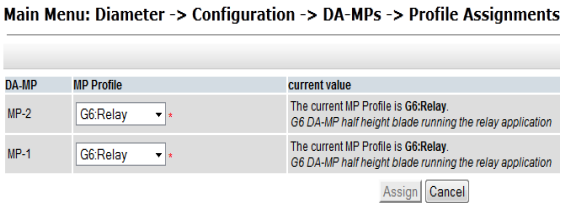
9 ☐	Disable comagent connections (if FABR/CPA is configured) and upgrade MP.	**If 1+1 configuration :-** Disable all the comagent connections associated with the Standby MP to be upgraded :- 1. Log into the Standby MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1** 3. Upgrade standby MP server using the below mentioned procedure :- a) Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) **If N+0 configuration :-** Choose half of the Active MP(s) to upgrade and disable all the comagent connections(if exists) :- 1. Log into the each Active MP which needs to be upgraded :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1** 3. Upgrade the MP Server(s) for which connections are disabled above in parallel follow the procedure mentioned below:- a) Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

10 ☐	Enable all comagent connections disabled for upgrade in step 9.	1. Log into the MP command prompt for each MP upgraded in Step 9:- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**
11 ☐	Disable comagent connections and Upgrade remaining MPs.	Disable all the comagent connections associated with the left over MP(s) to be upgraded for both 1+1 and N+0 configurations :- 1. Log into the left over Active MP(s) command prompt which needs to be upgraded :- **Use your SSH client to connect to the upgraded server (ex. ssh, putty):** **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1** Upgrade Left over MP(s) .Execute the following procedure in parallel for all the MP(s) left to be upgraded:- 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
12 ☐	Enable comagent connections disabled for upgrade in Step 11.	1. Log into the Active MP command prompt for each MP upgraded in Step 11:- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**

<table>
<tr>
<td>13
☐</td>
<td>Enable Global Provisioning and Configuration.</td>
<td>Enable Provisioning and Configuration updates on the entire network:

Provisioning and configuration updates may be enabled to the entire network.

1. Login to the Active Network OAM NE using the VIP
2. Select Status & Manage > Database
The Database Status screen gets displayed.
3. Click Enable Provisioning button.
4. Verify the text of the button changes to Disable Provisioning.</td>
</tr>
<tr>
<td>14
☐</td>
<td>Update services for MP(s).</td>
<td>1. Login to the Active Network OAM GUI using the VIP
2. Select Configuration > Services
The Services screen gets displayed.
3. Click Edit button.
4. Set the Intra-NE Network for ComAgent and Replication_MP to be the same as the value that is set for the Intra-NE Network of Replication.
For example if your Replication service has an Intra-NE network of “IMI”, then “IMI” should be selected as the Intra-NE for both ComAgent and Replication-MP.
 
<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>OAM</td><td>IMI</td><td>XMI</td></tr>
<tr><td>Replication</td><td>IMI</td><td>XMI</td></tr>
<tr><td>Signaling</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>HA_MP_Secondary</td><td>Unspecified</td><td>Unspecified</td></tr>
<tr><td>Replication_MP</td><td>IMI</td><td>Unspecified</td></tr>
<tr><td>ComAgent</td><td>IMI</td><td>Unspecified</td></tr>
</table>
5. Click ‘Ok’ button.</td>
</tr>
</table>

15 ☐	Assign the MP profiles	From the Active NO GUI, select **Main Menu->Diameter->Configuration->DA-MPs->Profiles Assignments**  For each MP, select the proper profile assignment based on the MP's hardware type and the function it will serve: Profile Name / Description: G6:Relay — G6 DA-MP half height blade running relay application G6:Database — G6 DA-MP half height blade running a database application G6:Session — G6 DA-MP half height blade running a session application G8:Relay — G8 DA-MP half height blade running the relay application G8:Database — G8 DA-MP half height blade running a database application G8:Session — G8 DA-MP half height blade running a session application G7:Relay — G7 DA-MP Full height blade running the relay application G7:Database — G7 DA-MP Full height blade running a database application G7:Session — G7 DA-MP Full height blade running a session application When finished, press the Assign button.	
16 ☐	Restart MP blade servers	From the NOAMP GUI, select the **Main menu->Status & Manage->Server** menu For each MP server: • Select the MP server. • Select the Restart button. • Answer OK to the confirmation popup. Wait for the message which tells you that the restart was successful.	

17 ☐	Enable all fixed diameter connections.	NOTE: - Execute this step **ONLY** if mated site is present. Before enabling connections make sure that all the MP upgrades are successful. To automatically enable all the connections that were previously disabled, run following commands on command line :- **# cd /usr/TKLC/dpi/bin** **# ./connAdmEnableAll** To manually enable all the connections disabled previously :- 1. Login into DSR GUI. 2. Go to Connections maintenance screen. 3. Enable all the connections that were disabled previously.	

3.a).5.3 Perform Health Check (Post-Upgrade of NOAM)

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

Procedure 35: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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 Follow Procedure 69 to suppress 32532 alarmId for all the upgraded servers(NO/SO) in following order :- a) Accept upgrade for standby NO. Wait till server reboots and is back in service. b) Accept upgrade for Active NO. Wait till server reboots and is back in service.
2 ☐	Turn Off COMCOL compatibility mode if upgrade is accepted for all the servers in Step1	Please follow Procedure 68 to turn off COMCOL compatibility mode.
3 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**

3.a).5.4 Perform Health Check (Post-Upgrade of MPs)

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

Procedure 36: Perform Health Check (Post-Upgrade of MPs)

S T	This procedure performs a Health Check.

E P #	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 for all the MP(s): 1. Select **Status & Manage > Server;** the Server Status screen gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported.
2 ☐	Log all current alarms	Log all current alarms for all MP(s) in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed. Following Alarm ID will be observed on all the upgraded servers :- Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :- Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# 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** Follow Procedure 69 to suppress 32532 alarmId for all the upgraded MP servers in following order :- a) Accept upgrade for standby MP. Wait till server reboots and is back in service. b) Accept upgrade for Active MP. Wait till server reboots and is back in service. 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 Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview
End of first maintenance window.		

3.a).6 Incremental upgrade for 3 tier RMS configuration(N+0)

This section contains upgrade steps for DSR 4.x (3-tier setup) incremental upgrade on RMS servers.

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)

This section covers the incremental upgrade steps for single site. For multi-site setup this section can be followed sequentially for each site which needs to be upgraded. For large systems containing multiple Signaling Network Elements or multiple sites, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. Therefore all the Primary NOAMP and DR NOAMP Network Element servers should be upgraded within the same maintenance window. Followed by upgrade of SO(s) and MP(s) in separate maintenance window. Provisioning can be re-enabled (if required) after first maintenance window i.e. after both DR NOAMP(s) and primary NOAMP(s) are upgraded successfully.

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

Table 11. Upgrade Execution Overview (For DSR 4.x RMS 3-tier (N+0) configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 37	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 38	0:25-0:30	0:26-0:35	1:25-1:30	1:26-1:35	Upgrade NO(s) of 3-Tier RMS configuration	TVOE upgrade will stop all the applications running on it.
Procedure 39	0:01-0:05	0:27-0:40	0:01-0:05	1:27-1:40	Perform Health Check(Post Upgrade of NOAM)	None

Procedure 40	0:25-0:30	0:52-1:10	0:25-0:30	1:52-2:10	Upgrade SO(s) of 3-Tier RMS configuration	TVOE upgrade will stop all the applications running on it.
Procedure 41	0:20-1:00	1:12-2:10	0:20-1:00	2:12-3:10	Upgrade IPFE(s) in 3-Tier RMS Configuration	None
Procedure 42	0:20-1:00	1:32-3:10	0:20-1:00	2:32-4:10	Upgrade Multiple MP(s) in 3-Tier RMS Configuration	Traffic will not be handled by the MP(s) which is being upgraded.
Procedure 43	0:01-0:05 Per MP	1:33-3:15	0:01-0:05 Per MP	2:33-4:15	Perform Health Check(Post Upgrade of MPs)	None

4)a).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 NO and SO.

Procedure 37: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 4. Do not proceed to upgrade if any of the server's status 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 gets 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.

3.a).6.2 Upgrade NO (3-tier)

Detailed steps are shown in the procedure below.

WARNING! **IT IS RECOMENDED THAT ONLY NOAMP(s) BE UPGRADED IN SINGLE MAINTENENCE WINDOW. SEPARATE MAINTENANCE WINDOWS WILL BE REQUIRED FOR EACH SOAMP SITES.**

Procedure 38. Upgrade NO(s) of 3-Tier RMS configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier RMS deployment 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 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.

3 ☐	Inhibit replication to NO and SO servers.	Inhibit database replication to NO and SO servers in the following order: • All the Standby SO's(For each site) • All the Active SO's(For each site) • Standby NO • Active NO • Standby DR NO • Active DR NO 1. Select **Status & Manage > Database** The Database Status screen gets 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** 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 active servers last to prevent unwanted HA switchovers.**
4 ☐	Upgrade Standby DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby DR NO if DR NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR DR NO (if exists) using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

5 ☐	Upgrade Active DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active DR NO if Active DR NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby DR NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR DR NO (if exists) using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

6 ☐	Upgrade Standby DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby NO if standby NO is running on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR NO using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the NO server upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

7 ☐	Upgrade Active DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active NO if NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR NO using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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** 4. Clear the browser cache after upgrade is completed.

8 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** 6. Repeat the **Allow** action link for Standby NO server. **Repeat steps 1 to 6 for DR NO(s) as well (if exists).** **Note: Replication to any SOAMs or 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).

6.a).6.3 Perform Health Check (Post-Upgrade of NO)

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

Procedure 39: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
End of first maintenance window		
Provisioning can be re-enabled between maintenance windows.		

3.a).6.4 Upgrade SO (3-tier)

Detailed steps are shown in the procedure below.

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

Procedure 40. Upgrade SO(s) of 3-Tier RMS configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier RMS deployment 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 2nd Maintenance Window(If required)	
1 ☐	Disable Site Provisioning Disable Site provisioning before starting with upgrade :- 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen gets 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 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** :

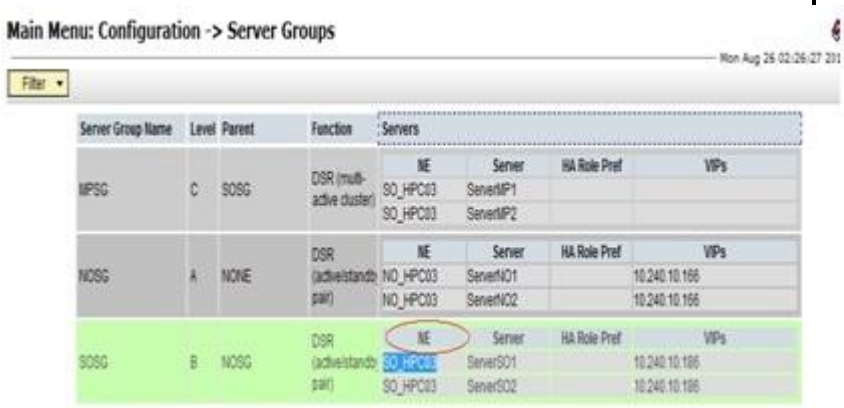
Log into Active NO(if logged out, else ignore this step) :

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

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 the above steps to inhibit replication on MP(s), no alarms are raised on the GUI, indicating that replication on the MP is disabled. Replication inhibit on the MPs can be verified by analyzing NodeInfo output. The InhibitRepPlans field for all 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 DSR SO	Upgrade Standby DSR SO server using Upgrade Single Server procedure :- 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby SO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

4 ☐	Upgrade Active DSR SO.	1. Login to standby SO server upgraded above. **# ssh root@<SO IP>** **login as: root** **password: <enter password>** Execute following command on SO:- **[root@SO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR SO server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the SO upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

3.a).6.5 Upgrade IPFE(s)

Following Procedure is used to upgrade IPFE(s).

Procedure 41. Upgrade IPFE(s) in 3-Tier 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the IPFE(s) to be upgraded :- 1. Log into each Active IPFE command prompt :- Use your SSH client to connect to the server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
2 ☐	Upgrade IPFE servers	Upgrade IPFEs serially of both the RMS servers using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Execute following steps :- a) Use ssh client to connect to each of the upgraded IPFE server :- **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** b) Execute following command on each upgraded IPFE server :- **# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh** c) Reboot each IPFE upgraded server.

3 ☐	IPFE: Edit the /etc/sysconfig/network file	Edit the /etc/sysconfig/network file: 1. Connect to each of the upgraded IPFE server. **ssh <each upgraded IPFE server>** **login as: root** **password: <enter password>** 2. Check out /etc/sysconfig/network using rcstool for version control: **# rcstool co /etc/sysconfig/network** 3. Open /etc/sysconfig/network in a text editor (for example, vi) and append the following lines: **IPV6FORWARDING=yes** **IPV6_AUTOCONF=no** 4. Save your changes. 5. Check in your changes with a log message: **# rcstool ci /etc/sysconfig/network "909-2243-001 upgrade IPFE procedure"** 6. Type at the prompt of each upgraded IPFE server:- **#init 6** **Repeat Steps 1 to 6 for each upgraded IPFE server.**
4 ☐	Enable all the comagent connections disabled in Step 2	Enable all the comagent connections disabled :- 1. Log into each IPFE upgraded server, command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**

2.a).6.6 Upgrade Multiple MP(s)

Following Procedure is used to upgrade multiple MP(s).

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

Procedure 42. Upgrade Multiple MP(s) in 3-Tier RMS Configuration

S T E P #	This procedure upgrades the 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 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the MP(s) to be upgraded :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
2 ☐	Upgrade Active MPs	Upgrade all the MPs using the Upgrade Single Server procedure in parallel. Note: - User can choose any number of MP(s) on which upgrade can be executed in parallel. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
3 ☐	Enable all the comagent connections disabled in Step 3	Enable all the comagent connections disabled :- 1. Log into each Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**

4 ☐	Allow replication to SO servers.	Allow database replication to upgraded SO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active SO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes). Execute following command on Active SO only if **source upgrade release was less than 41.16.0** (Do not use VIP address when doing ssh to the servers for this step) :- 1. Log into Standby SO command prompt :- 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 following command on command prompt :- **# ia.load** **/var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **# pm.set off inetrep** **# pm.set on inetrep** **Note: Re-verify if the replication inhibition gets removed successfully by executing the following command** **# iqt -h TableDef where "repPlanId='A' or repPlanId='B'"** Records with Replication Plan set to A or B shall be displayed as the output of the above command. **Execute above Steps 1 and 2 for mated SO as well.**

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. 1. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** **<u>Enable Site provisioning after upgrade is completed:-</u>** 1. Log into the SOAM VIP GUI upgraded above. 2. Select **Status & Manage > Database** the Database Status screen gets 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**
6 ☐	Update Max Allowed HA Role for NO and SO.	1. Login into DSR GUI. 2. Go to Status & Manage-> HA screen. 3. Click 'Edit' button. 4. 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. 5. Click 'Ok' button.
7 ☐	Upgrade DIH (if present)	Please refer DIH upgrade document for the same.
8 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute following commands :- **# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force** **# sleep 20** **# prod.start** **# pm.sanity** Repeat Steps 1 and 2 for all upgraded DA MP(s).
9 ☐	Install NetBackup 7.5 on NO and SO (If required).	Please refer to Appendix I.

2.a).6.7 Perform Health Check (Post-Upgrade of MPs)

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

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

Procedure 43: Perform Health Check (Post-Upgrade of MPs)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported.

2 ☐	Log all current alarms	Log all current alarms in the system:
		
		1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed.
		Following Alarm ID will be observed on all the upgraded servers :-
		Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
		
		Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :-
		
		Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty):
		`ssh <server address>`
		
		`login as: root`
		`password: <enter password>`
		
		`# 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`
		
		Follow Procedure 69 to suppress 32532 alarmId for all the servers.
		
		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 Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview.
End of second maintenance window		

Note: - If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 38 in another maintenance window.

3.a).7 Incremental upgrade for 3 tier RMS configuration (1+1)

This section contains upgrade steps for DSR 4.x (3-tier setup) incremental upgrade on RMS servers.

The following commercial deployment types are supported:

5) 2 RMS servers, one site, no DIH
6) 3 RMS servers, one site, with one server reserved for DIH (and DIH Storage)
7) 4 RMS servers, 2 sites with 2 servers per site, no DIH
8) 6 RMS servers, 2 sites with 3 servers per site, 1 server at each site reserved for DIH (and DIH Storage)

This section covers the incremental upgrade steps for single site. For multi-site setup this section can be followed sequentially for each site which needs to be upgraded. For large systems containing multiple Signaling Network Elements, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. Therefore all the Primary NOAMP Network Element servers should be upgraded within the same maintenance window. Followed by upgrade of SO(s) and MP(s) in separate

maintenance window. For multiple maintenance windows, replication may be allowed and provisioning re-enabled between scheduled maintenance windows.

Table 12. Upgrade Execution Overview (For DSR 4.x RMS 3-tier (1+1)configuration)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 44	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 45	0:25-0:30	0:26-0:35	1:25-1:30	1:26-1:35	Upgrade NO(s) of 3-Tier RMS configuration	TVOE upgrade will stop all the applications running on it.
Procedure 46	0:01-0:05	0:27-0:40	0:01-0:05	1:27-1:40	Perform Health Check(Post Upgrade of NOAM)	None
Procedure 47	0:25-0:30	0:52-1:10	0:25-0:30	1:52-2:10	Upgrade SO(s) of 3-Tier RMS configuration	TVOE upgrade will stop all the applications running on it.
Procedure 48	0:20-1:00	1:22-2:10	0:20-1:00	2:22-3:10	Upgrade DA MP in 3-Tier RMS Configuration	None
Procedure 49	0:01-0:05 Per MP	1:23-2:15	0:01-0:05 Per MP	2:23-3:15	Perform Health Check(Post Upgrade of MPs)	None

8)a).7.1 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 NO and SO.

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

Procedure 44: 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 VIP GUI 2. Select **Status & Manage > Server;** the Server Status screen gets displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 4. Do not proceed to upgrade if any of the server's statusdisplayed 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 gets 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.

3.a).7.2 Upgrade NO (3-tier)

Detailed steps are shown in the procedure below.

WARNING!

IT IS RECOMENDED THAT ONLY NOAMP(s) BE UPGRADED IN SINGLE MAINTENENCE WINDOW. SEPARATE MAINTENANCE WINDOWS WILL BE REQUIRED FOR EACH SOAMP SITES.

Procedure 45. Upgrade NO(s) of 3-Tier RMS configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier RMS deployment 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 1st 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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.
2 ☐	Inhibit replication to all servers.	Inhibit database replication to all the servers in the following order: • Standby MP's • Active MP's • Standby SO's • Active SO's • Standby NO • Active NO • Standby DR NO • Active DR NO 1. Select **Status & Manage > Database** The Database Status screen gets 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** 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 active servers last to prevent unwanted HA switchovers.**

3 ☐	Upgrade Standby DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby DR NO if DR NO is hosted on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR DR NO (if exists) using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

4 ☐	Upgrade Active DSR DR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active DR NO if Active DR NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby DR NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR DR NO (if exists) using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

5 ☐	Upgrade Standby DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Standby NO if standby NO is running on TVOE blade before proceeding with below mentioned steps. Upgrade Standby DSR NO using Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby NO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

6 ☐	Upgrade Active DSR NO server (using Upgrade Single Server procedure).	Note: - Execute Appendix J for Active NO if NO is on different TVOE blade before proceeding with below mentioned steps. 1. Login to standby NO upgraded above. **# ssh root@<NO IP>** **login as: root** **password: <enter password>** Execute following command on NO:- **[root@NO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR NO using Upgrade Single Server procedure: Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the NO upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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** 4. Clear the browser cache after upgrade is completed.

7 ☐	Allow replication to NO servers.	Allow database replication to NO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active NO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the server**.** 6. Repeat the **Allow** action link for Standby NO server. **Repeat steps 1 to 6 for DR NO(s) as well (if exists).** **Note: Replication to any SOAMs or 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).

6.a).7.3 Perform Health Check (Post-Upgrade of NO)

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

Procedure 46: 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/SO servers upgraded: 1. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 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 32532 AlarmId 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers.
2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view gets 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 ☐	Check the presence of backupDB.cron file	Execute following commands on each NO after upgrade is completed :- Use your SSH client to connect to each upgraded NO server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# cd /etc/cron.d** **# ls -ltr | grep 'backupDB.cron'** Following output shall be generated :- **-rw-r--r-- 1 root root 1330 Dec 4 01:02 backupDB.cron** If backupDB.cron is not present then execute following command :- **# cp /usr/TKLC/appworks/sbin/backupDB.cron /etc/cron.d**
End of first maintenance window		
Provisioning can be re-enabled between maintenance windows.		

3.a).7.4 Upgrade SO (3-tier)

Detailed steps are shown in the procedure below.

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

Procedure 47. Upgrade SO(s) of 3-Tier RMS configuration.

S T E P #	This procedure verifies that the OAM blade with TVOE platform upgrade steps has been completed. This Procedure is specific to 3-tier RMS deployment 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 2nd Maintenance Window(If required)	
1 ☐	Disable Site Provisioning Disable Site provisioning before starting with upgrade :- 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen gets 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 DSR SO	Upgrade Standby DSR SO server using Upgrade Single Server procedure :- 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Log into the Standby SO upgraded in Step 1 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

3 ☐	Upgrade Active DSR SO.	1. Login to standby SO server upgraded above. **# ssh root@<SO IP>** **login as: root** **password: <enter password>** Execute following command on SO:- **[root@SO1 ~]# pl | grep "cmha"** Following output shall 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** 2. Upgrade Active DSR SO server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 3. Log into the SO server upgraded in Step 2 above only if target upgrade release is less than 4.1.0-41.19.0:- 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**

3.a).7.5 Upgrade Active-Standby DA MP(s)

Following Procedure is used to upgrade multiple MP(s).

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

Procedure 48. Upgrade Active-Standby DA MP(s) in 3-Tier RMS Configuration

S T E P #	This procedure upgrades the 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 ☐	Upgrade Standby MP	Upgrade standby MP using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
2 ☐	Disable all the comagent connections.	Disable all the comagent connections associated with the Active MP to be upgraded :- 1. Log into the Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to disable all the comagent connections :- **# iset -fadminState=Disabled ComAgtConnectionAdmin where 1=1**
3 ☐	Upgrade Active MP servers	Upgrade active MP server using the Upgrade Single Server procedure. 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
4 ☐	Enable all the comagent connections disabled.	Enable all the comagent connections disabled :- 1. Log into the Active MP command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute the following command to enable all the comagent connections :- **# iset -fadminState=Enabled ComAgtConnectionAdmin where 1=1**

5 ☐	Allow replication to SO servers.	Allow database replication to upgraded SO servers: 1. Select **Status & Manage > Database** 2. The Database Status screen gets displayed. 3. Select the Active SO server. 4. Click **Allow Replication** button**.** 5. Verify the ***Inhibited*** text is not displayed for the 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.** After the Allow action, server HA requires time to recover (up to 3 minutes).
6 ☐	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. Login to the Active Network OAM NE using the VIP 2. Select **Status & Manage > Database** The Database Status screen gets displayed. 3. Click **Enable Provisioning** button. 4. Verify the text of the button changes to **Disable Provisioning.** **<u>Enable Site provisioning after upgrade is completed:-</u>** 5. Log into the SOAM VIP GUI upgraded above. 6. Select **Status & Manage > Database** the Database Status screen gets displayed 7. Click **Enable Site Provisioning** button. 8. Confirm the operation by clicking **Ok** in the popup dialog box. Verify the button text changes to **Disable Site Provisioning**
7 ☐	Update Max Allowed HA Role for NO and SO.	1. Login into DSR GUI. 2. Go to Status & Manage-> HA screen. 3. Click 'Edit' button. 4. 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. 5. Click 'Ok' button.
8 ☐	Upgrade DIH (if present)	Please refer DIH upgrade document for the same.

9 ☐	Execute Optimization commands for each upgraded DA MP(s) only if target upgrade release is less than 4.1.0-41.19.0.	1. Log into the Standby DA MP command prompt only if target upgrade release is less than 4.1.0-41.19.0 :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** 2. Execute following commands :- **# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force** **# sleep 20** **# prod.start** **# pm.sanity** Repeat Steps 1 and 2 for Active DA MP
10 ☐	Install NetBackup 7.5 on NO and SO (If required).	Please refer to Appendix I.

2.a).7.6 Perform Health Check (Post-Upgrade of MPs)

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

Procedure 49: Perform Health Check (Post-Upgrade of MPs)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). 3. Execute following commands on the upgraded servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported.

2 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active**; the Alarms & Events > View Active view gets displayed. Following Alarm ID will be observed on all the upgraded servers :- Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** Note :- If 32532 AlarmId is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :- Use your SSH client to connect to the each upgraded server which did not raise the alarm Id 32532(ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# 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** Follow Procedure 69 to suppress 32532 alarmId for all the servers. 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 Post Upgrade Overview.	Execute Section 3.6 Post-Upgrade Overview
End of second maintenance window		

Note: - If another site needs to be upgraded, please start following all the steps sequentially starting from Procedure 47 in another maintenance window.

3.a).8 Incremental upgrade for 3 - tier Policy DRA configuration

This section contains upgrade steps for DSR 4.x (3-tier P-DRA setup) upgrade with (N+0) i.e. multiple Active configuration.

For large systems containing multiple Signaling Network Elements or multiple sites, it may not be feasible to apply the software upgrade to every Network Element within a single maintenance window. Therefore all the Primary NOAMP and DR NOAMP Network Element servers should be upgraded within the same maintenance window. Followed by upgrade of SO(s) and MP(s) in separate maintenance window. Provisioning can be re-enabled (if required) after first maintenance window i.e. after both DR NOAMP(s) and primary NOAMP(s) are upgraded successfully.

Table 13. Upgrade Execution Overview (For 3 tier Policy DRA configuration Site 1)

Procedure	Elapsed Time (Hours: Minutes)				Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
Procedure 50	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 51	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 52	1:00-1:20	3:10-3:50	1:00-1:20	5:10-5:50	Policy SBR Upgrade – Site 1	
Procedure 53	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 54	0:30-1:00	4:40-6:50	0:30-1:00	6:40-8:20	IPFE Server Upgrade – Site 1	None
Procedure 55	0:01-0:05	4:41-6:55	0:01-0:05	6:41-8:25	Post Upgrade Steps	None
Procedure 56	0:10-0:15	4:51-7:10	0:10-0:15	6:51-8:35	Perform Health Check (Upgrade Preparation)	None

3.a).8.1 Maintenance Window 1 – Site (e.g. Lab-C)

This procedure is used to upgrade the NO servers in a mated pair.

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

Procedure 50. 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 SOAP replication of the HaResourceCfg table during incremental upgrade
	(If upgrading from DSR release < 40.19.0)
		On Active NOAMP ILO Terminal, execute the command:
		
		`#iset -fexcludeTables='HaResourceCfg HaNodeLocPref HaVipDef' NodeInfo where "1=1"`
		
		Verify that the NodeInfo table is updated with HaResourceCfg, HaVipDef and HaNodeLocPref entries under the –fexcludeTables column.
		
		Execute the following command on Active NOAM ILO
		#ivi NodeInfo
		
		`#!/bin/sh`
		`iload -ha -xU -fnodeId -fnodeName -fhostName -fnodeCapability \`
		`-finhibitRepPlans -fsiteId -fexcludeTables NodeInfo \`
		`<<'!!!!'`
		`A1954.015|labEe2b2dsrnob|labEe2b2dsrnob|Active||SSSTNOAMNE|HaResourceCfg HaNodeLocPref HaVipDef`
		`A1954.027|labEe1b1dsrnoa|labEe1b1dsrnoa|Active||SSSTNOAMNE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B0235.129|labFe2b1dsrsoa|labFe2b1dsrsoa|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B0235.130|labFe2b1dsrsob|labFe2b1dsrsob|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B0235.192|labEe2b2dsrsoc|labEe2b2dsrsoc|Spare||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B2803.042|labEe1b1dsrsoa|labEe1b1dsrsoa|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B2803.043|labEe1b2dsrsob|labEe1b2dsrsob|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`B2803.077|labFe1b2dsrsoc|labFe1b2dsrsoc|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C0501.057|labEe1b15ipfeA1|labEe1b15ipfeA1|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C0781.012|labFe1b16ipfeA1|labFe1b16ipfeA1|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1023.047|labFe2b15ipfeA2|labFe2b15ipfeA2|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1502.015|labFe2b6pdra4|labFe2b6pdra4|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1502.168|labFe2b3pdra1|labFe2b3pdra1|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1502.169|labFe2b4pdra2|labFe2b4pdra2|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1502.170|labFe2b5pdra3|labFe2b5pdra3|Active||SO_LABFSONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1681.092|labEe1b3pdra1|labEe1b3pdra1|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1681.093|labEe1b4pdra2|labEe1b4pdra2|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1681.150|labEe1b5pdra3|labEe1b5pdra3|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`
		`C1681.151|labEe1b6pdra4|labEe1b6pdra4|Active||SO_LABESONE|HaResourceCfg HaNodeLocPref HaVipDef`

2 ☐	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 gets 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) Before beginning upgrade, global provisioning and configuration updates must be disabled for the entire network.
3 ☐	Inhibit replication to MP servers.	**Replication of C level MP servers will be inhibited during site upgrade.**

4 ☐	Inhibit replication to all the SOAM Servers of each Site.	Inhibit database replication to all the SOAM servers in the following order**(for each Site)**: • All the Spare SO(s) (For each site) • All the Standby SO(s) (For each site) • All the Active SO(s) (For each site) 1. Select **Status & Manage > Database** The Database Status screen gets 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 SO servers in the order shown above. **NOTE: Inhibit the replication of the active servers last to prevent unwanted HA switchovers.**
5 ☐	Inhibit replication to all the NO and DR NO Servers	Inhibit database replication to all the NO and DR NO servers in the following order: • Standby DR NOAM(if applicable) • Active DR NOAM(if applicable) • Standby NO • Active NO 1. Select **Status & Manage > Database** The Database Status screen gets 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 NO servers in the order shown above. **NOTE: Inhibit the replication of the active servers last to prevent unwanted HA switchovers.**
6 ☐	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: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

8 ☐	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 DSR DR NO (if exists) using the Upgrade Single Server procedure: 1. Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.) 2. Clear the browser cache after upgrade is completed.
9 ☐	Allow replication to NO and DR NO servers only.	Allow database replication to all 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 gets 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: Allow the replication of the active servers first to prevent unwanted HA switchovers.**
10 ☐	Remove excluded tables from NodeInfo.	On Active NOAMP ILO Terminal, execute the command: `#iset -fexcludeTables='' NodeInfo where "1=1"`
End of maintenance window 1		
THIS PROCEDURE HAS BEEN COMPLETED		

5.a).8.2 Maintenance Window 2 – Site (e.g. Lab-C)

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 51. TVOE Upgrade and SO Servers Upgrade

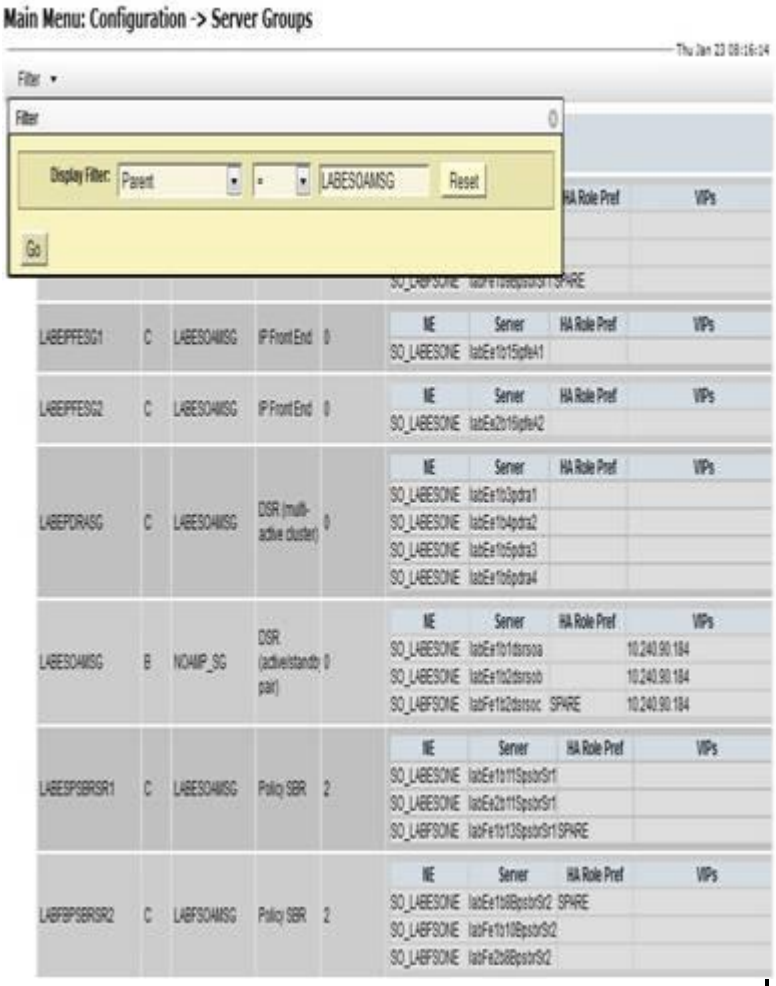
S T E P #		This procedure upgrade the TVOE of SOAM guests(if required) and upgrades SOAM servers of Site 1. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for **UPGRADE ASSISTANCE.**
		Start of maintenance window 2
1 ☐	Disable Site Provisioning	Disable Site provisioning before starting with upgrade :- 1. Log into the SOAM VIP GUI which needs to be upgraded. 2. Select **Status & Manage > Database** the Database Status screen gets 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 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='A`

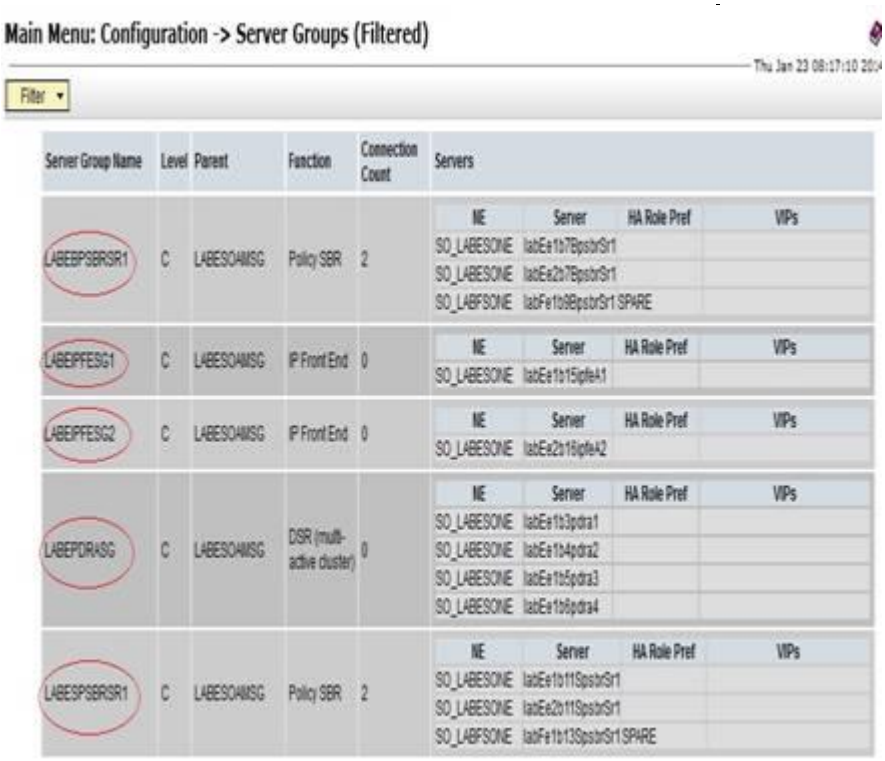
```
B'  NodeInfo where "nodeId like '$i*'"; done
```

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)



For e.g. Filtered output will look like :



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

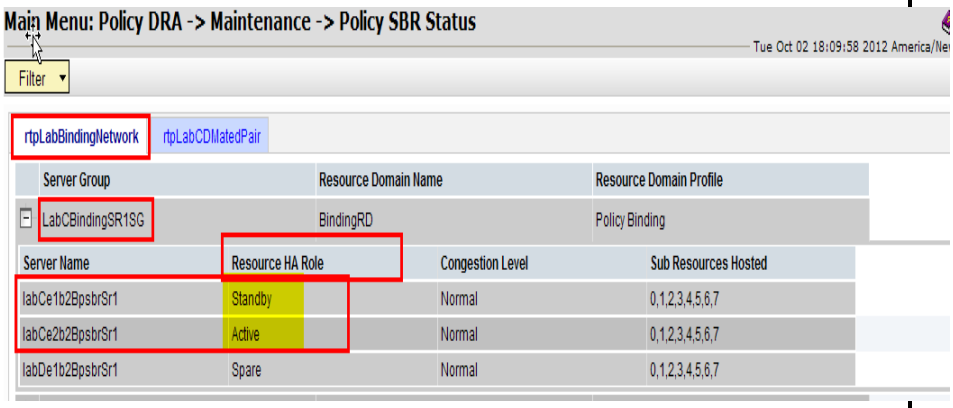
An e.g:

```
#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
```

3 ☐	Upgrade Standby DSR SO and Spare SO in parallel.	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 DSR SO server and spare SO in parallel using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
5 ☐	Allow replication to SO servers of the upgraded site ONLY (**This site – e.g. Lab C**).	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.**
		THIS PROCEDURE HAS BEEN COMPLETED

11.a).8.3 Policy SBR MP Server Upgrade

Procedure 52. 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 upgarde. The following figure provides and 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.** Step 1: Upgrade Standby Policy SBR and spare Policy SBR server server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

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. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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.
THIS PROCEDURE HAS BEEN COMPLETED		

4.a).8.4 Policy DRA Server Upgrade

Procedure 53. Policy DRA Upgrade – 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) server using Upgrade Single Server procedure :- Execute Appendix G. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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.
THIS PROCEDURE HAS BEEN COMPLETED		

1.a).8.5 IPFE Server Upgrade

Procedure 54. 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(LabC)	From the data captured in Table 3, 1. Pick one "**IP Front End**" Server Group in Site 1. 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. (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

3 ☐	Execute the following steps on the IPFE.	1. Ssh/connect as 'root' to into IPFE XMI IP address/ iLO
		2. Execute the performance update script:
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		3. Reboot the IPFE server using following command :
		`# init 6`

4 ☐	IPFE: Edit the /etc/sysconfig/network file	Edit the /etc/sysconfig/network file:
		1. Connect to each of the upgraded IPFE server.
		`ssh <each upgraded IPFE server>`
		`login as: root`
		`password: <enter password>`
		2. Check out /etc/sysconfig/network using rcstool for version control:
		`# rcstool co /etc/sysconfig/network`
		3. Open /etc/sysconfig/network in a text editor (for example, vi) and append the following lines:
		`IPV6FORWARDING=yes`
		`IPV6_AUTOCONF=no`
		4. Save your changes.
		5. Check in your changes with a log message:
		`# rcstool ci /etc/sysconfig/network "909-2243-001 upgrade IPFE procedure"`
		6. Type at the prompt of each upgraded IPFE server:-
		`#init 6`
		Repeat Steps 1 to 6 for each upgraded IPFE server.

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

6.a).8.6

Post Maintenance Window 2 – Site 1(e.g. Lab-C) – Post Upgrade Execution

Procedure 55. Site 1: Post Upgrade Steps

S T E P #		
	NOTE: Execute this step after Site 1 have 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 41.16.0)**
	
	NOTE: Do not use VIP address when doing ssh to the servers for this step
		Enable replication disabled previously only if **source upgrade release was less than 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 :-
		`# ia.load /var/TKLC/db/filemgmt/$(hostname).TableDef.backup`
		
		`# pm.set off inetrep`
		`# pm.set on inetrep`
		`Note: Re-verify if the replication inhibition is removed successfully by executing the following command`
		`# iqt -h TableDef where "repPlanId='A' or repPlanId='B'"`
		Records with Replication Plan set to A or B shall be displayed as the output of the above command.
		
		Execute above Steps 1 and 2 for upgraded mated 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 gets 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 upgraded site. 5. Select **Status & Manage > Database** the Database Status screen gets 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**

3 ☐	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**
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**

7.a).8.7

Maintenance Window 2 – Site 1(e.g. Lab-C) – Post Upgrade Health Check

This procedure is part of Post Maintenance Window 2 health check and is used to determine the health and status of the Policy DRA (DSR) network and servers after the Site 1 is upgraded completely. These steps compare data captured after upgrade with pre-upgrade health check data captured in Procedure 5

Procedure 56: Perform Health Check (Post-Upgrade Steps)

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.

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. Binding Region b. PDRAMatedSites 3. 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.
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.

Procedure 57. SITE 1 UPGRADE COMPLETE – STOP

S T E P #	THIS IS END OF MAINTENENCE WINDOW 2	
1 ☐	Execute signaling traffic on upgrade site 1 and verify that everything is okay.	1. Get a confirmation from customer before continuing to upgrading the second site.
End of maintenance window 2		

1.a).8.8 Maintenance Window 3 – Site 2 (e.g. Lab-D)

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

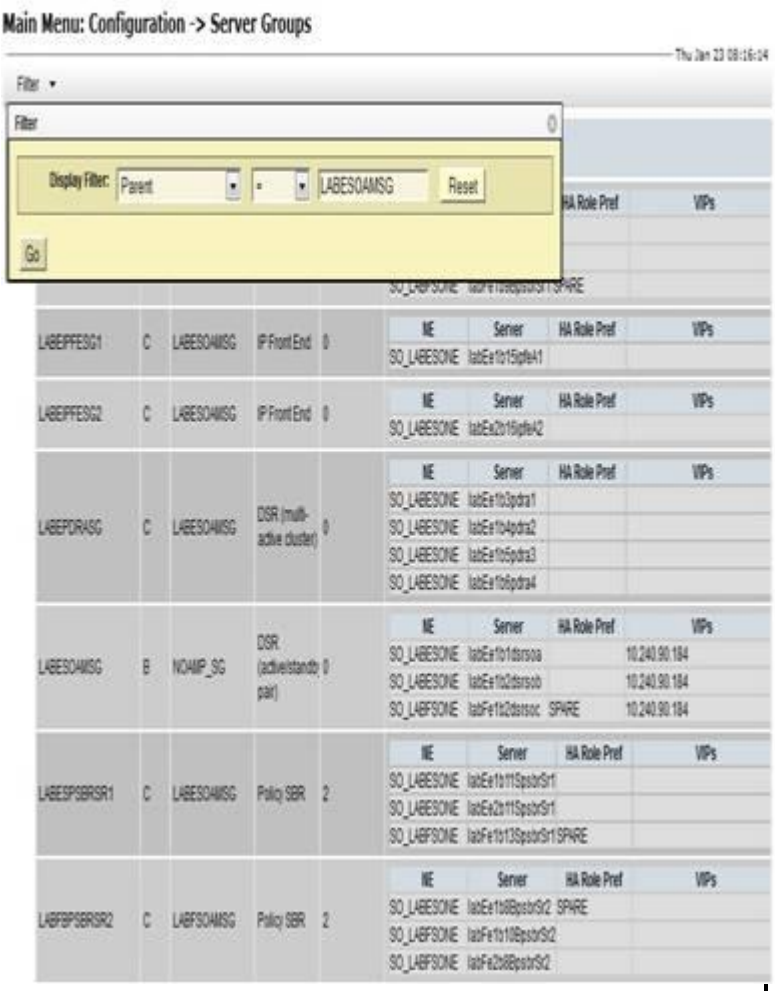
Procedure 58. TVOE Upgrade and OAM Servers Upgrade

S T E P #	This procedure provides steps to upgradeTVOE platform for OAM blade and steps to upgrade the SOAMs for LabD 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 ☐	Disable Site Provisioning Disable Site provisioning before starting with upgrade :- 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

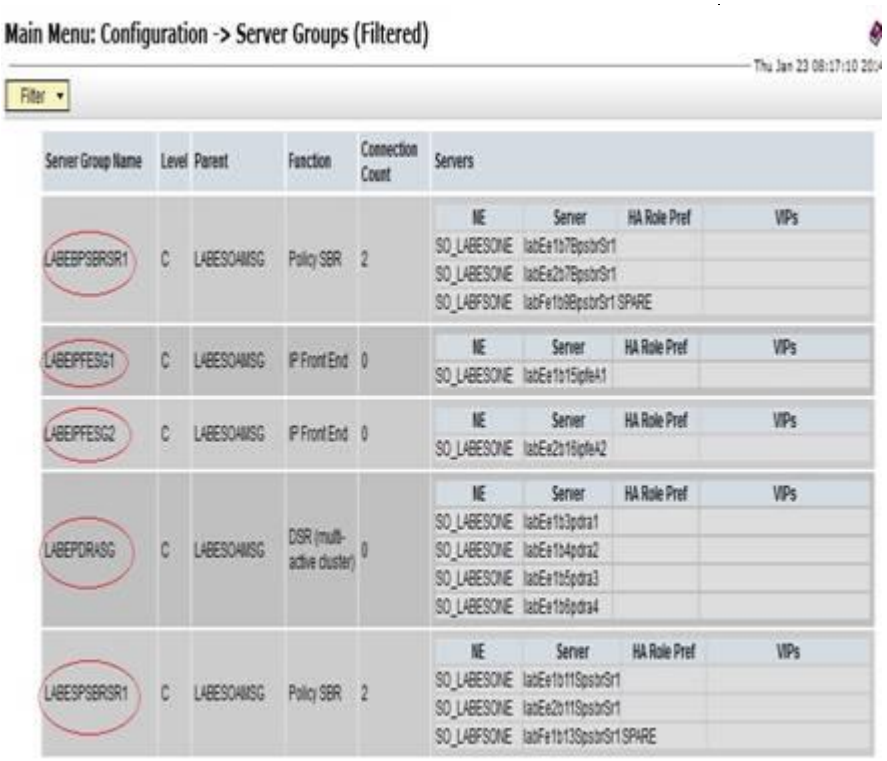
2 ☐	Inhibit replication to PDRA and pSBR MP servers.	**Record current release number___ex: 4.0.2_40.27.3_____**
		
		• **IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G Step 13). In this 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 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 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 :


Main Menu: Configuration -> Server Groups (Filtered)

Thu Jan 23 08:17:10 20

Filter

Server Group Name	Level	Parent	Function	Connection Count	Servers			
					NE	Server	HA Role Pref	VIPs
LABEBPSBRSR1	C	LABESOAMSG	Policy SBR	2	SO_LABESONE	labEe1b7BpsbrSr1		
					SO_LABESONE	labEe2b7BpsbrSr1		
					SO_LABFSONE	labFe1b9BpsbrSr1	SPARE	
LABEIPFESG1	C	LABESOAMSG	IP Front End	0	NE	Server	HA Role Pref	VIPs
					SO_LABESONE	labEe1b15ipfeA1		
LABEIPFESG2	C	LABESOAMSG	IP Front End	0	NE	Server	HA Role Pref	VIPs
					SO_LABESONE	labEe2b16ipfeA2		
LABEPDRASG	C	LABESOAMSG	DSR (multi-active cluster)	0	NE	Server	HA Role Pref	VIPs
					SO_LABESONE	labEe1b3pdra1		
					SO_LABESONE	labEe1b4pdra2		
					SO_LABESONE	labEe1b5pdra3		
					SO_LABESONE	labEe1b6pdra4		
LABESPSBRSR1	C	LABESOAMSG	Policy SBR	2	NE	Server	HA Role Pref	VIPs
					SO_LABESONE	labEe1b11SpsbrSr1		
					SO_LABESONE	labEe2b11SpsbrSr1		
					SO_LABFSONE	labFe1b13SpsbrSr1	SPARE	

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

An e.g:

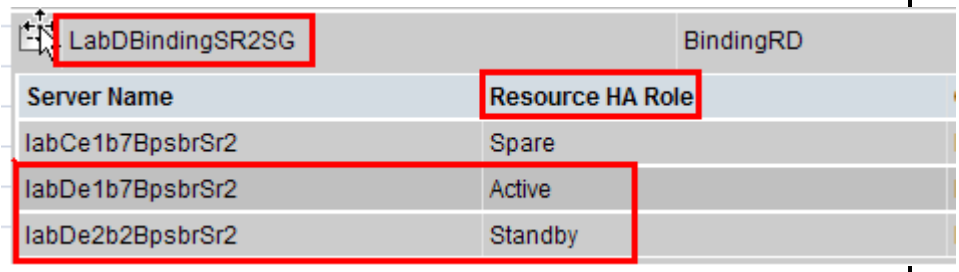
```
#srvrGrps="'LABEPDRASG','LABEBPSBRSR1','LABESPSBRSR1','LABEIPFESG1','LABEIPFESG2'";for i in $(iqt -p -z -h -fclusterId ServerGroup where "ServerGroupName in ($srvrGrps)");do iset -finhibitRepPlans='A B'  NodeInfo where "nodeId like '$i*'"; done
```

3 ☐	Upgrade Standby DSR SO and spare So in parallel.	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 DSR SO and spare DSR SO in parallelusing Upgrade Single Server procedure :- Execute Appendix G (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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 (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
5 ☐	Allow replication to SO servers of the upgraded site ONLY (**This site – e.g. Lab D**).	Allow database replication to SO servers of the currently upgraded site: 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.**

THIS PROCEDURE HAS BEEN COMPLETED

11.a).8.9 Policy SBR MP Server Upgrade

Procedure 59. Policy SBR Upgrade – Site 2

S T E P #	Policy SBR upgrade procedure for Site 2 Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the 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 
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 (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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 (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

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.
THIS PROCEDURE HAS BEEN COMPLETED		

4.a).8.10 Policy DRA Server Upgrade

Procedure 60. Policy DRA Upgrade – Site 2

S T E P #	Policy DRA server (DA-MP Server) upgrade procedure for Site 2 Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the 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 (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)
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.
THIS PROCEDURE HAS BEEN COMPLETED		

1.a).8.11 IPFE Server Upgrade

Procedure 61. 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 2	From the data captured in Table 3, 1. Pick one of the "**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 (Make note of this step. After executing the procedure above, return to this point and continue executing the remainder of the upgrade procedure.)

3 ☐	Execute the following steps on the IPFE.	1. Ssh/connect as 'root' to into IPFE XMI IP address/ iLO
		2. Execute the performance update script:
		`# /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh`
		3. Reboot the IPFE server using following command :
		`# init 6`

4 ☐	IPFE: Edit the /etc/sysconfig/network file	Edit the /etc/sysconfig/network file:
		1. Connect to each of the upgraded IPFE server.
		`ssh <each upgraded IPFE server>`
		`login as: root`
		`password: <enter password>`
		2. Check out /etc/sysconfig/network using rcstool for version control:
		`# rcstool co /etc/sysconfig/network`
		3. Open /etc/sysconfig/network in a text editor (for example, vi) and append the following lines:
		`IPV6FORWARDING=yes`
		`IPV6_AUTOCONF=no`
		4. Save your changes.
		5. Check in your changes with a log message:
		`# rcstool ci /etc/sysconfig/network "909-2243-001 upgrade IPFE procedure"`
		6. Type at the prompt of each upgraded IPFE server:-
		`#init 6`
		Repeat Steps 1 to 4 for each upgraded IPFE server.

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

6.a).8.12 Post upgrade steps

Procedure 62. Site 2: Post Upgrade Steps

S T E P #	NOTE: Execute this step after site 2 have 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 41.16.0)** **NOTE: Do not use VIP address when doing ssh to the servers for this step**	Enable replication disabled previously only if **source upgrade release was less than 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 :- **# ia.load** **/var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **# pm.set off inetrep** **# pm.set on inetrep** **Note: Re-verify if the replication inhibition gets removed successfully by executing the following command** **# iqt -h TableDef where "repPlanId='A' or repPlanId='B'"** Records with Replication Plan set to A or B shall be displayed as the output of the above command. **Execute above Steps 1 and 2 for upgraded mated 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 gets 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 gets 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**

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`

7.a).8.13

Maintenance Window 3 – Site 2(e.g. Lab-D) – Post Upgrade Health Check

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 63: Perform Health Check (Post-Upgrade steps)

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 servers 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 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 for 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 **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 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 2 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 3		

4.6 Post-Upgrade Overview

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 14. Post-Upgrade Procedure Overview

Procedure	Elapsed Time (Hours: Minutes)		Procedure Title	Impact
	This Step	Cum.		
Procedure 64	0:05-0:10	0:05-0:10	Perform Health Check (Software Upgrade Completion)	Software is upgraded with target release software.

4.6.1 Perform Health Check (Software Upgrade Completion)

This procedure is used to determine the health and status of the DSR 3.x/4.x network and servers.

Procedure 64: Perform Health Check (Software Upgrade Completion)

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 gets displayed. 2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting Status, 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 gets 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 ☐	Allow SOAP replication inhibited previously (If upgrading from DSR release < 40.19.0 and upgrade is already accepted)	If **upgrade is accepted** then execute following steps :- 1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **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 40.19.0.**
4 ☐	Clean up the upgrade ISO from PM&C	Login to PM&C server and clean up any ISOs no longer used at that site using below mentioned steps (for e.g. source release ISO(s)):- Log onto the PM&C GUI and navigate to **Software** -> **Software Configuration** -> **Manage Software Images screen :-** 1. Select all the images added during upgrade. 2. Click on 'Delete Image' button. 3. Click on **Task Monitoring** to monitor the progress, and wait for the **Progress Bar** to turn green.
5 ☐	Update value of Ingress MPS Percentile.	1. If IPFE is not configured move to step 2. Else, execute following command on both **Active NO and Active SO(if exists)** to find out the capacity configuration sets having Reserved Ingress MPS > 0 :- **ssh <Active NO and Active SO>** **login as: root** **password: <enter password>** **# iqt CapacityCfgSet where "reservedIngressMpsCapacity > 0";** If output of the above command does not return any rows then go to Step 2. Else exit this step. 2. Execute following command on **both Active NO and Active SO(if exists)** to update MpEngIngressMpsPercentile value :- **ssh <Active NO and Active SO>** **login as: root** **password: <enter password>** **# iset -fvalue=50 DpiOption where "name='MpEngIngressMpsPercentile'";**

6 ☐	Check if the setup previously have customer supplied certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	1. Verify if the setup had customer supplied 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.

2.7 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 is for a "Lab Environment", and that they might vary on Live Systems.

Table 15. 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 65	See Note	See Note	Backout 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.
Procedure 67	0:01-0:05	0:11-0:35	Perform Health Check (Post-Backout)	None

4. RECOVERY PROCEDURES

Upgrade procedure recovery issues should be directed to the Tekelec Customer Care Center. 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). Persons performing the upgrade should be familiar with these documents.

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.

4.1 Backout Setup

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

1. Select **Administration > Upgrade**
2. Based on the "Application Version" Column, Identify all the hostnames that need to be backed out.
3. Select **Configuration > Servers**
4. Identify the iLO IP addresses of all the hostnames identified in step 2. 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 3.x/4.x:-

NOTE: **Verify that the two backup archive files created using the procedure in section 3.3.3.3are present on every server that is to be backed-out.** These archive files are located in the /var/TKLC/db/filemgmt directory and have different filenames than other database backup files. The filenames will have the format

Backup.<application>.<server>.**FullDBParts**.<role>.<date_time>.**UPG**.tar.bz2

And

Backup. <application>.<server>.**FullRunEnv**.<role>.<date_time>.**UPG**.tar.bz2

4.2 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 as stated in the **Warning** box above to identify if all corrective setup steps have been taken.

4.2.1 Backout Entire Network

Detailed steps are shown in the sections below.

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

Procedure 65: Backout Entire Network

S T E P #	This procedure will back out an upgrade of DSR 3.x/4.x application software and can be used for MPs and NOs. 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 > Upgrade** The Upgrade Administration screen gets 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. 4. Execute all the remaining steps on the servers that require a 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 gets 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)

3 ☐	Inhibit SOAP replication (If backing out from DSR 4.0 system before or equal to 40.19.0 release)	1. Log into the Active NO command prompt :- Use your SSH client to connect to the upgraded 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** :- For e,g, **nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03 excludeTables= HaNodeLocPref HaVipDef** **Note: - This step needs to be executed only if backing out from any release before or equal to 40.19.0.**
4 ☐	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).
5 ☐	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.

6 ☐	Backout Standby MP Servers, Standby cSBR(s) and Standby pSBR(s) if exists	Backout **Standby MP** servers i.e servers with HA Status as Standby. Following servers can be backed out in parallel (whichever exists) 1. Standby MP(s) 2. Standby cSBR(s) 3. Standby pSBR(s) 4. Spare pSBR(s) Following procedure can be used for backout of each server :- Execute Section 4.2.2, Procedure 66: Backout Single Server.
7 ☐	Backout MP Server(s).(IPFE(s),cSBR(s) and DA MP(s) whichever exists)	Backout **MP server** (the mate, if dealing with a server pair),Else backout all the remaining IPFE(s),SBR(s), pSBR(s) and DA MP(s) in parallel Execute Section 4.2.2, Procedure 66: Backout Single Server.
8 ☐	Backout Spare DA MP Server(s).(If exists)	Backout spare **DA MP server** : Execute Section 4.2.2, Procedure 66: Backout Single Server.
9 ☐	Backout DSR Standby SO Server (If exists).	Backout Standby **DSR SO** server: Execute Section 4.2.2, Procedure 66: Backout Single Server.
10 ☐	Backout Left over DSR SO Server (If exists).	Backout Leftover **DSR SO** server: Execute Section 4.2.2, Procedure 66: Backout Single Server.
11 ☐	Backout Standby DR NO Server (if exists).	Backout **Primary Standby DR NO** server: Execute Section 4.2.2, Procedure 66: Backout Single Server.
12 ☐	Backout 2nd DR NO Server (if exists).	Backout **2nd Primary DR NO server** (the mate): Execute Section 4.2.2, Procedure 66: Backout Single Server.
13 ☐	Backout Standby NO Server.	Backout **Primary Standby NO** server: Execute Section 4.2.2, Procedure 66: Backout Single Server.
14 ☐	Backout 2nd NO Server.	Backout **2nd Primary NO server** (the mate): Execute Section 4.2.2, Procedure 66: Backout Single Server.

15 ☐	Backout 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 VIP GUI
		b) Select **Status & Manage > Server;** the Server Status screen gets 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`
		
		Backout TVOE current blade, refer TVOE upgrade document [3].

16 ☐	Enable Virtual Guest Watchdogs if disabled previously	1. Please follow Procedure 3.12.1 of [9]document to Enable Virtual Guest Watchdogs If disabled for TVOE blade backed out, Else execute following steps:- a) Login to 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 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 gets 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 15. **Execute Steps 15 and 16 again for another TVOE blade hosting NO/SO (if exists) which could have upgraded previously.**
17 ☐	Allow replication to NO servers.	**Note: - If major backout from DSR 4.x to DSR 3.x is performed then clear the browser cache before continuing with below mentioned steps.** Allow database replication to NO servers: 1. Select **Status & Manage > Database** the Database Status screen gets displayed. 2. Select the Active NO server. 3. Click **Allow Replication** button. 4. Verify the ***Inhibited text*** is not displayed for server. 5. Repeat the allow substeps, 3 through 4, for Standby NO server. **Repeat steps 1 to 5 for DR NO(s) as well (if exists).** **Note: Replication to any SOAMs or 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. . After the Allow action, server HA requires time to recover (up to 3 minutes). OAM Report Status is shown as Auditing, and then becomes Normal.

18 ☐	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 displays. 2. Select the Active SO server. 3. Click **Allow Replication** button**.** 4. Verify the ***Inhibited*** text is not displayed for the server**.** 5. Repeat the **Allow** action link for Standby SO server. After the Allow action, server HA requires time to recover (up to 3 minutes). 6. Repeat 1) to 5) for all remaining SO servers in all Signaling NEs.
19 ☐	Allow replication MP servers.	Allow database replication to MP servers(leaving PSBR servers): The following steps are to be executed for all MP servers in all Signaling NEs(leaving PSBR servers). 1. Select **Status & Manage > Database** the Database Status screen gets displayed. 2. Select the Active MP server. 3. Click **Allow Replication** button. 4. Verify the ***Inhibited text*** is not displayed for the server. 5. Repeat the **Allow** action link for Standby MP server (if dealing with a server pair). After the Allow action, server HA requires time to recover (up to 3 minutes). 6. While server HA is recovering, monitor Server Status for recovery. Select **Status & Manage > Servers** The Server Status screen gets 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 1) to 9) for all remaining MP servers in all Signaling NEs(leaving PSBR servers).
20 ☐	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.
21 ☐	Enable Global Provisioning and Configuration.	Enable Global Provisioning and Configuration updates on the entire network: Login to Active NO GUI :- 1. Select **Status & Manage > Database** The Database Status screen gets displayed. 2. Click **Enable Provisioning** button. 3. Verify the button text changes to **Disable Provisioning.** Login to Active SO GUI :- 1. Select **Status & Manage > Database** The Database Status screen gets displayed. 2. Click **Enable Site Provisioning** button. If site provisioning is disabled, Else move to next Step. 3. Verify the button text changes to **Disable Site Provisioning.**

22 ☐	Remove 'Ready' state (if exists) for any backed out server	From DSR 3.x/4.x Active NO GUI :- 1. Select Status & Manage > Servers; the Server Status screen gets displayed. 2. If the any of the backed-out servers Application Status is 'Disabled', then select and press the Restart button. 3. Select **Administration > Upgrade;** the Upgrade Administration screen gets 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

23 ☐	Allow SOAP replication inhibited previously (If backing out from DSR 4.0 system before or equal to 40.19.0 release)	1. Log into the Active NO command prompt :-
		
		Use your SSH client to connect to the upgraded server (ex. ssh, putty):
		`ssh <server address>`
		
		`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 backing out from any release before or equal to 40.19.0.

2.2.2 Backout Single Server

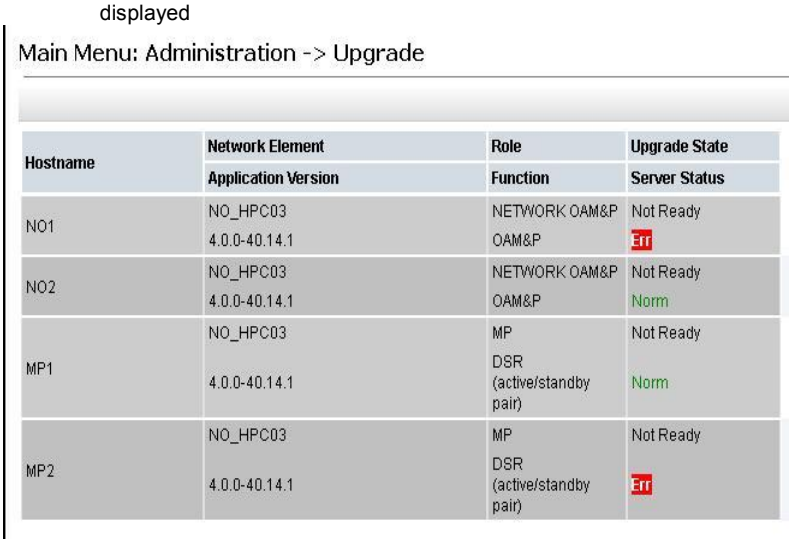
Detailed steps are shown in the procedure below.

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

Procedure 66: Backout Single Server

S T E P #	This procedure will back out an upgrade of DSR 3.x/4.x application software and can be used for MPs and NOs. 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:

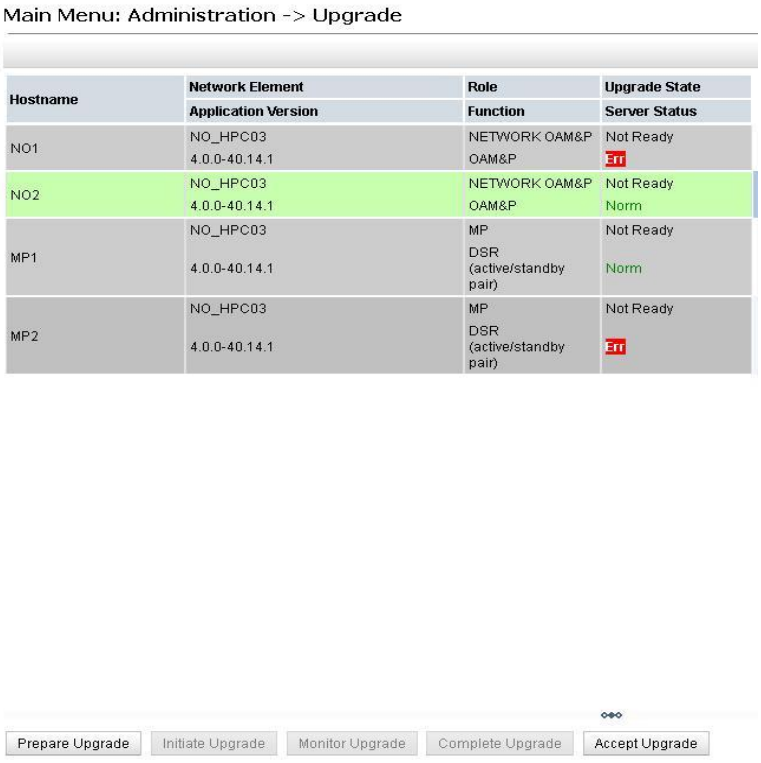
1. Select **Administration >Upgrade;** the Upgrade Administration screen gets displayed


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)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

2. Select the server to backout and check its upgrade state :-
   a) If the upgrade state is “Ready” then press “Complete Upgrade” button.
   b) Else, select the server to be downgraded and press the **Prepare Upgrade** button.

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

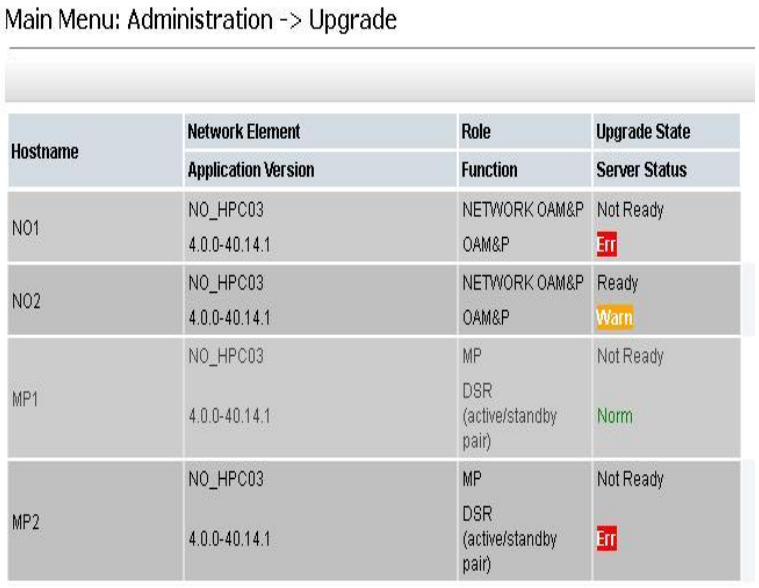

Main Menu: Administration -> Upgrade

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)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

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

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**.



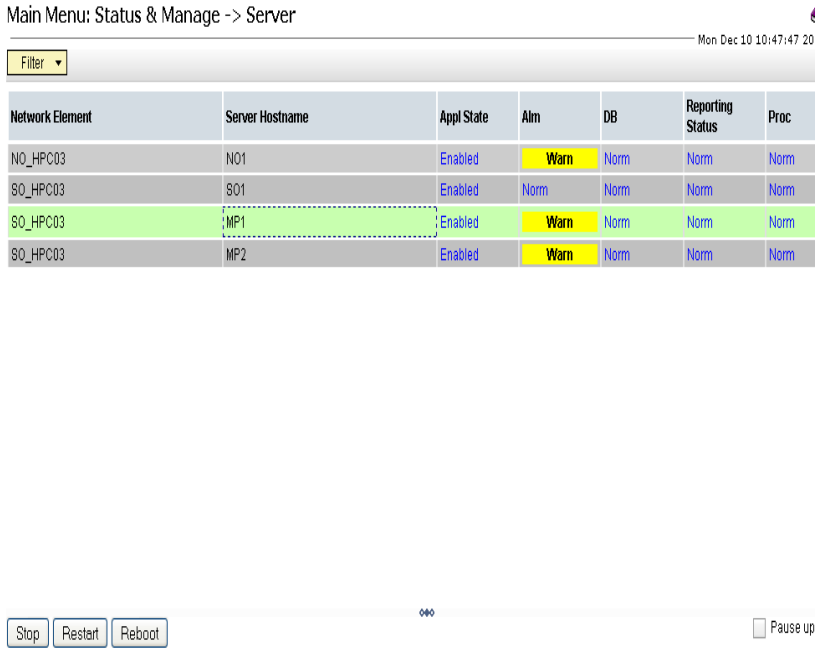
		Note: If this is the Active server in an Active-Standby pair, the Make Ready action WILL cause an HA switchover. The HA switchover is an expected outcome from the Make Ready action. ***Note: Preparing a server for upgrade performs the required preparation steps for backout as well.***
2 ☐	SSH to server	Use your SSH client to connect to the server iLO (ex. ssh, putty): Note: You must consult your own software client's documentation to learn how to launch a connection. For example: **# ssh Administrator@<server iLO address>** **password:** **</>hpiLO-> vsp** Starting virtual serial port. Press 'ESC (' to return to the CLI Session. Press the "Enter" key to obtain access to the login prompt if it is not displayed. Note: If you do not have direct access to the iLO or if TVOE is installed on blades, 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>**
8 ☐	Verify the Backout	1. Execute following commands on the backed out servers :- Use your SSH client to connect to the upgraded server (ex. ssh, putty): **ssh <server address>** **login as: root** **password: <enter password>** **# verifyUpgrade** Examine the output of the above command to determine if any errors were reported. 2. If the backout was not successful because other errors were recorded in the logs, then contact Tekelec Customer Care Center for further instructions. 3. If the backout was successful (no errors or failures), then continue with the remaining steps.
9 ☐	Restore the full DB run environment for DSR 3.x/4.x only	Execute the backout_restore utility to restore the full database run environment: **# screen** **# /var/tmp/backout_restore** **NOTE**: If asked 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 for further instructions.
10 ☐	Reboot the server	Enter the following command to reboot the server: **# init 6** This step can take several minutes.

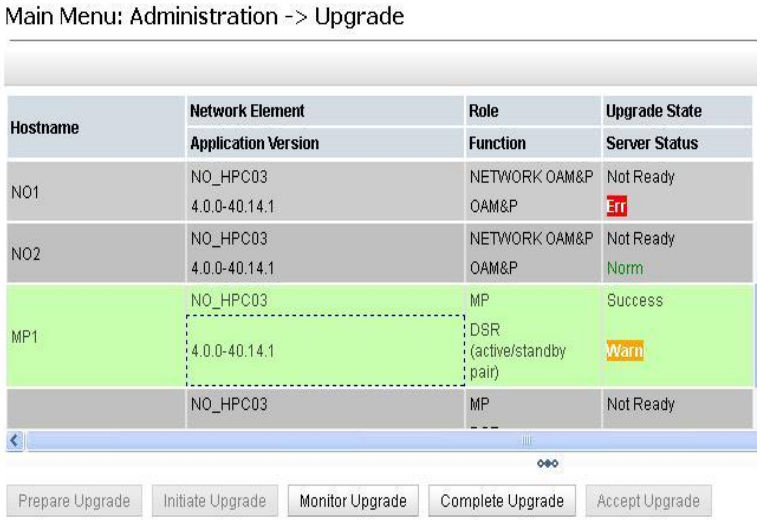
11 ☐	Verify services restart	After the server has rebooted, re-execute steps 2 and 3 of this procedure to log back into the now backed-out server.
		
		Verify services have restarted:
		
		1. You must wait several (approx. 6 minutes) minutes for a reboot to complete before being able to log back into the server.
		2. SSH and log back into the server as root. The method is the same as Steps 2 and 3 of Procedure 66 (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 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 for further instructions. Execute following command to gather output :-
		
		`# syscheck -v`

12 ☐	Workaround for Major Backout (DSR 4.x -> DSR 3.x)	If the backed out server is Standby NO
		1. Login to 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.

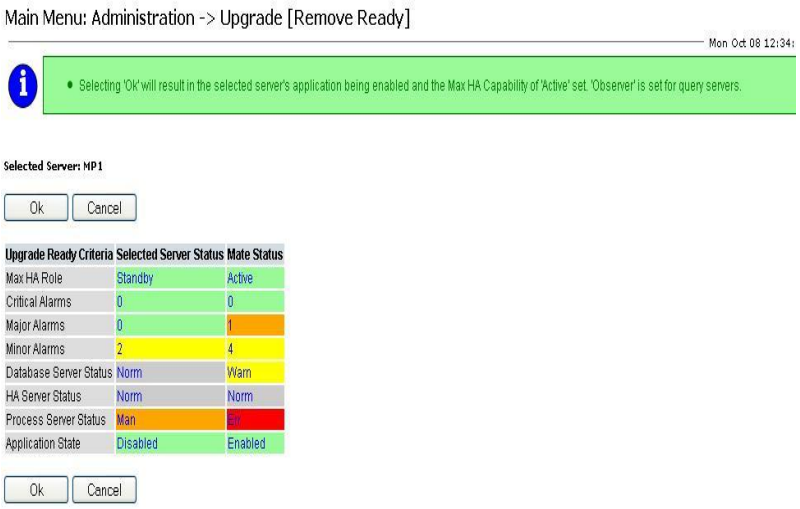
13 ☐	Remove Downgrade Ready status	From the DSR Active NODSR 4.x GUI: 1. Select Status & Manage > Server; the Server Status screen gets displayed. 2. If the server just backed-out shows Application Status Enabled, then select and **press the Stop button.**



3. Select **Administration > Upgrade;** the Upgrade Administration screen gets 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** button. Otherwise, skip to sub-step 6 below.



The **Upgrade [Remove 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.

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

14	Backout is done	The backout procedure is complete.

6.3 Post-Backout Procedures

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

6.3.1 Perform Health Check (Post-Backout)

This procedure is used to determine the health and status of the DSR 3.x/4.x network and servers.

Procedure 67: 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 gets 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's status 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 gets displayed. 2. Click **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.

3.4 Turn off COMCOL compatibility mode (major upgrade only)

This procedure is used to disable COMCOL compatibility services after a major upgrade from Appworks 4.x to Appworks 5.x.

COMCOL database replication between version 5.16 databases (used in Appworks 4.0) and version 6.1 databases (used in Appworks 5.0) requires a mediation service. Therefore during major upgrades servers are placed into a compatibility mode and run this mediation service. The performance and functionality of data replication is degraded while compatibility mode is engaged, so it is recommended that the mode be turned off on all servers once the full system has successfully completed major upgrade.

Appworks provides a simple command line utility that may be used to turn off compatibility mode on all servers in the topology, and should be executed on the active NOAMP server.

Note: - Once the COMCOL compatibility is turned off, a backout to the previous release from which upgrade was done will not be allowed

Procedure 68: Turn off COMCOL compatibility mode (DSR 3.x->4.x upgrade only)

S T E P #	This procedure disables COMCOL compatibility mode. 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 to active NOAMP	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>`

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

3 ☐	Execute the setccupgrade complete utility	Execute the script to turn off compatibility mode: `# /usr/TKLC/appworks/bin/setccupgradecomplete`
4 ☐	Verify utility completes	Verify that compatibility mode has been disabled on all servers: 3. Query the CCUpgCompStatus database table with the command: `# iqt CCUpgCompStatus.1` 4. The output of this query lists each server in the system with an indication of completion in the "Result" field. (Y for complete, No for incomplete) If the Result field is 'Y' then the "Timestamp" field will indicate the time when compatibility mode was disabled. 5. A few seconds after executing the setccupgradecomplete command the query above should indicate 'Y" as the Result for each server in the system.

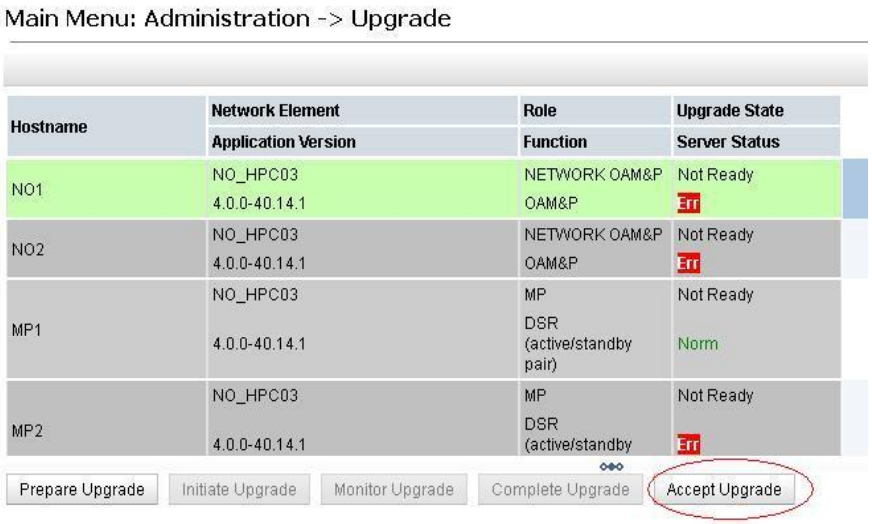
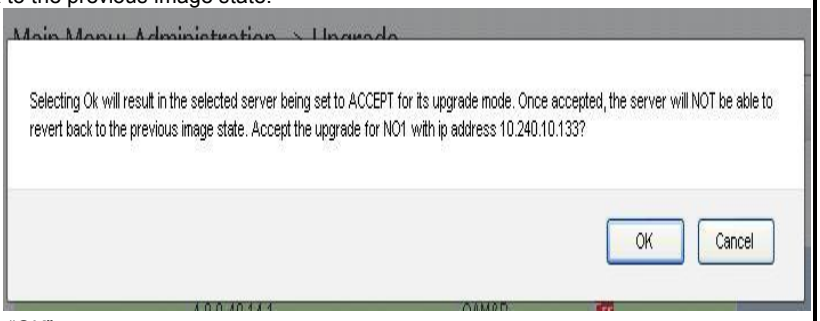
5.5 Accept Upgrade

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 69: Accept Upgrade (Post-Upgrade of full system)

S T E P #	This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Accept upgrade for a single server	Accept upgrade of a single server 1. Select **Administration > Upgrade;** the Upgrade Administration screen displays. 2. Select the first server record in the table. 3. Click the "Accept Upgrade" 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.
2 ☐	Accept upgrade of the rest of the system	Accept Upgrade all Servers in the system: 1. Repeat all step 1 of Procedure 15 (this procedure) until the upgrade of all Servers within the system have been accepted.

3 ☐	Verify accept	Check that alarms are removed: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view displays. 2. As upgraded is accepted on each server the corresponding Alarm ID **32532** (**Server Upgrade Pending Accept/Reject)** should be removed.

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 above completed 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. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE

Access to the Tekelec's Customer Support site is restricted to current Tekelec customers. This section describes how to log into Tekelec's Customer Support site and how to locate upgrade procedures. Viewing these files requires Adobe Acrobat Reader.

1. Go to Tekelec's Customer Support login page at https://support.tekelec.com/index.asp
2. Enter your assigned username and chosen password and click **Login.**

   Or, if you do not have access to the Customer Support site, click **Need an Account?**
   Follow instructions on the screen. Note that obtaining a new online support account can take up to 48 hours.

   Note: After 20 minutes of inactivity, you will be logged off, and you must repeat this step to regain access.
3. After successful login, select a product from the Product Support drop-down menu.
4. Select a release number from the Product Support Release drop-down menu.
5. Locate the Upgrade Procedures section.
6. To open the procedure in the same window, click the procedure name. To open the procedure in a new window, right-click the procedure name and select **Open in New Window**.

Appendix E. CHECKING IF TVOE UPGRADE IS REQUIRED.

1. Check the TVOE release that is part of the DSR release on the node to be upgraded.

i. Login to the server on which TVOE is installed.

ii. Execute the following command to get the current TVOE installed version :-

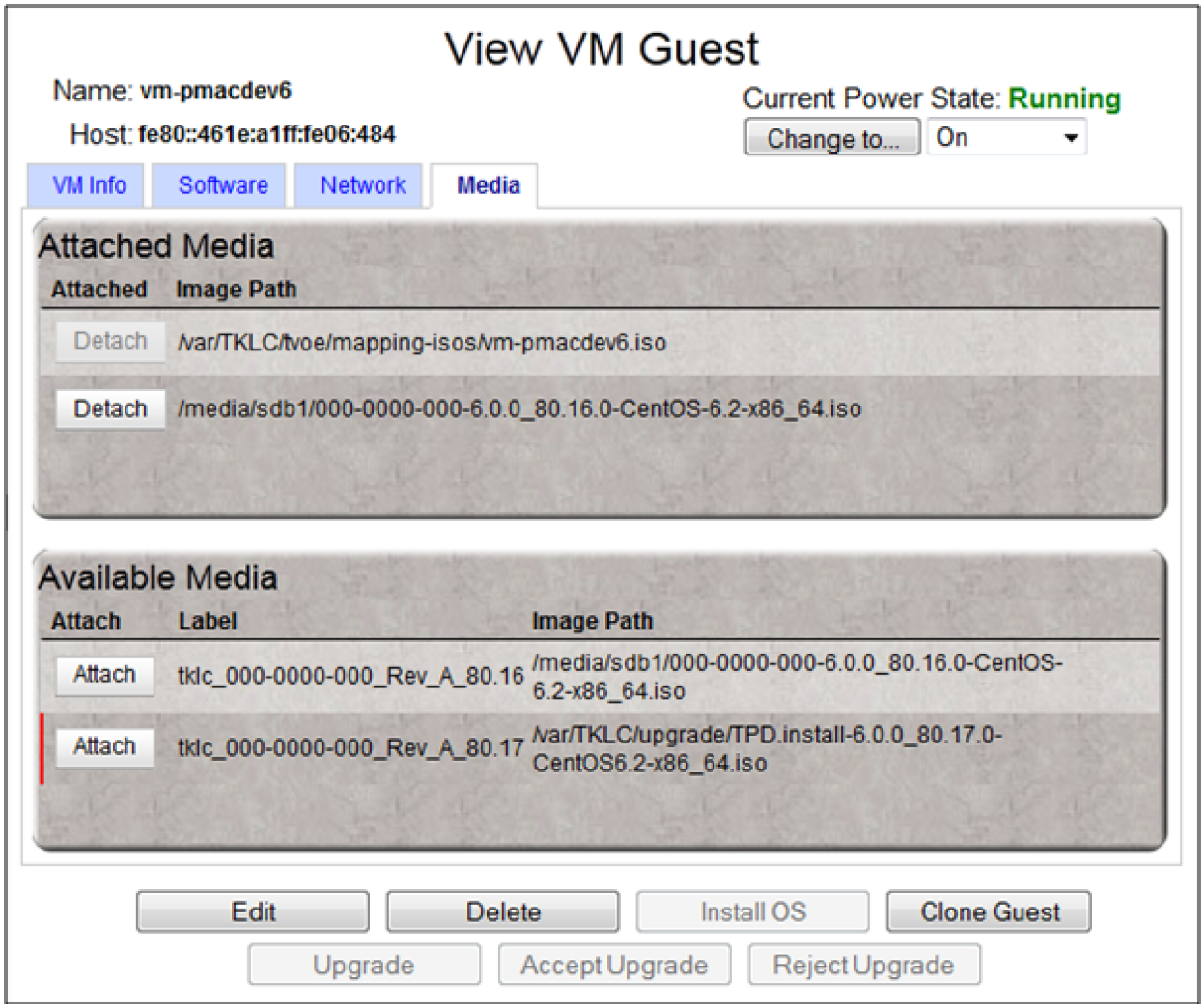
```
[root@dsrTVOEblade2 ~]# appRev
        Install Time: Tue Aug  7 08:17:52 2012
        Product Name: TVOE
     Product Release: 2.0.0_80.16.0
     Part Number ISO: 872-2290-104
     Part Number USB: 872-2290-104
 Base Distro Product: TPD
 Base Distro Release: 6.0.0_80.16.0
    Base Distro ISO:
TPD.install-6.0.0_80.16.0-CentOS6.2-x86_64.iso
                  OS: CentOS 6.2
```

2. Check the TVOE release version required for target DSR release.
3. If the release in Step 1 is less than what is required in Step 2 then upgrade of TVOE is required.

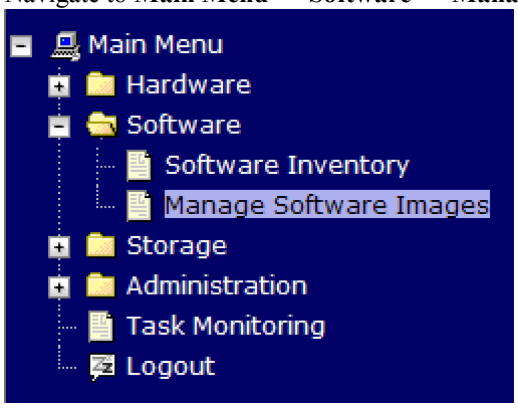
Appendix F. ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY

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.

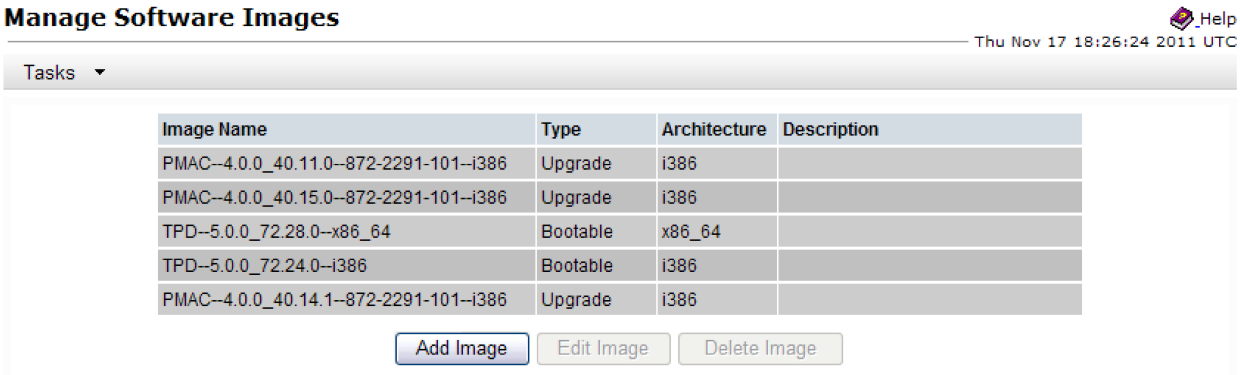
1. In the PM&C GUI, navigate to **Main Menu ➢ VM Management.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.
2. Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button.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

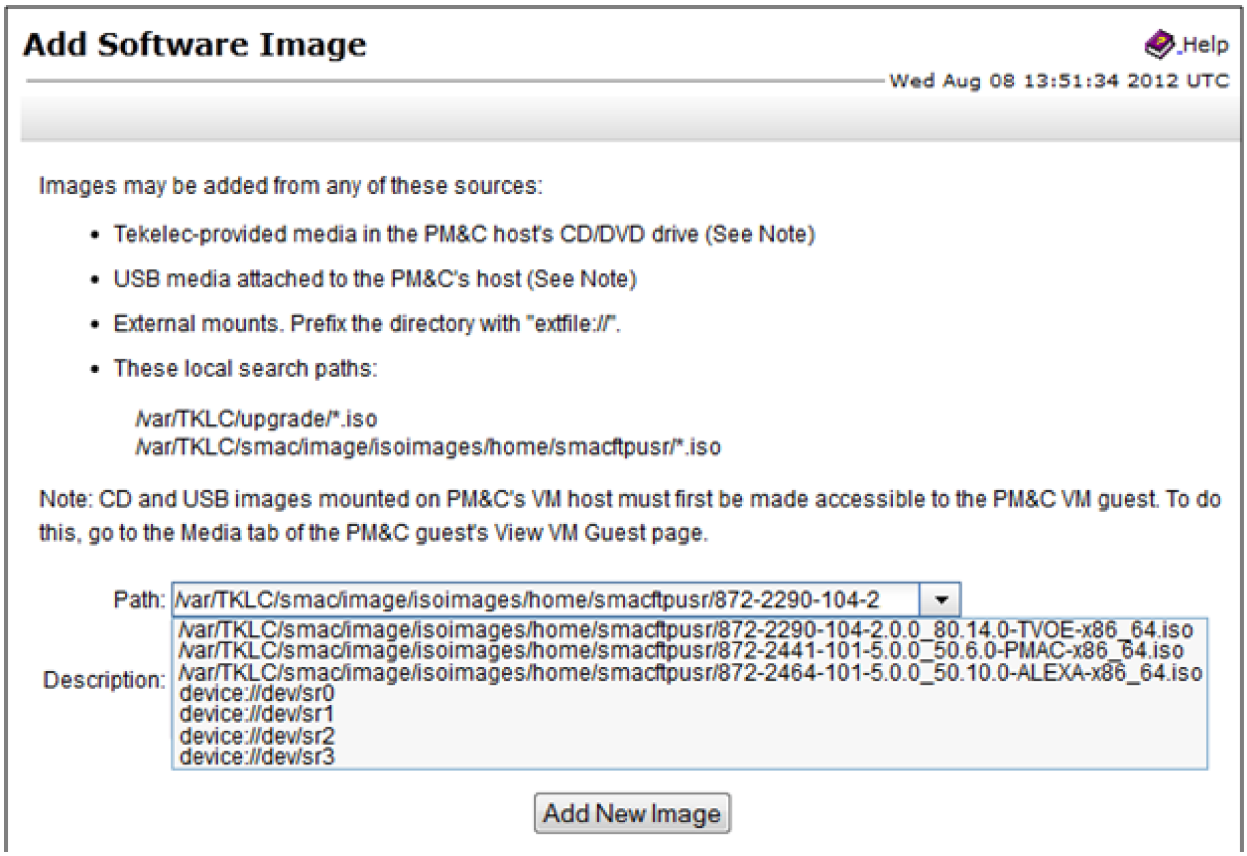


4. **PM&C GUI:**Add image
   Press the **Add Image** button .



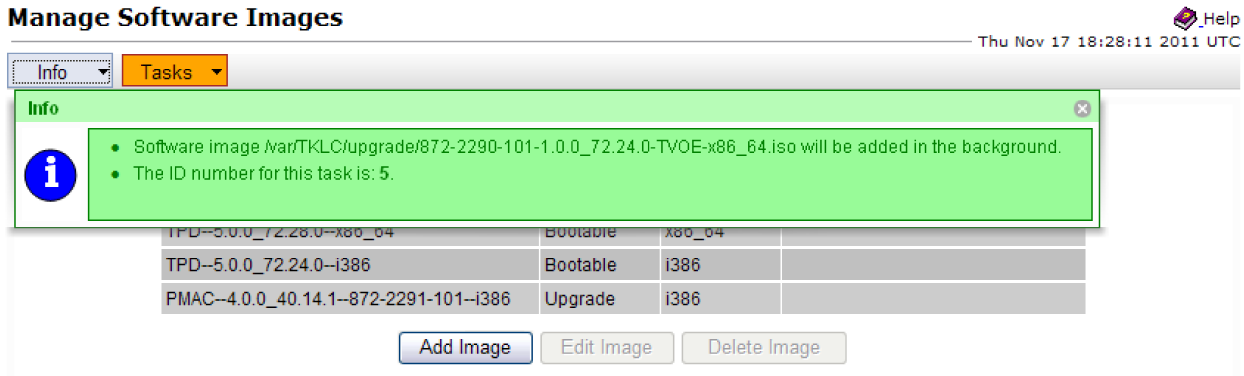
5. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:
   - If the image was transferred to PM&C via sftp it will appear in the list as a local file"/var/TKLC/...".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…").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



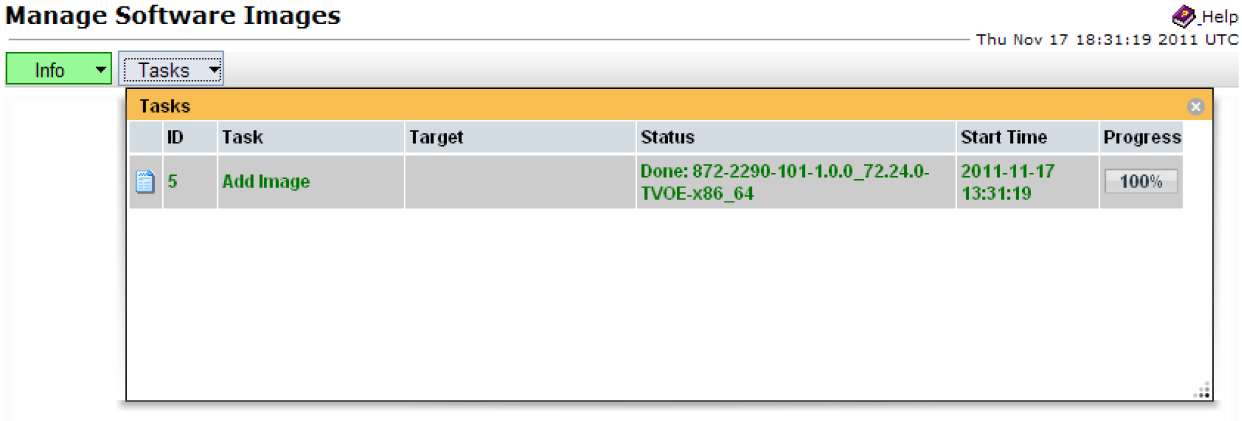
6. **PM&C GUI** Monitor the Add Image status

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

Detailed steps are shown in the procedure below.

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**.	
1 ☐	View Pre-Upgrade Status.	View Pre-upgrade Status of the server: Multiple iterations of this procedure are executed during the upgrade procedure. This is dependent on the number or servers within your network. Make multiple copies of Appendix G to mark up or keep another form of written record of the steps performed. 1. If not already viewing Upgrade Administration: Select **Administration > Upgrade** The Upgrade Administration screen gets displayed. Main Menu: Administration -> Upgrade 2. Verify the **Application Version** value for the server is the source software release version. 3. Verify the Upgrade State of the server to be upgraded is Not **Ready**. If the server is in 'Ready' state then skip Step 2 below and move to Step 3(Initiate Upgrade) directly. **For any server being upgraded, the following applies:** 4. Active NO server will have the following expected alarm: Alarm ID = **10008** (Provisioning Manually Disabled) Servers with replication disabled will have the following expected alarm: Alarm ID = **31113** (Replication Manually Disabled) Alarm ID = **10075** (Application processes have been manually stopped (result of make ready) Alarm ID = **31228** (High Availabilty Server failed to receive mate heartbeats) Alarm ID = **10010** (Stateful db from mate not yet synchronized)

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

2 ☐	Make Server Upgrade Ready (prepare)	Make the server 'Upgrade Ready': 1. Select **Administration > Upgrade;** the Upgrade Administration screen gets displayed.

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)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

2. Select the server to be upgraded

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)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Err

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

3. Click the "**Prepare Upgrade**" button; the **Upgrade [Make Ready]** screen gets displayed.

Note 1: If this is the pSBR server, then HA Role for the selected server may differ from the Resource HA Role. It is safe to ignore the Selected server status and follow the sequence that was identified in [Procedure 52***] Step[4].***

Note 2: 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. The HA switchover will cause the session to be logged out in case of Active NO. If Logged out then Log in back into the DSR 3.x/4.x GUI.

Note 3:The Make Ready action on MP server MAY cause the value in the Selected Server Status be shown as 'Active' for both the MP(s). Please proceed with upgrade.

4. Click **OK**; this starts the Make Ready action on the server. The Upgrade Administration screen gets displayed.
5. Select **Administration >Upgrade;** the Upgrade Administration screen gets displayed.

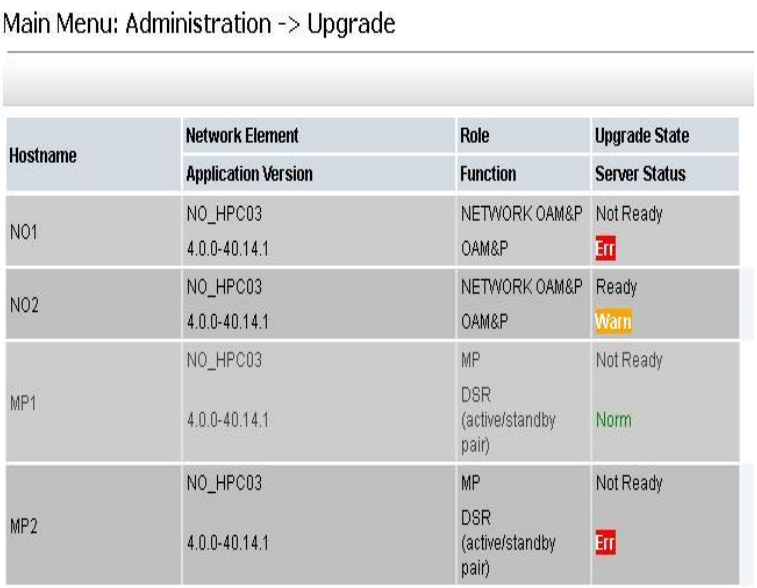
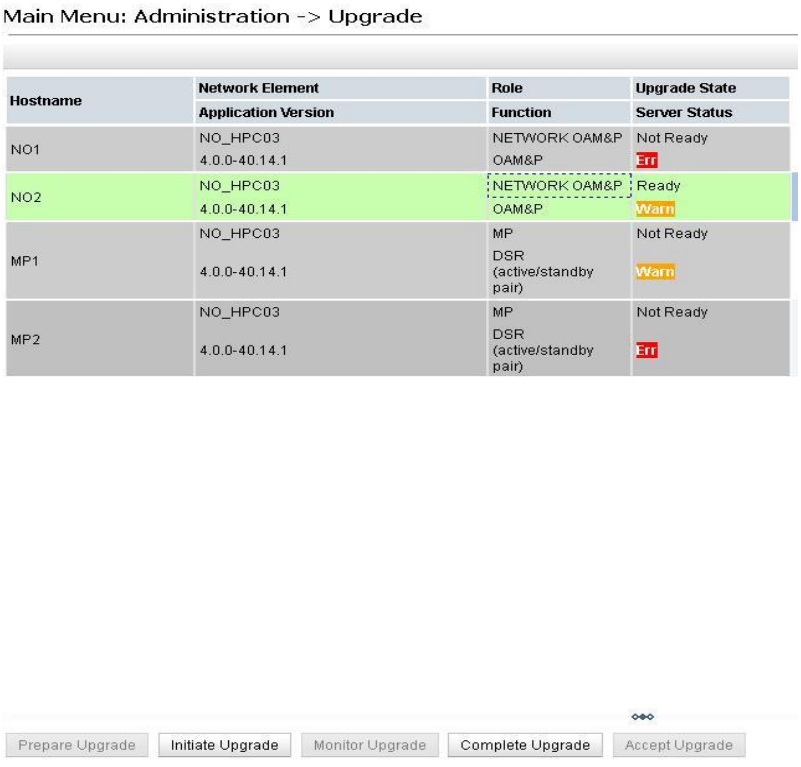
6. Wait for the screen to refresh and show the **Upgrade State** is **Ready** and the **Upgrade** action link is enabled for the server that was to be upgraded. It may take up to a minute for the **Upgrade State** to change to **Ready**.

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	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

7. Servers will have a combination of the following expected alarms. Note: Not all servers have all alarms:

Alarm ID = **10008** (Provisioning Manually Disabled)
Alarm ID = **10075** (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)

3	Initiate Upgrade (initiate)	Initiate Upgrade on the server: 1. Select **Administration >Upgrade** The Upgrade Administration screen gets displayed.  2. Select the server to be upgraded 

Main Menu: Administration -> Upgrade

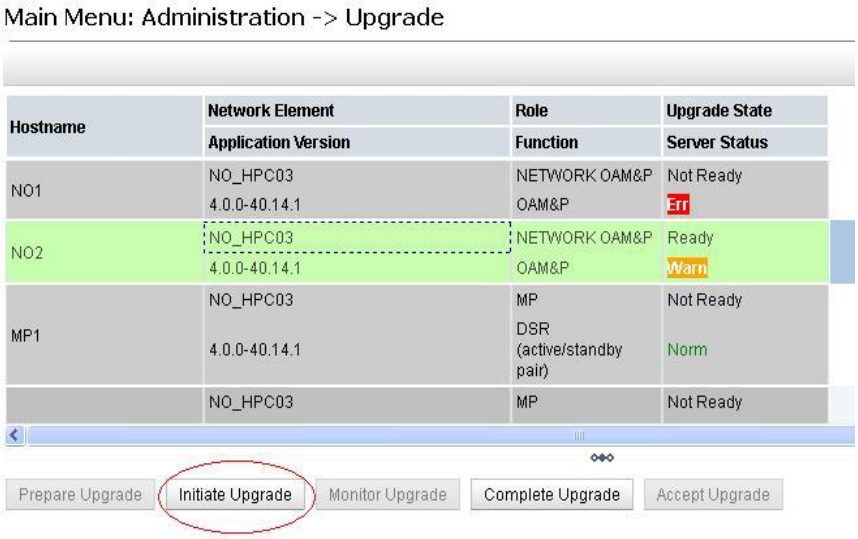
Hostname	Network Element Application Version	Role Function	Upgrade State Server Status
NO1	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Err
NO2	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Ready Warn
MP1	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1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

Main Menu: Administration -> Upgrade

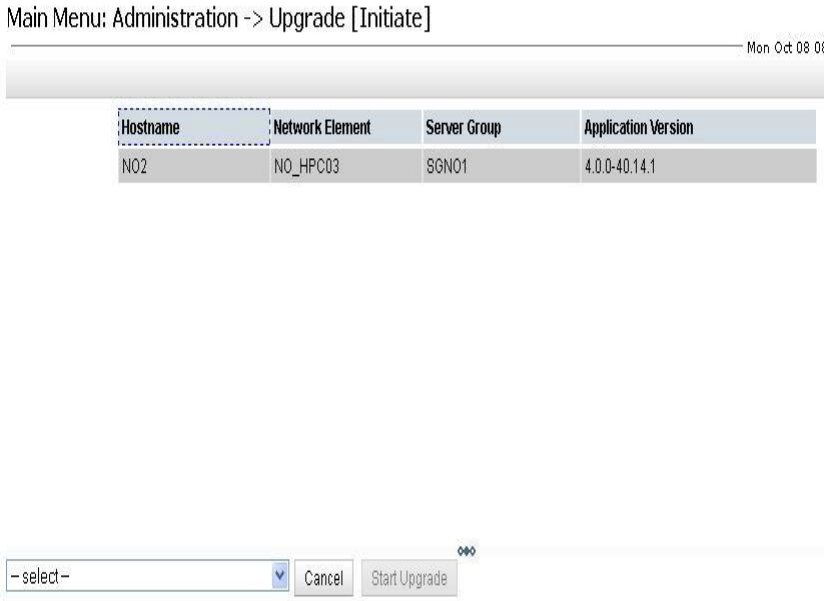
Hostname	Network Element Application Version	Role Function	Upgrade State Server Status
NO1	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready Err
NO2	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Ready Warn
MP1	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready Warn
MP2	NO_HPC03 4.0.0-40.14.1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

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

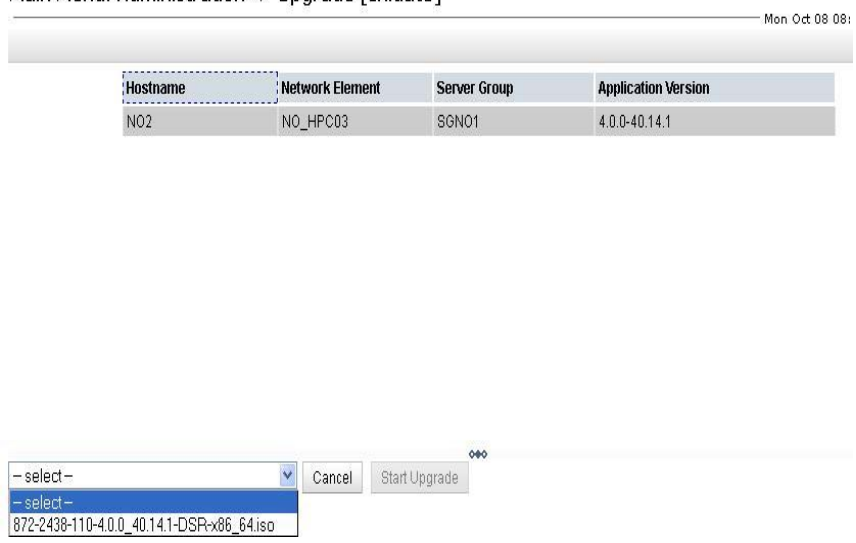
3. Ensure that the "**Initiate Upgrade"** button is enabled for the server to be upgraded.
4. Click "**Initiate Upgrade"** button.



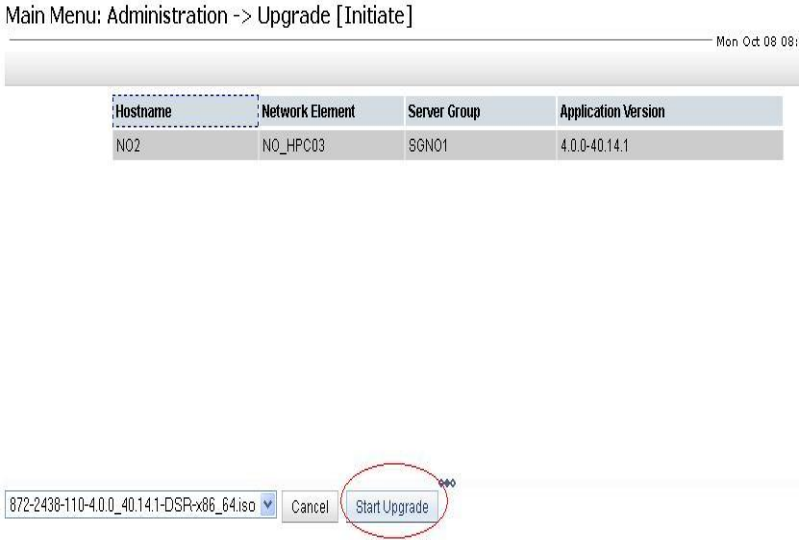
5. The **Administration > Upgrade [Initiate]** view gets displayed. The target server is identified with associated data (Hostname, Network Element, Server Group and application version)

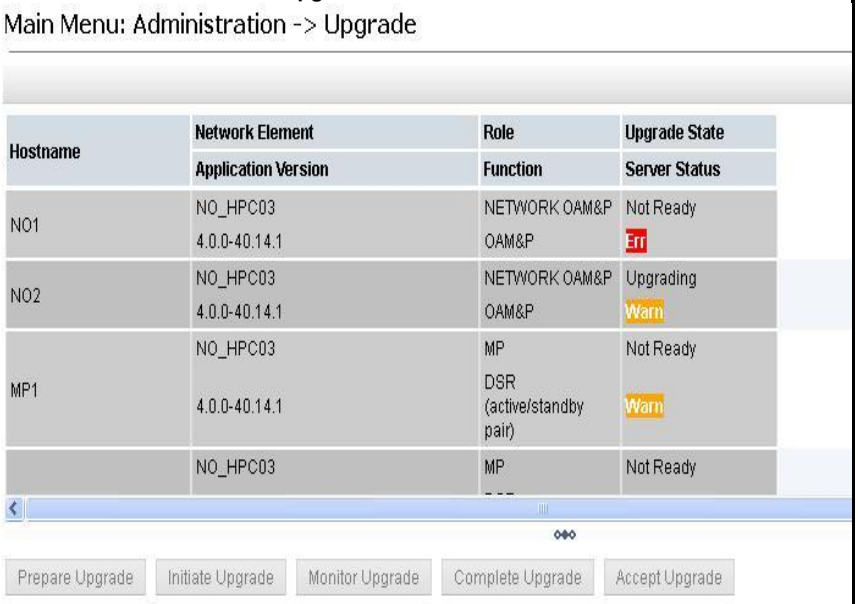
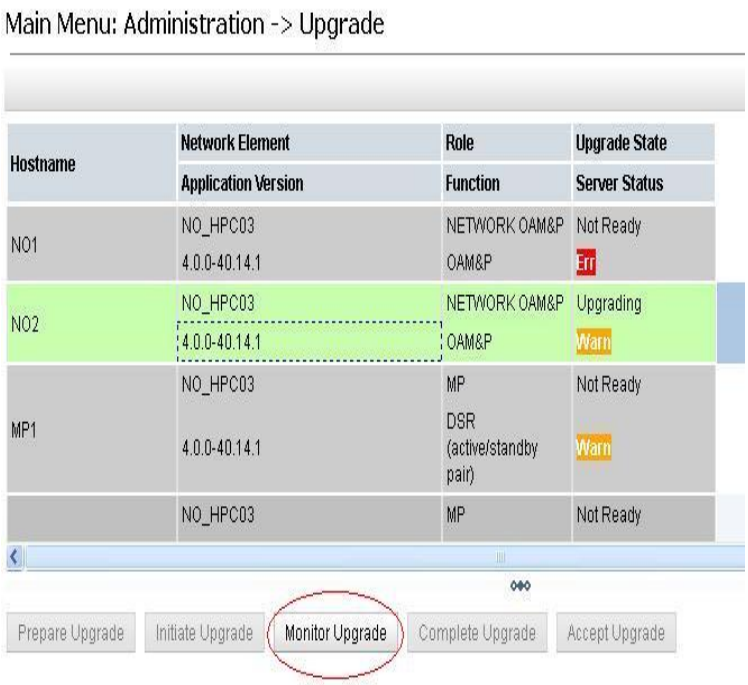


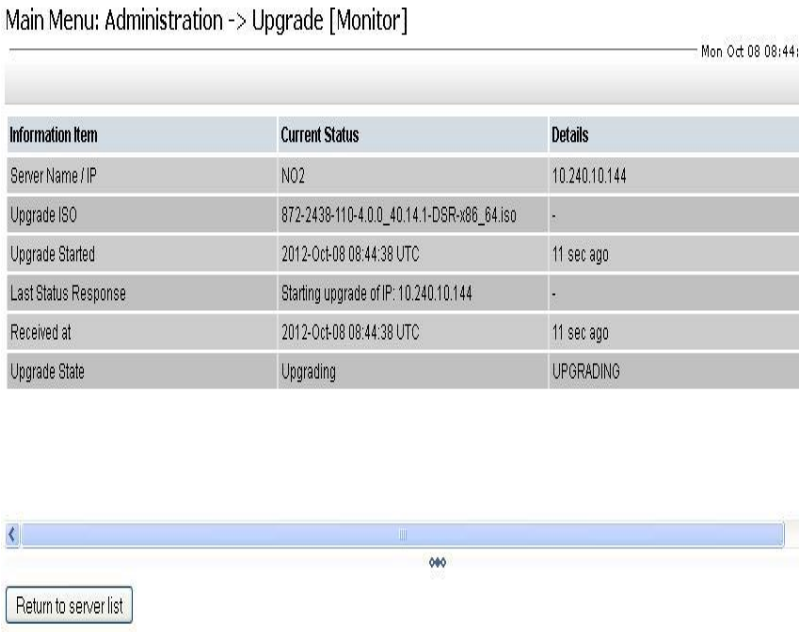
6. Select the ISO to use in the server upgrade.



7. Click the **Start Upgrade** button; the upgrade will begin and you will be returned to the **Administration > Upgrade** screen.



4 ☐	View In-Progress Status (monitor)	View In-Progress Status: 1. Select **Administration > Upgrade**  2. Observe the **Upgrade State** of the server of interest. 3. For more detailed status of the upgrade for a given server select the server, and click the **Monitor Upgrade** button  a. The **Administration > Monitor** Upgrade screen is displayed, and upgrade progress data is presented.



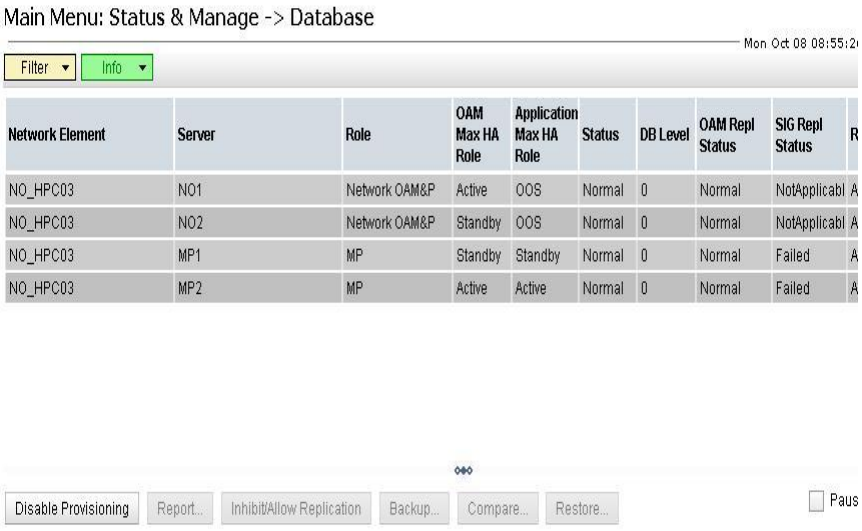
4. Wait for the upgrade to complete. The "**Upgrade State**" under the "**Current Status**" column will show "**Success**".This step will take around 15-20 mins. Contact Tekelec customer service in the event of a failure
5. Execute following commands as mentioned in the table below depending upon the source upgrade release and the condition specified (not needed if source upgrade release is 3.x). These steps will inhibit replication to MPs but will be executed on NO/SO command prompt as mentioned below.

Note: - Skip to execute steps mentioned in table below if source upgrade release is DSR 3.x. Following table needs to be executed only for if source upgrade release is 4.x.

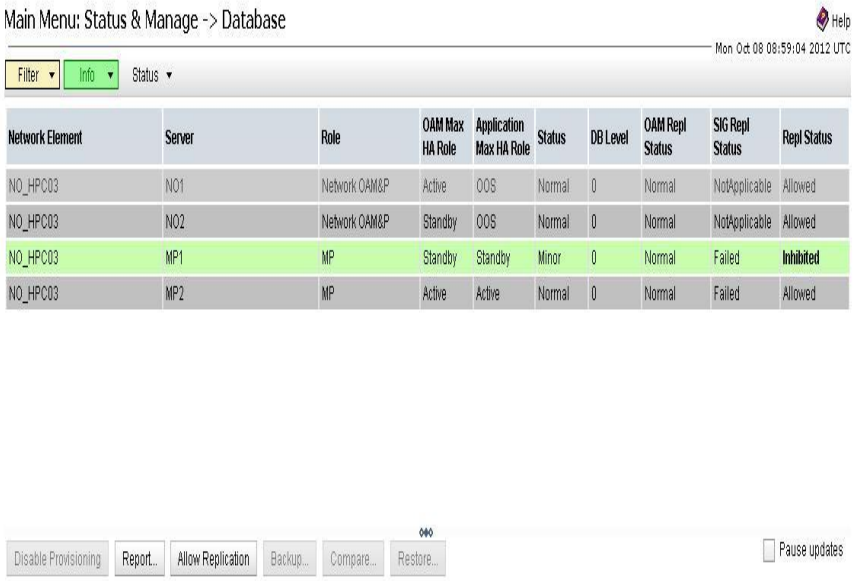
Source Upgrade Release	Condition	Steps To be Executed
Source Upgrade release is less than 41.16.0	**1. Setup is 2 tier on multi-Active (N+0) configuration** **2. Server currently being upgraded is NO.**	**Note: These steps will inhibit the A to C level replication i.e. upgraded NO will stop replicating data to MPs** Login to the upgraded NO server:- **# ssh root@<Stanby NO IP>** **login as: root** **password: <enter password>** Take the backup of the TableDef table Execute following commands on the upgraded NO :- **# ia.mkscript TableDef | sh > /var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **Note: Re-verify if the backup file gets created in the /var/TKLC/db/filemgmt directory by executing the following command** **#ls –ltr /var/TKLC/db/filemgmt/$(hostname).TableDef.backup**

			Inhibit the A to C level replication **# iset –frepPlanId=Off TableDef where "repPlanId='A'"** Look for the output similar to **" === changed <Number of Records> records ==="** to ensure that command 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 -h TableDef where "repPlanId='A'"** No records shall be displayed as the output of the above command.
	Source Upgrade release is less than 41.16.0	**1. Setup is 3 tier on multi-Active (N+0) configuration** **2. Server currently being upgraded is SO.**	**Note: These steps will inhibit the A and B level replication to C level i.e upgraded NO and SO will stop replicating data to MPs** Login to upgraded SO server:- **# ssh root@<Stanby SO IP>** **login as: root** **password: <enter password>** Take the backup of the TableDef table Execute following commands on the upgraded SO :- **# ia.mkscript TableDef | sh > /var/TKLC/db/filemgmt/$(hostname).TableDef.backup** **Note: Re-verify if the backup file gets created in the /var/TKLC/db/filemgmt directory by executing the following command** **#ls –ltr /var/TKLC/db/filemgmt/$(hostname).TableDef.backup** Inhibit the A and B level replication to C level **# iset –frepPlanId=Off TableDef where "repPlanId='A' or repPlanId='B'"** Look for the output similar to **" === changed < Number of Records > records ==="** to ensure that command 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 -h TableDef where "repPlanId='A' or repPlanId='B'"** No records shall be displayed as the output of the

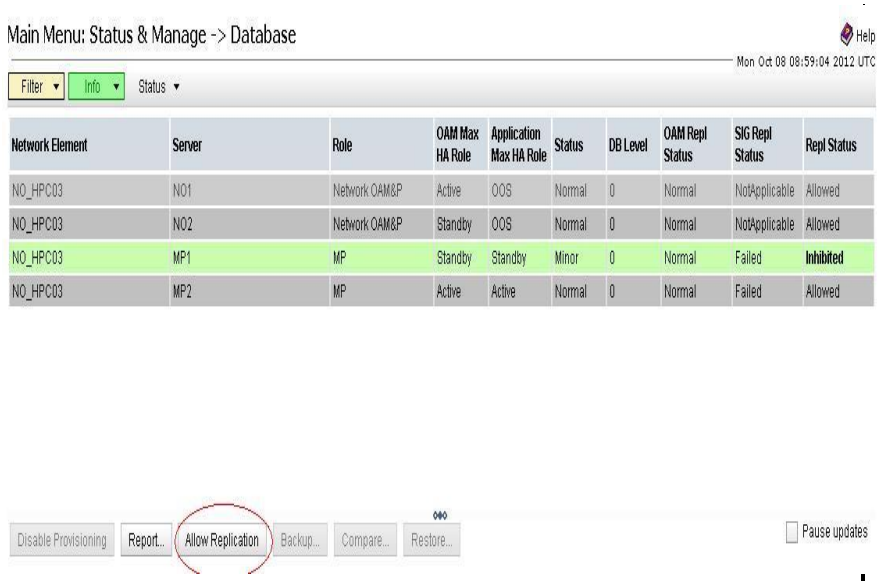
				above command.
		Source Upgrade release greater than or equal to 41.16.0	**Server currently being upgraded is MP**	Allow replication on each upgraded MP(s) using below mentioned command :- Login to Active NO:- **# ssh root@<Active NO IP>** **login as: root** **password: <enter password>** Execute following command on the Active NO for the just upgraded MP :- **# iset -finhibitRepPlans=' ' NodeInfo where "nodeName='<upgraded MP nodename>'"** **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
5	Allow replication for only MP servers.	**Following steps needs to be performed for DSR 3.x/4.x after upgrade is successful if the server is MP :-** Using the DSR 3.x/4.x GUI: 1. Select **Status & Manage > Database** the Database Status screen gets displayed.		



2. Select the MP server that was just upgraded.



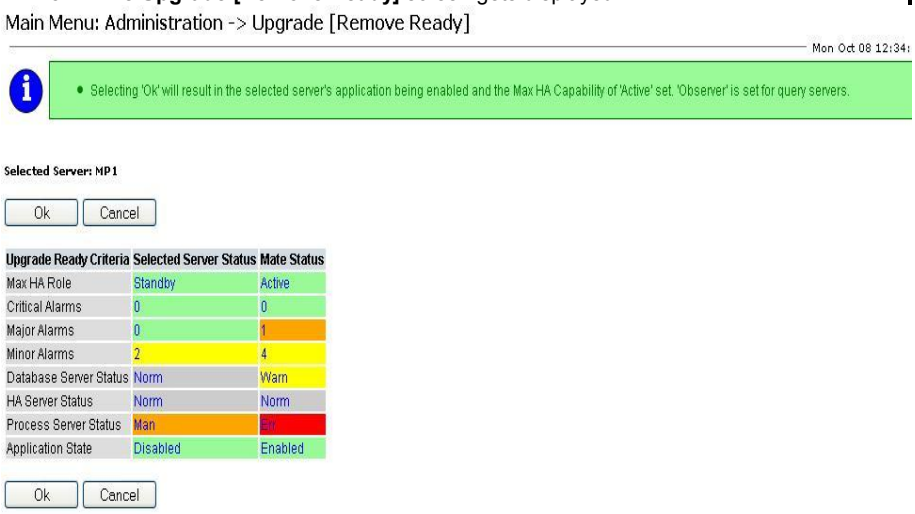
3. Click **Allow Replication** button only if replication is Inhibited, Else move to next step.



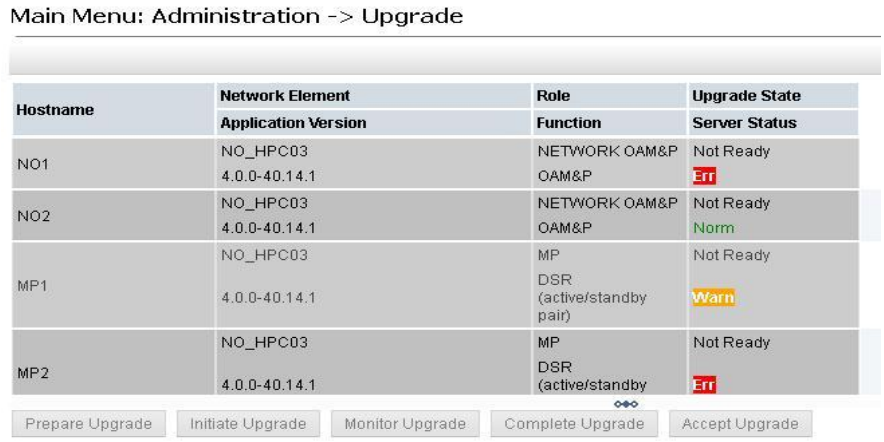
4. Verify the ***Inhibited*** text is not displayed for server.
5. Wait for the screen to refresh and show the Replication Status field as ***Allowed*** for the server.

5 ☐	Remove Upgrade Ready state from server.	Remove Upgrade Ready state from server: 1. Select **Administration > Upgrade;** the Upgrade Administration screen gets displayed. 2. Verify the **Application Version** value for this server has been updated to the target software release version. 3. Verify status: a) Verify the **Upgrade State** of the server that was upgraded is **Success**. 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 b) Select the server that was upgraded, and Verify the **Complete Upgrade** button is enabled for the server that was upgraded 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

4. Click **Complete Upgrade** button.
5. The **Upgrade [Remove Ready]** screen gets displayed.



6. Record all the **Upgrade Ready Criteria** and **Server Status** values for this server. Keep this information for future reference.
7. Click **OK**.
8. This completes the Remove Ready action on the server. The Upgrade Administration screen gets displayed.
9. Select **Administration >Upgrade;** the Upgrade Administration screen gets displayed.
10. 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**.



6 ☐ View Post-Upgrade Status.

View Post-Upgrade Status of the server:

1. Active NO server will have some or all the following expected alarm(s):
   Alarm ID = **10075** (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 db from mate not yet synchronized)

   Servers that still have replication disabled will have the following expected alarm:
   Alarm ID = **31113** (Replication Manually Disabled)

7 ☐	Procedure Complete.	is complete: Return to the procedure from where you came into this procedure.

Appendix H. UPGRADE FIRMWARE

This section finds out the firmware version installed and steps needed to upgrade the firmware.

<table>
<tr><td>S
TE
P
#</td><td colspan="2">This procedure will provide the steps to upgrade the firmware on the Blade servers.

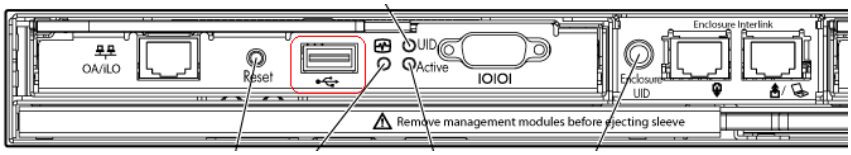
Needed material:
– HP Smart Update Firmware DVD
– HP Solutions Firmware Upgrade Pack Release Notes [1]

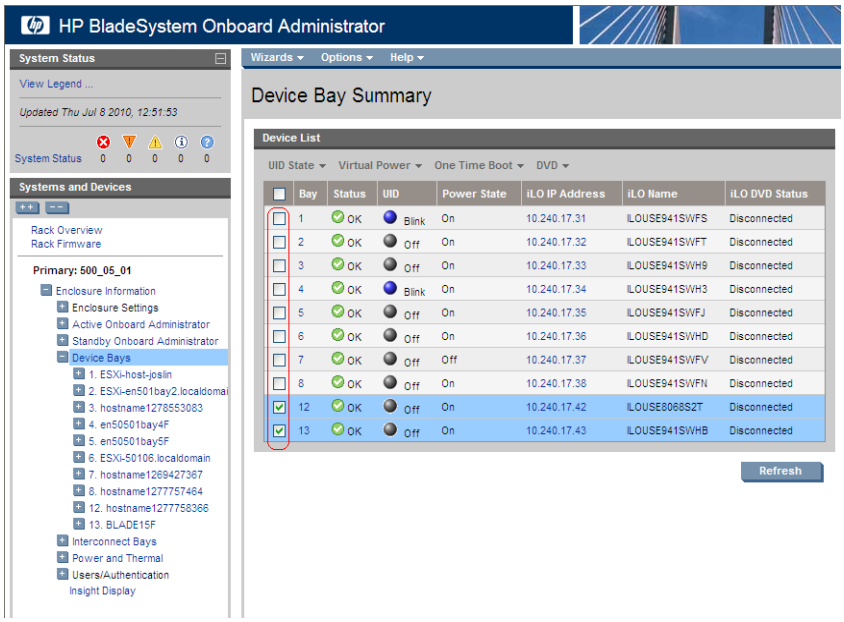
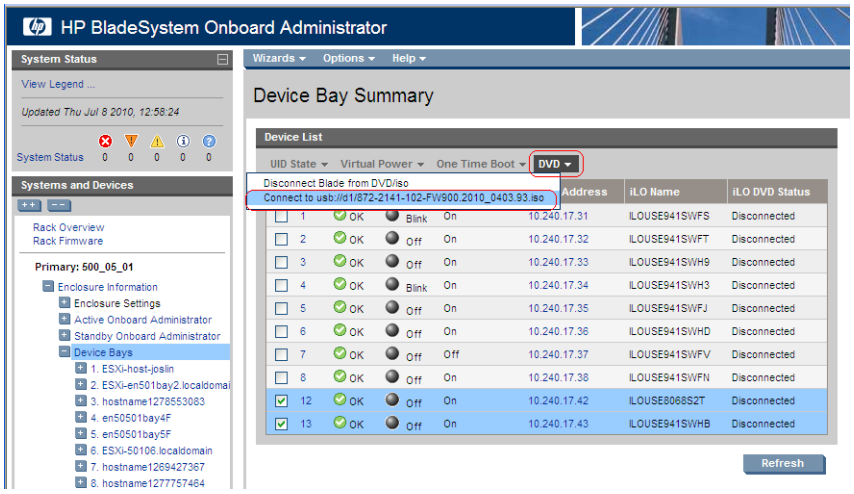
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

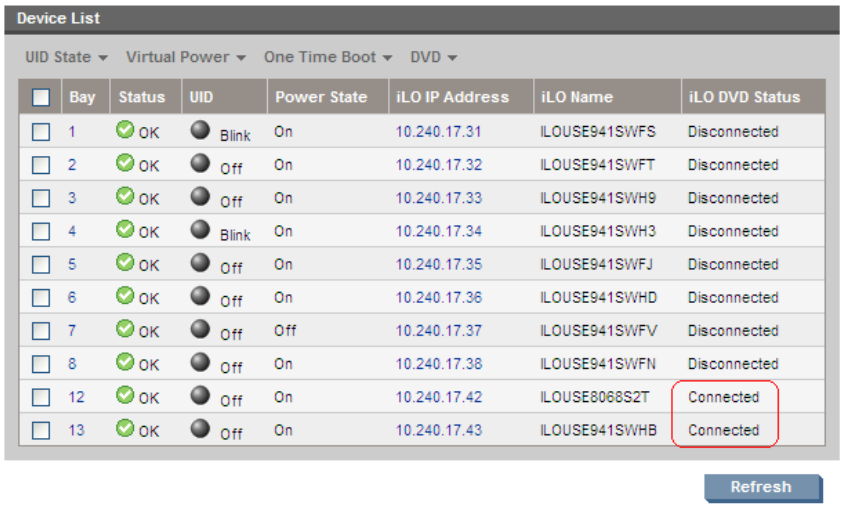
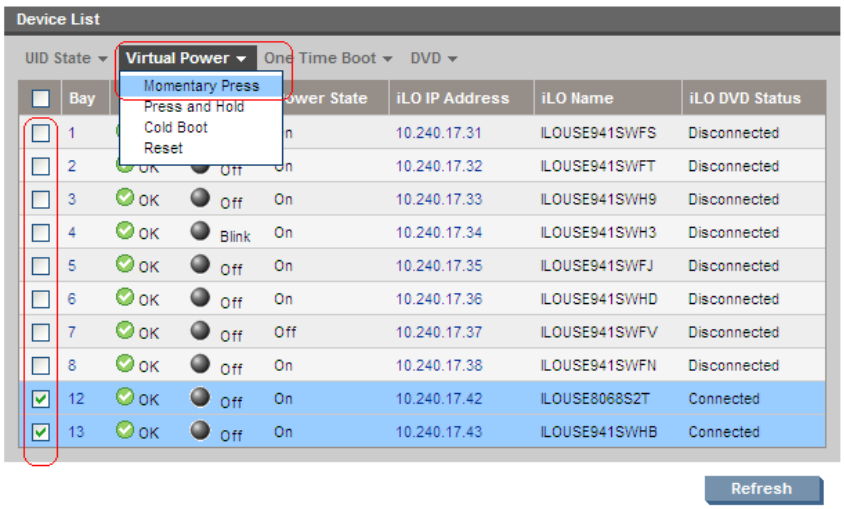
IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.</td></tr>
<tr><td>1
☐</td><td>OA iLO: Check if Firmware upgrade is needed</td><td>Log onto the OA iLO using IE and navigate to Rack Firmware, you should be presented with the overview of all components in the enclosure as shown below. Scroll down the view the blades firmware. Check the ROM Version for all the blades in the enclosure.

Device Firmware Information
<table><tr><th>Bay</th><th>Device Model</th><th>Firmware Component</th><th>Current Version</th></tr><tr><td>1</td><td>ProLiant BL460c G6</td><td>System ROM</td><td>I24 05/20/2010</td></tr><tr><td></td><td></td><td>iLO2</td><td>iLO2 2.00 Jun 21 2010</td></tr><tr><td></td><td></td><td>Power Management Controller</td><td>3.4</td></tr><tr><td>2</td><td>ProLiant BL460c G6</td><td>System ROM</td><td>I24 05/20/2010</td></tr><tr><td></td><td></td><td>iLO2</td><td>iLO2 2.00 Jun 21 2010</td></tr><tr><td></td><td></td><td>Power Management Controller</td><td>3.4</td></tr><tr><td>3</td><td>ProLiant BL460c G6</td><td>System ROM</td><td>I24 05/20/2010</td></tr><tr><td></td><td></td><td>iLO2</td><td>iLO2 2.00 Jun 21 2010</td></tr><tr><td></td><td></td><td>Power Management Controller</td><td>3.4</td></tr><tr><td>4</td><td>ProLiant BL460c G6</td><td>System ROM</td><td>I24 05/20/2010</td></tr><tr><td></td><td></td><td>iLO2</td><td>iLO2 2.00 Jun 21 2010</td></tr><tr><td></td><td></td><td>Power Management Controller</td><td>3.4</td></tr></table>
If the current verion is at or greater than the minimum supported version, skip this procedure, no upgrade is necessary.</td></tr>
</table>

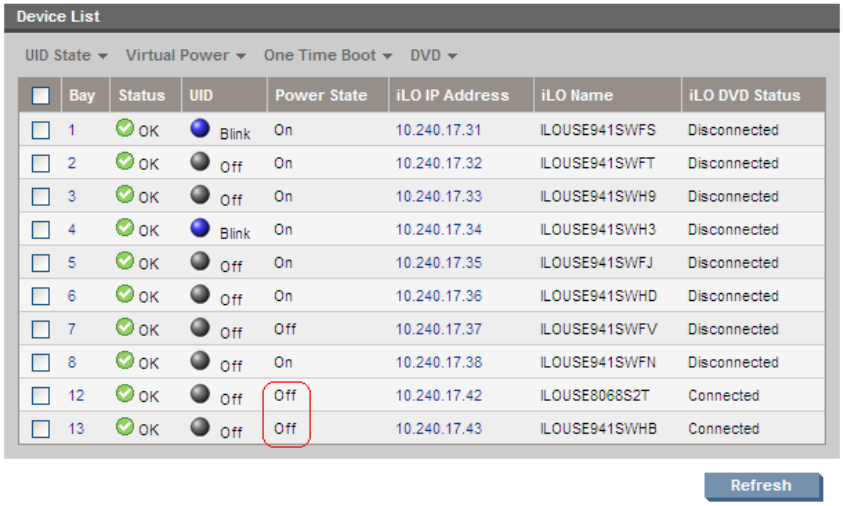
2 ☐	**Local Workstation:** Import HP Firmware Maintenance CD	Insert the HP Smart Update Firmware DVD into the removable media drive of your local workstation. Use HP Solutions Firmware Upgrade Pack Release Notes [1] to select the proper part number.
		If your local workstation is a Linux machine, extract the iso image using the following commands, otherwise skip to the next step. Use the correct iso image part number from HP Solutions Firmware Upgrade Pack Release Notes [1].
		`# getCDROM`
		`# dd if=/dev/scd0 of=/tmp/<image_part_number>.iso`
		Verify checksum of the extracted with the value listed in HP Solutions Firmware Upgrade Pack Release Notes [1].
		`# /usr/bin/md5sum /tmp/<image_part_number>.iso`
		`422275a25353030fb5338876761ee1ca`
		`/tmp/872-XXXX-XXX-firmware.iso`
		Note: The actual iso image in the output is for illustrative purposes only

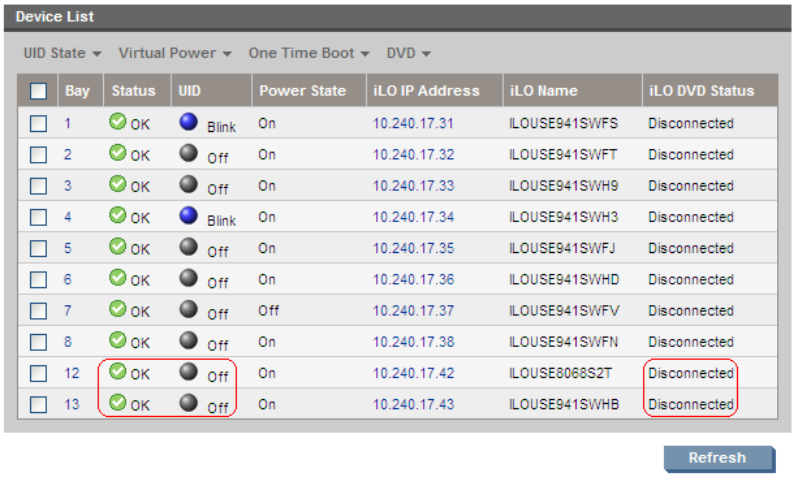
3 ☐	**Local Workstation:** Create ISO file	If your local workstation is a windows machine, use an ISO creation tool such as "ImgBurn" to create an iso from the inserted disk. Use the correct iso image part number from HP Solutions Firmware Upgrade Pack Release Notes [1].
4 ☐	**Local Workstation:** Copy ISO to USB Media	Take the ISO you just mounted/created and copy it to USB media.
5 ☐	**c7000 Enclosure** Insert USB Flash Drive	Insert the USB Flash Drive with the *HP Smart Update Firmware* ISO into the USB port of the Active OA Module. 
6 ☐	**Local Workstation:** Access the Active OA	Access the Active OA Login Page from an Internet Explorer ® session using the following URL: `https://<OA_IP>/`
7 ☐	**OA Web GUI:** Log in to the Active OA Log in as an administrator user.	`User Name = <OA_admin_user>` `Password = <OA_admin_password>`

8 ☐	**OA Web GUI:** Access the Device Summary page On the left pane, expand the **Device Bays** node to display the **Device Bay Summary** window. Select the individual blades to be upgraded by clicking and enabling the corresponding UID checkbox.	 Note: **A maximum of 8 blades should be upgraded concurrently at one time. If the c7000 enclosure has more than 8 blades they will need to be upgraded to multiple sessions.**
9 ☐	**OA Web GUI:** Connect to USB Drive	Once the blades are selected, connect them to the ISO on the USB Drive, by selecting the **Connect to usb…** item from the **DVD** menu. 

10 ☐	**OA Web GUI:** Verify Drive Connection	Once each blade has mounted the ISO media the **Device List** table should indicate an **iLO DVD Status** as *Connected* for each blade that was previously selected.  **Note**: The **Refresh** button may need to be clicked in order to see the current status of all blades.
11 ☐	**OA Web GUI:** Power Down Blades	If needed, reselect the UID checkbox for each blade to be upgraded and then select the **Momentary Press** option under the **Virtual Power** menu.  When prompted click the **OK** button to confirm the action.

Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
1	OK	Blink	On	10.240.17.31	ILOUSE941SWFS	Disconnected
2	OK	Off	On	10.240.17.32	ILOUSE941SWFT	Disconnected
3	OK	Off	On	10.240.17.33	ILOUSE941SWH9	Disconnected
4	OK	Blink	On	10.240.17.34	ILOUSE941SWH3	Disconnected
5	OK	Off	On	10.240.17.35	ILOUSE941SWFJ	Disconnected
6	OK	Off	On	10.240.17.36	ILOUSE941SWHD	Disconnected
7	OK	Off	Off	10.240.17.37	ILOUSE941SWFV	Disconnected
8	OK	Off	On	10.240.17.38	ILOUSE941SWFN	Disconnected
12	OK	Off	On	10.240.17.42	ILOUSE8068S2T	Connected
13	OK	Off	On	10.240.17.43	ILOUSE941SWHB	Connected

<table>
<tr><td>12
☐</td><td>OA Web GUI:
Verify Power Down</td><td>The power down sequence can take several minutes to complete. When it completes the Device List table will indicate the Power State of each select blade to be Off.
 

Note: The Refresh button may need to be clicked in order to see the current status of all blades.</td></tr>
<tr><td>13
☐</td><td>OA Web GUI:
Initiate Firmware Upgrade</td><td>To power the blades back on and begin the automated firmware upgrade process, repeat Steps 11 and 12 this time being sure the Power State indicates On for each selected blade.</td></tr>
<tr><td>14
☐</td><td>OA Web GUI:
Monitor Firmware Upgrade</td><td>From this point on each blade will boot into an automated firmware upgrade process that will last between 20 to 25 minutes.
 

Upon a successful firmware upgrade, the Device List table will list each blade with a Status of OK, UID of Off and the iLO DVD Status as Disconnected. At this time the blades will automatically be rebooted. If the status does not update to disconnected, you can verify completion by opening an iLo window (via the OA) for each blade and watching the console for indication of firmware upgrade progress and successful completion

If necessary, repeat Steps 8 through 14 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.</td></tr>
<tr><td>15
☐</td><td>c7000 Enclosure
Remove USB Flash Drive</td><td>The USB flash drive may now safely be removed from the Active OA module.</td></tr>
</table>

16 □	Remove temporary file	After all blade servers have been upgraded, the file copied to laptop in Step 3 may be removed.
17 □	Check for Additional Updates	Before proceeding, it is necessary to determine if additional firmware upgrades have been included in the HP Smart Update Firmware DVD/ISO [1] to determine which (if any) HP Errata Firmware Component upgrades must be installed manually
18 □	Update Mezzanine Cards Firmware (Optional)	If the blades have mezzanine cards installed, please refer to [1], section 4.10 on how to upgrade the mezzanine cards firmwares.

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 NOAMP) as root using the management network for the PM&C or XMI network for the NOAMP.

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

Upgrade TVOE platform for selected OAM blade:-

If the NO/SO servers are hosted on the TVOE software then check if TVOE upgrade is required (refer Appendix E). If upgrade is not required then skip this appendix:-

1. Disable all the applications running on current TVOE blade:-
   a) Log into the NOAM VIP GUI
   b) Select **Status & Manage > Server;** the Server Status screen gets displayed
   c) Select all the applications (NO(s) /SO(s)) 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 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 current TVOE host.

3. Execute the following command for each guest identified in Step 2 :-

```
# virsh shutdown <guestname>
```

4. Periodically execute following command until the command displays no entries. This means that all VMs have been properly shut down :-

```
# virsh list
```

5. Upgrade TVOE. Following two sections can be referred during TVOE upgrade :-
   a) If PM&C and DSR NO are on same TVOE guests then follow section 2.1.1 of TVOE upgrade document [3].
   b) If PM&C and DSR NO are on different TVOE guests and PM&C is available for TVOE upgrade then follow section 2.1.2 of TVOE upgrade document [3].

Note: If Active NO is hosted on the TVOE blade which is being upgraded then VIP may be lost till TVOE is successfully upgraded.

6. Please follow Procedure 3.12.1 of [9] to Enable Virtual Guest Watchdogs If disabled, Else execute following steps :-
   a) Login to 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 running on current TVOE blade:-
   a) Log into the NOAM VIP GUI
   b) Select **Status & Manage > Server;** the Server Status screen gets displayed
   c) 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.
   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'.