Oracle® Communications Diameter Signaling Router DSR Software Upgrade Procedure

Release 5.x

909-2277-001

March 2014

909-2277-001 Revision A, March 2014



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

Copyright © 2012,2013,2014 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

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

2 of 252 Version 4.0 909-2277-001 Revision A, March 2014

TABLE OF CONTENTS

1.	INTRODUCTION	10
	1.1 Purpose and Scope	10
	1.1.1 What is Not Covered by this Document	10
	1.2 References	10
	1.3 Acronyms	10
	1.4 Terminology	12
	1.5 How to Use this Document	13
	1.5.1 Executing Procedures	13
	1.6 Recommendations	14
	1.6.1 Frequency of Health Checks	14
	1.6.2 Large Installation Support	14
	1.6.3 Logging of Upgrade Activities	14
ſ		45
Ζ.	GENERAL DESCRIPTION	
	2.1 Supported Opgrade Paths	10
	2.2 Z-Tier VS 3-Tier Upgrades	
	2.3 Active/Standby (1+1) vs Multi-Active (N+0) DA-MPS	
	2.4 Geo-diverse 3-Tier SOAM (Active/Standby/Spare)	1/
	2.5 Firmware Updates	17
	2.6 PMAC (Management Server) Upgrades	17
	2.7 TVOE Upgrade	17
	2.8 SDS Upgrade	18
	2.9 Traffic Management during Upgrade	18
	2.10 Optional NetBackup	18
	2.11 RMS Deployments	18
2		20
J.	2.4 Dequired Meteriole	20
	3.1 Required Materials	20
	3.1.1 Application ISO Image File / Media	20 20
	2.2 Dian Lingrada Maintananaa Windowa	20 22
	3.2 Fidit Opyraue Maintenance Window for PMAC and TVOE Upgrades (optional)	ZS 24
	3.2.1 Maintenance Window for FMAC and TVOE Opyrades (optional)	
	3.2.3 Maintenance Window 1 (3-Tier NOAM servers)	25
	3.2.4 Maintenance Window 2 (First Site upgrade)	
	3.2.5 Maintenance Window 3 (Additional site upgrade)	
	3.3 Pre-Upgrade Procedures	
	3.3.1 Hardware Upgrade Preparation	
	3.3.2 Review Release Notes	30
	3.3.3 Required Materials Check	
	3.3.4 Collect/Backup all Global and Site Provisioning Data	
	3.3.5 Full Backup of DB Run Environment at each server	
	3.3.6 Perform Health Check (Upgrade Preparation)	
	3.3.7 Create new Logical Volume for NetBackup Client on NO/SO(if needed)	
	3.3.8 ISO Administration	
	3.3.9 Upgrade IVUE Hosts at a site (prior to Application upgrade MW)	51
4.	SOFTWARE UPGRADE EXECUTION	53
	4.1 Select Upgrade Path	54
909	0-2277-001 Revision A, March 2014 Version 4.0	3 of 252

4.2 3-Tier DSR Upgrade for (1+1) DA-MP configuration (possibly including TVOE)	55
4.2.1 NO Upgrade Execution for 3-Tier (1+1) setup	55
4.2.2 Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAMs)	57
4.2.3 Inhibit Replication for 3-tier (1+1) setup	61
4.2.4 Upgrade DR-NOs of 3-Tier (1+1) setup	65
4.2.5 Upgrade NOs of 3-Tier (1+1) setup	67
4.2.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier (1+1)	
configuration	68
4.2.7 Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup	69
4.2.8 Site Upgrade for (1+1) 3-tier Configuration	72
4.2.9 Upgrade SO of 3-Tier (1+1) configuration	73
4.2.10 Upgrade DA-MP(s) of 3-Tier (1+1) configuration	75
4.2.11 Verify Post-Upgrade Status (1+1 3-Tier)	76
4.3 3-Tier DSR Upgrade for (N+0) DA-MP configuration (possibly including TVOE)	78
4.3.1 NO Upgrade Execution for 3-Tier (N+0) setup	78
4.3.2 Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAMs)	79
4.3.3 Inhibit Replication for 3-tier(N+0) setup	83
4.3.4 Upgrade DR-NOs of 3-Tier (N+0) setup	86
4.3.5 Upgrade NOs for 3-Tier(N+0) setup	88
4.3.6 Allow Replication between NO and DR NO Servers ONLY for 3-Tier(N+0) setup	89
4.3.7 Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)	90
4.3.8 Site Upgrade for 3-Tier (N+0) Configuration.	92
4.3.9 Upgrade SO of (N+0) 3-Tier configuration	94
4.3.10 Upgrade cSBR(s)	97
4.3.11 Upgrade All Active DA-MPs	98
4.3.12 Upgrade IPFE(s) in 3-Tier(N+0) configuration	98
4.3.13 Allow Replication for Upgraded Site in 3-Tier(N+0) configuration	100
4.3.14 Verify Post Upgrade status (N+0 3-Tier)	102
4.4 3-Tier DSR Upgrade for (N+0) DA-MP configuration on RMS servers (including	
TVOE)	103
4.4.1 NO Upgrade Execution for RMS servers (N+0) setup	104
4.4.2 Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAMs on RMS blade)	106
4.4.3 Inhibit Replication for 3-tier(N+0) RMS configuration	110
4.4.4 Upgrade DR-NOs of 3-Tier(N+0) setup on RMS servers	112
4.4.5 Upgrade NOs for 3-Tier(N+0) RMS setup	114
4.4.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier(N+0) RMS	115
configuration	115
4.4.7 Verify Post Opgrade Status of Rivis Servers (3-tier(N+0) NO Opgrade)	110
4.4.0 Site Upgrade for (N+0) 5-Tiel Rivis Configuration.	120
4.4.9 Ferrorin frequencies for 5-freq(N+0) RMS configuration	120
4.4.11 Upgrade All Active DA-MPs of 3-Tier(N+0) RMS configuration	12/
4.4.11 Opyrade IDEE(s) in 3-Tier(N+0) RMS Configuration	124
4.4.13 Allow Replication for Upgraded Site(N+0) configuration of RMS blade	124
4 4 14 Verify Post Ungrade status on RMS servers (N+0 3-Tier)	128
4.5.3-Tier DSR Upgrade for (1+1) DA-MP configuration on RMS servers (including	120
	130
4.5.1 NO Upgrade Execution for PMS servers $(1+1)$ setup	130
4.5.2 Perform Health Check on RMS servers (Pre-I Ingrade of 3-Tier(1+1) NOAMs)	122
4.5.3 Inhibit Replication for 3-tier(1+1) setup on RMS servers	136
4.5.4 Upgrade DR-NOs of 3-Tier(1+1) RMS servers setun	130
4.5.5 Upgrade NOs for 3-Tier(1+1) RMS configuration	141
4.5.6 Allow Replication between NO and DR NO Servers ONLY of 3-Tier(1+1) RMS	
configuration	142
* * · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

	4.5.7	Verify Post Upgrade Status (3-	tier(1+1) RMS NO Upgrade)	
	4.5.8	Site Upgrade for (1+1) 3-Tier F	RMS Configuration.	
	4.5.9	Upgrade SO of RMS configura	tion(3-tier (1+1))	
	4.5.10)Upgrade DA-MP(s) of 3-Tier (1	+1) configuration on RMS servers	147
	4.5.1 ⁻	Verify Post Upgrade status of I	RMS servers(3-Tier(1+1))	149
	4.6 Policy	DRA Upgrade for 3-tier Conf	iguration	151
	4.6.1	Perform Health Check (Pre-Up	grade of NOAM)	
	4.6.2	Upgrade NOs	· · ·	
	4.6.3	Policy SBR MP Server Upgrad	e	
	4.6.4	Upgrade Multiple DA-MPs in 3	-tier DSR running PDRA-Site 1	
	4.6.5	Upgrade IPFE	-	
	4.6.6	Post Upgrade Execution – Site	91	
	4.6.7	Site 1 – Verify Post Upgrade S	tatus	
	4.6.8	SOAM Upgrade - Site 2		
	4.6.9	Policy SBR MP Server Upgrad	e	
	4.6.10) Upgrade Multiple DA-MPs in 3	-tier DSR running PDRA-Site 2	
	4.6.1 ²	IPFE Server Upgrade		174
	4.6.12	Post Upgrade Execution – Site	2	
	4.6.13	Site 2– Verify Post Upgrade St	atus	
	4.7 Site U	ograde for (1+1) 2-Tier Config	guration	179
	4.7.1	Perform Health Check (Pre-Up	grade of 2-tier NOAM)	
	4.7.2	Upgrade 2-Tier NOAM(s)	· ·	
	4.7.3	Perform Health Check		
	4.7.4	2-Tier Upgrade DA-MP(s)		
	4.7.5	Verify Post Upgrade Status (1-	⊦1 2-Tier)	
	4.8 Site U	ograde for (N+0) 2-Tier config	guration	189
	4.8.1	Perform Health Check (Pre-Up	grade of NOAM)	
	4.8.2	Upgrade 2-Tier NOAM	· · · · · · · · · · · · · · · · · · ·	
	4.8.3	Perform Health Check (Post-U	pgrade of NOAM)	
	4.8.4	Upgrade All Active DA-MPs	, , ,	
	4.8.5	Upgrade IPFE(s)		
	4.8.6	Allow Replication for upgraded	2 tier (N+0) Setup	
	4.8.7	Verify Post Upgrade Status (N	+0 2-Tier)	
	4.9 Post-L	pgrade Procedures	, 	201
	4.9.1	Perform Post-Upgrade		
	4.9.2	Accept Upgrade		
	-			-
5.	BACKOU	FPROCEDURE OVERVIEW	1	
•••	5 1 Recov	erv Procedures		206
	5.2 Backo	it Setup		206
	5.2 Dacku	n Bookout		200
	5.5 Ferron	Back Out Entire Natural		207
	5.3.1	Back Out Entire Network		
	5.3.2	Back Out Single Server		
	5.4 Post-E	ackout Procedures	1 ()	
	5.4.1	Perform Health Check (Post-B	ackout)	
•				
6.	APPENDI	xes		221
AP	PENDIX A	COMMAND OUTPUTS		221
AP	PENDIX B	SWOPS SIGN OFF		222
AP	PENDIX C	CUSTOMER SIGN OFF		223
909	-2277-001 R	evision A, March 2014	Version 4.0	5 of 252

APPENDIX D. SECTION DELETED	.224
APPENDIX E. DETERMINE IF TVOE UPGRADE IS REQUIRED	.225
APPENDIX F. ADDING ISO IMAGES TO PM&C IMAGE REPOSITORY	.226
APPENDIX G. UPGRADE SINGLE SERVER – UPGRADE ADMINISTRATION	.230
APPENDIX H. UPGRADE FIRMWARE	.247
APPENDIX I. NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL	.248
APPENDIX J. UPGRADE TVOE PLATFORM	.249
APPENDIX K. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE	.251

LIST OF FIGURES

Figure 1.	Example Procedure steps used in this document	14
Figure 2.	Supported Upgrade Paths	15
Figure 3.	Upgrade Maintenance Windows for 3-Tier Upgrade	23

List of Tables

Table 1. Acronyms	10
Table 2. Terminology	12
Table 3. Logins, Passwords and Server IP Addresses	21
Table 4. Pre-Upgrade Overview	30
Table 5. TVOE Upgrade (multiple site servers in a MW)	51
Table 6. 3-Tier Upgrade Path Reference	54
Table 7. 2-Tier Upgrade Path Reference	55
Table 8. NO Upgrade Execution Overview (For DSR 3-tier configuration)	55
Table 9. Site Upgrade Execution Overview (For DSR (1+1) 3-tier configuration)	72
Table 10. NO Upgrade Execution Overview (For DSR 3-tier configuration)	78
Table 11. Upgrade Execution Overview (For DSR (N+0) 3 tier configuration)	93
Table 12. NO Upgrade Execution Overview (For DSR 3-tier(N+0) RMS configuration)	104
Table 13. Upgrade Execution Overview (For DSR (N+0) 3 tier configuration)	119
Table 14. NO Upgrade Execution Overview (For DSR 3-Tier(1+1) RMS configuration)	131
Table 15. Upgrade Execution Overview (For DSR (1+1) 3 tier RMS configuration)	145
Table 16. Upgrade Execution Overview for PDRA (Site 1)	151
Table 17 Upgrade Execution Overview for PDRA (Site 2)	152
Table 18. Upgrade Execution Overview (For DSR (1+1) 2-tier configuration)	179
Table 19. Upgrade Execution Overview (For (N+0) 2-tier configuration)	189
Table 20. Post-Upgrade Procedures Overview	201
Table 21. Backout Procedure Overview	205

List of Procedures

Procedure 1: Required Materials Check	31
Procedure 2: Backup Global and Site Provisioning Data	31
Procedure 3: Full DB Run Environment Backup	33
Procedure 4: Perform Health Check (Upgrade Preparation)	36
Procedure 5: Perform Health Check (Upgrade Preparation for PDRA configuration)	39
Procedure 6: New LV for NetBackup Client	41
Procedure 7: ISO Administration.	45
Procedure 8: Upgrade TVOE Hosts for a site	51
Procedure 9: Perform Health Check (Pre-Upgrade of 3-Tier (1+1) NOAM)	57
Procedure 10. Inhibit Replication for 3-Tier (1+1) setup	61
Procedure 11. Upgrade DR-NO(s) 3 – Tier (1+1) configuration	65
Procedure 12. Upgrade NO for 3 – Tier (1+1) configuration	67
Procedure 13. Allow Replication between NO and DR NO Servers of 3-Tier(1+1)	68
Procedure 14: Verify Post Upgrade Status (NO Upgrade) for 3-Tier (1+1) setup	69
Procedure 15. Upgrade SO(s) of (1+1) 3 -Tier configuration	73
Procedure 16: Upgrade MP(s) of (1+1) 3-Tier configuration	75
Procedure 17: Verify Post-Upgrade Status (1+1 3 Tier)	76
Procedure 18: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM)	79
Procedure 19. Inhibit Replication for 3-Tier(N+0) setup.	83
Procedure 20. Upgrade DR-NO(s) 3 - Tier configuration	86
Procedure 21. Upgrade NO for 3 – Tier(N+0) configuration	88
Procedure 22. Allow Replication between NO and DR NO Servers for 3-Tier (N+0) setup	89
Procedure 23: Verify Post Upgrade Status (3-Tier(N+0) NO Upgrade)	90
Procedure 25. Upgrade cSBR(s) in 3-Tier(N+0) Configuration	97
Procedure 26. Upgrade All Active DA-MPs in a 3-Tier Configuration	98
Procedure 27. Upgrade IPFE(s) in 3-Tier(N+0) Configuration	98
Procedure 28: Allow Replication for upgraded Site in 3-Tier(N+0) configuration	100
Procedure 29: Verify Post Upgrade status (N+0 3-Tier)	102
Procedure 30: Perform Health Check (Pre-Upgrade of 3-Tier(N+0) NOAM on RMS blade)	106
Procedure 31. Inhibit Replication for 3-Tier(N+0) RMS setup	110
Procedure 32. Upgrade DR-NO(s) 3 – Tier(N+0) RMS configuration	112
Procedure 33. Upgrade NO for 3 – Tier(N+0) RMS configuration	114
Procedure 34. Allow Replication between NO and DR NO Servers on RMS servers (3-tier(N+0))	115
Procedure 35: Verify Post Upgrade Status on RMS servers (3-tier(N+0) NO Upgrade)	116
Procedure 36: Perform Health Check for Site Upgrade (3-Tier (N+0) RMS blade)	120
Procedure 37 Upgrade SO(s) of (N+0) 3-Tier RMS configuration	121
Procedure 38. Upgrade All Active DA-MPs in a 3-Tier(N+0) RMS Configuration	124
Procedure 39 Upgrade IPEE(s) in 3-Tier(N+0) RMS Configuration	124
Procedure 40: Allow Replication for upgraded Site(N+0) configuration of RMS blade	126
Procedure 41: Verify Post Upgrade status on RMS servers (N+0 3-Tier).	128
Procedure 42: Perform Health Check on RMS servers (Pre-Upgrade of 3-Tier(1+1) NOAM)	132
Procedure 43. Inhibit Replication for 3-Tier(1+1) setup on RMS servers	136
Procedure 44. Upgrade DR-NO(s) 3 –Tier(1+1) RMS configuration	139
Procedure 45. Upgrade NO for 3 – Tier(1+1) RMS configuration	141
Procedure 46. Allow Replication between NO and DR NO Servers on RMS servers(3-tier(1+1))	142
909-2277-001 Revision A, March 2014 Version 4.0	7 of 252

Procedure 47: Verify Post Upgrade Status (3-tier(1+1) RMS NO Upgrade)	143
Procedure 48. Upgrade SO(s) of (1+1) 3-Tier configuration	146
Procedure 49: Upgrade MP(s) of (1+1) 3-Tier configuration on RMS servers	147
Procedure 50: Verify Post Upgrade status of RMS servers(3-Tier(1+1))	149
Procedure 51: Perform Health Check (Pre-Upgrade of NOAM)	153
Procedure 52. TVOE Upgrade and NO Servers Upgrade	154
Procedure 53. TVOE Upgrade and SO Servers Upgrade	156
Procedure 54. Policy SBR Upgrade – Site 1	160
Procedure 55. Upgrade Multiple DA-MPs of PDRA setup – Site 1	162
Procedure 56. IPFE Server Upgrade – Site 1	163
Procedure 57. Site 1: Post Upgrade Steps	164
Procedure 58: Verify Post Upgrade Status	166
Procedure 59. SOAM Servers Upgrade	167
Procedure 60. Policy SBR Upgrade – Site 2	172
Procedure 61: Upgrade Multiple DA-MPs of PDRA setup – Site 2	173
Procedure 62. IPFE Server Upgrade – Site 2	174
Procedure 63. Site 2: Post Upgrade Steps	175
Procedure 64: Verify Post Upgrade Status	177
Procedure 65: Perform Health Check	180
Procedure 66: Upgrade NO(s) of (1+1) 2-Tier configuration	181
Procedure 67: Perform Health Check (Post-Upgrade of NOAM)	184
Procedure 68: Upgrade MP(s) of (1+1) 2-Tier configuration	186
Procedure 69: Verify Post Upgrade Status (1+1 2-Tier)	187
Procedure 70: Perform Health Check (Pre-Upgrade of NOAM)	190
Procedure 71. Upgrade NO(s) of (N+0) 2-Tier configuration	191
Procedure 72: Perform Health Check (Post-Upgrade of NOAM)	195
Procedure 73. Upgrade Multiple DA-MPs in 2-Tier Configuration	197
Procedure 74. Upgrade IPFE(s) in 2-Tier Configuration	198
Procedure 75: Allow Replication for Upgraded Site	199
Procedure 76: Verify Post Upgrade Status (N+0 2-Tier)	199
Procedure 77: Perform Post Upgrade Health Check	201
Procedure 78: Accept Upgrade (Post-Upgrade of full system)	202
Procedure 79: Back Out Entire Network	207
Procedure 80: Back out Single Server	214
Procedure 81: Perform Health Check (Post-Backout)	220
Procedure 82: Determine if TVOE Upgrade is Required	225
Procedure 83: Upgrade Single Server – Upgrade Administration	230
Procedure 84: Upgrade TVOE	249

This page intentionally left blank.

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform a major upgrade from DSR 4.x to 5.x, or incremental upgrade from an earlier DSR 5.x release to a later DSR 5.x release. The upgrade of both HP C-Class blades and RMS servers is covered by this document. The audience for this document includes Tekelec customers as well as following internal groups: Software Development, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document provides step-by-step instructions to execute any incremental or major software upgrade.

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

1.1.1 What is Not Covered by this Document

- Distribution of DSR 5.x software loads. Please contact Tekelec Customer Service for the same refer Appendix K.
- Initial installation of DSR software. Refer [5] and [6].

1.2 References

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

1.3 Acronyms

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

Table 1. Acronyms

Table 1. Acronyms

DSR	Diameter Signaling Router
DSR DR NO	Disaster Recovery DSR NO
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
НА	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NO	Network OAM
NOAM	Network OAM
OA	HP Onboard Administrator
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PM&C	Platform Management and Configuration
P-DRA	Policy Diameter Routing Agent
pSBR	Policy Session Binding Repository
RMS	Rack Mount Server
SBR	Session Binding Repository
SDS	Subscriber Database Server
SO	System OAM
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XIH	Intelligent Hub for Tekelec XG elements
XMI	External Management Interface
XSI	External Signaling Interface

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

Upgrade	The process of converting an application from its current release on a system to a
	newer release.
Major Upgrade	An upgrade from one DSR release to another DSR release. e.g. DSR 4.x to DSR 5.x.
Incremental Upgrade	An upgrade within a given DSR release e.g. 5.0.x to 5.0.y.
Release	Release is any particular distribution of software that is different from any other
	distribution.
Single Server Upgrade	The process of converting a DSR $4.x/5.x$ server from its current release to a newer
	release.
Blade (or Managed Blade)	Single Server upgrade performed on a blade. This upgrade requires the use of the
Upgrade	PM&C GUI.
Backout	The process of converting a single DSR 5.x server to a prior version. This could
	be performed due to failure in Single Server Upgrade or the upgrade cannot be
Deserve and le /Deselve and	The process of converting a DSD 5 receiver from its superior related process.
Downgrade/Backout	release. This could be performed due to a michabaving system. Once the ungrade
	is accepted, server cap't be backed out to previous release
Pollback	Automatic recovery procedure that puts a server into its pro-upgrade status. This
KOIIDACK	procedure occurs automatically during ungrade if there is a failure
	procedure occurs automatically during upgrade if there is a failure.
Source release	Software release to upgrade from.
Source release Primary NOAM Network	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM
Source release Primary NOAM Network Element	Software release to upgrade from.The network element that contains the active and standby NOAM servers in aDSR. In a 2-tier DSR, there is only a single network element, and it contains theNOAMs and all MPs. So this single network element is both the primary NOAMnetwork element and the signaling network element. In a 3-tier DSR, there are
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the
Source release Primary NOAM Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same.
Source release Primary NOAM Network Element Signaling Network	Software release to upgrade from.The network element that contains the active and standby NOAM servers in aDSR. In a 2-tier DSR, there is only a single network element, and it contains theNOAMs and all MPs. So this single network element is both the primary NOAMnetwork element and the signaling network element. In a 3-tier DSR, there aremore possible combinations. If the NOAMs are deployed on a rack-mount server(and often not co-located with any other site), that RMS is considered the primaryNOAM network element. If the NOAMs are virtualized on a C-class blade that ispart of one of the sites, then the primary NOAM network element and thesignaling network element hosting the NOAMs are one and the same.Any network element that contains DA-MPs (and possibly other C-level servers),
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs that contains pathwork element includes a server that hosts
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM notwork of the primary hood the same is also considered to be the primary NOAM setup.
Source release Primary NOAM Network Element Signaling Network Element	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element.
Source release Primary NOAM Network Element Signaling Network Element Site	Software release to upgrade from. The network element that contains the active and standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations. If the NOAMs are deployed on a rack-mount server (and often not co-located with any other site), that RMS is considered the primary NOAM network element. If the NOAMs are virtualized on a C-class blade that is part of one of the sites, then the primary NOAM network element and the signaling network element hosting the NOAMs are one and the same. Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element. See Signaling Network Element. For a 2-tier DSR, the site is defined by the NOAM network element.
Source release Primary NOAM Network Element Signaling Network Element Site Target release	Software release to upgrade from.The network element that contains the active and standby NOAM servers in aDSR. In a 2-tier DSR, there is only a single network element, and it contains theNOAMs and all MPs. So this single network element is both the primary NOAMnetwork element and the signaling network element. In a 3-tier DSR, there aremore possible combinations. If the NOAMs are deployed on a rack-mount server(and often not co-located with any other site), that RMS is considered the primaryNOAM network element. If the NOAMs are virtualized on a C-class blade that ispart of one of the sites, then the primary NOAM network element and thesignaling network element that contains DA-MPs (and possibly other C-level servers),thus carrying out Diameter signaling functions. In a 2-tier DSR, the signalingnetwork element and the "site" are one and the same. In a 3-tier DSR, eachSOAM pair and its associated C-level servers are considered a single signalingnetwork element. And if a signaling network element includes a server that hoststhe NOAMs, that signaling network element is also considered to be the primaryNOAM network element.

Health Check	Procedure used to determine the health and status of the DSR's internal network.	
	This includes statuses displayed from the DSR GUI and PM&C GUI. This can	
	be observed pre-server upgrade, in-progress server upgrade, and post-server	
	upgrade.	
Upgrade Ready	State that allows for graceful upgrade of a server without degradation of service.	
	It is a state that a server is required to be in before upgrading a server. The state is	
	defined by the following attributes:	
	• Server is Forced Standby	
	• Server is Application Disabled (signaling servers will not process any	
	traffic)	
UI	User interface. Platcfg UI refers specifically to the Platform Configuration Utility	
	User Interface which is a text-based user interface.	
Management Server	Server deployed with HP c-class or RMS used to host PM&C application, to	
	configure Cisco 4948 switches and to serve other configuration purposes.	
PM&C Application	PM&C is an application that provides platform-level management functionality	
	for HPC/RMS system, such as the capability to manage and provision platform	
	components of the system so it can host applications.	
1+1	Setup with one active and one standby DA-MP.	
N+0	Setup with N active DA-MP(s) but no standby DA-MP.	
NO	Network OAM for DSR.	
SO	System OAM for DSR.	
Migration	Changing policy and resources after upgrade(if required). For E.g. changing from	
	1+1 (Active Standby) policy to N+0 (Multiple Active) policy.	
RMS geographic site	Two rack-mount servers that together host 1) an NOAM HA pair; 2) an SOAM	
	HA pair; 3) two DA-MPs in either a 1+1 or N+0 configuration; 4) optional	
	IPFE(s).	
RMS Diameter site	One or two RMS geographic sites that implement a single Diameter network	
	element. If there are two RMS geographic sites, they are always configured as a	
	geo-redundant pair, and only one handles the signaling duties of the network	
	element at any given time. The primary RMS Diameter site contains the NOAM	
	pair used to manage the network element, while the geo-redundant RMS Diameter	
	site contains a disaster recovery NOAM pair.	

1.5 How to Use this Document

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

- 1) Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- 2) Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
- 3) If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP and contact Tekelec Customer Service (*US: 1-888-367-8552, Intl: +1-919-460-2150*) for assistance before attempting to continue.

1.5.1 Executing Procedures

The figure below shows an example of a procedural step used in this document.

• Each step has a checkbox that the user should check-off to keep track of the progress of the procedure.

909-2277-001 Revision A, March 2014

13 of 252

- 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.
		 Select Configuration > Network Elements to view Network Elements Configuration screen. Click Report at the bottom of the table to generate a report for all entries. The report opens in a new window. Verify the configuration data is correct for your network. Save the report and print the report. Keep these copies for future reference. Close report window.

1.6 Recommendations

Here are some recommendations to consider when preparing to execute the procedures in this document.

1.6.1 Frequency of Health Checks

The user may execute the **Perform Health Check** or **View Logs** steps repetitively between procedures during the upgrade process. It is not recommended to do this between steps in a procedure, unless there is a failure to troubleshoot.

1.6.2 Large Installation Support

For large systems containing multiple Signaling Network Elements, it's impossible to upgrade multi-site systems in a single maintenance window. However, whenever possible, primary NOAM Network Element servers should be upgraded within the same maintenance window.

1.6.3 Logging of Upgrade Activities

It is a best practice to use a terminal session with logging enabled to capture user command activities and output during the upgrade procedures. These can be used for analysis in the event of issues encountered during the activity. These logs should be saved off line at the completion of the activity.

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

2. GENERAL DESCRIPTION

This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 4.x to target release 5.x. An incremental upgrade advances the DSR from an earlier DSR 5.x source release to a more recent 5.x target release.

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

2.1 Supported Upgrade Paths

The supported paths to upgrade to a DSR 5.x target release are shown in Figure 2 below.

Note: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.







2.2 2-Tier vs 3-Tier Upgrades

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

In DSR 4.0, the 3-Tier (Split Network Level and Site Level OAM functions) was introduced for new installs of the DSR system. [2-Tier OAM supports site only management] As a result, there are both 2-Tier and 3-Tier DSR 4.0 network deployments. Both may be upgraded to DSR 5.0, while retaining the existing 2-Tier or 3-Tier configuration. For 2-Tier Upgrade, the upgrade will upgrade a site-at-a-time to DSR 5.0.

Note: A feature is provided in DSR 5.0 to allow migration from 2-Tier to 3-Tier architecture. This would be performed after the upgrade to DSR 5.0 is completed. See Reference [8].

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

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

Assumptions:

- It is assumed that only sites with N+0 redundancy will have IPFE.
- It is assumed that all sites of a 3-tier deployment will have the same redundancy (either N+0 or 1+1), but not a mix of the two in the same 3-tier network.

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

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

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

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

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

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

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

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

2.5 Firmware Updates

Firmware upgrades are not in the scope of this document, but may be required before upgrading DSR.. It is assumed that these are done when needed by the hardware, and there is typically not a dependency between Firmware version and the DSR 5.0 release. See Release Notes for any dependencies.

2.6 PMAC (Management Server) Upgrades

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

2.7 TVOE Upgrade

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

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

- PMAC
- DSR NOAM and SOAM Applications
- SDS NOAM and SOAM Applications

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

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

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

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

- Option A: Upgrade TVOE environments as a separate activity that is planned and executed days or weeks before the Application upgrades (perhaps site-at-a-time) (Preferred)
- Options to Upgrade TVOE and Application at the same maintenance window:
 - Option B: Upgrade TVOE and Application, followed by another TVOE and Application. Example: for Standby SOAM Upgrade – stop application, upgrade TVOE, upgrade Application, start application; then repeat for Active SOAM.

- Option C: Upgrade multiple TVOE Hosts at a site, and then start upgrading the Applications (same Maintenance Window)

Note that TVOE upgrades require a brief shutdown of the guest application(s) on the server. Note also that the TVOE virtual hosts may be hosting SDS NOAM or SOAM applications also these applications will also be affected.

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

2.8 SDS Upgrade

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

2.9 Traffic Management during Upgrade

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

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

2.10 Optional NetBackup

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

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

2.11 RMS Deployments

DSR 4.1 added support for Rack Mount Server (RMS) deployments of DSR. All Deployments with RMS will be 3-Tier. In these smaller deployments, the Message Processing (MP) servers may be virtualized (deployed on a TVOE HOST) to reduce the number of servers required.

The following commercial deployment types are supported:

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

When an RMS-based DSR is without geographic redundancy, there is just a single RMS geographic site, functioning as a single RMS Diameter site. The upgrade of this DSR deployment should be done in two maintenance windows: one for the NOAMs, and the second for all remaining servers.

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

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

3. UPGRADE PLANNING AND PRE-UPGRADE PROCEDURES

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

There are overview tables throughout this section that help you plan the upgrade and estimate how long it will take to perform various actions. The stated time durations for each step or group of steps <u>are estimates only</u>. Do not use the overview tables to execute any actions on your system. Only the procedures should be used when performing upgrade actions, beginning with Procedure 1: Required Materials Check.

3.1 Required Materials

The following materials and information are needed to execute an upgrade:

- Target-release application ISO image file, or target-release application media.
- The capability to log into the DSR 4.x/5.x Network OAM servers with Administrator privileges. Note: All logins into the DSR 4.x/5.x NO servers are made via the External Management VIP unless otherwise stated.
- User logins, passwords, IP addresses and other administration information. See Section 3.1.2.
- VPN access to the customer's network is required if that is the only method to log into the OAM servers.
- Direct access to the blades iLO/XMI IP addresses (whichever applicable) from the workstations directly connected to the DSR servers is required.

3.1.1 Application ISO Image File / Media

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

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

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

Note: Prior to the execution of this upgrade procedure it is assumed that the DSR 5.x ISO image file has already been delivered to the customer's premises. The ISO image file must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image file. If the user performing the upgrade is at a remote location, it is assumed the ISO file is already available to them before starting the upgrade procedure.

3.1.2 Logins, Passwords and Server IP Addresses

Obtain all the information in the following table. This ensures that the necessary administration information is available prior to an upgrade.

Consider the sensitivity of the information recorded in this table. While all of the information in the table is required to complete the upgrade, there may be security policies in place that prevent the actual recording of this information in hard-copy form.

Item	Description	Recorded Value
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username ¹	
	GUI Admin Password	
	Root Password ²	
	Blades iLO Admin Username	
	Blades iLO Admin Password	
	PM&C GUI Admin Username	
	PM&C GUI Admin Password	
	PM&C root Password	
	PM&C pmacftpusr password	
	OA GUI Username	
	OA GUI Password	
VPN Access	Customer VPN information (if needed)	
Details		
NO	XMI VIP address ³	
	NO 1 XMI IP Address	
	NO 2 XMI IP Address	
SO	XMI VIP address	
	SO 1 XMI IP Address (Site 1)	
	SO 2 XMI IP Address (Site 1)	
	Policy DRA (DSR) Spare System OAM&P server – Site 1	
	Spare in Site 2, XMI IP Address	
	SO 1 XMI IP Address (Site 2)	
	SO 2 XMI IP Address (Site 2)	
	Policy DRA (DSR) Spare System OAM&P server – Site 2	
	Spare in Site 1, XMI IP Address	
Binding pSBR	Binding pSBR SR1 Server Group Servers (Site 1)	
Server Groups	Binding pSBR SR2 Server Group Servers (Site 1)	
	Binding pSBR SR3 Server Group Servers (Site 1)	
	Binding pSBR SR4 Server Group Servers (Site 1)	
Session pSBR	Session pSBR SR1 Server Group Servers (Site 1)	
Server Groups	Session pSBR SR2 Server Group Servers (Site 1)	
	Session pSBR SR3 Server Group Servers (Site 1)	
	Session pSBR SR4 Server Group Servers (Site 1)	
P-DRA MP	Policy DRA MP Server Group Servers (Site 1)	
Server Group		
	Policy DRA MP Server Group Servers (Site 1)	
IPFF Server	P-DRA IPFE A1 Server Group Server(Site 1)	
Groups(For	P-DRA IPFE A 2 Server Group Server(Site 1)	
PDRA)	P-DRA IPEE B 1 Server Group Server(Site 1)	
-		

 Table 3. Logins, Passwords and Server IP Addresses

909-2277-001 Revision A, March 2014

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

² Note: This is the password for the **root** login on the servers. This is not the same login as the GUI Administrator. The root password is required if recovery procedures are needed. If the **root** password is not the same on all other servers, then all those servers' root passwords must also be recorded; use additional space at the bottom of this table. ³ Note: All logins into the NO servers are made via the External Management VIP unless otherwise stated.

	P-DRA IPFE B 2 Server Group Server(Site 1)	
Binding PSBR	Binding pSBR SR1 Server Group Servers (Site 2)	
Server Groups	ver Groups Binding pSBR SR2 Server Group Servers (Site 2)	
	Binding pSBR SR3 Server Group Servers (Site 2)	
	Binding pSBR SR4 Server Group Servers (Site 2)	
Session PSBR Session pSBR SR1 Server Group Servers (Site 2)		
Server Groups	Session pSBR SR2 Server Group Servers (Site 2)	
	Session pSBR SR3 Server Group Servers (Site 2)	
	Session pSBR SR4 Server Group Servers (Site 2)	
P-DRA MP	Policy DRA MP Server Group Servers (Site 2)	
Server Group		
IPFE Server	P-DRA IPFE A1 Server Group Server(Site 2)	
PDRA)	P-DRA IPFE A 2 Server Group Server(Site 2)	
	P-DRA IPFE B 1 Server Group Server(Site 2)	
	P-DRA IPFE B 2 Server Group Server(Site 2)	
iLO	NO 1 iLO IP Address	
	NO 2 iLO IP Address	
	SO 1 iLO IP Address	
	SO 2 1LO IP Address	
	MP 1 1LO IP Address	
	MP 2 1LO IP Address	
	MP (n) 1LO IP Address	
	IPFE MP iLO IP Address (optional)	
	IPFE MP 1LO IP Address (optional)	
	IPFE MP (n) 1LO IP Address (optional)	
	CSBR MP ILO IP Address (optional)	
	CSBR MP ILO IP Address (optional)	
	CSBR MP ILO IP Address (optional)	
	CSBK MP ILO IP Address (optional)	
	CSBK MP(n) 1LO 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 1LO IP Address (optional)	
DMAG	DA MP(n) 1LO IP Address (optional)	
PM&C	PM&C Management IP Address(Site 1)	
PM&C	PM&C Management IP Address(Site 2)	
Software	Target Release Number	

	ISO Image (.iso) file name	
Misc. ⁴	Miscellaneous additional data	

3.2 Plan Upgrade Maintenance Windows

This section provides a high-level checklist to help you keep track of individual server upgrades. The servers have been grouped by maintenance window, and it is expected that all servers in a group can be successfully upgraded in a single maintenance window. Use this high-level checklist together with the detailed procedures that appear later in this document.

Below mentioned figure shows a recommended approach to collecting the upgrade activities into Maintenance windows. This document supports this approach.

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

Figure 3. Upgrade Maintenance Windows for 3-Tier Upgrade

⁴ As instructed by Tekelec Customer Service.



!! WARNING!!

MATED SITES MUST BE UPGRADED IN SEPARATE MAINTENANCE WINDOWS

3.2.1 Maintenance Window for PMAC and TVOE Upgrades (optional)

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

• PMAC Upgrade procedure is provided in Reference [4].

• TVOE Host environment upgrade procedures are included in architecture-specific sections this document.

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

It may be done a site-at-a-time.

3.2.2 Calculating Maintenance Windows Required

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

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



3.2.3 Maintenance Window 1 (3-Tier NOAM servers)

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

This Maintenance Window will not be required for 2-Tier deployments.

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

 DSR Standby NOAM: DSR Active NOAM:
TVOE for Standby SOAMs:
TVOE for Active SOAMs:

3.2.4 Maintenance Window 2 (First Site upgrade)

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

Maintenance Window 2	 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:
Date:	 "Check off" the associated Check Box as upgrade is completed for each server.
	SOAM/2-Tier NOAM Site1:
	DA-MP1: DA-MP2: DA-MP3:

DA-MP4: DA-MP5:
DA-MP16:
Note: For 1+1 configuration, only 2 DA-MP(s) will be present, one is Active while another is standby.

3.2.5 Maintenance Window 3 (Additional site upgrade)

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

The following form does also apply to 2-Tier upgrade, where the SOAM is replaced with a 2-Tier NOAM.

Maintenance Window 3 Date:	 Record the Site NE Name of the DSR SOAM Site 2 and the MP(s) to be upgraded during Maintenance Window 3 in the space provided below: "Check off" the associated Check Box as upgrade is completed for each server.
NOTE: The NE Name may be viewed from the Primary Provisioning Site GUI under [Main Menu → Configuration → Network Elements	SOAM/2-Tier NOAM Site2: IPFE1: IPFE2: cSBR: pSBR: pSareSBR: SpareSBR: DA-MP1: DA-MP2: DA-MP3: DA-MP5: DA-MP6: DA-MP6: DA-MP8: DA-MP9:
	DA-MP10:

DA-MP11:
DA-MP12:
DA-MP13:
DA-MP14:
DA-MP15:
DA-MP16:

3.3 Pre-Upgrade Procedures

The pre-upgrade procedures shown in the following table are executed outside a maintenance window, if desired. These steps don't have any effect on the live system and can save upon maintenance window time, if executed before the start of the Maintenance Window. Note that the elapsed time is for a "Lab Environment", and that they might vary on Live Systems.

Procedure Number	Elapsed (Hours: M	d Time /linutes)	Procedure Title	Impact
	This Step	Cum.		
Procedure 1	0:10- 0:30	0:10- 0:30	Required Materials Check	None
Procedure 2	0:10- 0:60	0:20- 1:30	Backup all Global and Site Provisioning Data	None
Procedure 3	0:10- 2:00	0:30- 3:30	Full DB Backup	None
Procedure 4	0:10- 1:15 (Depends upon number of servers)	0:40- 1:45	Perform Health Check(Upgrade Preparation)	None
Procedure 5	0:20- 0:30 (Depends upon number of servers and sites)	1:00- 5:15	Perform Health Check(Upgrade Preparation for PDRA configuration only))	None
Procedure 6	0:15- 0:20	1:15- 5:35	New LV for NetBackup Client	None
Procedure 7	0:02- 0:10*	0:57- 5:45	ISO Administration	None

Note: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed and require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

3.3.1 Hardware Upgrade Preparation

There is no hardware preparation necessary when upgrading to DSR release 5.x

3.3.2 Review Release Notes

Before starting the upgrade, review the Release Notes for the new DSR5.x release to understand the functional differences and possible traffic impacts of the upgrade.

3.3.3 Required Materials Check

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

Procedure 1: Required Materials Check

S	This procedure verifi	es that all required materials are present.	
T E	Check off (\checkmark) 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.		
π			
1	Verify all required	Materials are listed in Section 3.1: Required Materials. Verify required materials are	
	materials are present		
2	Verify all administration data needed during upgrade	Double-check that all information in Section 3.1.2 is filled-in and accurate.	
3	Contact Tekelec Customer Care Center	Contact the Tekelec Customer Care Center and inform them of your plans to upgrade this system. See Appendix K for these instructions.	
		Note that obtaining a new online support account can take up to 48 hours.	

3.3.4 Collect/Backup all Global and Site Provisioning Data

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

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

Procedure 2: Backup Global and Site Provisioning Data

S	This procedure performs a backup of the Global and Site Provisioning Data		
T E	Check off (ψ) 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 and collect Network Element	View the Network Elements configuration data; verify the data; save and print report:	
	Configuration data	Log into the NOAM GUI using the VIP.	
		 Select Configuration > Network Elements to view Network Elements Configuration screen. Click Report at the bottom of the table to generate a report for all entries. Verify the configuration data is correct for your network. Save the report and/or print the report. Keep these copies for future reference. 	
2	Verify and collect Server Group Configuration data	 View the Server Group configuration data; verify the data; save and print report: From the NOAM VIP GUI Select Configuration > Server Groups to view Server Group screen. Click Report at the bottom of the table to generate a report for all entries. 	

Procedure 2: Backup Global and Site Provisioning Data

		3. Verify the configuration data is correct for your network.
		4. Save the report and/or print the report. Keep these copies for future reference.
3	Verify and collect	View the Servers configuration data; verify the data; save and print report:
	Servers Configuration	From the NOAM VIP CI II
	uala	1 Select Configuration > Servers to view Servers screen
		 Click Report at the bottom of the table to generate a report for all entries.
		3. Verify the configuration data is correct for your network.
		4. Save the report and/or print the report. Keep these copies for future reference.
4	Verify and collect Services Configuration	View the Services configuration data; verify the data; save and print report:
	data	From the NOAM VIP GUI
		1. Select Configuration > Services to view Services screen.
		2. Click Report at the bottom of the table to generate a report for all entries.
		3. Verify the configuration data is correct for your network.
		4. Save the report and/or print the report. Keep these copies for future reference.
_	Verify and callest	View the Circulian Networks configuration data, with the data, and print an esti-
	Signaling Network	view the Signaling Networks configuration data, verify the data, save and print report.
	Configuration data	From the NOAM VIP GUI
		1. Select Configuration > Network to view the Signaling Networks.
		2. Click Report (or " Report All " for DSR 5.x) at the bottom of the table to generate a
		report for all entries .
		3. Verify the configuration data is correct for your network.
		4. Save the report and/or print the report. Keep these copies for future reference.
		 Select Configuration > Network > Devices and repeat sub steps 3 through 5(not required for DSD 5 x)
		Figure 101 DSK 5.X). 6 Select Configuration > Network > Poutes and repeat sub steps 3 through 5(not)
		required for DSR 5 x)
6	Collect database reports	Backup the global database from the primary active NO server:
		From the NOAM VIP GUI
		1. Select Status & Manage > Database to view Database Status screen.
		2. Click to highlight the Active NO server to be backed up, and click Report .
		3. Save the report and print the report. Keep these copies for future reference.
		4. Click to highlight each of the Active SO(S) (if exists) to be backed up, and click Bonort Name the backup file to identify the SO
		5 Save the report and print the report. Keen these copies for future reference
7	Backup all global and	Backup the global database from the primary active NO and all Active SO servers:
	site provisioning	
	databases for NO (and SO's)	For the active NO server (and all active SO's for 3-Lier)
	,	Login to NO or SO GUI
	IMPORTANT: Required	1. Select Status & Manage > Database to return to the Database Status screen.
	for Disaster Recovery	 Click to highlight the Active NO server (if logged into Active NOAM GUI) or Active SO
		server (if logged into Active SOAM server) click Backup ; the Backup and Archive
		screen is displayed. (Note: the Backup button will only be enabled when the
		active server is selected.)
		3. Click Backup and archive both Configuration and Provisioning Data(Note:
		Provisioning check box is not selectable from the GUI)
		4. Enter Comments (optional)
		5. Click OK .
		Repeat substeps 1 to 5 for each Active NO and active SO server (if exists)
		Note: Active NO/SO can be found out by going to Status & Manage->HA screen, and see
		which server is currently assigned the VIP in the "Active VIPs" field. The server having VIP

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

3.3.5 Full Backup of DB Run Environment at each server

This procedure is part of software upgrade preparation and is used to conduct a full backup of the run environment on each server, to be used in the event of a backout of the new software release.



!! WARNING!!

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

Procedure 3: Full DB Run Environment Backup

S	This procedure (executed form the Active NO server) conducts a full backup of the run environment			
Т	on each server, so that	on each server, so that each server has the required data to perform a Backout.		
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	Log into the Active NO	Use the ssh command (on UNIX systems – or putty if running on Windows) to log in the Active NO:		
		ssh root@ <no_vip></no_vip>		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)		

Procedure 3: Full DB Run Environment Backup

S	This procedure (ever	$r_{\rm uted}$ form the Active NO server) conducts a full backup of the run environment
Г	on each server so that	each server has the required data to perform a Backout
F	on each server, so that	tach server has the required data to perform a backout.
P	Check off (\checkmark) each step as it is	s completed. Boxes have been provided for this purpose under each step number.
#	SHOULD THIS PROCEDURE	FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.
2	SSH to Active NO: Execute Full Backup for all servers (managed	Execute the backupAllHosts utility on 'Active NO'. [This utility will remotely access every server in the scope of the NO, and run the backup command for the server.]
	from this NO)	SSH to the Active NO server:
		# screen
		(the screen tool will create a no-hang-up shell
		session, so that the command will continue to execute if the user session is lost.)
		<pre># /usr/TKLC/dpi/bin/backupAllHosts</pre>
		Following output will be generated for DSR 5.x servers
		only :
		Do you want to remove the old backup files (if exists
) from all the servers (y/[n])?y
		It may take from 10 mins to 2 hrs for this command to complete, depending upon the data in the database.
		Do not proceed until backup on each server is completed.
		Output similar to the following will indicate successful completion:
		Script Completed Status:
		HOSTNAME STATUS
		HPC3blade02 PASS
		HPC3blade01 PASS
		HPC3blade03 PASS
		(Errors will also report back to the command line.)
		Note: There is no progress indication for this command.Only the final report when it completes.
		# exit (to close screen session) (screen -ls and screen -x are used to show active screen sessions on a server, and re-enter a screen session, respectively)
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, login to each server in the system individually, and Execute the following to manually generate a full backup on that server
		<pre># /usr/TKLC/appworks/sbin/full_backup</pre>
		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.
	2	Version 4.0 909-2277-001 Revision A, March 2 gz written in /var/TKLC/db/filemgmt.

Procedure 3: Full DB Run Environment Backup

S	This procedure (executed form the Active NO server) conducts a full backup of the run environment		
Т	on each server, so that each server has the required data to perform a Backout.		
E P	Check off (\checkmark) each step as it is completed. Boxes have been provided for this purpose under each step number.		
#	SHOULD THIS PROCEDURE	FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.	
3	Active NO GUI: Verify that backups are created for all servers	For the active NO: Login to Active NO or SO GUI 1. Select Status & Manage > Files; the Files menu is displayed. 2. Click on each server tab, in turn 3. Verify that the following two files have been created: Backup.DSR. <server_name>.FullDBParts.NETWORK_OAMP.<time_stam p="">.UPG.tar.bz2 Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stam p="">.UPG.tar.bz2</time_stam></server_name></time_stam></server_name>	

3.3.6 Perform Health Check (Upgrade Preparation)

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

Procedure 4: Perform Health Check (Upgrade Preparation)

S	This procedure performs a Health Check.
T E	Check off (\checkmark) each step as it is completed. Boxes have been provided for this purpose under each step number.
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.
#	
Procedure 4: Perform Health Check (Upgrade Preparation)

Verify Software Versions	From the	Active NO	GUI:				
UN DOK Servers	Select Un	arado Adm	inistratio	n form			
			Inistration				
		" Administ	ration > 0	Softu	ie Iaro Mana	acmont -> Unar	ado")
	DSR 5.X.	Adminis	tration ->	5010	are Mana	gement -> Opgr	ade)
	The Upgra	ade Adminis	tration scr	een is	displayed	(example below)	:
	Nete Lee		(
	Note: Loo	k and feel c	of the Upgr	ade so	the energy	changed betweer	DSR 4.X and DSR 5.X
	releases, i	ine example	e below pro	vides	the shaps	not from both the	releases.
	Upgrade	Screen in F	SR 4 x				
	opgrade						
	Unetname	1	Network Elem	ent		Role	Upgrade State
	Hostname	1	Application We	ersion		Function	Server Status
	NO		NO_HPC03			NETWORK OAM	16P Not Ready
	NUT		4.0.0-40.14.1			OAM&P	11
	N02		NO_HPC03			NETWORK OA	16P Not Ready
	102		4.0.0-40.14.1			OAMSP	Norm
			NO_HPC03			MP	Not Ready
	MP1					DSR	2 2 2002
		1	4.0.0-40.14.1			(active/standby pair)	Norm
			NO_HPC03			MP	Not Ready
	MP2					DSR	
			4.0.0-40.14.1			(active/standby	
						hand.	
	Upgrade	Screen in D	DSR 5.x G	UI			
		Server Status	Server Role	Function	Upgrade State	Status Message	
	Hostname	OAM Max HA Rol Max Allowed	e Network Element		Start Time	Finish Time	Mate Server Status
		HA Role	Application versio	n OAMED	Upgrade ISO		
	Viper-NO1	Active	NO_Viper	OAM&P	Not Ready		Viper-NO2
		Active	5.0.0-50.15.1 Network OAM&P	OAM&P	Not Ready		
	Viper-NO2	Standby	NO_Viper				Viper-NO1
		Active	5.0.0-50.15.1 System OAM	OAM	Not Ready		
	Viper-SO1-A	Active	SO1_Viper				Viper-SO1-B
		Norm	System OAM	OAM	Not Ready		
	Viper-SO1-B	Standby	SO1_Viper				Viper-SO1-A
		Norm	System OAM	OAM	Not Ready		
	Viper-SO2-A	Active	SO2_Viper				Viper-SO2-B
		Norm	System OAM	OAM	Not Ready		
	Viper-SO2-B	Standby Active	SO2_Viper 5.0.0-50.15.1				Viper-SO2-A
		Norm	MP	DSR (multi-	Not Ready		
	Viper-MP05	NOTT	iar-	active cluster)	Noticeady		Viper-MP06

Procedure 4: Perform Health Check (Upgrade Preparation)

2	Verify Server Status is	Verify Server Status is Normal:
	Normai	Log in to Active NOAM GUI.
		1. Select Status & Manage > Server; the Server Status screen is displayed.
		2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), Reporting
		status, and Processes (Proc).
		3. Do not proceed to upgrade if any of the server statuses displayed is not Norm .
		4. Do not proceed if there are any Major or Critical alarms.
		Note: It is not recommended to continue executing upgrade if any server status has
		unexpected values. An upgrade should only be executed on a server with unexpected alarms
		if the upgrade is specifically intended to clear those alarm(s). This would mean that the target
		to clear the alarm(s). Do not continue otherwise.
3	Log all current alarms	Log all current alarms in the system:
		From the Active NO GUI
		1. Select Alarms & Events > View Active; the Alarms & Events > View Active view isis
		displayed.
		 Set collection interval as 1 Day or more it needed and click Report button to generate an Alarms report.
		 Save the report and print the report. Keep these copies for future reference.
		4. Select Alarms & Events > View History and repeat substeps 3 and 4.
		5. Log into Active SO (if exists) and repeat substeps 2 to 5.
4	Check If new Firmware Release may be	to find out the minimum supported firmware release required for the target DSP release
	required for the system.	to find out the minimum supported firmware release required for the target DSR release.
		months.
		Target Firmware Rev:
		Example: FW rev 2.2.4
		If upgrade is required, acquire the Firmware release package and follow procedures
		provided with this package to determine which specific system components (Switches,
		Servers, etc) may require upgrade.
		Dien fan Firmwaar I is mede Maintenanse windewe if needed, sie e this estivituis turiselly
		Plan for Firmware Upgrade Maintenance windows, if needed, since this activity is typically performed before the DSP Upgrade
		penormed before the DON opgrade.
5	Check the existing	1. Record the target DSR Release on which servers needs to be upgraded. (5.x.y-5x.nn.a).
	PM&C version and	
	upgrade is required.	2. Find out the PM&C version.
	before starting with DSR	
	upgrade(applies to servers that are already	3. For upgrade to DSR 5.x minimum PM&C required is 5.5 .
	running PM&C)	4 If PM&C version is below 5.5, then identify proper PM&C upgrade document (to be used
		later) based on the indented DSR upgrade path. :
		a) For major DSR upgrade I.e. from DSR 4.x->5.x follow reference [3].
		For Incremental upgrade i.e. from DSR 5.0->DSR 5.x follow reference [4].

6	Check the TVOE Host server software version	1.	Find the target DSR release from Table 3.
		2.	Contact the Tekelec Customer Care Center by referring to Appendix K of this document to find out the minimum supported TVOE OS version required for the target DSR release.
			Required TVOE Release:
			Example: 872-2525-101-2.5.0_82.22.0-TVOE-x86_64.iso
		3.	Follow Appendix E for the procedure to check the current TVOE HOST OS version, for all TVOE Hosts.
		IMF upg	PORTANT: If TVOE Hosts are not on the correct release, then need to plan for TVOE Host rades. See planning section of this document.
7	Check if netbackup	1.	Check the Netbackup server version before starting with DSR upgrade.
	client installed on 2. NOAM/SOAM(if exists)	2.	Supported versions of Netbackup client and Netbackup server for DSR 5.x release are 7.1 or 7.5.
		3.	If Netbackup server is not on 7.1 or 7.5 then plan a Netbackup upgrade before starting with DSR upgrade.
8	Check if the setup has customer supplied	1.	Verify if the setup has customer supplied apache certificate installed and protected with passphrase.
	installed and protected with a passphrase.	2.	If the certificate is installed then rename the certificate. (Make sure that original name is noted down for further usage in Section 4.9.1 Step 4)

Procedure 4: Perform Health Check (Upgrade Preparation)

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

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

Procedure 5: Perform	n Health Chec	k (Upgrade Pre	paration for PDRA	configuration)
-----------------------------	---------------	----------------	-------------------	----------------

S	This procedure perform	This procedure performs a Health Check.						
T E	Check off (\checkmark) 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 <u>UPGRADE ASSISTANCE</u>.						
1	Verify all servers status are normal	 Log in to GUI using NOAMP VIP Select the Status & Manage -> Server menu item. Verify all servers status are Normal (Norm). 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.	 Select the Alarms & Events -> View Active menu item. Click the Export button to generate an Alarms Export file. Record the filename of Alarms CSV file generated and all the current alarms in the system 						

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

		4	
		4.	Keep this information for future reference on client machine.
3	Capture the Diameter	1.	Select Main Menu-> Diameter-> Maintenance
	Maintenance Status	2	Select Maintenance->Route Lists screen
	On Active SOAM VIP	3	Filter out all the Route Lists with Route List Status as "Is Not Available" and "Is
	for all the sites	0.	Available".
		4	Record the number of "Not Avaiable" and "Available" Route Lists
		т. 5	Select Maintenance->Route Groups screen
		6	Filter out all the Boute Groups with "PeerNode/Connection Status as "Is Not
		0.	Available" and "Is Available"
		7	Peccent the number of "Not Available" and "Available" Pouto Groupe, Select
		1.	Maintenance-> Dear Nodes screen
		0	Filter out all the Deer Nodes with "Beer Nede Operational Status" as "Is Not
		0.	Available" and "Is Available"
		0	Available and is Available.
		9.	Record the humber of Not Available and Available peer houes.
		10.	Select Maintenance->Connections screen.
		11.	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	1.	Select Main Menu-> Policy DRA->Maintenance-> Policy SBR Status
	Status	2.	Capture and archive the maintenance status of the following tabs on the client machine
	On Active NOAMP GUI		by either taking screen captures or documenting it in some editor.
			a. BindingRegion
			b. PDRAMatedSites
		2	Source this off to a client machine
_	Conturn the IDEE	J.	Save this of to a client machine.
5	Capture the IPFE	1.	Select Main Menu: IPFE->Configuration->Options
	Screens	2.	Capture and archive the screen capture of the complete screen.
	On Active SOAM GUI on	3.	Save this off to a client machine.
	all the Sites.		
6	Capture the IPFE	1.	Select Main Menu: IPFE->Configuration->Target Sets
	Configuration Target Set	2.	Capture and archive the screen capture of the complete screens.
	screens	3.	Save this off to a client machine.
	On Active SOAM GUI on		
-	all the Sites.	4	Colort Main Manuel Discussion Configuration Frances
7	Export and archive the	1.	Select wain wenu-> Diameter Configuration->Export
		2.	Capture and archive the Diameter and P-DRA data by choosing the drop down entry
	On Active SOAM GUI on		named "ALL".
	all the Sites.	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.
0		_	
8	Data shall be captured	Exe	cute steps 1 to / for each PDRA Site.
	IUI EACH PURA SITE.		

3.3.7 Create new Logical Volume for NetBackup Client on NO/SO(if needed)

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

This section only applies if Symantec's NetBackup utility is already installed on one or more OAM(NO or SO) servers in the DSR to be upgraded. If you know NetBackup is not installed on any of the OAM servers, you can skip this section entirely. If you are not sure if NetBackup is installed on any OAM server, the first step of Procedure 5 below gives instructions on how to check. And if NetBackup is installed on one or more OAM servers, but is already located in its own logical volume on each server where NetBackup is installed, it will not be necessary to create a new logical volume, and this section can be skipped.

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

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

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

Procedure 6: New LV for NetBackup Client



S	This procedure create	his procedure creates a new logical volume for NetBackup client software and moves the existing					
Т	NetBackup client software to this new volume.						
Ε							
Р	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.						
#	SHOULD THIS PROCEDURE	RE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.					
E P #	Check off (1) each step as it is SHOULD THIS PROCEDURE	<pre>completed. Boxes have been provided for this purpose under each step number. FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE. If this file exists then a version of the NB client has been installed on this application. If file doesn't exist then move to Step 9. # su = platcfg The platcfg utility menu will be displayed, Now navigate to following submenus : 1. Navigate to NetBackup configuration and select the Verify NetBackup Client Installation option</pre>					
		X EXIC X					
		X X					
		wadaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa					
		2. If NetBackup client is installed, the following screen will appear					

S	This procedure creates a new logical volume for NetBackup client software and moves the existing							
Т	NetBackup client software to this new volume							
F	NetDackup chefit software to uns new volume.							
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.						
		Platform Configuration Utility 3.06 (C) 2003 - 2012 Tekelec. Inc.						
		Hostname: MO2						
		Verify WetBackum Client Installation						
		IOVI - Looke like a 7 l Client is installed						
		[UK] - LOOKS 11Ke a /.1 Lilent 13 installed						
		[OK] - RC script: netbackup						
		[OK] - rpm: SYMCpddea						
		[OK] - pkgKeep: SYMCpddea						
		[OK] - rpm: SYMCnbjre						
		[OK] - pkgKeep: SYMCnbire						
		[OK] - rnm: SYMCnhiava						
		[OV] _ nbwVeen, CVWCnbjeve						
		[OK] - pkykcep. Jindimjava						
		[OK] - rpm: SiMundeit						
		[UK] - pkgkeep: SYMChbolt						
		[OK] - rpm: VRTSpbx						
		[OK] - pkgKeep: VRTSpbx						
		10 81 61 61 940 Dave						
		lqqqqqqqqk lqqqqqqk lqqqqqqk lqqqqqqk lqqqqqqk lqqqqqqk x Forward x x Backward x x Top x x Bottom x x Exit x mqqqqqqqqi mqqqqqqi mqqqqqqi mqqqqqqi mqqqqqqj mqqqqqqj Note : Following error in verify NetBackup Client Installation output is acceptable : [ERROR] - RC script: vxpbx_exchanged 3. Select Exit to return to previous menu. If NetBackup is installed move to Step 2, otherwise move to Step 9.						
2	Check if NetBackup Logical volume already exists	Execute the following command to check if logical volume for NetBackup client already exists : # df -B M						
		Following output will show that NetBackup Logical Volume already exists :						
		Filesystem1M-blocksUsed AvailableUse% Mounted on /dev/mapper/vgroot-netbackup_lv 2016M1223M37% /usr/openv692M1223MIf NetBackup logical Volume exists then move to Step 9. otherwise move to next step 3						

S	This procedure creates a new logical volume for NetBackup client software and moves the existing						
T	NetBackup client software to this new volume.						
E P	Check off (ψ) each step as it is completed. Boxes have been provided for this purpose under each step number.						
#	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.						
3	Mount the upgrade Insert Diameter Signaling Router 5.xISO into drive of the application server.						
		Log in as root to the application server and execute the following steps:					
		Determine the cdrom of the server :					
		# cetCDROM					
		/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					
		<pre># mount /dev/sr0 /media/cdrom</pre>					
		Run the following to mount ISO:					
		<pre># mount -o loop DSR_5.x.iso /media/cdrom</pre>					
4	Verify that the script is	To be sure it is available on the upgrade media, execute the "Is" command to list the					
	available on the media	relocateNetBackup script, like this:					
		<pre># ls <mount point="">/upgrade/bin/relocateNetBackup</mount></pre>					
		Verify that the relocateNetBackup script is present, otherwise contact Tekelec.					
_							
5	Verify that there is sufficient space	Verify that the filemgmt filesystem has more than 2049 Megabytes of free space. Execute the df command and examine the response.					
	available	# df _P M /man/WKIC/db/filomomt/					
		" di -B M / Val/IKic/ db/IIIengmc/					
		Verify that the available space is 2049 Megabytes or greater.					
		If there is not sufficient space, remove unneeded files until there is sufficient space.					
6	Execute the relocate	Execute the relocate script:					
	script .						
		<pre># <mount point="">/upgrade/bin/relocateNetBackup</mount></pre>					
		Verify that it executes without error. Following warnings are acceptable :					
		WARNING: Start of vxpbx_exchanged service exited with value 0 WARNING: Start of netbackup service exited with value 2					
	These warnings are a function of the NetBackup client software and can be safely ignore						

S This procedure creates a new logical volume for NetBackup client software and moves the existing Т NetBackup client software to this new volume. Ε Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number. Р # SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE. Check if NetBackup 7 Execute the following command to check if Logical volume for NetBackup client exists : logical volume exists. # df -B M Following output will show that NetBackup Logical Volume already exists : Filesystem Used Available 1M-blocks Use% Mounted on /dev/mapper/vgroot-netbackup lv 692M 1223M 2016M 37% /usr/openv If NetBackup logical Volume exists then move to next Step,otherwise contact Tekelec customer service by referring to Appendix K of this document. 8 Unmount mount point Execute the following command to unmount the mount point : # umount /media/cdrom Remove the media from the drive. Check if NetBackup Repeat this procedure on every NOAM and SOAM server. Logical volume already exists on other servers

3.3.8 ISO Administration

Detailed steps on ISO Administration are given in Procedure 6.

Note: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed and require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 7: ISO Administration

#

- **S** This procedure verifies that ISO Administration steps have been completed.
- $\frac{\mathbf{T}}{\mathbf{E}}$ Check off (\mathbf{v}) each step as it is completed. Boxes have been provided for this purpose under each step number.
- **P** Should this procedure fail, contact the Tekelec Customer Care Center and ask for <u>UPGRADE ASSISTANCE</u>.

1 Upload ISO to Active NO server via the DSR 4.x/5.x GUI session.	 There are 2 methods to upload the application ISO to the Active NO based on the type of the media: Execute either Option 1(Using NOAM GUI Upload function for ISO file transfer over the network) <u>OR</u> Option 2 (Local site media ISO transfer, using PM&C). <u>OPTION 1:</u> Using NOAM GUI Upload function for ISO file transfer over the network Upload the target release ISO image file to the File Management Area of the active NO server⁵: 1. Log in to the active NO GUI. 2. Select Status & Manage > Files; the Files menu is displayed 						
	Main Menu: Status & Manage -> Files			Help Mon Oct 08 11:56:42 2012 UTC			
	Filter •						
	NO1 NO2 MP1 MP2						
	File Name	Size	Туре	Timestamp			
	872-2438-110-4.0.0_40.14.1-DSR-x86_64.iso	836.1 MB	iso	2012-10-03 08:05:02 UTC			
	Backup DSR N01 FullDBParts NETWORK_OAMP.20121003_044130.UPG tar.bz2	458.4 КВ	bz2	2012-10-03 08:41:35 UTC			
	Backup.DSR.NO1.FullRunEnv.NETWORK_OAMP.20121003_044130.UPG tar.bz2	222.2 КВ	bz2	2012-10-03 08:41:38 UTC			
	DSR3.0/myfile.iaaf	984.5 KB	iaaf	2012-10-03 08:40:27 UTC			
	TKLCConfigData.MP1.sh	2.2 KB	sh	2012-10-03 07:07:59 UTC			
	TKLCConfigData.MP2.sh	2.2 KB	sh	2012-10-03 07:07:59 UTC			
	 Delete View Upload Download Pause Updates OB used (0.00%) of 0B available System utilization: 0 B (0.00%) of 0B available. Click the active NO server in your network. All files stored in the file management storage area of this server display on the screen. 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. Click the Upload button. Browse window will open up : 						
				0			
	File: Browse Upload 7. Click Browse to select the file to upload.			Cancel			

 $^{^{5}}$ The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

8. The Choose File	e window displays, allowing ye	ou to select the file	to upload.
🛞 File Upload	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Statement of the local division of the local	
Desktop +	• 49	Search Desktop	Q
Organize • New folder	,,,,,,,,	圖•[
Organize New folder	Network Netwo	∰ • [
🖙 Local Disk (E) 💡	Mozilla Firefox		-
File na	me 872-2526-101-50.0_50.50-D5R-x86_6 +	All Files	•
9. Select the targe 10. The selected file File: op\872-2438-110- Upload	t release ISO image file and c and its path display on the s 4.0.0_4 Browse	click Open . creen.	8
		Ca	ancel
11 Click Upload			
 12. The ISO file beg 13. Wait for screen This will usually speed is slow. (I 14. Backup the ISO following comma desired space is a) cd ir loca # b) Usi # spma pma # pma 	to refresh and display the uple take between 2 to 10 minutes Depending on your network s file to the PMAC by ssh from and, Refer to [4] Procedure 12 s not available on PM&C:: not the directory on the active ted cd /var/TKLC/db/f ng sftp, connect to the PM&C sftp acftpusr@ <pmac_mar put <image/>.iso</pmac_mar 	agement storage ar oaded ISO filenamo s, but more if your i peed, up to 25 min the Active NO and 2 for creating space NOAM where your filemgmt management serv	rea. e in the files list. network upload utes). d executing the e on PM&C if r ISO image is rer
c) Afte	er the image transfer is 100%	complete, close the	e connection
# d Note: Userld	quit and password should alrea	ndy be recorded in	Table 3.
Copy the ISO file to t	he Standby NO using the follo	owing command: fr	om the Active NO.

<pre>scp /var/TKLC/db/filemgmt/<dsr_iso_filename></dsr_iso_filename></pre>
root@ <standby ip="" no="">:/var/TKLC/db/filemgmt</standby>
Execute Steps 3 to 7 of Appendix F to add ISO image to PM&C repository
OPTION 2 (Local site media ISO transfer, using PM&C):
Using a Media containing the application (recommended for slow network connections
between the client computer and the DSR frame – Applicable for DSR 4.x (PM&C 5.0))
 Execute Appendix F to load the ISO onto the PM&C server at the site.
2. SSH into the PM&C server and scp the ISO to the active NO using the following
commands:
For PM&C 5.0
SCD
/war/TKIC/amag/imago/ronogitorw/DSP_ISO_Filena
/var/inte/smac/image/repositorycosk_ISO_Filena
<pre>me> root@<active_no_ip>:/var/TKLC/db/filemgmt</active_no_ip></pre>
For PM&C less than 5.0 version :
<pre>scp /var/TKLC/smac/image/<dsr_iso_filename></dsr_iso_filename></pre>
root@ <active_no_ip>:/var/TKLC/db/filemgmt</active_no_ip>
3. Log in to Active NO and Execute following command :
<pre>chmod 644 /var/TKLC/db/filemgmt/<dsr_iso_filename></dsr_iso_filename></pre>
4. From the active NOAM, copy the ISO file to the standby NOAM using following
command:
<pre>scp /var/TKLC/db/filemgmt/<dsr_iso_filename></dsr_iso_filename></pre>
root@ <standby_no_ip>:/var/TKLC/db/filemgmt</standby_no_ip>

Transfer ISO to all DSR 4.x/5.x Servers to be	Transfer the target release ISO image file from the active NO to all other DSR 4.x/5.x servers.				
upgraded.	 From the Active NO GUI, navigate to Administration -> ISO for DSR 4.x or navigate to Administration->Software Management-> ISO Deployment for DSR 5.x GUI. 				
	Main Menu: Administration -> ISO				
	Display Filter None -	Go (LIKE wildcard: "*")			
	• No ISO Validate or Transfer in Progress.				
	Table description: List of Systems for ISO transfer.				
	System Name / Hostname ISO Transfer Statu	IS			
	MP1 No transfer in progress N/A				
	NO1 No transfer in progress N/A				
	NO2 No transfer in progress N/A				
	2 Click on "Transfer ISO"				
	Main Menu: Administration -> ISC	D [Transfer ISO] 🤣 Неір			
	 Note: ISOs are located in the connect 	ted server's File Management			
	Area. Target Systems are configured GUI connection is to Standalone Ser self before Upgrade.	via Systems Configuration. If ver, ISO must be transferred to			
	Select ISO to Transfer:	Select Target System(s):			
	872-2526-101-5.0.0_50.5.0-DSR-x86_64.iso 💌	Select All Deselect All MP1 MP1 MP2 MP3 MP4 N01 N02 S01			
		so2			
	Perform Media Validation before Transfer 🗹				



 Under the "Select ISO to Transfer:" drop do Under the "Select Target System(s):" select Select the checkbox next to "Perform Media Main Menu: Administration -> ISC 	own menu select the DSR 5.x ISO. tt " Select All ". a Validation before Transfer ". D [Transfer ISO]
Note: ISOs are located in the connec Area. Target Systems are configured GUI connection is to Standalone Ser self before Upgrade.	ted server's File Management via Systems Configuration. If ver, ISO must be transferred to
Select ISO to Transfer: 872-2526-101-5.0.0_50.5.0-DSR-x86_64.iso ♥	Select Target System(s): Select All MP1 MP2 MP3 MP4 NO1 NO2 SO1 SO2
Perform Media Validation before Transfer 🗹 Ok Cancel	
 Click Ok You will be returned to the ISO screen, Moni have completed. Click refresh to update the fails, it must be retried. 	itor the progress until all file transfers status of the transfer. If a file transfer
Note: In the unlikely event that an ISO file transfer the specific system to which the transfer failed. If Tekelec support for assistance.	r fails, repeat the transfer selecting only file transfers fail repeatedly, contact

3.3.9 Upgrade TVOE Hosts at a site (prior to Application upgrade MW)

This procedure applies if the TVOE Hosts at a site will be upgraded BEFORE the start of the DSR 5.0 Upgrades of the NO's and other servers. Performing the TVOE upgrades BEFORE will reduce the time required for DSR Application Upgrade procedures.

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

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

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

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

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

Note: Depending on the risk tolerance of the customer, it is possible to execute multiple TVOE Upgrades in parallel.

Detailed steps are shown in the procedure below.

Procedure 8: Upgrade TVOE Hosts for a site

S	This procedure upgrades the TVOE Hosts for a site.							
T E	Check off (\mathbf{v}) each step as it is completed. Boxes have been provided for this purpose under each step number.							
P #	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.						
		Start of maintenance window						
1	Record site							
		Record Site to be upgraded						
2	server upgrades	Record the TVOF hosts to be ungraded in order:						
		(It is best to upgrade Standby Servers before Active servers, to minimize failovers. Otherwise,						
		any order is OK.)						
		Note: the site PMAC, "Software Inventory" form, will typically list the TVOE Hosts at a site, and their versions.						

Procedure 8: Upgrade TVOE Hosts for a site

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

4. SOFTWARE UPGRADE EXECUTION

Call the Tekelec Customer Care Center at 1-888-FOR-TKLC (1-888-367-8552); or 1-919-460-2150

(international) prior to executing this upgrade to ensure that the proper media are available for use.

Before upgrade, users must perform the system health check in Section 3.3.6. This check ensures that the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if upgrade can proceed with alarms.

**** WARNING ****

If there are servers in the system which are not in Normal state, these servers should be brought to the Normal or the Application Disabled state before the upgrade process is started. The sequence of upgrade is such that servers providing support services to other servers will be upgrade first.

If alarms are present on the server, contact Tekelec Customer Support to diagnose those alarms and determine whether they need to be addressed or if it is safe to proceed with the upgrade.

Please read the following notes on upgrade procedures:

- Procedure completion times shown here are estimates. Times may vary due to differences in database size, user experience, and user preparation.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
 - Session banner information such as *time* and *date*.
 - System-specific configuration information such as *hardware locations*, *IP addresses* and *hostnames*.
 - ANY information marked with "*XXXX*" or "*YYYY*." Where appropriate, instructions are provided to determine what output should be expected in place of "*XXXX* or *YYYY*"
 - Aesthetic differences unrelated to functionality such as *browser attributes: window size, colors, toolbars* and *button layouts*.
- After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A check box is provided. For procedures which are executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).
- Captured data is required for future support reference if Tekelec Technical Services is not present during the upgrade.

4.1 Select Upgrade Path

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

Answer these questions, and record:

What is the DSR Application version to be upgraded?
What is the DSR Application new version to be applied?
Is this a Major or Incremental Upgrade?
Is this a 2-Tier or 3-Tier NOAM deployment?
Is the DA-MP redundancy (1+1) or (N+0)?
Are there IPFE servers to upgrade?
Are there PDRA or SBR servers to upgrade?
What DSR applications are running in a TVOE Host environment?
Is SDS also deployed (co-located) at the DSR site?
Note: SDS does not need to be upgraded at the same time.
Is DIH also deployed (co-located) at the DSR site?
Note: DIH does not need to be upgraded at the same time.
Is this setup deployed on RMS server(s)?

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

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

Record Upgrade type selected from the Tables below:

Table 6. 3-Tier Upgrade Path Reference

Туре	Supported Configurations	Upgrade Path	Section Reference
1	DSR 5.x upgrade for 3-tier (1+1) setup (major or incremental)	3-Tier DSR Upgrade for (1+1) DA-MP configuration.	Section 4.2
2	DSR 5.x upgrade for 3 tier (N+0) setup (major or incremental)	3-Tier DSR Upgrade for (N+0) DA-MP configuration.	Section 4.3
3	DSR 5.x upgrade for 3 tier (N+0) RMS server setup (major or incremental)	3-Tier DSR Upgrade for (N+0) DA-MP configuration on RMS servers.	Section 4.4
4	DSR 5.x upgrade for 3-tier (1+1) RMS server setup (major or incremental)	3-Tier DSR Upgrade for (1+1) DA-MP configuration on RMS servers.	Section 4.5
5	Policy DRA DSR 5.x upgrade (major or incremental)	Upgrade for Policy DRA application	Section 4.6

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

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

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

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

Procedures for the 3-tier NO Upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning will be disabled before upgrading the NO servers (which will also disable provisioning at the SO servers), and provisioning activities at the NO and SO servers will have certain limitations during the period where the NOs are upgraded and the sites are not yet upgraded.

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

These times are estimates.

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

Table 8	NO	Ungrade	Execution	Overview	(For DSR	3-tier	configuration)
I able c	. INO	Opgraue	Execution	Over view	(FOL DON	J-uer	configuration)

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

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

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

S	This procedure perfo	This procedure performs a Health Check.		
T E	Check off (\mathbf{i}) each step as it is	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
Р #	SHOULD THIS PROCEDURE	FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR <u>UPGRADE ASSISTANCE</u>.		
1	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.x) , then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (this can be done from PMAC Software Inventory form) Complete this information: NO-A TVOE Host Rev NO-B TVOE Host Rev DR-NO-B TVOE Host Rev Will TVOE Upgrades be performed during the DSR Application Upgrades?		

O GUI: Verify NO	For the ser	vers with R	ole = Netv	work C	DAM&P, cor	nfirm Application	Version (pre-upgrade
ervers existing	Note: Look	and feel of	f the Upar	ade so	reen has c	hanged betweer	DSR 4 x and DSR 5
	releases, th	e example	below pro	ovides	the snapsh	not from both the	releases.
	Upgrade S	creen in D	<u>SR 4.x</u>				
		-					
	Main M	enu: Ac	iminist	trati	on -> U	pgrade	
			Netw	ork Ele	ement		Role
	Hostname		Appli	ication	Version		Function
			то			0	NETWORK OAM&P
	T2-NO-228	3-A 🛛	40.2	40.27			OAMER
			4.0.2	-40.27	.5		
	T2-NO-228	3-В	12_N	10_228	3		NETWORK OAM&P
			Unkn	iown			OAM&P
			T2_N	10_228	3		MP
	MP2		4.0.2	-40.27	3		DSR (multi-active cluster)
			T2_N	10_228	3		MP
	MP3		4.0.2	-40.27	3		DSR (multi-active cluster)
	inter d		T2_N	10_228	3		MP
	Ipre 1		4.0.2	-40.27	3		IP Gront End
	1		T2_N	10_228	3		MP
	ipre2		4.0.2	-40.27	3		IP Front End
			T2 N	10 228	3		MP
	MP1		4.0.2	-40.27	3		DSR (multi-active
							clustery
	Upgrade S	creen in D	SR 5.x				
		Server Status	Server Role	Function	Upgrade State	Status Message	
	Hostname	OAM Max HA Role	Network Element		Start Time	Finish Time	Mate Server Status
		Max Allowed HA Role	Application Version	n	Upgrade ISO		
	Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAMEP	Not Ready		Viper-NO2
	Viper-NO2	Norm Standby Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO1
	Viper-SO1-A	Norm Active Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-B
	Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-A
	Viper-SO2-A	Norm Active	System OAM SO2_Viper	OAM	Not Ready		Viper-SO2-B
		Norm	System OAM	OAM	Not Ready		
	Viper-SO2-B	Standby Active	SO2_Viper 5.0.0-50.15.1				Viper-SO2-A
	Viper-MP05	Norm	MP	DSR (multi- active cluster)	Not Ready		Viper-MP06
	Viper-MP05	Norm Active	MP SO1_Viper	DSR (multi- active cluster)	Not Ready		[Viper-MP06]

3	NO GUI: Verify ISO for	Verify DSR ISO file has been Transferred to all servers:
	Upgrade has been	Eveneele
	рерюуеа	Example:
		Main Menu: Administration -> ISO
		Wed Sep 25 17:39:13 2013 UTC
		Display Filter: - None Go (LIKE wildcard: ***)
		Transfer ISO Complete. ISO: 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso
		7 of 7 Transfers Successful. 0 of 7 Transfers Failed.
		Table description: List of Systems for ISO transfer.
		Displaying Records 1-7 of 7 total First Prev Next Last
		System Name / Hostname ISO Iransfer Status
		MP2 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		MP3 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		T2-NO-228-A 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		T2-NO-228-B 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		Ipte1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		Displaying Records 1-7 of 7 total First Prev Next Last
		ITransfer ISO
		IF Not, see ISO Administration 3.3.8.
4	Verify Server Status is	Verify Server Status is Normal:
	Normal	
		Log Into the NOAM GUI using the VIP.
		 Select Status & Manage > Server; the Server Status screen is displayed.
		2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High
		Availability (HA), and Processes (Proc).
		3. Do not proceed to upgrade if any of the server statuses displayed is not Norm .
		4. Do not proceed if there are any Major or Critical alarms.
		Note: It is not recommended to continue executing upgrade if any server status has
		unexpected values. An upgrade should only be executed on a server with unexpected alarms
		release software contains a fix to clear the "stuck" alarm(s). This would mean that the target
		to clear the alarm(s). Do not continue otherwise.
-		
5	Log all current alarms at NOAM	Log all current alarms in the system:
		1. Select Alarms & Events > View Active; the Alarms & Events > View Active view is
		displayed.
		2. Click Report button to generate an Alarms report.
		3. Save the report and/or print the report. Keep these copies for future reference.
6	Repeat for active	Log all current alarms in the SOAM:
	SOAMs	
		1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

7	Verify that a recent version of the Full DB	Verify that a recent version of the Full DB backup has been performed.
	backup has been performed	Select Status and Manage → Files Check time stamp on two files:
		Backup.DSR. <hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.ta r.bz2</time_stamp></hostname>
		Backup.DSR. <hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.t ar.bz2</time_stamp></hostname>
		See section 3.3.5 to perform (or re-perform) a full Backup, if needed.

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



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

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

S T E P #	 This Procedure inhibits replication for 3-Tier NO (and DR-NO) servers, prior to upgrade. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (1+1) DA-MP server configurations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE. 		
		Start of next maintenance window	
	Disable global provisioning and configuration.	 Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. 1. Select Status & Manage > Database; the Database Status screen is displayed 2. Click Disable Provisioning button. 3. Confirm the operation by clicking Ok in the popup dialog box. 4. Verify the button text changes to Enable Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 002] - Provisioning is manually disabled. 5. Active NO server will have the following expected alarm: Alarm ID = 10008 (Provisioning Manually Disabled) 	

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

2	Inhibit SOAP replication	Record current DSR release numberex: 4.0.2_40.27.3
	(This step will NOT be required for most	SKIP THIS STEP if current release is DSR 4.0.0_40.19.0 or greater.
	upgrades!)	Use your SSH client to connect to the active NO server (ex. ssh, putty): ssh <active address="" ip="" no=""></active>
		login as: root password: <enter password=""></enter>
		1. Execute the following command to disable SOAP replication :
		<pre># iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"</pre>
		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 Nodeld present on the setup :
		E,g,
		nodeId=A2823.152
		Note: SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO,SO or MP servers.
3	Inhibit replication to MP servers (1+1) redundancy	Inhibit database replication to MP servers in the following order: Standby DA-MP Active DA-MP
		From Active NO: 1. Select Status & Manage > Database The Database Status screen is displayed
		2. Select the appropriate DA-MP server . 3. Click Inshibit Republication button
		 Click Infibit Replication button. Verify the <i>Inhibited</i> text is displayed for server.
		5. Repeat the above steps for all remaining servers in the order: standby, then active).
		Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.
		ALL DA-MPs must be inhibited.

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

4	Inhibit replication to SO	Inhibit database replication to SO servers in the following order:
	servers at a site	a Sito:
		• She. • Standby SO
		 Active SO
		From Active NO:
		1. Select Status & Manage > Database
		The Database Status screen is displayed.
		2. Select the appropriate SO server.
		Click Inhibit Replication button.
		4. Verify the <i>Inhibited</i> text is displayed for server.
		5. Repeat the above steps for all remaining Site (servers) in the order: standby, then
		active).
		ALL SOAM must be inhibited.
_		
5	Verify that MPs and SO Servers are Inhibited	Select Status & Manage > Database
		oloci olato a manage > batabase
		Verify that the Replication status is Inhibited for all MPs and all SOs, at all sites.
		The following clarme are expected:
		Active NO server has:
		Alarm ID = 10008 (Provisioning Manually Disabled)
		All other MDs and SO converse must have
		All other MPS and SO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
6	Inhibit replication to NO	Inhibit database replication to all servers in the following order:
	servers.	Standby NO
		Active NO Standby DR NO(if applicable)
		Active DR NO(if applicable)
		Select Status & Manage > Database
		The Database Status screen is displayed.
		1. Select the appropriate NO or DR-NO server based on the list above.
		2. Click Inhibit Replication button.
		3. Verify the Inhibited text is displayed for server.
		 Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above.
		Note: It is important to inhibit the replication of the standby server before the
		active server, to prevent unwanted HA switchovers.
7	Verify that All Servers	Calast Status & Manage > Database
1		Select Status & Manage > Database
		Verify that the Replication status is Inhibited for all servers, at all sites.
		The following alarms are expected:
		Active NO server has:
		Alarm ID = 10008 (Provisioning Manually Disabled)
		All other servers must have:
		Alarm ID = 31113 (Replication Manually Disabled)

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

8	Disable Site Provisioning	Disable Site provisioning for all the sites present in the setup :
	FIOUSIONING	 Log into the GUI of the SOAM for all the sites using the VIP. Select Status & Manage > Database the Database Status screen is displayed Click Disable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled. Repeat substeps 2 through 5 for all the sites present in the setup.

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

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

S T	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO and DSR MP) deployment only				
Ē	It applies to (1+1) DA-MP server configurations.				
P #	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
1	Begin Upgrade of DR-	Next Steps will begin Upgrade of the DR-NO servers.			
	NOS	SKIP this Procedure if the deployment does not include DR-NO servers.			
2	Upgrade Host TVOE for Standby DR-NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)			
	100000)	Execute Appendix J for the standby DR NO			
3	Upgrade Standby DR-	Upgrade the standby DSR DR NO:			
	Upgrade Single Server	Execute Appendix G Single Server Upgrade Procedure			
	p. cocca. c)	After successfully completing the procedure in Appendix G, return to this point and continue with step mentioned below.			
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.			
4	Upgrade Host TVOE for Active DR-NO (if needed)	 Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 			
		Execute Appendix J for the active DR NO to upgrade TVOE.			
5	Verify if cmha is running on upgraded DR NO	Log into the just-upgraded standby DR NO upgraded above, execute the following command:			
		ssh <no address="" ip="" xmi=""></no>			
		login as: root			
		password: <enter password=""></enter>			
		[root@NO1 ~]# pl grep "cmha"			
		The following output should be generated:			
		A 10128 cmha Up 11/20 00:15:58 1 cmha			
		If no output is generated then execute following command:			
		service start_cmha start			

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

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

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

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

S	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO,							
Ť	and DSR MP) deployment only							
Ē	It applies to $(1+1)DA$ -MP server configurations							
P								
#	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.							
1	Upgrade Host TVOE for Standby NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)						
		Execute Appendix J for the standby NO						
2	Upgrade Standby NO	Upgrade the standby DSR NO:						
	server (using Upgrade Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure						
	p. coccus. c)	After successfully completing the procedure in Appendix G, return to this point and continue with step mentioned below.						
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.						
3	Upgrade Host TVOE for Active NO (if needed)	 Skip this step if: the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 						
		Execute Appendix J for the active NO to upgrade TVOE.						
4	Verify that cmha is	Log into the just-upgraded standby NO upgraded above, execute the following						
	running on upgraded	command:						
		ssh <no address="" ip="" xmi=""></no>						
		login as: root						
		password: <enter password=""></enter>						
		[root@NO1 ~]# pl grep "cmha"						
		The following output should be generated:						
		A 10128 cmha Up 11/20 00:15:58 1 cmha						
		If no output is generated then execute following command:						
		service start_cmha start						

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

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

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

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

S This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, and (1+1) DA-MP server configurations.
 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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.

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

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

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

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

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

S	This procedure verifies Post Upgrade Status for 3-Tier NO upgrade.
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.
#	

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

1	SSH: Verify NO and	Verify Server Status after NO servers upgraded:				
	DR-NO Server Status					
		 Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers : Use your SSH client to connect to the upgraded server (ex. ssh, putty): 				
		ssh <no address="" ip="" xmi=""></no>				
		Jamin and most				
		login as: root password: <enter password=""></enter>				
		password. Center password				
		Note: The static XMI IP address for each NO server should be available in Table 3.				
		# verifyUpgrade				
		Examine the output of the above command to determine if any errors were reported. In case of errors please contact Tekelec.				
		# alarmMgralarmstatus				
		Following alarm output should be seen, indicating that the upgrade completed.				
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33				
		[Alarm ID 32532 will be cleared after the upgrade is accepted.]				
		Contact Tekelec in case above output is not generated.				
2	NO GUI: Verify Alarm status	Log all current alarms in the system:				
		1. Log into the NOAM GUI via the VIP.				
		2. Select Alarms & Events > View Active; the Alarms & Events > View Active view is				
		aispiayed. 3. Click Report button to generate an Alarms report				
		4. Save the report and/or print the report. Keep these copies for future reference.				
		Expected Alarms include:				
		Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)				
		All other converse might have:				
		All other servers might have: Alarm ID = 31113 (Replication Manually Disabled)				
		Observed on all the upgraded servers :				
		Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)				
3	Verify Traffic status	View KPI reports to verify traffic is at the expected condition.				

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

4 Enable global provisioning and configuration(if new	Enable provisioning and configuration updates on the entire network (if new Network elem is required to be added):			
Network element is required to be added)	Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning new data provisioned at NOAM will be replicated to only upgraded SO(s).			
	1. Log in to the active NOAM GUI using the VIP.			
	2. Select Status & Manage > Database			
	The Database Status screen is displayed.			
	3. Click Enable Provisioning button.			
	4. Verify the text of the button changes to Disable Provisioning.			
	Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM.			
End of maintenance window				

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

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

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

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

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

During the Site upgrade, the site provisioning should be Disabled. It may re-enabled at the completion of the site upgrade.

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

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

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

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

This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that S hosts an SOAM guest. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments Т Е only. Р Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number. ₩ Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE. Start of next maintenance window. Verify that site provisioning is disabled. Else disable site provisioning for the site that is Verify that Site 1 Provisioning is disabled currently being upgraded : Log into the SOAM VIP GUI which needs to be upgraded. 1. Select Status & Manage > Database the Database Status screen is displayed 2. Click Disable Site Provisioning button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. 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 Upgrade TVOE Host for If the TVOE Host for the Standby SO needs to be upgraded: 2 Standby Server Execute Appendix J for the standby SO TVOE Host 3 Upgrade Standby SO Upgrade Standby SO Execute Appendix G - Single Server Upgrade for Standby SO After successfully completing the procedure in Appendix G, return to this point and continue with step 3 below. Upgrade TVOE Host for IF Active SO is hosted on TVOE blade, and the TVOE Host needs to be upgraded: 4 Active SO Server Execute Appendix J to upgrade the Active SO TVOE Host

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

5	Verify cmha process is	Execute following steps to make sure that cmha process is up on upgraded server:
	running on upgraded SO	+ +
		1. Log into the just-upgraded standby SO, execute the following command:
		<pre># ssh root@<so address="" ip="" xmi=""></so></pre>
		login as: root
		<pre>password: <enter password=""></enter></pre>
		Execute following command on SO:
		[root@SO1 ~]# pl grep "cmha"
		The following output should be generated:
		A 10128 cmha Up 11/20 00:15:58 1 cmha
		If no output is generated then execute following command:
		service start_cmha start
6	Upgrade Active SO	Upgrade Active DSR SO server using Upgrade Single Server procedure :
		Execute Appendix G Single Server Upgrade Procedure
		After successfully completing the procedure in Appendix G, return to this point and continue with step 6 below.
7	Allow replication to SO servers.	Allow database replication to SO servers:
		1. Select Status & Manage > Database
		2. The Database Status screen is displayed.
		3. Select the Active SO server.
		4. Click Allow Replication button.
		5. Verify the <i>inhibited</i> text is not displayed for the server. After the Allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that
		 Server. Repeat the Allow action link for Standby SO server.
		Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.
8	Install NetBackup on	If Netbackup is to be installed on your DSR, execute the procedure found in Appendix I.
	NU and SU (If required)	Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.

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

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

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

S	This procedure upgrades the DA-MP(s).						
T	Check off ($$) each step as it	is completed. Boxes have been provided for this purpose under each step number.					
E							
г #	Should this procedure fail, contact the Tekelec Customer Care Center and ask for <u>UPGRADE ASSISTANCE</u> .						
1	Verify and Record the	Verify and Record the status and hostname of the active DA-MP and of the standby DA-MP by					
	status of the MP before	going to Status & Manage -> HA.					
	upgrade	Note: Active DA-MP server can be identified by looking out for the VIP. The server with VIP in the row is the active DA-MP.					
2	Upgrade the standby DA-MP server (using Upgrade Single Server	Upgrade Standby MP server ⁶ using Upgrade Single Server procedure:					
	procedure)	Execute Appendix G – Single Server Upgrade for Standby DA-MP					
		After successfully completing the procedure in Appendix G, return to this point and continue with Step 3 below.					
3	Upgrade the Active DA-	Upgrade active MP server using the Upgrade Single Server procedure.					
	MP server.	Execute Appendix G – Single Server Upgrade for Active DA-MP					
		After successfully completing the procedure in Appendix G, return to this point and continue with Step 4 below.					
		Note: The DA-MP server replication is enabled in Appendix G, executed above.					
4	Enable global	Enable provisioning and configuration updates on the entire network:					
	provisioning and configuration(if not already enabled).	Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning new data provisioned at NOAM will be replicated to only upgraded SO(s).					
		 Log in to the active NOAM GUI using the VIP. Select Status & Manage > Database 					
		The Database Status screen is displayed.					
		 Click Enable Provisioning button. Verify the text of the button changes to Disable Provisioning 					
		o. Venty the text of the button changes to Disable i Tovisioning.					
		Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM.					
5	Enable Site Provisioning	Enable Site provisioning :					
		 Log into the SOAM VIP GUI of the site just upgraded above. Select Status & Manage > Database the Database Status screen is displayed Click Enable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Disable Site Provisioning 					

⁶ The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

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

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

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

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

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

S	This procedure verifi	es Post-Upgrade site status								
T F	Check off (\checkmark) 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.								
E P #	SHOULD THIS PROCEDURE Verify Server Status is Normal	<pre>FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE. Verify Server Status is Normal: Log in to the active NOAM GUI using the VIP. Select Status & Manage > Server; the Server Status screen isis displayed. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). Execute following commands on the upgraded servers : Use your SSH client to connect to each of the upgraded DA-MP server (ex. ssh, putty): ssh <server address="" da-mp="" ip=""> login as: root password: <enter password=""> # verifyUpgrade Examine the output of the above command, and determine if any errors were reported. Please contact Tekelec in case of errors. # alarmMgralarmstatus Following output shall be raised: SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33 Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on cash scorer. </enter></server></pre>								

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

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

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

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

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

Procedures for the 3-tier NO Upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning will be disabled before upgrading the NO servers (which will also disable provisioning at the SO servers), and provisioning activities at the NO and SO servers will have certain limitations during the period where the NOs are upgraded and the sites are not yet upgraded.

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

These times are estimates.

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

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

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

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

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

S	This procedure performs a Health Check.						
Г Е Р #	Check off (\checkmark) 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 <u>UPGRADE ASSISTANCE</u> .						
	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If there are not on the required release (typically 2.5.x), then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (this can be done from PMAC Software Inventory form) Complete this information: NO-A TVOE Host Rev DR-NO-A TVOE Host Rev DR-NO-B TVOE Host Rev Will TVOE Upgrades be performed during the DSR Application Upgrades?					

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

NO GUI: Verify NO	For the ser	vers with R	ole = Net	work C	DAM&P, co	nfirm Applicatio	on Version (pre-upgrade	э).		
Servers existing Application Version	Example:									
	Note: Look	Note: Look and feel of the Upgrade screen has changed between DSR 4 x and DSR 5 x								
	releases, tl	ne example	below pro	ovides	the snaps	hot from both th	ne releases.			
	Upgrade S	creen in D	SR 4.x							
	Main M	Main Menu: Administration -> Upgrade								
							2.1			
	Hostname	Hostname T2-NO-228-A			Version	Function				
					Version		NETWORK OAM&P	>		
	T2-NO-22				3		OAM&P			
			T2_N	10_228	3		NETWORK OAM&P			
	T2-NO-22	8-B	Unkr	iown			OAM&P			
			T2_N	10_228	3		MP			
	MP2		4.0.2	-40.27	3		DSR (multi-active cluster)			
			T2_N	10_228	3		MP			
	MP3	MP3			3	DSR (multi-active cluster)				
	infe1	ipfe1			3	MP				
	ipie i				3	IPL ront End				
	ipfe2	ipfe2			3	MP				
		4.0.2-40.27.3 IP Front End					IP Front End			
	MP1	MP1			3	MP DSR (multi-active				
		4.0.2-40.27.3				cluster)				
	Upgrade S	creen in D	<u> SR 5.x</u>							
	Hostname	Server Status OAM Max HA Role	Server Role Network Element	Function	Upgrade State Start Time	Status Message Finish Time	Mate Server Status			
		Max Allowed HA Role	Application Versio	n	Upgrade ISO					
	Viper-NO1	Norm Active Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAMSP	Not Ready		Viper-NO2			
	Viper-NO2	Norm Standby Active	Network OAM&P NO_Viper 5.0.0-50.15.1	OAM&P	Not Ready		Viper-NO1			
	Viper-SO1-A	Norm Active Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-B			
	Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-A			
	Viper-SO2-A	Norm Active Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-B			
	Viper-SO2-B	Norm Standby Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-A			
	Viper-MP05	Norm	MP	DSR (multi- active cluster)	Not Ready		Viper-MP06			
		Active	CO1 Vinor							

3	NO GUI: Verify ISO for Upgrade has been	Verify DSR ISO file has been Transferred to all servers:
	Беріоуеа	Example.
		Main Menu: Administration -> ISO
		Display Filter: - None -
		Transfer ISO Complete. ISO: 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso 7 of 7 Transfers Successful. 0 of 7 Transfers Failed.
		Table description: List of Systems for ISO transfer.
		Displaying Records 1-7 of 7 total First Prev Next Last
		System Name / Hostname ISO Transfer Status
		MP1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete MP2 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		MP3 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		T2-NO-228-A 872-2526-101-5.050.12.0-DSR-x86_64.iso Complete
		ipfe1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		ipfe2 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		Displaying Records 1-7 of 7 total First Prev Next Last
		IF Not, see ISO Administration 3.3.8.
4	Verify Server Status is	Verify Server Status is Normal:
	Normal	Log Into the NOAM GUI using the VIP.
		 Select Status & Manage > Server; the Server Status screen is displayed.
		2. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High
		Availability (HA), and Processes (Proc).
		 Do not proceed to upgrade if any of the server statuses displayed is not Norm. Do not proceed if there are any Major or Critical alarms.
		Note: It is not recommended to continue executing upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
5	Log all current alarms at	Log all current alarms in the system:
	NUAW	1. Select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed
		 Click Report button to generate an Alarms report. Save the report and/or print the report. Keep these copies for future reference.
6	Repeat for active	Log all current alarms in allSOAM(s):
	SOAMs	 Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

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

Procedure	18: Perform	Health	Check	(Pre-Upgra	de of 3-	Tier(N+0)	NOAM)
I I Occuaite .	IOI I CIIOI III	II CUIVII	Chiech		ac or c		

7	Verify that a recent version of the Full DB	Verify that a recent version of the Full DB backup has been performed.
	backup has been	Select Status and Manage → Files
	performed	Check time stamp on two files:
		Backup.DSR. <hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.ta r.bz2</time_stamp></hostname>
		Backup.DSR. <hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.t ar.bz2</time_stamp></hostname>
		See section 3.3.5 to perform (or re-perform) a full Backup, if needed.

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

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



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

S T E P #	 This Procedure inhibits replication for 3-Tier NO (and DR-NO) servers, prior to upgrade. Also inhibits replication from NOs to SOs. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. It applies to (N+0) redundant DA-MP server configurations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. 		
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.	
	Start of next maintenance window		
	Disable global provisioning and configuration.	 Disable global provisioning and configuration updates on the entire network: Log into the NOAM VIP GUI. Select Status & Manage > Database; the Database Status screen is displayed Click Disable Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. 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. Active NO server will have the following expected alarm: Alarm ID = 10008 (Provisioning Manually Disabled) 	

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

2	Inhibit SOAP replication	Record current DSR release numberex: 4.0.2_40.27.3
	(This step will NOT be required for most	SKIP THIS STEP if current release is DSR 4.0.0_40.19.0 or greater.
	upgrades!)	Use your SSH client to connect to the active NO server (ex. ssh, putty): ssh <active address="" ip="" no=""></active>
		login as: root password: <enter password=""></enter>
		1. Execute the following command to disable SOAP replication :
		<pre># iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"</pre>
		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 Nodeld present on the setup :
		E,g,
		<pre>nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03</pre>
		excludeTables= HaNodeLocPref HaVipDef
		SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO,SO or MP servers.
3	Inhibit replication to MP servers (N+0)	Replication of MP's will be inhibited during site upgrade.
4	Inhibit replication to SO servers at a site	Inhibit database replication to SO servers in the following order:
		Site: Standby SO Active SO
		 From Active NO: Select Status & Manage > Database The Database Status screen is displayed. Select the appropriate SO server. Click Inhibit Replication button. Verify the Inhibited text is displayed for server. Repeat the above steps for all remaining servers in the order: standby, then active).
		ALL SOAM must be inhibited.

are Inhibited	Select Status & Manage > Database
	Verify that the Replication status is Inhibited for all SOs, at all sites.
	The following alarms are expected:
	Active NO server has:
	Alarm ID = 10008 (Provisioning Manually Disabled)
	All SO(s) servers must have:
	Alarm ID = 31113 (Replication Manually Disabled)
Inhibit replication	Inhibit database replication between NO servers in the following order:
between NO servers.	Standby NO
	 Active NO Standby DR NO/if applicable)
	Active DR NO(if applicable)
	Select Status & Manage > Database
	The Database Status screen is displayed.
	 Select the appropriate NO or DR-NO server based on the list above.
	2. Click Inhibit Replication button.
	3. Verify the Inhibited text is displayed for server.
	4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the
	order shown above.
	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites.
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected:
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has:
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have:
Verify that All NO and SO Servers are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
Verify that All NO and SO Servers are Inhibited Disable Site	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup :
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button.
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box.
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004]
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled.
Verify that All NO and SO Servers are Inhibited Disable Site Provisioning at all SOAMs	 Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for NO and SO servers, at all sites. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : Log into the GUI of the SOAM for all the sites using the VIP. Select Status & Manage > Database the Database Status screen is displayed Click Disable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled.

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

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

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

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

S	This Procedure upgrade	es the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR
Т	SO, and DSR MP) deployment only.	
Ε	It applies to (N+0) redundant DA-MP server configurations.	
Р	,	
#	Check off $(\sqrt{)}$ each step as it is completed. Boxes have been provided for this purpose under each step number.	
	Should this procedure fail or	antact the Tekelec Customer Care Center and ask for LIPCRADE ASSISTANCE
	Should this procedure fail, et	Shale the refere customer care center and ask for <u>or oktober Asolo Mixed</u> .
1	Begin Upgrade of DR-	Next Steps will begin Upgrade of the DR-NO servers.
	NOs	
		SKIP this Procedure if the deployment does not include DR-NO servers.
2	Upgrade Host TVOE for	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the
	Standby DR-NO (if	previous procedure)
	needed)	Execute Annendix 1 for the standby DR NO
		Execute Appendix 5 for the standby DR NO
3	Upgrade Standby DR-	Upgrade the standby DSR DR NO:
	NO server (using	
	NO Server (using	
	Upgrade Single Server	Execute Appendix G Single Server Upgrade Procedure
	Upgrade Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure
	Upgrade Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue
	Upgrade Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below.
	Upgrade Single Server procedure)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails – do not proceed. Consult with support on the best course of action.
	Upgrade Single Server procedure)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails – do not proceed. Consult with support on the best course of action.
4	Upgrade Single Server procedure)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails - do not proceed. Consult with support on the best course of action. Skip this step if:
4	Upgrade Single Server procedure) Upgrade Host TVOE for Active DR-NO (if	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails - do not proceed. Consult with support on the best course of action. Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the procedure)
4	Upgrade Single Server procedure) Upgrade Host TVOE for Active DR-NO (if needed)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails - do not proceed. Consult with support on the best course of action. Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)
4	Upgrade Single Server procedure) Upgrade Host TVOE for Active DR-NO (if needed)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails - do not proceed. Consult with support on the best course of action. Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) Execute Appendix J for the active DR NO to upgrade TVOE
4	Upgrade Single Server procedure) Upgrade Host TVOE for Active DR-NO (if needed)	 Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails - do not proceed. Consult with support on the best course of action. Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) Execute Appendix J for the active DR NO to upgrade TVOE.

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

5 Verify cmha process is running on upgraded DR NO	Log into the just-upgraded standby DR NO upgraded above, execute the following command:
	ssh <no address="" ip="" xmi=""></no>
	login as: root password: <enter password=""></enter>
	[root@NO1 ~]# pl grep "cmha"
	The following output should be generated:
	A 10128 cmha Up 11/20 00:15:58
	1 cmha
	If no output is generated then execute following command:
	service start_cmha start
Upgrade Active DSR DR-NO server (using	Upgrade the active DSR DR NO:
procedure).	Execute Appendix G Single Server Upgrade Procedure
	After successfully completing the procedure in Appendix G, return to this point and continue with step below.
	IF Upgrade fails – do not proceed. Consult with support on the best course of action.
Proceed to next procedure	Proceed to upgrade the NO servers, using the next procedure

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

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

S T E	This Procedure upgrade and DSR MP) deploym It applies to (N+0) redu	es the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, nent only. Indant DA-MP server configurations.
P #	Check off ($$) each step as it	is completed. Boxes have been provided for this purpose under each step number.
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.
1	Upgrade Host TVOE for Standby NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)
		Execute Appendix J for the standby NO
2	Upgrade Standby NO	Upgrade the standby DSR NO:
	Single Server	Execute Appendix G Single Server Upgrade Procedure
	procedurey	After successfully completing the procedure in Appendix G, return to this point and continue with step below.
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.
3	Upgrade Host TVOE for Active NO (if needed)	 Skip this step if: the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure)
		Execute Appendix J for the active NO to upgrade TVOE.
4	Verify cmha process is running on upgraded NO	Log into the just-upgraded standby NO upgraded above, execute the following command:
		ssh <no address="" ip="" xmi=""></no>
		login as: root password: <enter password=""></enter>
		[root@NO1 ~]# pl grep "cmha"
		The following output should be generated:
		A 10128 cmha Up 11/20 00:15:58 1 cmha
		If no output is generated then execute following command:
		service start_cmha start

Upgrade Active DSR NO server (using Upgrade Single Server procedure).	Upgrade the active DSR NO: Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with step below. IF Upgrade fails – do not proceed. Consult with support on the best course of action.
Verify NO GUI access via VIP Address	Close and re-open Browser using the VIP address for the NOAM.
	Note that Replication is still disabled between the NO servers, and from the NO servers to the SO and MP servers. This is expected.
	The NOAM GUI will show the new DSR 5.0 release.
	Expected Alarms include:
	Active NO server has:
	Alam ID = 10000 (FIONSIONING Manually Disabled)
	All other SO(s) and MP servers must have
	Alarm ID = 31113 (Replication Manually Disabled)
Proceed to next procedure	Proceed to next procedure, to allow replication between NOs.

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

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

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

S	This Procedure re-established the Replication between the NO servers, and the DR-NO servers.
Т	It applies to 3-tier, (N+0) redundant DA-MP server configurations.
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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.

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

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

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

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

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

S	This procedure verifies Post Upgrade Status for 3-Tier(1+1) NO upgrade.
T E	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.
#	

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

SSH: Verify NO and DR-NO Server	Verify Server Status after NO servers upgraded:
Status(optional)	 Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers :
	Use your SSH client to connect to the upgraded server (ex. ssh, putty): <pre>ssh <no address="" ip="" xmi=""></no></pre>
	login as: root
	password: <enter password=""></enter>
	Note: The static XMI IP address for each NO server should be available in $Table\ 3.$
	# verifyUpgrade
	Examine the output of the above command to determine if any errors were reported. In case of errors please contact Tekelec.
	# alarmMgralarmstatus
	Following alarm output should be seen, indicating that the upgrade completed.
	SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33
	[Alarm ID 32532 will be cleared after the upgrade is accepted.]
	Contact Tekelec in case above output is not generated.
NO GUI: Verify Alarm	Log all current alarms in the system:
514105	 Log into the NOAM GUI via the VIP. Select Alarms & Events > View Active; the Alarms & Events > View Active view is
	displayed. 3. Click Report button to generate an Alarms report.
	4. Save the report and/or print the report. Keep these copies for future reference.
	Expected Alarms include:
	Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)
	All other servers might have: Alarm ID = 31113 (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)

	End of maintenance window					
		NOTE: (SO replication inhibit will prevent most NO configuration changes from being propagated to the SOs.)				
	status	disabled till further upgrades are performed on the sites. SO provisioning shall also remain disabled.				
	Note on Provisioning	NOTE: This command may execute without any output if no changes are required (no devices were found to update). Provisioning on the SOs, and Replication from NO to the Site level SO, will typically remain				
		 Login to Active NO console and execute the following command /usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh 				
		Note 3: The steps below will update the locally stored information with the performance optimization parameters. This script check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices				
	on the Active NO server	Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs audit on the configured IPFE Ethernet devices and will update them with the locally stored information in case of any discrepancies.				
	Update Appworks NetworkDeviceOption Table for the configured	Note 1: This step is only applicable if the setup includes IPFE servers. This step will handle the possible audit discrepancies which can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.				
	Verify Traffic status	Login to SOAM GUI to view KPI reports to verify traffic is at the expected condition.				
		Alarm ID = 31113 (Replication Manually Disabled)				
		Active SO server has: Alarm ID = 10008 (Provisioning Manually Disabled)				
		Expected Alarms include:				
		 Click Report button to generate an Alarms report. Save the report and/or print the report. Keep these copies for future reference. 				
		 Select Alarms & Events > view Active, the Alarms & Events > view Active view is displayed. Observed between the second and a second secon				
		1. Log into the SOAM GUI via the VIP.				
,	status	Log all current alarms in the system:				

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

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

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

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

Global provisioning can be re-enabled after Site upgrade(if required).

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

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

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

Detailed steps are shown in the procedure below.

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

S	This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that							
Т	hosts an SOAM guest. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments							
Е	only.							
Р								
#	Check off (\mathbf{v}) each step as it is completed. Boxes have been provided for this purpose under each step number.							
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.						
		Start of next maintenance window(If required)						
1	Verify Traffic status	Login to Active SOAM and verify KPI reports to verify traffic is at the expected condition.						
2	Verify that site	Verify that site provisioning for the site which is currently being upgraded is disabled. By						
	Provisioning is disabled	logging into the site VIP and checking for Provisioning disabled alarm.						
		If provisioning disabled alarm is not present then execute following steps :						
		1 Log into the GUI of the SOAM which needs to be ungraded using the VIP						
		 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 vellow information box						
		should also be displayed at the top of the view screen which states: [Warning Code 004]						
		- Site provisioning has been manually disabled.						
3	Inhibit replication to MP	Record current release number ex: 4.0.2_40.27.3						
	servers (N+0)							
		 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="" tp="" xmt=""></active>						
		login as: root						
		Togin as. Tool						
		password: <enter password=""></enter>						
		Execute following command on active NO :						
		<pre># for i in \$(iqt -p -z -h -fhostName NodeInfo</pre>						
		where "nodeId like 'C*' and siteId=' <ne name="" of<="" th=""></ne>						
		the site which is being upgraded>'"); do iset -						
		finhibitRepPlans='A B' NodeInfo where						
		"nodeName='\$i'"; done						

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

	Main Men	Note: Ni and goir below fo upgrade u: Configurat	Ena Igte rm dth	ame of t o Config ore deta nen site > Server (the site c guration- ails. E.g. Id will be Groups	an b >Ser if Se SO_	e fo ver erve HP	ound out I Groups s rSO1 belo C03.	by loggin screen. I ong to th	ng into the Activ Please see the s he site which is I	e NO GUI napshot being
	Filter +										
		Server Group Name	Leve	i Parent	Function	Servers					
		NPSG	с	SOSG	DSR (multi- active cluster)	SO_HPI SO_HPI	NE C03 C03	Servert/P1 Servert/P2	HA Role Pref	WPs	
					DSR		NE	Server	HA Role Pref	VIPs	
		NOSG	*	NONE	(adveistand)	NO_HP	C03	Severi/01		10.240 10.166	
						IN THE		JENENUL		10.240.10.100	
		909G	8	NOSC	DSR (adheistand)	1000	RE .	SeverS01	HA NOIE Pref	10.240 10.185	
					99K)	SOUHP	C03	Sener902		10.240.10.186	
	raised in can be d selected [root@N node siteld ex A1386 NO_HP0 B1754 SO_HP0 C2254 SO_HP0 C2254 SO_HP0	forming tha lone by ana site e.g. S O1 ~]# iqt cludeTable .099 C3 .109 C03 .131 C03 .233 C3	at realyz ite { Noc nod ss	eplication ing Node SO_HPC leInfo eName NO1 SO1 MP2 MP1	n on MP i eInfo outp C03 shall ho	s disa but. In be se ostNa NO1 SO1 MP2 MP1	able nhib et as ame	d. Verifica itRepPlan s 'A B' : nodeCap Active Active Active Active	ation of reas field fo	eplication inhibitio r all the MP serve inhibitRepPlans A B A B	n on MPs ers for the
Upgrade TVOE Host for Standby SO(if needed)	IF stand Verify th	by SO is ho at the TVO	oste E H	d on TV lost is U	OE blade pgraded.	Э,					
	Execute	Appendix	J	for the s	standby S	0 т\	/OE	Host if ne	eded.		
Upgrade standby SO	Upgrade standby SO server using Upgrade Single Server procedure : Execute Appendix G Single Server Upgrade Procedure										
	After suc with step	ccessfully c 5 below.	om	pleting t	he proced	dure	in A	ppendix G	6, return f	to this point and c	continue

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

6	Active SO TVOE Host Upgrade (if needed)	IF Active SO is hosted on TVOE blade, and the TVOE Host needs to be upgraded:
		Execute Appendix J to upgrade the Active SO TVOE Host
		Execute following commands on upgraded server:
7	Verify cmha process is running on upgraded SO	1. Log into the just-upgraded standby SO, execute the following command:
	· · · · · · · · · · · · · · · · · · ·	# ssh root@ <so address="" ip="" xmi=""></so>
		login as: root
		password: <enter password=""></enter>
		Execute following command on SO:
		[root@SO1 ~]# pl grep "cmha"
		The following output should be generated:
		A 10128 cmha Up 11/20 00:15:58 1 cmha
		If no output is generated then execute following command:
		<pre># service start_cmha start</pre>
8	Upgrade Active SO.	Upgrade Active SO server using Upgrade Single Server procedure :
		Execute Appendix G Single Server Upgrade Procedure
		After successfully completing the procedure in Appendix G, return to this point and continue with next procedure.
		Note: At this point, SO replication is still inhibited (from the GUI), and the C-level servers replication is "AB Inhibitied: (INH Plans=A,B) from the iset command. However, Repl Status shows Allowed for the C Level servers (from the GUI)
9	Install NetBackup on NO and SO (If required).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I.
		Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document

4.3.10 Upgrade cSBR(s)

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

This section covers only the upgrade of Charging SBRs (cSBR), associated with the OFCS application, and NOT Policy SBRs (pSBR), associated with PDRA. Any DSR running PDRA must follow the upgrade procedures found in Section 4.6.2 of this document

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

S	This procedure upgrades the cSBR(s).					
Т	Check off (1) each step as it is completed. Boxes have been provided for this purpose under each step number					
E	Check off (v) each step as it	is com	preted. Boxes have been provided for this purpose under each step number.			
Р #	Should this procedure fail, co	ontact	the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
1	Find the enclosures in the system.	Find cSB	the enclosures in the system. Each enclosure shall contain an IPFE, Active MPs, active Rs and a standby cSBR.			
2	Find the active cSBR(s) in the enclosure	Find Stat	d and record the hostname of Active and Standby cSBR(s) in the enclosure by going to rus & Manage -> HA screen and finding the servers with role as cSBR.			
3	Upgrade cSBRs in OFCS configuration	1.	Upgrade each of the standby cSBR servers identified in step 2, following the Upgrade Single Server procedure. All the standby cSBR servers can be upgraded in parallel.			
			Execute Appendix G Single Server Upgrade Procedure			
			After successfully completing the procedure in Appendix G, return to this point and continue with sub-step 2 below.			
		2.	Upgrade each of the leftover cSBRs identified in step 2, following the Upgrade Single Server procedure. All the Leftover cSBR servers can be upgraded in parallel.			
			Execute Appendix G Single Server Upgrade Procedure			
			After successfully completing the procedure in Appendix G, return to this point and continue with next procedure below.			

4.3.11 Upgrade All Active DA-MPs

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

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

<u>Procedure 26 needs to be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 25 must be executed four distinct times.</u>

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

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

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

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

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

S	This procedure upgrades the IPFE(s).					
T E	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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.					
1	Identify IPFE upgrade	User can choose any number of IPFEs on which upgrade can be executed in parallel				
	order	first enclosure has been successfully upgraded should the IPFE(s) in the second enclosure be				
		upgraded.				

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

Upgrade IPFE servers	 Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure.
	Execute Appendix G Single Server Upgrade Procedure
	2. Upgrade remaining IPFEs of the current site in parallel using Appendix G
Execute ipfeNetUpdate on each upgraded IPFE	Execute following steps on each IPFE server just upgraded :
server	1. Use ssh client to connect to the IPFE server :
	ssh <ipfe address="" ip="" xmi=""></ipfe>
	login as: root
	password: <enter password=""></enter>
	2. Execute following command on the IPFE server :
	<pre># grep "IPV6_AUTOCONF=no" /etc/sysconfig/network # grep "IPV6FORWARDING=yes" /etc/sysconfig/network</pre>
	If the outcome of any of the above command is blank then execute the steps below else skip the steps below
	<pre># /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # init 6</pre>
	Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.

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

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

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

S	This procedure allow replication for SO and MP servers.								
T E	Check off (\checkmark) each step as it is	Check off ($\sqrt{2}$ 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.								
	Enable 'A B' level replication inhibited for MP(s)(Only if source upgrade release is earlier than 4.1.0_41.16.0)	<pre>Note: The following steps will uninhibit replication to C level servers Enable replication disabled previously only if source upgrade release was earlier than 4.1.0_41.16.0 : 1. Log into the standby SO using ssh client or puTTy : ssh <standby address="" ip="" so="" xmi=""> login as: root password: <enter password=""> 2. Execute the following command to enable replication : # iload /var/TKLC/db/filemgmt/\$(hostname).TableDef_bac kup.xml # pm.set off inetrep # pm.set on inetrep Execute above sub-steps 1 and 2 for the active SO as well.</enter></standby></pre>							
2	Allow replication to SO servers.	 Allow database replication to SO servers: Log into the active NO GUI using the VIP. Select Status & Manage > Database The Database Status screen is displayed. Select the Active SO server. Click Allow Replication button. After the Allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. Note: "Allowed" text dialog may be hidden beneath the Provisoing disabled text dialog. Verify the Inhibited text is not displayed for the server. Repeat the Allow action link for Standby SO server. Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps. 							

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

3	Enable global provisioning and configuration (if not	Enable provisioning and configuration updates on the entire network(if not already enabled, else ignore this step):
	already enabled).	Provisioning and configuration updates may be enabled to the entire network. Please note that by enabling global provisioning new data provisioned at NOAM will be replicated to only upgraded SO(s).
		1. Log into the active NOAM GUI using the VIP.
		2. Select Status & Manage > Database
		The Database Status screen is displayed.
		3. Click Enable Provisioning button.
		4. Verify the text of the button changes to Disable Provisioning.
ļ	Enable site provisioning	Enable Site provisioning :
		1. Log into the SOAM VIP GUI of the site just upgraded.
		2. Select Status & Manage > Database the Database Status screen is displayed
		3. Click Enable Site Provisioning button.
		4. Confirm the operation by clicking Ok in the popup dialog box.
		5. Verify the button text changes to Disable Site Provisioning
5	Update Max Allowed HA	
	Role for NO and SO.	1. While logged in to the active NOAM GUI, go to the Status & Manage-> HA screen.
		2. Click 'Edit' button.
		 Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list.
		4. Click 'Ok' button.

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

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

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

5	This procedure verifies Post Upgrade Status							
3	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
,	SHOULD THIS PROCEDURE	E FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.						
ŧ								
1	Verify Server Status is Normal	Verify Server Status is Normal:						
		 Select Status & Manage > Server: the Server Status screen is displayed. 						
		3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc).						
		4. Execute following commands on the upgraded servers :						
		Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. ssh, putty): ssh <mp address="" imi="" ip="" server=""></mp>						
		login as: root						
		password: <enter password=""></enter>						
		<pre># verifyUpgrade</pre>						
		Examine the output of the above command to determine if any errors were reported. Contact Tekelec in case of errors.						

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

2	Log all current alarms	Log all current alarms in the system:					
		 Log in to the active NOAM GUI using VIP and select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed. 					
		Following Alarm ID will be observed on all the upgraded MP servers i.e IPFEs,DA-MPs and					
		C-SBRS (whichever exists) : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)					
		Note : If ALARM ID 32532 is not raised on any of the upgraded MP server, then execute following commands on that particular server to check the existence of alarm :					
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. ssh, putty):					
		ssh <mp address="" ip="" server=""></mp>					
		login as: root					
		password: <enter password=""></enter>					
		<pre># alarmMgralarmstatus</pre>					
		The following output should be raised :					
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33					
		Contact Tekelec in case above output is not raised.					
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each MP server					
		3. Click Report button to generate an Alarms report.					
		4. Save the report and print the report. Keep these copies for future reference.					
3	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade					
	End of second maintenance window.						

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

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

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

The following commercial deployment types are supported:

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

In DSR 4.x/5.x, RMS-based DSRs are deployed in one of two supported configurations: without geographic redundancy, or with geographic redundancy. In both cases, the RMS-based DSR implements just a single Diameter network element.

When an RMS-based DSR is without geographic redundancy, there is just a single RMS geographic site, functioning as a single RMS Diameter site. The upgrade of this DSR deployment should be done in two maintenance windows: one for the NOAMs, and the second for all remaining servers.

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

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

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

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

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

This section contains upgrade steps for DSR 5.x (3-tier setup) NO upgrade with (N+0) configuration (major or incremental).

Procedures for the 3-tier NO Upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning will be disabled before upgrading the NO servers (which will also disable provisioning at the SO servers), and provisioning activities at the NO and SO servers will have certain limitations during the period where the NOs are upgraded and the sites are not yet upgraded.

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

These times are estimates.

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

Table 12. NO Upgrade Execution Overview (For DSR 3-tier(N+0) RMS configuration)

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

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

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

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

5	This procedure performs a Health Check.					
Г Е	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.					
	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.x), then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (this can be done from PMAC Software Inventory form) Complete this information: NO-A TVOE Host Rev DR-NO-A TVOE Host Rev DR-NO-B TVOE Host Rev Will TVOE Upgrades be performed during the DSR Application Upgrades?				

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

JI: Verify NO For the sexisting	For the servers with Role = Network OAM&P, confirm Application Version (pre-upgrade).							
ation Version Examp	Example: Note : Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the example below provides the snapshot from both the releases.							
Note: release								
Upgra	de Screen in D	SR 4.x						
Maii	Main Menu: Administration -> Upgrade							
	llestreme		ork El	ement	Role			
HOST	Hostname			Version	Function			
TON	0.000 4	T2_1	10_220			NETWORK OAM&P		
12-10	J-228-A	4.0.2	-40.27	.3		OAM&P		
T2-N0	D-228-B	T2_N Unkr	10_228 10wn	3		NETWORK OAM&P		
		T2 N	10 229	3		MP		
MP2		4.0.2	-40.27	.3		DSR (multi-active cluster)		
		T2 N	10 228	3		MP		
МРЗ	MP3			.3	DSR (multi-active cluster)			
ipfe1				3	MP			
		4.0.2	-40.27	.3	IPL Front End			
ipfe2	ipfe2			3	MP			
		4.0.2	-40.27	.3		IP Front End		
MP1	MP1		10_228 -40.27	MP DSR (multi-active				
Upgra	<u>de Screen in D</u>	<u>SR 5.x</u>						
	Server Status	Server Role	Function	Upgrade State	Status Message			
Hostname	OAM Max HA Role Max Allowed	Network Element		Start Time	Finish Time	Mate Server Status		
	HA Role Norm	Network OAM&P	OAM&P	Not Ready				
Viper-NO1	Active Active	NO_Viper 5.0.0-50.15.1	\mathcal{I}			Viper-NO2		
Viper-NO1 Viper-NO2	Active Active Norm Standby Active	NO_Viper 5.0.0-50.15.1 Network OAM&P NO_Viper 5.0.0-50.15.1	OAM8P	Not Ready		Viper-NO2		
Viper-NO1 Viper-NO2 Viper-SO1-A	Active Active Norm Active Norm Active Active	NO_Viper 5.0.0-50.15.1 Network OAM&P NO_Viper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1	OAM&P	Not Ready Not Ready		Vper-N02 Vper-N01 Vper-S01-B		
Viper-NO1 Viper-NO2 Viper-SO1-A Viper-SO1-B	Active Active Norm Active Active Active Active Active Standby Active	NO_Viper 5.0.0-50.15.1 Network OAM&P NO_Viper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1	OAM&P OAM OAM	Not Ready Not Ready Not Ready		Vper-N02 Vper-N01 Vper-S01-B Vper-S01-A		
Viper-NO1 Viper-NO2 Viper-SO1-A Viper-SO1-B Viper-SO2-A	Active Active Norm Active Active Active Active Active Standby Active Active	NO_Ulper 5.0.0-50.15.1 Network OAM8P NO_Ulper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1 System OAM SO2_Viper 5.0.0-50.15.1	OAM&P OAM OAM OAM	Not Ready Not Ready Not Ready Not Ready		Vper-NO2 Vper-NO1 Vper-SO1B Vper-SO1A Vper-SO2B		
Viper-NO1 Viper-NO2 Viper-SO1-A Viper-SO1-B Viper-SO2-A Viper-SO2-B	Active Active Active Active Active Active Active Active Active Active Active Active Active Active Active Active Active Active Active	NO_Wper 5.0.50.15.1 Network OMM&P NO_Wper 5.0.050.15.1 System OAM SO1_Viper 5.0.050.15.1 System OAM SO1_Viper 5.0.050.15.1 System OAM SO2_Viper 5.0.050.15.1	OAM&P OAM OAM OAM OAM	Not Ready Not Ready Not Ready Not Ready		Wper-N02 Wper-N01 Wper-S014 Wper-S024 Wper-S024		
Viper-NO1 Viper-NO2 Viper-SO1-A Viper-SO1-B Viper-SO2-A Viper-SO2-B Viper-MP05	Active Standby Active Norm Standby Active Norm	NO_Wper 5.0.50.15.1 Network OMMAP NO_Wper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1 System OAM SO1_Viper 5.0.0-50.15.1 System OAM SO2_Viper 5.0.0-50.15.1 System OAM SO2_Viper 5.0.0-50.15.1	OAM&P OAM OAM OAM OAM OAM DSR (multi- active)	Not Ready Not Ready Not Ready Not Ready Not Ready		Wper-N02 Wper-N01 Wper-S01-8 Wper-S02-8 Wper-S02-4 Wper-M06		

3	NO GUI: Verify ISO for	Verify DSR ISO file has been Transferred to all servers:						
	Jpgrade has been Example:							
	Deployed	LAIIIPIC.						
		Main Manue Administration > 160						
		Main Mellu: Administration -> 130						
		Display Filter: - None -						
		 Transfer 100 Operativity 						
		ISO: 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso						
		7 of 7 Transfers Successful.						
		0 of 7 Transfers Failed.						
		Table description: List of Systems for ISO transfer						
		System Name / Hostname ISO Transfer Status						
		MP1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete						
		MP2 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete						
		MP3 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete						
		T2-NO-228-B 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete						
		ipfe1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete						
		prez 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete Displaving Records 1-7 of 7 total First Prev Next Last						
		[Transfer ISO]						
		IE Not see ISO Administration 2.2.8						
4	Verify Server Status is	Verify Server Status is Normal:						
	Normal	Les lete the NOAM OUT union the MD						
		Log into the NOAM GUI using the VIP.						
		 Select Status & Manage > Server, the Server Status screen is displayed. Verify all Server Status is Normal (Norm) for Alarm (Alm). Database (DB). High 						
		Availability (HA), and Processes (Proc).						
		3. Do not proceed to upgrade if any of the server statuses displayed is not Norm .						
		4. Do not proceed if there are any Major or Critical alarms.						
		Note: It is not recommended to continue executing upgrade if any server status has						
		if the upgrade is specifically intended to clear those alarm(s). This would mean that the target						
		release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method						
		to clear the alarm(s). Do not continue otherwise.						
5	Log all current alarms at	Log all current alarms in the system:						
	NOAM							
		1. Select Alarms & Events > View Active; the Alarms & Events > View Active view is						
		displayed.						
		2. Click Report button to generate an Alarms report.						
		3. Save the report and/or print the report. Keep these copies for future reference.						
6	Repeat for active	Log all current alarms in the SOAM:						
	SOAMs							
		1. Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM						
		GUI itself.						

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

7	Verify that a recent version of the Full DB backup has been performed	Verify that a recent version of the Full DB backup has been performed.
		Select Status and Manage → Files Check time stamp on two files:
		Backup.DSR. <hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.ta r.bz2</time_stamp></hostname>
		Backup.DSR. <hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.t ar.bz2</time_stamp></hostname>
		See section 3.3.5 to perform (or re-perform) a full Backup, if needed.

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



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

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

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

This Procedure inhibits replication for 3-Tier NO (and DR-NO) servers, prior to upgrade. This Procedure S Т is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only. Е It applies to (N+0) redundant DA-MP server configurations on RMS servers. Р Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number. # Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE. Start of next maintenance window Disable global Disable global provisioning and configuration updates on the entire network: provisioning and configuration. Log into the NOAM VIP GUI. 1. Select Status & Manage > Database; the Database Status screen is displayed Click Disable Provisioning button. 2. Confirm the operation by clicking **Ok** in the popup dialog box. 3. Verify the button text changes to Enable Provisioning; a yellow information box should 4 also be displayed at the top of the view screen which states: [Warning Code 002] -Provisioning is manually disabled. Active NO server will have the following expected alarm: 5. - Alarm ID = 10008 (Provisioning Manually Disabled) 2 Inhibit replication to MP Replication of MPs will be inhibited during site upgrade. servers (N+0) Inhibit replication to SO Inhibit database replication to SO servers in the following order: 3 servers at a site Site: Standby SO 0 Active SO 0 From Active NO: 1. Select Status & Manage > Database The Database Status screen is displayed. 2. Select the appropriate SO server. Click Inhibit Replication button. 3. Verify the Inhibited text is displayed for server. 4. 5. Repeat the above steps for all remaining servers in the order: standby, then active). ALL SOAMs must be inhibited.

Procedure 31.	Inhibit I	Replication	for 3-Tie	r(N+0)	RMS setup
roccuure 51.	minute	<i>icplication</i>	101 5-110		inito secup

4	Verify that SO Servers are Inhibited	Select Status & Manage > Database
		Verify that the Replication status is Inhibited for all SOs, at all sites.
		The following alarms are expected:
		Active NO server has:
		Alarm ID = 10008 (Provisioning Manually Disabled)
		All SO(s) servers must have:
		Alarm ID = 31113 (Replication Manually Disabled)
5	Inhibit replication	Inhibit database replication between NO servers in the following order:
	between NO servers.	Standby NO
		 ACTIVE NO Standby DR NO(if applicable)
		 Active DR NO(if applicable)
		Select Status & Manage > Database
		The Database Status screen is displayed.
		5. Select the appropriate NO or DR-NO server based on the list above.
		6. Click Inhibit Replication button.
		7. Verify the Inhibited text is displayed for server.
		8. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the
		order snown above.
		Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.
6	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database
5	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers.
	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected:
Ó	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has:
Í	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)
5	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
6	Verify that NOs and SOs are Inhibited	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled)
7	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup :
7	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP.
	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database
	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button.
7	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box.
	Verify that NOs and SOs are Inhibited Disable Site Provisioning	 Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box
7	Verify that NOs and SOs are Inhibited Disable Site Provisioning	 Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004]
7	Verify that NOs and SOs are Inhibited Disable Site Provisioning	Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers. Select Status & Manage > Database Verify that the Replication status is Inhibited for all NO servers and all sites SOAM servers. The following alarms are expected: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All SO(s) and NO servers must have: Alarm ID = 31113 (Replication Manually Disabled) Disable Site provisioning for all the sites present in the setup : 1. Log into the GUI of the SOAM for all the sites using the VIP. 2. Select Status & Manage > Database the Database Status screen is displayed 3. Click Disable Site Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled. 6 Repeat substeps 2 through 5 for all the sites present in the setup

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

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

S T	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only.						
Ē	It applies to (N+0) redundant DA-MP server configurations on RMS servers.						
Р #	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.						
	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.						
1	Begin Upgrade of DR-	Next Steps will begin Upgrade of the DR-NO servers.					
		SKIP this Procedure if the deployment does not include DR-NO servers.					
2	Upgrade Host TVOE for Standby DR-NO (if	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)					
	needed)	Execute Appendix J for the standby DR NO					
3	Upgrade Standby DR-	Upgrade the standby DSR DR NO:					
	Upgrade Single Server	Execute Appendix G Single Server Upgrade Procedure					
	procedurey	After successfully completing the procedure in Appendix G, return to this point and continue with step below.					
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.					
4	Upgrade Host TVOE for Active DR-NO (if needed)	 Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 					
		Execute Appendix J for the active DR NO to upgrade TVOE.					
5	Verify cmha process is running on upgraded DR NO	Log into the just-upgraded standby DR NO upgraded above, execute the following command:					
		ssh <no address="" ip="" xmi=""></no>					
		login as: root					
		password: <enter password=""></enter>					
		[root@NO1 ~]# pl grep "cmha"					
		The following output should be generated:					
		A 10128 cmha Up 11/20 00:15:58 1 cmha					
		If no output is generated then execute following command:					
	service start_cmha start						

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

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

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

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

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

S	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO,						
T E	and DSR MP) deployment only. It applies to (N+0) redundant DA-MP server configurations on RMS servers.						
P							
#	Check off (\mathbf{v}) each step as it is completed. Boxes have been provided for this purpose under each step number.						
	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.						
1	Upgrade Host TVOE for Standby NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)					
		Execute Appendix J for the standby NO					
2	Upgrade Standby NO	Upgrade the standby DSR NO:					
	Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure					
	, ,	After successfully completing the procedure in Appendix G, return to this point and continue with step below.					
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.					
3	Upgrade Host TVOE for Active NO (if needed)	 Skip this step if: the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 					
4	Verify cmba process is	Execute Appendix . I for the active NO to upgrade TVOE					
	running on upgraded						
	NO server.	command:					
		ssh <no address="" ip="" xmi=""></no>					
		login as: root					
		password: <enter password=""></enter>					
		[root@NO1 ~]# pl grep "cmha"					
		The following output should be generated:					
		A 10128 cmha Up 11/20 00:15:58 1 cmha					
		If no output is generated then execute following command:					
	service start_cmha start						

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

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

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

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

S This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, and either (1+1) or (N+0) redundant DA-MP server configurations.
 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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.

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

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

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

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

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

S	This procedure verifies Post Upgrade Status for 3-Tier(N+0) NO upgrade on RMS servers.
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.
#	

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

SSH: Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:				
	 Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers : 				
	Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <no address="" ip="" xmi=""></no>				
	login as: root				
	password: <enter password=""></enter>				
	Note: The static XMI IP address for each NO server should be available in Table 3.				
	# verifyUpgrade				
	Examine the output of the above command to determine if any errors were reported. In case of errors please contact Tekelec.				
	<pre># alarmMgralarmstatus</pre>				
	Following alarm output should be seen, indicating that the upgrade completed.				
	SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33				
	[Alarm ID 32532 will be cleared after the upgrade is accepted.]				
	Contact Tekelec in case above output is not generated.				
NO GUI: Verify Alarm	Log all current alarms in the system:				
olado	1. Log into the NOAM GUI via the VIP.				
	2. Select Alarms & Events > View Active; the Alarms & Events > view Active view is displayed.				
	 Click Report button to generate an Alarms report. Save the report and/or print the report. Keep these copies for future reference. 				
	Expected Alarms include:				
	Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)				
	All other servers might have: Alarm ID = 31113 (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)				

3	SO GUI: Verify Alarm	Log all current alarms in the system:
	status	1 Log into the SOAM GUI via the VIP
		 Select Alarms & Events > View Active; the Alarms & Events > View Active view is
		displayed.
		3. Click Report button to generate an Alarms report.
		4. Save the report and/or print the report. Keep these copies for future reference.
		Expected Alarms include:
		Active SO server has: Alarm ID = 10008 (Provisioning Manually Disabled)
		Alarm ID = 31113 (Replication Manually Disabled)
4	Verify Traffic status	Login to SOAM GUI to view KPI reports to verify traffic is at the expected condition.
5	Update Appworks	Note 1: This step is only applicable if the setup includes IPFE servers. This step will
	Table for the configured	servers. We are preparing the Active NO to handle any such discrepancies.
	on the Active NO server	Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs audit on the configured IPFE Ethernet devices and will update them with the locally stored information in case of any discrepancies.
		Note 3: The steps below will update the locally stored information with the performance optimization parameters. This script check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices
		 Login to Active NO console and execute the following command /usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh
		NOTE: This command may execute without any output when no changes are required (no devices were found to update).
6	Note on Provisioning status	Provisioning on the NO and SOs, and Replication from NO to the Site level SO, will typically remain disabled till further upgrades are performed on the sites. SO provisioning shall also remain disabled.
		NOTE: (SO replication inhibit will prevent most NO configuration changes from being propagated to the SOs.)
		End of maintenance window

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

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

This section contains the steps required to upgrade a 3-tier DSR site that has a SOAM function, and multiple-active (N+0) DA-MP configuration on RMS servers.

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

Global provisioning can be re-enabled(if required) after any one of the site has been upgraded.

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

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

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

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

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

S	This procedure performs a Health Check.							
T F	Check off (\checkmark) each step as it is	s 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 Verify Server Status after NO servers upgraded:							
		1. Execute following commands on both the active and standby NOAM servers:						
		Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <no address="" ip="" xmi=""></no>						
		login as: root password: <enter password=""></enter>						
		Note: The static XMI IP address for each NO server should be available in Table 3.						
		# verifyUpgrade						
		Examine the output of the above command to determine if any errors were reported. Contact Tekelec if any errors are observed.						
		 Log in to Active NOAM VIP GUI and select Alarms & Events-> View Active screen to verify Servers alarms. Servers have following expected alarms: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) 						
		All other servers might have: Alarm ID = 31113 (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)						
		Note : If ALARM ID 32532 is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :						
		# alarmMgralarmstatus						
		The following output will be raised :						
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33						
		Contact Tekelec in case above output is not raised.						
		3. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each server.						

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

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

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

Detailed steps are shown in the procedure below.

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

S	This procedure upgrades the SOAM(s) in a 3-tier DSR. This Procedure is specific to 3-tier (DSR NO, DSR								
Т	SO, and DSR MP) RM	S deployments only.							
E	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
P									
#	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.							
		Start of next maintenance window(If required)							
1	Verify Traffic status	Login to Active SOAM and verify KPI reports to verify traffic is at the expected condition.							
2	Verify that site Provisioning is disabled	Verify that site provisioning for the site which is currently being upgraded is disabled. By logging into the site VIP and checking for Provisioning disabled alarm. If provisioning disabled alarm is not present then execute following steps :							
		 Log into the GUI of the SOAM which needs to be upgraded, using the VIP. Select Status & Manage > Database the Database Status screen is displayed Click Disable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled. 							
3	Inhibit replication to MP servers (N+0)	 Record current release numberex: 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 ip="" no="" xmi=""> login as: root</active> 							

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

	Execute # for where the s finhi "node Note: N and go below f upgrad	e following c c i in s e "nodel site whi bitRepl eName='s NE name of ing to Confi or more de ed then site	omi (i cd ich ?la ithe igu tail eld	mand o like n is ans=''; d e site c ration-: s. E.g. will be	n active N p -z - being A B' N lone an be fou >Server G if ServerS SO_HPCO	NO: and upgra lodeI: and out sroups: SO1 belo 03.	hostNa siteId aded>' nfo wh by loggir screen. F ong to th	ame Noo d=' <ne "); do nere ng into th Please se e site wh</ne 	deInfo name of o iset - e Active NO GUI e the snapshot ich is being
	Filter •		050						Non Aug 25 02
		Server Groen Name	Int	Parent	Feaction	Servers			
		IPSC	C	505G	DSR (muß- achie duster)	NE SO_HPC03 SO_HPC03	Sener SeverliP1 SeverliP2	HA Role Pref	VPs
		NCSG		NONE	OSR (activeistando pair)	ND_HPC03 NO_HPC03	Serverti/O1 Serverti/O2	HA Role Pref	VPs 10.240 10.166 10.240.10.166
		505G	B	NOSG	DSR (achielstandb pair)	NE BOILLASS SO_HPC83	Server ServerSO1 ServerSO2	HA Role Pref	WPs 10.240 10.166 10.240 10.186
	Note: After execut raised informing th can be done by ar selected site e.g. 3 [root@NO1 ~]# iq nodeld siteld excludeTab A1386.099 NO_HPC3 B1754.109 SO_HPC03 C2254.131 SO_HPC03 C2254.233 SO_HPC3	ing above s nat replication nalyzing Noo Site SO_HP t NodeInfo nodeName les NO1 SO1 MP2 MP1	tep: on o delr cO:	s to inh n MP is ifo outp 3 shall I hc	ibit replica s disabled. but. InhibitF be set as f ostName n NO1 SO1 MP2 MP1	tion on l Verifica RepPlar A B' : odeCap Active Active Active Active	MP(s), no ation of re ns field for pability	alarms o plication i r all the M inhibitRe A B A B	n GUI would be nhibition on MPs P servers for the pPlans
Upgrade standby SO	Upgrade standby	SO server	usir	ig Upgr	ade Single	e Server	. procedu	re :	
	Execute App After success continue with Note: In an RMS- upgraded as part	sfully compl sfully compl step 4 belo based DSR t of the NO	Sin etin ow. th e AM	gle Ser g the pr e SOAN upgrad	ver Upgra rocedure in M is a gue de.	de Proc n Apper est on a	edure ndix G, ref TVOE ho	turn to this ost that h	s point and as already been

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

4	Upgrade Active SO.	Upgrade Active SO server using Upgrade Single Server procedure :					
		Execute Appendix G Single Server Upgrade Procedure					
		After successfully completing the procedure in Appendix G, return to this point and continue with next procedure.					
		Note: In an RMS-based DSR the SOAM is a guest on a TVOE host that has already been upgraded as part of the NOAM upgrade.					
		Note: At this point, SO replication is still inhibited (from the GUI), and the C-level servers replication is "AB Inhibitied: (INH Plans=A,B) from the iset command. However, Repl Status shows Allowed for the C Level servers (from the GUI)					
5	Install NetBackup on NO and SO (If required).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I.					
		Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to					
		/var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.					

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

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

Procedure 26 needs to be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 26 must be executed four distinct times.

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

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

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

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

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

S	This procedure upgrades the IPFE(s).							
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
Р #	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.							
1	Identify IPFE upgrade order	User can choose any number of IPFEs on which upgrade can be executed in parallel considering traffic impact. All the IPFEs should belong to same RMS geographic site and only						
		after the first RMS geographical site has been successfully upgraded should the IPFE(s) in the second RMS geographic site be upgraded.						
2	Upgrade IPFE servers	 Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure. 						
		Execute Appendix G Single Server Upgrade Procedure						
		2. Upgrade remaining IPFEs of the current site in parallel using Appendix G						

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

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

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

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

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

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

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

3	Enable global	Enable provisioning and configuration updates on the entire network:
	configuration.	Provisioning and configuration updates may be enabled to the entire network. Note: Please note that by enabling global provisioning new data provisioned at NOAM will be replicated to only upgraded SO(s).
		1. Log into the active NOAM GUI using the VIP.
		2. Select Status & Manage > Database
		The Database Status screen isis displayed.
		3. Click Enable Provisioning button.
		Verify the text of the button changes to Disable Provisioning.
ļ	Enable site provisioning.	Enable Site provisioning :
		1. Log into the SOAM VIP GUI of the site just upgraded above
		 Select Status & Manage > Database the Database Status screen is displayed
		3. Click Enable Site Provisioning button.
		4. Confirm the operation by clicking Ok in the popup dialog box.
		5. Verify the button text changes to Disable Site Provisioning.
;	Update Max Allowed HA	
	Role for NO and SO.	1. While logged in to the active NOAM GUI, go to the Status & Manage-> HA screen.
		2. Click 'Edit' button.
		3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be
		'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list.
		4. Click 'Ok' button.

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

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

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

S	This procedure verifies Post Upgrade Status								
Т	Check off (A) each stan as it is completed. Bayes have been provided for this purpose under each stan number								
Ε	Check on (v) 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.								
#									
	Verify Server Status is Normal	 Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select Status & Manage > Server; the Server Status screen isis displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 4. Execute following commands on the upgraded servers : Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. ssh, putty): ssh <mp address="" imi="" ip="" server=""></mp> login as: root password: <enter password=""></enter> 							
		Tekelec in case of errors.							

Procedure 41: V	/erify Post	Upgrade s	status on	RMS	servers	(N+0.	3-Tier)
-----------------	-------------	-----------	-----------	-----	---------	-------	---------

2	Log all current alarms	Log all current alarms in the system:
		 Log in to the active NOAM GUI using VIP and select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed.
		Following Alarm ID will be observed on all the upgraded MP servers i.e IPFEs,DA-MPs and
		Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
		Note : If ALARM ID 32532 is not raised on any of the upgraded MP server, then execute following commands on that particular server to check the existence of alarm :
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. ssh, putty):
		ssh <mp address="" ip="" server=""></mp>
		login as: root
		password: <enter password=""></enter>
		# alarmMgralarmstatus
		The following output should be raised :
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33
		Contact Tekelec in case above output is not raised.
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on
		each MP server.
		3. Click Report button to generate an Alarms report.
		4. Save the report and print the report. Keep these copies for future reference.
3	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
		End of second maintenance window.

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

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

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

The following commercial deployment types are supported:

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

In DSR 4.x/5.x, RMS-based DSRs are deployed in one of two supported configurations: without geographic redundancy, or with geographic redundancy. In both cases, the RMS-based DSR implements just a single Diameter network element.

When an RMS-based DSR is without geographic redundancy, there is just a single RMS geographic site, functioning as a single RMS Diameter site. The upgrade of this DSR deployment should be done in two maintenance windows: one for the NOAMs, and the second for all remaining servers.

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

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

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

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

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

This section contains upgrade steps for DSR 5.x (3-tier setup) NO upgrade with (1+1) configuration (major or incremental).

Procedures for the 3-tier NO Upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning will be disabled before upgrading the NO servers (which will also disable provisioning at the SO servers), and provisioning activities at the NO and SO servers will have certain limitations during the period where the NOs are upgraded and the sites are not yet upgraded.

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

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

Table 14. NO Upgrade Execution Overview (For DSR 3-Tier(1+1) RMS configuration)

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

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

S	This procedure perfo	rms a Health Check.			
T E	Check off (\mathbf{v}) each step as it is	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	Determine if TVOE Host Upgrades will be required during the Upgrade (or have been performed prior to this upgrade)	IMPORTANT: Verify the revision level of the TVOE Host systems for the NO and DR-NO virtual servers. If they are not on the required release (typically 2.5.x) , then the optional steps in this procedure to upgrade the TVOE Hosts will be required. See Appendix E for the steps to verify the TVOE Host revision level. (this can be done from PMAC Software Inventory form) Complete this information: NO-A TVOE Host Rev NO-B TVOE Host Rev DR-NO-A TVOE Host Rev Will TVOE Upgrades be performed during the DSR Application Upgrades?			

O GUI: Verify NO	For the se	ervers with R	ole = Net	work C	AM&P, co	nfirm Applica	tion Version (pre-upgrade
Application Version	Example:						
	Note: Loo	k and feel of	f the Upgr	ade so	creen has c	hanged betw	een DSR 4.x and DSR 5
	releases,	the example	below pr	ovides	the snaps	hot from both	the releases.
	Upgrade	Screen in D	SR 4.x				
	Main M	Menu: Ac	lminis	trati	on -> U	lpgrade	
				orde Ele			Data
	Hostnam	e	Appl	Application Version			Function
	·		Аррі		Version		
	T2-NO-22	28-A 🛛	4.0.2	-40.27	3		OAM&P
			T2 N	10 228	3		NETWORK OAM&P
	T2-NO-22	28-B	Unkr	nown			OAM&P
			T2_N	10_228	3		MP
	MP2		4.0.2	-40.27	3		DSR (multi-active cluster)
			T2_N	10_228	3		MP
	MP3		4.0.2	-40.27	3		DSR (multi-active cluster)
	infe1		T2_N	10_228	3		MP
	ipio i		4.0.2	-40.27	3		IPL ront End
	ipfe2		T2_N	10_228	3		MP
			4.0.2	-40.27	3		IP Front End
	MP1	MP1			3	MP DSD (multi active	
					3		cluster)
	Upgrade Hostname	Screen in D Server Status OAM Max HA Role Max Allowed HA Role	SR 5.X Server Role Network Element Application Version	Function	Upgrade State Start Time Upgrade ISO	Status Message Finish Time	Mate Server Status
	Viper-NO1	Norm Active	Network OAM&P NO_Viper	OAMEP	Not Ready		Viper-NO2
	Viper-NO2	Active Norm Standby	5.0.0-50.15.1 Network OAM&P NO_Viper	OAM&P	Not Ready		Viper-NO1
		Active	5.0.0-50.15.1 System OAM	OAM	Not Ready		
	Viper-SO1-A	Active Active	SO1_Viper 5.0.0-50.15.1				Viper-SO1-B
	Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-A
	Viper-SO2-A	Norm Active Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-B
	Viper-SO2-B	Norm Standby	System OAM SO2_Viper	OAM	Not Ready		Viper-SO2-A
		Active	5.0.0-50.15.1	DSR			
	Viper-MP05	Norm	MP SO1_Viper	(multi- active cluster)	Not Ready		[Viper-MP06]

3	NO GUI: Verify ISO for Upgrade has been Deploved	Verify DSR ISO file has been Transferred to all servers: Example:
		Main Menu: Administration -> ISO
		Transfer ISO Complete. ISO: 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso 7 of 7 Transfers Successful. 0 of 7 Transfers Failed.
		Table description: List of Systems for ISO transfer.
		Displaving Records 1-7 of 7 total First Prev Next Last
		System Name / Hostname ISO Transfer Status
		MP1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		MP3 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		T2-NO-228-A 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		ipfe1 872-2526-101-5.0.0_50.12.0-DSR-x86_64.is0 Complete
		ipfe2 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso Complete
		Displaying Records 1-7 of 7 total Hirst Prev Next Last
		[Transfer ISO]
		IF Not, see ISO Administration 3.3.8.
4	Verify Server Status is Normal	Verify Server Status is Normal:
		Log Into the NOAM GUI using the VIP.
		 Select Status & Manage > Server; the Server Status screen is displayed. Varify all Server Status is Normal (Norm) for Alarm (Alm). Database (DD) Urah
		2. Venity an Server Status is Normal (Norm) for Alarm (Aim), Database (DD), Fight Availability (HA), and Processes (Proc)
		3. Do not proceed to upgrade if any of the server statuses displayed is not Norm .
		4. Do not proceed if there are any Major or Critical alarms.
		Note: It is not recommended to continue executing upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms
		if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method
		to clear the alarm(s). Do not continue otherwise.
5	Log all current alarms at	Log all current alarms in the system:
	NOAW	1. Select Alarms & Events > View Active; the Alarms & Events > View Active view is
		displayed.
		2. Click Report button to generate an Alarms report.
		3. Save the report and/or print the report. Keep these copies for future reference.
6	Repeat for active SOAMs	Log all current alarms in the SOAM:
	-	 Log into the active SOAM GUI and repeat Steps 1 and 2 of this procedure from SOAM GUI itself.

7	Verify that a recent version of the Full DB	Verify that a recent version of the Full DB backup has been performed.
	backup has been performed	Select Status and Manage → Files Check time stamp on two files:
		Backup.DSR. <hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.ta r.bz2</time_stamp></hostname>
		Backup.DSR. <hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.t ar.bz2</time_stamp></hostname>
		See section 3.3.5 to perform (or re-perform) a full Backup, if needed.

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



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

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

S	This Procedure inhibits replication for 3-Tier NO (and DR-NO) servers, prior to upgrade. This Procedure						
Т	is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only.						
Ē	It applies to either $(1+1)$ or $(N+0)$ redundant DA-MP server configurations.						
D	it applies to entire (1+1) of (1+6) redundant DA for server configurations.						
Р #	Check off ($$) each step as it	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
	Should this procedure fail, co	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.					
		Start of next maintenance window					
1	Disable global	Disable global provisioning and configuration updates on the entire network:					
	provisioning and						
	configuration.	Log into the NOAM VIP GUI.					
		1. Select Status & Manage > Database; the Database Status screen is displayed					
		2. Click Disable Provisioning button.					
		3. Confirm the operation by clicking Ok in the popup dialog box.					
		4. Verify the button text changes to Enable Provisioning; a yellow information box should					
		also be displayed at the top of the view screen which states: [Warning Code 002] -					
		Provisioning is manually disabled.					
		5. Active NO server will have the following expected alarm:					
		- Alarm ID = 10008 (Provisioning Manually Disabled)					
2	Inhibit replication to MP	Inhibit database replication to MP servers in the following order:					
	servers (1+1)	Standby DA-MP					
		Active DA-MP					
		From Active NO:					
	1 Select Status & Manage > Database						
	The Database Status screen is displayed						
		2 Select the appropriate DA-MP server					
		Click Inhibit Replication button					
		4. Verify the Inhibited text is displayed for server					
		4. Vehicy the minuted text is displayed for server.					
		Note: It is important to inhibit the replication of the standby conver before the active					
		server, to prevent unwanted HA switchovers.					
		ALL DA-MPs must be inhibited.					

convore at a cita	Inhibit database replication to SO servers in the following order.
Servers at a site	Site:
	 Standby SO
	• Active SO
	From Active NO:
	1. Select Status & Manage > Database
	The Database Status screen is displayed.
	2. Select the appropriate 50 server.
	5. Click IIIIbit Replication button.
	4. Vehicy the minimed text is displayed for servers in the order: standby, then
	5. Repeat the above steps for all remaining servers in the order, standby, then
	active).
	ALL SOAM must be inhibited
Verify that MPs and SO	
Servers are Inhibited	Select Status & Manage > Database
	Verify that the Replication status is Inhibited for all MPs and all SOs, at all sites.
	The following alarms are expected:
	Active NO server has:
	Alarm ID = 10008 (Provisioning Manually Disabled)
	All other MP(s) and SO(s) servers should have:
	Alarm ID = 31113 (Replication Manually Disabled)
Inhibit replication to NO	Inhibit database replication to all servers in the following order:
servers.	Standby NO
	Active NO
	Standby DR NO(if applicable)
	• Active DR NO(ir applicable)
	Select Status & Manage > Database
	The Database Status screen is displayed.
	1. Select the appropriate NO or DR-NO server based on the list above.
	2. Click Inhibit Replication button.
	3 Varify the liphited text is displayed for sorver
	J. VEIIIV LIE ITITIDILEU LEXT IS UISPLAYEU IOI SELVEL.
	 Verify the infibiled text is displayed for server. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the
	 Verify the infibilited text is displayed for server. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above.
	 Verify the infibilited text is displayed for server. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above.
	 4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. Note: It is important to inhibit the replication of the standby server before the
	 4. Repeat the Inhibit substep actions, steps 2 through 4, for all remaining servers in the order shown above. Note: It is important to inhibit the replication of the standby server before the active server, to prevent unwanted HA switchovers.

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

6	Verify that All Servers are Inhibited	Select Status & Manage > Database			
		Verify that the Replication status is Inhibited for all servers, and all sites.			
		The following alarms are expected:			
		Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other MP(s)/SO(s) and NO servers should have: Alarm ID = 31113 (Replication Manually Disabled)			
7	Disable Site Provisioning	 Disable Site provisioning for all the sites present in the setup : Log into the GUI of the SOAM for all the sites using the VIP. Select Status & Manage > Database the Database Status screen is displayed Click Disable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] Site provisioning has been manually disabled. Repeat substeps 2 through 5 for all the sites present in the setup. 			

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

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

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

S T	This Procedure upgrades the 3-Tier DR-NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployment only.				
E P	It applies to (1+1) DA-MP server configurations on RMS servers.				
#	Check off (1) each step as it	is completed. Boxes have been provided for this purpose under each step number.			
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
1	Begin Upgrade of DR- NOs	Next Steps will begin Upgrade of the DR-NO servers.			
		SKIP this Procedure if the deployment does not include DR-NO servers.			
2	Upgrade Host TVOE for Standby DR-NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)			
		Execute Appendix J for the standby DR NO			
3	Upgrade Standby DR- NO server (using	Upgrade the standby DSR DR NO:			
	Upgrade Single Server procedure)	Execute Appendix G Single Server Upgrade Procedure			
	1,	After successfully completing the procedure in Appendix G, return to this point and continue with step below.			
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.			
4	Upgrade Host TVOE for Active DR-NO (if needed)	 Skip this step if: the DR-NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 			
		Execute Appendix J for the active DR NO to upgrade TVOE.			
5	Verify cmha process is running on upgraded DR NO	Log into the just-upgraded standby DR NO upgraded above, execute the following command:			
		ssh <no address="" ip="" xmi=""></no>			
		login as: root			
		password: <enter password=""></enter>			
		[root@NO1 ~]# pl grep "cmha"			
		The following output should be generated:			
		A 10128 cmha Up 11/20 00:15:58 1 cmha			
		If no output is generated then execute following command:			
		service start_cmha start			

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

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

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

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

C	T1' D 1 1					
б т	This Procedure upgrades the 3-Tier NO servers. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSP MP) deployment only.					
I F	and DSK MF) deproyment only. It applies to $(1 + 1)$ DA MP server configurations on PMS servers					
Р		it applies to (1+1) DA-MP server configurations on RMS servers.				
∎ #	Check off (\mathbf{v}) each step as it	is completed. Boxes have been provided for this purpose under each step number.				
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.				
1	Upgrade Host TVOE for Standby NO (if needed)	Skip this step if the TVOE Host release is up-to-date (as determined in the health checks of the previous procedure)				
		Execute Appendix J for the standby NO				
2	Upgrade Standby NO server (using Upgrade	Upgrade the standby DSR NO:				
	Single Server	Execute Appendix G Single Server Upgrade Procedure				
	procedurey	After successfully completing the procedure in Appendix G, return to this point and continue with step below.				
		IF Upgrade fails – do not proceed. Consult with support on the best course of action.				
3	Upgrade Host TVOE for Active NO (if needed)	 Skip this step if: the deployment does not have a NO site the NO Host TVOE release is up-to-date (as determined in the health checks of the previous procedure) 				
		Execute Appendix J for the active NO to upgrade TVOE.				
4	Verify cmha process is running on upgraded NO.	Log into the just-upgraded standby NO upgraded above, execute the following command:				
		ssh <no address="" ip="" xmi=""></no>				
		login as: root				
		<pre>password: <enter password=""></enter></pre>				
		[root@NO1 ~]# pl grep "cmha"				
		The following output should be generated:				
		A 10128 cmha Up 11/20 00:15:58				
		1 cmha				
		If no output is generated then execute following command:				
		service start_cmha start				

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

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

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

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

S This Procedure re-established the Replication between the NO servers, and the DR-NO servers. It applies to 3-tier, (1+1) DA-MP server configurations on RMS servers
 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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.

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

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

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

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

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

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

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

1	SSH: Verify NO and DR-NO Server Status	Verify Server Status after NO servers upgraded:			
		 Execute following commands on active NOAM, standby NOAM, active DR NOAM, standby DR NOAM servers : 			
		Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <no address="" ip="" xmi=""></no>			
		login as: root			
		<pre>password: <enter password=""></enter></pre>			
		Note: The static XMI IP address for each NO server should be available in Table 3.			
		# verifyUpgrade			
		Examine the output of the above command to determine if any errors were reported. In case of errors please contact Tekelec.			
		# alarmMgralarmstatus			
		Following alarm output should be seen, indicating that the upgrade completed.			
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33			
		[Alarm ID 32532 will be cleared after the upgrade is accepted.]			
		Contact Tekelec in case above output is not generated.			
2	NO GUI: Verify Alarm	Log all current alarms in the system:			
		 Log into the NOAM GUI via the VIP. Select Alarms & Events > View Active; the Alarms & Events > View Active view is 			
		displayed.			
		 Save the report and/or print the report. Keep these copies for future reference. 			
		Expected Alarms include:			
		Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled)			
		All other servers might have: Alarm ID = 31113 (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)			
3	Verify Traffic status	View KPI reports to verify traffic is at the expected condition.			
4	Note on Provisioning status	Provisioning on the NO and SOs, and Replication from NO to the Site level SO and MPs, will typically remain disabled till further upgrades are performed on the sites.			
	End of maintenance window				
4.5.8 Site Upgrade for (1+1) 3-Tier RMS Configuration.

This section contains the steps required to upgrade a 3-tier DSR site that has a SOAM function, and active/standby (1+1) DA-MP configuration.

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

Global provisioning can be re-enabled between after one of the site is completely upgraded.

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

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

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

Detailed steps are shown in the procedure below.

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

S	This procedure upgrades the SOAM(s) in a 3-tier DSR, including, if necessary, TVOE on each server that								
Т	hosts an SOAM guest. This Procedure is specific to 3-tier (DSR NO, DSR SO, and DSR MP) deployments								
Ε	only.								
Р									
#	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.							
		Start of next maintenance window(If required)							
1	Verify site provisioning is disabled.	Verify site provisioning is disabled. Else execute following steps :							
		1. Log into the GUI of the SOAM which needs to be upgraded, using the VIP.							
		2. Select Status & Manage > Database the Database Status screen is displayed							
		3. Click Disable Site Provisioning button.							
		4. Confirm the operation by clicking Ok in the popup dialog box.							
		5. Verify the button text changes to Enable Site Provisioning; a yellow information box							
		should also be displayed at the top of the view screen which states: [Warning Code 004]							
		- Site provisioning has been manually disabled.							
2	Upgrade standby SO	Upgrade standby SO server using Upgrade Single Server procedure :							
		Execute Appendix G Single Server Upgrade Procedure							
		After successfully completing the procedure in Appendix G, return to this point and continue with step 3 below.							
		Note: In an RMS-based DSR the SOAM is a guest on a TVOE host that has already been upgraded as part of the NOAM upgrade.							
3	Upgrade Active SO.	Upgrade Active SO server using Upgrade Single Server procedure :							
		Execute Appendix G Single Server Upgrade Procedure							
		After successfully completing the procedure in Appendix G, return to this point and continue with next procedure.							
		Note: In an RMS-based DSR the SOAM is a guest on a TVOE host that has already been upgraded as part of the NOAM upgrade.							
4	Install NetBackup on NO and SO (If required).	1. If NetBackup is to be installed on your DSR, execute the procedure found in Appendix I.							
		Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.							

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

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

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

S	This procedure upgrades the DA-MP(s).								
T E	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
P	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.								
#									
1	Verify and Record the status of the MP before upgrade	Verify and Record the status and hostname of the active DA-MP and of the standby DA-MP by going to Status & Manage -> HA.							
	upgrade	Note: Active DA-MP server can be identified by looking out for the VIP. The server with VIP in the row is the active DA-MP.							
2	Upgrade the standby DA-MP server (using Upgrade Single Server	Upgrade Standby MP server ⁷ using Upgrade Single Server procedure:							
	procedure)	Execute Appendix G – Single Server Upgrade for Standby DA-MP							
		After successfully completing the procedure in Appendix G, return to this point and continue with Step 3 below.							
3	Upgrade the Active DA-	Upgrade active MP server using the Upgrade Single Server procedure.							
	IVIF Server.	Execute Appendix G – Single Server Upgrade for Active DA-MP							
		After successfully completing the procedure in Appendix G, return to this point and continue with Step 4 below.							
		Note: The DA-MP server replication is enabled in Appendix G, executed above.							
4	Allow replication to SO	Allow database replication to SO servers:							
	servers.	1. Log into the active NO GUI using the VIP.							
		 Select Status & Manage > Database The Database Status screen is displayed 							
		4. Select the Active SO server.							
		5. Click Allow Replication button. After the Allow action, server HA requires time to recover							
		 Verify the Inhibited text is not displayed for the server. 							
		7. Repeat the Allow action link for Standby SO server.							
		Note: The SO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for SOs is necessary to prevent an unwanted HA switchover in between Allow steps.							

 $^{^{7}}$ The Status & Manage > HA screen will show the current HA status (active/standby) for all servers.

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

5	Enable global	Enable provisioning and configuration updates on the entire network:						
	configuration.	Provisioning and configuration updates may be enabled to the entire network. Note: Please note that by enabling global provisioning new data provisioned at NOAM will I replicated to only upgraded SO(s).						
		1. Log in to the active NOAM GUI using the VIP.						
		2. Select Status & Manage > Database						
		The Database Status screen isis displayed.						
		3. Click Enable Provisioning button.						
		4. Verify the text of the button changes to Disable Provisioning.						
		Note: Step 4 is NOT executed on the active DR NOAM, it is only executed on the "primary" active NOAM						
	Enable site provisioning.	Enable Site provisioning :						
	5							
		 Log into the SOAM VIP GUI of the site just upgraded above. 						
		2. Select Status & Manage > Database the Database Status screen is displayed						
		3. Click Enable Site Provisioning button.						
		Confirm the operation by clicking Ok in the popup dialog box.						
		5. Verify the button text changes to Disable Site Provisioning						
	Update Max Allowed HA							
	Role for NO and SO.	1. While logged in to the active NOAM GUI, go to Status & Manage-> HA screen.						
		2. Click 'Edit' button.						
		3. Check the 'Max Allowed HA Role' for all the NO(s) and SO(s). By Default, It should be						
		'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list.						
		4. Click 'Ok' button.						

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

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

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

5	This procedure verifi	nis procedure verifies Post Upgrade Status							
]	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
•	SHOULD THIS PROCEDURE	E FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR <u>UPGRADE ASSISTANCE</u>.							
	Verify Server Status is Normal	 Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select Status & Manage > Server; the Server Status screen isis displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 4. Execute following commands on the upgraded servers : Use your SSH client to connect to the upgraded MP(DA-MPs,IPFEs and cSBRs) servers (ex. ssh, putty): ssh <mp address="" imi="" ip="" server=""></mp> login as: root password: <enter password=""></enter> # verifyUpgrade Examine the output of the above command to determine if any errors were reported. Contact Tekelec in case of errors. 							

2	Log all current alarms	Log all current alarms in the system:					
		 Log in to the active NOAM GUI using VIP and select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed. Following Alarm ID will be observed on all the upgraded MP servers i.e IPFEs,DA-MPs and c-SBRs (whichever exists) : Alarm ID = 32532 (Server Lingrade Pending Accent/Poinct) 					
		Alam ID = 52552 (Server Opgrade Fending Accepticeject)					
		Note : If ALARM ID 32532 is not raised on any of the upgraded MP server, then execute following commands on that particular server to check the existence of alarm :					
		Use your SSH client to connect to the each upgraded MP server which did not raise the alarm Id 32532(ex. ssh, putty):					
		ssh <mp address="" ip="" server=""></mp>					
		login as: root					
		<pre>password: <enter password=""></enter></pre>					
		<pre># alarmMgralarmstatus</pre>					
		The following output should be raised :					
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33					
		Contact Tekelec in case above output is not raised.					
		2. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each MP server.					
		3. Click Report button to generate an Alarms report.					
		4. Save the report and print the report. Keep these copies for future reference.					
3	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade					
		End of second maintenance window.					

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

4.6 Policy DRA Upgrade for 3-tier Configuration

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

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

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

T-11.10	TT	E	^	f		(6.4.	1)
Table 16.	Upgrade	Execution	Overview	IOr	PDKA	(Site	I)

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

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

Table 17 Upgrade Execution Overview for PDRA (Site 2)

4.6.1 Perform Health Check (Pre-Upgrade of NOAM)

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

Procedure 51: Perform Health Check (Pre-Upgrade of NOAM)

S	This procedure performs a Health Check.								
Т	Check off (1) each stan as it is completed. Boyes have been provided for this purpose under each stan number								
Ε	Check on (w) each step as it is completed, boxes have been provided for this purpose under each step number.								
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.								
#									
1	Verify Server Status is	Verify Server Status is Normal:							
	Normal	1 Log into the NOAM CI II using the V/IP							
		 Log into the NOAM GOI using the VIP. Select Status & Manage > Server: the Server Status screen isis displayed 							
		 Verify all Server Status is Normal (Norm) for Alarm (Alm). Database (DB) High 							
		Availability (HA), and Processes (Proc).							
		4. Do not proceed to upgrade if any of the server statuses displayed is not Norm .							
		5. Do not proceed if there are any Major or Critical alarms.							
		. , ,							
		Note: It is not recommended to continue executing upgrade if any server status has							
		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.							
		Papezt the shove steps for SO VIP GUI							
2	Log all current alarms	Log all current alarms in the system:							
		1. Select Alarms & Events > View Active; the Alarms & Events > View Active view isis							
		Click Report button to generate an Alarms report							
		 Save the report and/or print the report. Keep these copies for future reference 							
		Repeat the steps for SO VIP GUI.							

4.6.2 Upgrade NOs

Procedure 52. TVOE Upgrade and NO Servers Upgrade

S	This procedure upgrades the TVOE of NOAM servers and upgrades NOAM servers of the setup.									
T	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.									
E										
Р #	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.									
π	Start of maintenance window 1									
1	Disable global	Disable global provisioning and configuration updates on the entire network:								
	provisioning and									
	configuration.	1 Log into the NOAM GUI using the VIP								
		 Select Status & Manage > Database: the Database Status screen is displayed 								
		3. Click Disable Provisioning button.								
		4. Confirm the operation by clicking Ok in the popup dialog box.								
		5. Verify the button text changes to Enable Provisioning; a yellow information box should								
		also be displayed at the top of the view screen which states:								
		[Warning Code 002] – Global Provisioning has been manually disabled.								
		6. Active NO server will have the following expected alarm:								
		 Alarm ID = 10008 (Provisioning Manually Disabled) 								
2	Inhibit replication to	Replication of C level MP servers will be inhibited during site upgrade.								
	PDRA and pSBR MP									
	servers.									
3	Inhibit replication to NO	Inhibit database replication to all the NO/SO servers in the following order:								
	and SO servers	All the Spare SO(s) (For each site)								
		All the Standby SO(s) (For each site)								
		All the Active SO(s) (For each site)								
		Standby DR NOAM(if applicable)								
		Standby NO								
		Active NO								
		a) Select Status & Manage > Database								
		The Database Status screen is displayed.								
		b) Select the appropriate server based on the list above.								
		c) Click Inhibit Replication button.								
		d) Verify the <i>Inhibited</i> text is displayed for server.								
		e) Repeat the Inhibit sub-step actions, steps a through e, for all remaining servers in								
		the order shown above.								
		Note: It is important to inhibit the replication of the standby server before the								
		active server to prevent unwanted HA switchovers								
4	Disable Site	Disable Site provisioning for all the sites present in the setup :								
	Provisioning									
		1. Log into the GUI of the SOAM for all the sites using the VIP.								
		 Select status & Manage > Database the Database Status screen is displayed Click Disable Site Provisioning button 								
		4. Confirm the operation by clicking Ok in the popula dialog box								
		5. Verify the button text changes to Enable Site Provisioning: a vellow information box								
		should also be displayed at the top of the view screen which states: [Warning Code 004]								
		- Site provisioning has been manually disabled.								
		6. Repeat substeps 2 through 5 for all the sites present in the setup.								

Procedure 52. TVOE Upgrade and NO Servers Upgrade

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

4.6.2.1 Maintenance Window 2 - Site 1

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

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

Procedure 53. TVOE Upgrade and SO Servers Upgrade

S	This procedure upgrade	e the TVOE of SOAM guests(if required) and upgrades SOAM servers of Site 1.				
T F	Check off $()$ each step as it	is completed. Boxes have been provided for this purpose under each step number.				
e P	Should this presedure foil contact the Teleles Outeman Core Contar and self for UDCDADE ASSISTANCE					
#	Should this procedure fail, contact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.					
	Start of maintenance window 2					
1	Verify site provisioning	Verify site provisioning is disabled. Else execute following steps :				
	is disabled	 Log into the GUI of the SOAM which needs to b upgraded using the VIP. Select Status & Manage > Database the Database Status screen isis displayed Click Disable Site Provisioning button. Confirm the operation by clicking Ok in the popup dialog box. Verify the button text changes to Enable Site Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 004] - Site provisioning has been manually disabled 				
2	Inhibit replication to	Record current release numberex: 4.0.2_40.27.3				
	servers.	 IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G Step 13). In this case, SKIP THIS STEP. [Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.] 				
		 IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands to inhibit replication A and B level replication on <u>all</u> <u>MP servers of this site</u>: 				
		Log into Active NO(if logged out, else ignore this step) :				
		<pre># ssh root@<active ip="" no="" xmi=""></active></pre>				
		login as: root				
		password: <enter password=""></enter>				
		Execute following command on active NO for each of the C level server groups present in this Site(which needs to be upgraded) :				
		# srvrGrps="				
		<pre>'<servergroup1>','<servergroup2>','<servergroup 3="">'</servergroup></servergroup2></servergroup1></pre>				
		B' NodeInfo where "nodeId like '\$i*'"; done				
		<u>NOTE</u> Server Group names of the site can be found out by logging into the Active NO GUI and going to Configuration->Server Groups screen. Filter out the server groups on the basis of Parent. Here parent is the site which				

Procedure 53. TVOE Upgrade and SO Servers Upgrade

- Tv A							ε.
0	(8
	set	AMSG Re	LABESOA			Parent	Display Filter:
HA NOR PTEL VI	eneerd						
STISHRE	NOTE LOODED OF	SULVEYSUE		_		_	20
HA Role Pref Vi	Server labEx1015ipteA1	NE Sojlaeesche	8	PFrontEnd	LABESCHILISG	C	LABERFESGI
HA Role Pref W	Server labEx2016iptex2	NE SO_LABESONE	ŧ.	PFrontEnd	LABESCHWSG	с	LABERFESS2
HA Role Pref VI	Server IsbEiertb3pdra1 IsbEiertb4pdra2 IsbEiertb5pdra3 IsbEiertb5pdra4	IE So_lagesone So_lagesone So_lagesone So_lagesone	0	DSR (mult- adive duster)	LABESCHINSG	c	LABEFORASS
HA Role Pref VII a 10.240.90.184 b 10.240.90.184 c SPARE 10.240.90.184	Server labEx101darson labEx102darsob labFx1102darsoc	NE Sojjagesone Sojjagesone Sojjagesone	1	DSR (activelstandb pair)	NCHIP_SC	B	LNGESCHWSG
HA Role Prof V IST1 IST1 IST1SPARE	Server labE+1011SpsbrSr labE+2b11SpsbrSr labF+1013SpsbrSr	NE Sojlagesone Sojlagesone Sojlagesone	2	Poliq SBR	LABESCHINSG	с	LABESPSBRSR1
HA Role Pref V SV2 SPHRE VSV2 SV2	Server labE=116BpstrSr2 labF=1110BpstrSr2 labF=216BpstrSr2	NE Sojlaeesone Sojlaefsone So laefsone	2	Palicy SBR	LABFSCAMSG	c	LABFBPSERSR2

	Main Menu: Configuration -> Server Groups (Filtered)								
	B	ter 🔹							
		Server Group Name Level Pa		el Parent	Function	Connection Count	Servers		
		LABEBPSERSR1	с	LABESCANISG	Palicy SBR	2	NE SO_LABESONE SO_LABESONE SO_LABESONE	Server labEx1b7BpsbrSr1 labEx2b7BpsbrSr1 labFx1b9BpsbrSr1	HA Role Pref Spare
		LABERFESG1	c	LABESCHINSG	IP Front End	0	NE SO_LABESONE	Server labEe1b15ipfeA1	HA Role Pref
		LABEPFESC2	c	LABESCHINSC	IP Front End	0	NE SO_LABESONE	Server labEx2016ipfeX2	HA Role Pref
		LAGEPORASG	с	LABESCHWSG	DSR (multi- active duster)	0	NE SO_LABESONE SO_LABESONE SO_LABESONE SO_LABESONE	Server labEe1b3pdta1 labEe1b4pdta2 labEe1b6pdta3 labEe1b6pdta4	HA Role Pref
		\bigcirc		LARFSOLUSC	Paler SRR	,	NE SO_LABESONE	Server labEe1b11SpsbrSr	HA Role Pre
	Exe	Cute the ab	ove	mention	ed comr	nand fo	SO_LABESONE SO_LABESONE	latEs2b113pstrSr latFs1b133pstrSr	1 ISPARE ed out
	Exe Ser #s SP in wh is "n	ecute the ab vergroups. <u>e.g:</u> rvrGrps= SBRSR1', \$(iqt - ere "Sen et -finh odeId li	ove ,'I -p rve hik	E mention LABEIPI -z -h erGroup DitRepl e '\$i*	ed comr DRASG FESG1 -fclu DName Plans= '"; dd	nand fo ','LA ','LA uster in (='A E one	SO JAESONE SO JAESONE OF each of BEBPSI BEIPFI SId Set (\$srvr(3' Noc	affedontisesson affettolidesson f the filtered BRSR1 ' , ESG2 ' " ; rverGrc Grps) ") deInfo	'LAB for jup ;do wher
Upgrade standby SO and spare SO in parallel	Exe Ser An #s SP in wh is "n Note: - Execute Append Spare DSR SO are host 1. Upgrade Standby procedure : Execute Appendix G	ecute the ab vergroups. <u>e.q:</u> rvrGrps= SBRSR1', \$(iqt - ere "Sea et -finh odeId li lix J for Stand ted on TVOE DSR SO ser	eove	E mention LABEPI -z -h erGroup bitRepi e '\$i* DSR SO a ide before and spare	ed comr DRASG FESG1 -fclu pName Plans= '''; do and Spai proceed s SO in p	mand fo	SO JAESONE SO JAESONE SO JAESONE OF each of BEBPSI SEIPFI CID Sea (\$STVTO SO if State below m using Upg	affet 13 and 14	d out LAB: for ; do where SO and teps.

Procedure :	53.	TVOE	Upgrade	and SO	Servers	Upgrade
			- F 8			- F 8

Procedure 53. TVOE Upgrade and SO Servers Upgrade

4	Upgrade active DSR SO.	 Note: - Execute Appendix J for Active DSR SO if Active DSR SO is hosted on TVOE blade before proceeding with below mentioned steps. 1. Upgrade active DSR SO server using Upgrade Single Server procedure : Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with next step.
5	Allow replication to SO servers of the upgraded site ONLY (upgraded site only).	 Allow database replication to SO servers of the currently upgraded site only: Log into the NOAM GUI using the VIP. Select Status & Manage > Database The Database Status screen is displayed. Select the Active SO server recently upgraded. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for the server.After the Allow action, server HA requires time to recover(up to 3 minutes) before 'Allowed' text is displayed. Repeat the Allow action for Standby SO server recently upgraded. Repeat the Allow action for Spare SO server recently upgraded. 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. While server HA is recovering, monitor Server Status for recovery. Select Status & Manage > HA The HA Status screen isis displayed. Wait for "OAM Max HA Role" field to display "Active", "Standby" or "Spare". It may take up to 3 minutes of "server "Active", "Standby" or "Spare". It may take up to 3 minutes of server and for Server Status HA field to display the current operational status of "Active", "Standby" or "Spare". Note: SOAM server replication shall be allowed only for the currently upgraded site. For the leftover sites which are not yet upgraded, replication for each SOAMs of that sites shall remain inhibited else DB corruption can occur.

4.6.3 Policy SBR MP Server Upgrade

Procedure 54. Policy SBR Upgrade – Site 1

Policy SBR upgrade pr	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.					
Identify the pSBR	From the data capture	d from Table 3,			
Upgrade	1. Pick the " Policy server groups). C be executed similar	SBR " Server Group)ne server group can ultaneously.	o(s) (e.g. Binding pS to be executed at a t	SBR Server Group, or multiple time or multiple server groups can	
	2. Identify all the se	rvers in server group	o(s) selected for up	grade in sub-step 1.	
	3. Log into the NOA	MP GUI using the V	IP		
	4. Select the "Main server group cho Resource HA Ro provides an exan labCe2b2Bps labCe1b2Bps labDe1b2Bps	Menu: Policy DRA sen in sub-step 1, No le) for each server gr nple: brSr1 - Active brSr1 – Standby brSr1 - Spare	Maintenance->Pol ote which server is roup chosen for up	licy SBR Status", and open each active, standby and spare(the grade. The following figure	
	Main Menu: Dolicy DBA - N	Maintenance -> Dolicy (CRD Status		
				Tue Oct 02 18:09:58 2012 A	
	Filter -				
	rtpLabBindingNetwork rtpLabC	DMatedPair			
	Server Group	Resource Dom	ain Name	Resource Domain Profile	
	LabCBindingSR1SG	BindingRD		Policy Binding	
	Server Name	Resource HA Role	Congestion Level	Sub Resources Hosted	
	labCe1b2BpsbrSr1	Standby	Normal	0,1,2,3,4,5,6,7	
	labCe2b2BpsbrSr1	Active	Normal	0,1,2,3,4,5,6,7	
	labDe1b2BpsbrSr1	Spare	Normal	0,1,2,3,4,5,6,7	
Upgrade standby and spare Policy SBR Servers as identified in Step 1 in this procedure.	Note: Spare P-SBF 1. Upgrade Standby Server procedure Execute Appendix G After successfully corr with next step.	₹ of this triplet wi / Policy SBR server ∋ : Single Server Upç npleting the procedur	II be present in and spare Policy S grade Procedure re in Appendix G, re	the different site. BR server using Upgrade Single	

Procedure 54. Policy SBR Upgrade – Site 1

3	Upgrade Active Policy SBR Server as identified	1. Upgrade Active Policy SBR server using Upgrade Single Server procedure :
	in Step 1 in this	Execute Appendix G Single Server Upgrade Procedure
	procedure	After successfully completing the procedure in Appendix G, return to this point and continue with next step.
4	Reneat steps 1 through	Repeat the steps 1-4 for all remaining hinding and session server groups that need to be
	4 for all the Binding and	upgraded.
	with Active, Standby in	
	Site 1 and Spare in Site 2	

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

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

S	Policy DRA server (DA	A-MP Server) upgrade procedure for Site 1			
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
P #	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
1	Identify the "DSR	From the data captured from Table 3,			
	(multi-active cluster)" to Upgrade in	1. Pick the "DSR (multi-active cluster)" Server Group in Site 1			
	Sile	2. Identify the servers in Server Group identified in sub-step1 .			
2	Upgrade Policy DRA Server as identified in Step 1	 Upgrade half of the Policy DRA (DA-MP) servers in parallel I using Upgrade Single Server procedure : 			
		Execute Appendix G Single Server Upgrade Procedure			
		After successfully completing the procedure in Appendix G, return to this point and continue with next step.			
3	Repeat steps 2 for all the server identified in Step 1 in this procedure.	Repeat the steps in step 2 in this procedure for rest of the Policy DRA (DA-MP) servers.			

4.6.5 Upgrade IPFE

Procedure 56. IPFE Server Upgrade – Site 1

S	IPFE server upgrade procedure for Site 1				
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
Р #	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	1. Pick one " IP Front End " Server Group in Site 1.			
		2. Identify the servers in Server Group identified in sub-step 1 above			
2	Upgrade IPFE Server as identified in Step 1 in this procedure	Step 1: Upgrade IP Front End server using Upgrade Single Server procedure :			
		Execute Appendix G Single Server Upgrade Procedure			
		After successfully completing the procedure in Appendix G, return to this point and continue with next step.			
3	Execute the following	Execute following steps on each IPFE server just upgraded :			
	steps on the IPFE.	1. Use ssh client to connect to the IPFE server :			
		<pre>ssh <ipfe address="" ip="" xmi=""> login as: root password: <enter password=""> 2. Execute following command on the IPFE server :</enter></ipfe></pre>			
		<pre># grep "IPV6_AUTOCONF=no" /etc/sysconfig/network # grep "IPV6FORWARDING=yes" /etc/sysconfig/network</pre>			
		If the outcome of any of the above command is blank then execute the steps below else skip the steps below			
		<pre># /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # init 6</pre>			
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.			
5	Repeat steps 1 through 4 for all the " IP Front End "	Repeat the steps in step 1-4 in this procedure.			

4.6.6 Post Upgrade Execution – Site 1

Execute this procedure after the site has been upgraded.

Procedure 57. Site 1: Post Upgrade Steps

S T	Post Upgrade steps after Si under each step number.	te 1 is upgraded. Check off ($$) each step as it is completed. Boxes have been provided for this purpose
E P	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.
#		
1	Enable 'A B' level	Note: The following steps will uninhibit replication to C level servers
	replication inhibited for	
	MP(s)(only if source upgrade release was	Enable replication disabled previously only if source upgrade release was less than
	less than 4.1.0_41.16.0)	4.1.0_41.16.0 :
	NOTE: Do not use	1. Log into Standby SO command prompt upgraded in Site 1 :
	VIP address when doing ssh to the servers for this step	Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <so address="" ip="" xmi=""></so>
		login as: root
		password: <enter password=""></enter>
		2. Execute the following command to enable replication :
		# iload
		/var/TKLC/db/filemgmt/\$(hostname).TableDef_backup.xml
		<pre># pm.set off inetrep</pre>
		# pm.set on inetrep
		Execute above Steps 1 and 2 for upgraded Active SO of Site 1 as well.
2	Enable global	Enable global provisioning and configuration updates on the entire network:
	configuration.	1. Select Status & Manage > Database
	-	The Database Status screen isis displayed.
		2. Click Enable Provisioning button.
		3. Verify the button text changes to Disable Provisioning.
}	Enable global	Enable Site provisioning after upgrade is completed:
1	provisioning and	1 Log into the SOAM VIP CI II for the ungraded site
Ĵ	configuration.	Log into the SOAWI VIF GOLIOI the upgraded site. Select Status & Manage > Database: The Database Status screen isis displayed
		2. Click Enable Site Provisioning button
		5. Click Eliable Site Flovisioning button.
		Verify the button text changes to Disable Site Provisioning
	Execute FQDN – NE ID	NOTE: Execute this step if upgrading from a release < 4.0.5_41.6.0 to a later release.
	Mapping script	1. Ssh into Active NOAMP using the XMI VIP IP Address:
		2. Execute this step
		#/var/TKLC/appworks/library/Pdra/scripts/syncFqdnReferen
		ces.sh

Procedure 57. Site 1: Post Upgrade Steps

5	Truncate PDRA local table –	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.
	(Only if source upgrade release was less than	1. Download the script <u>truncateLocalTable.sh</u> .
	4.1.0-41.24.0)	2. Transfer the truncateLocalTable.sh file to /root of the Active SOAM Server.
		3. Log into Active SO command prompt upgraded in Site 1 :
		ssh <server address=""></server>
		login as: root
		password: <enter password=""></enter>
		4. Change directory to /root
		# cd /root
		5. Convert the script to unix format:
		<pre># dos2unix truncateLocalTable.sh</pre>
		Execute the following command to ensure that the script has the required permissions:
		<pre># chmod +x truncateLocalTable.sh</pre>
		7. Execute the script:
		<pre># ./truncateLocalTable.sh</pre>

4.6.7 Site 1 – Verify Post Upgrade Status

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

Procedure 58: Verify Post Upgrade Status

S	This procedure performs a Health Check.				
Т	Check off (\checkmark) each step as it is completed. Boxes have been provided for this purpose under each step number.				
E D					
Р #	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR <u>UPGRADE ASSISTANCE</u> .				
π	Verify all servers status 1 Log in to GUL using NOAMP VIP				
	are normal	1.			
		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.	unexpected Major or Critical alarms.		
		Note	b. It is not recommended to continue executing ungrade if any server status has		
		une	spected values. An upgrade should only be executed on a server with unexpected alarms		
		if the	e upgrade is specifically intended to clear those alarm(s). This would mean that the target		
		relea	ase software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method ear the alarm(s). Do not continue otherwise		
		10 01			
2	Log all current alarms	1.	Select the Alarms & Events -> View Active menu item.		
	Active NOAMP VIP and	2.	Click the Export button to generate an Alarms Export file.		
	site 1.	3.	Record the filename of Alarms CSV file generated and all the current alarms in the		
		4	System. Keep this information for future reference on client machine		
		4.			
3	Capture the Diameter	1.	Select Main Menu-> Diameter-> Maintenance		
	Maintenance Status On Active SOAM VIP for site 1.	2.	Select Maintenance->Route Lists screen.		
		3.	Filter out all the Route Lists with Route List Status as "Is Not Available" and "Is		
		4. 5	Record the number of "Not Available" and "Available" Route Lists.		
		э. 6	Select maintenance->Route Groups Screen. Filter out all the Route Groups with "PeerNode/Connection Status as "Is Not		
		0.	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		
		40	Available".		
		13.	Select Maintenance->Annlications screen		
		15.	Filter out all the Applications with "Operational State" as "Is Not Available" and "Is		
			Available".		
		16.	Record the number of "Not Available" and "Available" applications.		
		17.	Save this off to a client machine		
		18.			
4	Capture the Policy SBR	1.	Select Main Menu-> Policy DRA->Maintenance-> Policy SBR Status		
	Status	2.	Capture and archive the maintenance status of the following tabs on the client machine		

Procedure 58:	Verify P	ost Upgrade	Status
----------------------	----------	-------------	--------

	On Asthe NOAMD OLU	have a fillen and a fillen and a second state and a second state of the second state of the second state of the				
	On Active NOAMP GUI	by either taking screen captures or documenting it in some editor.				
		a. Binding Region				
		b. PDRAMatedSites				
		Save this off to a client machine.				
5	Capture the IPFE	1. Select Main Menu: IPFE->Configuration->Options				
	Configuration Options	2. Capture and archive the screen capture of the complete screen.				
	Screens.	3. Save this off to a client machine				
	On Active SOAM GUI on Site 1					
6	Capture the IPFE	 Select Main Menu: IPFE->Configuration->Target Sets 				
	Configuration Target Set	2. Capture and archive the screen capture of the complete screens.				
	screens	3. Save this off to a client machine.				
	On Active SOAM GUI on	4				
	Site 1					
7	Export and archive the	1. Select Main Menu-> Diameter Configuration->Export				
	Diameter and P-DRA	2. Capture and archive the Diameter and P-DRA data by choosing the drop down entry				
	configuration data. On Active SOAM GUI on	named "ALL"				
		Verify the requested data is exported using the APDE status button at the top of the				
	Site 1	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				
		making				
		machine.				
0	Compare this date to the	Disease worth if the health sheely statue of the upgraded site 1 is some as the upgrade health				
δ	Compare this data to the	Please verify if the health check status of the upgraded site 1 is same as pre-upgrade health				
	eheelt to verify if the	check taken in Procedure 5. If it is any worse, report it to Tekelec Customer service.				
	system has degraded					
	alter the second					
	maintenance window.					
	End of maintenance window 2					

4.6.8 SOAM Upgrade – Site 2

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

S	This procedure verifies that the SOAM server with TVOE platform upgrade steps have been completed and			
Т	upgrade the SOAMs.			
Ε				
Р	Check off (\mathbf{v}) each step as it	is completed. Boxes have been provided for this purpose under each step number.		
#	Should this procedure fail, co	ntact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.		
		Start of maintenance window 3		
1	Verify site provisioning is disabled	 Verify site provisioning is disabled. Else execute following steps: Log into the SOAM VIP GUI which needs to be upgraded. 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.		
		 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 numberex: 4.0.2_40.27.3		

 IF this release is less than DSR 4.1.0_41.16.0, then replication for MP(s) (all C level servers) will be inhibited when you run the single server upgrade (Appendix G Step 13). In this case, SKIP THIS STEP. [Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so this step would be skipped in this example.] IF this release is greater than or equal to DSR 4.1.0_41.16.0, execute the following commands to inhibit replication A and B level replication on <u>all MP servers of this site</u>:
Log into Active NO(if logged out, else ignore this step) :
<pre># ssh root@<active ip="" no="" xmi=""></active></pre>
login as: root
<pre>password: <enter password=""></enter></pre>
Execute following command on $\$ active NO for each of the C level server groups present in this Site(which needs to be upgraded) :
<pre># srvrGrps="</pre>
<pre>'<servergroup1>','<servergroup2>','<servergroup 3="">'</servergroup></servergroup2></servergroup1></pre>
<u>NOTE</u> 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)

Filter	_						0	
Display Filter: Pr	aert		•	LABESOAMS	SG F	leset	HE Role Drof	VE
and a	_						- Ne Ave Fres	
Gà							-	
					on the one	c while machania	IONNE	
L48EPFESG1	C	LABESCHUSG	PFrontEnd	0	NE SO_LABESON	Server E kabEe1015ipleA1	HA Role Pref	VP
LABERFESG2	с	LABESCHARSC	IP Front End	1	NE SO_LABESONA	Server E labEx2015iptex2	HA Role Pref	VP
1					IE	Sener	HA Role Pref	WP
			DSR Imilia		SO_LABESON	E labEe1b3pdra1		
LABEPORASC	C	LABESCHINSG	adive cluster)	\$.	SO_LABESON	E labEe104pdra2		
					SO_LABESON	E labEe105pdta3		
2					SULABESUN	e 18069100p0/34		
			DSR		Æ	Server	HA Role Pref	VP
LABESCHMISG	B	NOHIP_SG	(adveistand)	E.	SO_LHEESON	E labErioldersoa		10,240,90,184
			par)		SO_LARESONE	E latEntization	SPURE	10/240/30 104
					A generation	a law a requiring	WID CLOSED	a a mare ref
					R LICCOM	Server	HA Role Pre	W VS
LABESPSBRSR1	C	LABESCHINSG	Paliq SBR	2	SO LARESON	E 100E0101100500	an Sel	-
					SO_LAEFSONE	E labFe1b13Spsbr3	IT SPARE	
					IF.	Samar	HE Role Draf	
					SO LARESON	E labEe1b8BosbrSr	2 SPARE	
LABHOMSBASH2	ç	LARPSONING	HIND SER	2	SO_LAEFSONE	E labFe1b108psbr5	12	
					SO_LASFSONS	E latFe2ti8bestrSr	2	

	Main Menu: Configuration -> Server Groups (Filtered)				
	Fiter •				
	Server Group Name Level Parent Function Connection Servers				
	LABEBYSBRISR1 C LABESCHAILSG Parky SBR 2 Server SO_LABESCHAILSG Parky SBR 2 SO_LABESCHAE labE+1078p SO_LABESCHAE labE+2078p SO_LABESCHAE labE+2058p	HA Role Pref DISIT DISIT DISIT SPARE			
	LABEPFESST C LABESCHASS IP Front End 0 NE Server SO_LABESCHASS	HA Role Pref			
	LABEIPFESG2 C LABESCHAISG IP Front End 0 NE Service SO_LABESCHIE labEk201500	HA Role Pref			
	LABEPDRASG C LABESCHARSG DSR (multi- active duster) 0 SO_LABESCHE labE+113pd SO_LABESCHE labE+114pd SO_LABESCHE labE+115pd SO_LABESCHE labE+115pd	HA Role Pref			
	LABESPERSR1 C LABESCHARSG Policy SER 2 NE Serve SO_LABESCHE labE+10115g SO_LABESCHE labE+20115g SO_LABESCHE labE+20115g	HA Role Pref arSr1 arSr1 arSr1SPARE			
Upgrade TVOE platform	Execute the above mentioned command for each of the fill Servergroups. <u>An e.g:</u> #srvrGrps="'LABEPDRASG', 'LABEBPSBRSR1 SPSBRSR1', 'LABEIPFESG1', 'LABEIPFESG2' in \$(iqt -p -z -h -fclusterId ServerG where "ServerGroupName in (\$srvrGrps) iset -finhibitRepPlans='A B' NodeInf "nodeId like '\$i*'"; done	<pre>','LABE ';for i roup ');do o where D) If</pre>			
on SOAM blades	upgrade is required, follow Appendix J Upgrade TVOE platform. is displayed	B SO and			
and spare SO in parallel.	Spare DSR SO are hosted on TVOE blade before proceeding with below mentioned steps.				
		31003.			
	I. Upgrade standby SO and spare SO server using Upgrade Single Server proce	dure :			
	 Upgrade standby SO and spare SO server using Upgrade Single Server proce Execute Appendix G Single Server Upgrade Procedure 	dure :			

 Note: - Execute Appendix J for Active DSR SO if Active DSR SO is hosted on TVOE blade before proceeding with below mentioned steps. 1. Upgrade active DSR SO server using Upgrade Single Server procedure : Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue
 Upgrade active DSR SO server using Upgrade Single Server procedure : Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue.
Execute Appendix G Single Server Upgrade Procedure
After successfully completing the procedure in Appendix G, return to this point and continue
with next step.
Allow database replication to SO servers of the currently upgraded site only:
 Log into the NOAM GUI using the VIP. Select Status & Manage > Database The Database Status screen gets displayed. Select the Active SO server recently upgraded. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for the server. Repeat the Allow action for Standby SO server recently upgraded. 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). While server HA is recovering, monitor Server Status for recovery. Select Status & Manage > HA The HA Status screen gets displayed. Wait for "OAM Max HA Role" field to display "Active", "Standby" or "Spare". It may take up to 3 minutes for server HA to recover and for Server Status HA field to display the current operational status of "Active", "Standby" or "Spare". Note: SOAM server replication shall be allowed only for the currently upgraded site. For the leftover sites which are not yet upgraded, replication for each SOAMs of that sites shall remain inhibited else DB corruption can occur.

4.6.9 Policy SBR MP Server Upgrade

Procedure 60. Policy SBR Upgrade – Site 2

S T	Policy SBR upgrade procedure for Site 2					
E	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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.					
# 1	Identify the pSBR Server Group to	From the data captured in Table 3.				
	 Upgrade 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. Identify the servers in Server Group in site 2 or multiple server groups in site 2. Login into NOAMP VIP Go to "Main Menu: Policy DRA->Maintenance->Policy SBR Status", NOTE down the Resource HA Role 					
		•				
		LabDBindingSR2SG		BindingRD		
		Server Name	Resource HA	Role		
		abCe1b7BpsbrSr2	Spare			
		labDe1b7BpsbrSr2	Active			
		labDe2b2BpsbrSr2				
2	Upgrade standby and spare Policy SBR	Note: Spare P-SBR of this triplet will be pro	esent in the d	ifferent site.		
	Servers as identified in Step 1 in this procedure.	Step 1: Upgrade standby Policy SBR server and sp Single Server procedure :	pare Policy SBR	server using Upgrade		
		Execute Appendix G Single Server Upgrade Pro	ocedure			
		After successfully completing the procedure in Apper with next step.	endix G, return to	o this point and continue		
3	Upgrade active Policy	Step 1: Upgrade active Policy SBR server using Up	grade Single Se	rver procedure :		
	in Step 1 in this	Execute Appendix G Single Server Upgrade Procedure				
	procedure	After successfully completing the procedure in Appr with next step.	endix G, return to	o this point and continue		
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 s upgraded.	session server g	roups that need to be		

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

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

S	Policy DRA server (DA-MP Server) upgrade procedure for Site 2				
T E	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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.				
1	Identify the " DSR (multi-active	From the data captured in Table 3,			
	cluster)" to Upgrade in Site 2	 Pick the "DSR (multi-active cluster)" Server Group in Site 2. Identify the servers in Server Group identified in sub-step1. 			
2	Upgrade Policy DRA Server as identified in Step 1	1. Upgrade Policy DRA (DA-MP) server using Upgrade Single Server procedure :			
		Execute Appendix G Single Server Upgrade Procedure			
		After successfully completing the procedure in Appendix G, return to this point and continue with next step.			
3	Repeat steps 2 for all the servers identified in Step 1 in this procedure.	Repeat the steps in step 2 in this procedure for rest of the Policy DRA (DA-MP) servers.			

4.6.11 IPFE Server Upgrade

Procedure 62. IPFE Server Upgrade – Site 2

S	IPFE server upgrade procedure for Site 2			
I E	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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
1	Identify the IP Front End Server Group to	From the data captured in Table 3,		
	Upgrade in Site 1(LabC)	1. Pick one " IP Front End " Server Group in Site 2.		
		2. Identify the servers in Server Group identified in sub-step 1 above		
2	Upgrade IPFE Server as identified in Step 1 in this strep 2 in Step 1: Upgrade IP Front End server using Upgrade Single Server procedure :			
		Execute Appendix G Single Server Upgrade Procedure		
		After successfully completing the procedure in Appendix G, return to this point and continue with next step.		
3	Execute the following	Execute following steps on each IPFE server just upgraded :		
	steps on the IPFE.	1. Use ssh client to connect to the IPFE server :		
		ssh <ipfe address="" ip="" xmi=""></ipfe>		
		login as: root		
		password: <enter password=""></enter>		
		2. Execute following command on the IPFE server :		
		<pre># grep "IPV6_AUTOCONF=no" /etc/sysconfig/network # grep "IPV6FORWARDING=yes" /etc/sysconfig/network</pre>		
		If the outcome of any of the above command is blank then execute the steps below else skip the steps below		
		<pre># /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # init 6</pre>		
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.		
5	Repeat steps 1 through 4 for all the " IP Front End "	Repeat the steps in step 1-4 in this procedure.		

4.6.12 Post Upgrade Execution – Site 2

Procedure 63. Site 2: Post Upgrade Steps

S	NOTE: Execute this step after site has been upgraded.					
Ť						
Ē	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
P	Should this presedure fail, contract the Takalas Customer Care Conter and ask for LIDCD ADE ASSISTANCE					
#	Should this procedure ran, contact the Tekelec Customer Care Center and ask for <u>OFGRADE ASSISTANCE</u> .					
1	Enable 'A B' level Note: The following steps will uninhibit replication to C level servers					
	replication inhibited for					
	MP(s)(only if source ungrade release was Enable replication disabled previously only if source upgrade release was less					
	less than	4.1.0_41.16.0 :				
	4.1.0_41.16.0)					
		1. Log into Standby SO command prompt upgraded in Site 2:				
	NUTE: DO NOT USE					
	doing ssh to the	Use your SSH client to connect to the upgraded server (ex. ssh, putty):				
	servers for this step	SSI (50 AMI IF address/				
		login as: root				
		password: <enter password=""></enter>				
		2. Execute the following command to enable replication :				
		# iload				
		/var/TKLC/db/filemgmt/\$(hostname).TableDef_backup.xml				
		<pre># pm.set off inetrep</pre>				
		# pm.set on inetrep				
		Execute above Steps 1 and 2 for upgraded Active SO of Site 2 as well.				
2	Enable global	Enable global provisioning and configuration updates on the entire network:				
	provisioning and	1 Select Status & Manage > Database				
	configuration.	The Database Status screen isis displayed.				
		2. Click Enable Provisioning button.				
		3. Verify the button text changes to Disable Provisioning.				
		Enable Site provisioning after upgrade is completed:				
		4 Log into the SOAM VIP GUI for the site upgrade above				
		5. Select Status & Manage > Database the Database Status screen isis displayed				
		6. Click Enable Site Provisioning button.				
		7. Confirm the operation by clicking Ok in the popup dialog box.				
		Verify the button text changes to Disable Site Provisioning				

Procedure 63. Site 2: Post Upgrade Steps

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		
	<pre>#dos2unix install_backward_compat_patch.sh</pre>		
	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		
Truncate PDRA local	NOTE: Execute this step if upgrading from a release < 4.1.0-41.24.0, to a later release.		
table – TopoHidingListLocal	This procedure needs to be executed after each site has been upgraded.		
(Only if source upgrade release was less than	1. Download the script <u>truncateLocalTable.sh</u> .		
4.1.0-41.24.0)	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=""></server>		
	login as: root		
	password: <enter password=""></enter>		
	 4. Change directory to /root # cd /root 		
	5. Convert the script to unix format: # dos2unix truncateLocalTable.sh		
	C Even to the following command to answe that the parint has the required		
	 Execute the following command to ensure that the script has the required permissions: 		
	<pre># chmod +x truncateLocalTable.sh</pre>		
	7. Execute the script:		
	# ./truncateLocalTable.sh		

4.6.13 Site 2– Verify Post Upgrade Status

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

Procedure 64:	Verify Post	Upgrade Status
---------------	-------------	-----------------------

S	This procedure verifies Post Upgrade Status				
Т					
Ε	Check off (v) each step as it is completed. Boxes have been provided for this purpose under each step number.				
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.				
#					
1	Verify all servers status	1. Log in to GUI using NOAMP VIP			
	are normal	2. Select the Status & Manage -> Server menu item.			
		3. Verify all server status are Normal (Norm).			
		4. Do not proceed without consent from Engineering/Customer Service (refer Appendix K) to			
		upgrade if any of the server's status displayed is not Norm .			
		5. Do not proceed without consent from Engineering/Customer Service (refer Appendix K) if			
		there are any unexpected Major or Critical alarms.			
		Note: It is not recommended to continue executing ungrade 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 me				
		to clear the alarm(s). Do not continue otherwise.			
2	Log all current alarms	1. Select the Alarms & Events -> View Active menu item.			
	Active NOAMP VIP and	2. Click the Export button to generate an Alarms Export file.			
	Active SOAM VIP on	3. Record the filename of Alarms CSV file generated and all the current alarms in the			
	Site 2.	system.			
		4. Keep this information for future reference on client machine.			
3	Capture the Diameter	1. Select Main Menu-> Diameter-> Maintenance			
	On Active SOAM VIP	 Select Maintenance->Route Lists screen. Eiker out all the Doute Lists with Doute List Statue on #a Net Available? and #a 			
	of site 2).	3. Filler out all the Route Lists with Route List Status as "Is not Available" and "Is Available"			
	-	A 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 scient. 15. Filter out all the Applications with "Operational State" as "Is Not Available" and "Is			
		16. Record the number of "Not Available" and "Available" applications			
		17. Save this off to a client machine.			
4	Capture the Policy SBR	1. Select Main Menu-> Policy DRA->Maintenance-> Policy SBR Status			
	Status	2. Capture and archive the maintenance status of the following tabs on the client machine			

Procedure 64: Verify Post Upgrade Status

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

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

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

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

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

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

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

Procedure 65: Perform Health Check

S	This procedure performs a Health Check.			
T E	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:		
		 Log Into the NOAM GUI using the VIP. Select Status & Manage > Server; the Server Status screen is displayed. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). Do not proceed to upgrade if any of the server statuses displayed is not Norm. 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: Select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed. Click Report button to generate an Alarms report. Save the report and/or print the report. Keep these copies for future reference. 		
4.7.2 Upgrade 2-Tier NOAM(s)

Detailed steps are shown in the procedure below.

S	This procedure verifies	that the NOAM upgrade steps have been completed. This procedure is specific to 2-
ь Е	uer DSK OAW deploy	
P	Check off (\mathbf{N}) each step as it	is completed. Boxes have been provided for this purpose under each step number.
#	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for <u>UPGRADE ASSISTANCE</u> .
1	Disable global	Start of maintenance window
	provisioning and configuration.	 Log into the NOAM VIP GUI. Select Status & Manage > Database; The Database Status screen is displayed. Click Disable Provisioning button.
		 Confirm the operation by clicking Ok in the popul dialog box. 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. Active NO server will have the following expected alarm: Alarm ID = 10008 (Provisioning Manually Disabled)
2	Inhibit SOAP replication	Record current DSR release numberex: 4.0.2_40.27.3
	(This step will NOT be required for most upgrades)	SKIP THIS STEP if current release is 4.0.0_40.19.0 or greater
		1. Log into the Active NO command prompt :
		Use your SSH client to connect to the Active NO server (ex. ssh, putty): ssh <server address=""></server>
		login as: root password: <enter password=""></enter>
		2. Execute the following command to disable SOAP replication :
		<pre># iset -fexcludeTables=' HaNodeLocPref HaVipDef ' NodeInfo where "1=1"</pre>
		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 Nodeld present on the setup :
		e,g,
		nodeId=A2823.152 nodeName=NO2 hostName=NO2 nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03
		CNOTAGETADIES- MANAGEDOLIEI MAVIPPEL
		SOAP replication for HaNodeLocPref and HaVipDef needs to be disabled so that new data from upgraded NO doesn't flow down to second NO or MP servers.

3	Inhibit replication to all servers.	Inhibit database replication to all servers in the following order: Standby DA-MP
		Active DA-MP Standby NO
		Active NO
		1. Select Status & Manage > Database
		2. Select the appropriate server based on the list above.
		3. Click Inhibit Replication button.
		4. Verify the <i>Inhibited</i> text is displayed for server.
		order shown above.
		Note: It is important to inhibit the replication of the standby server before the
		active server, to prevent unwanted HA switchovers.
4	Upgrade TVOE Host (if needed)	If TVOE Host for the Standby NO needs to be upgraded.
	,	Execute Appendix J for the standby NO TVOE Host
4	Liparada Standby NO	
4	server (using Upgrade	Execute Appendix G –Single Server Upgrade for standby NO
	procedure).	After successfully completing the procedure in Appendix G, return to this point and continue with step 5 below.
5	Upgrade TVOE Host (if needed)	If TVOE Host for the Active NO needs to be upgraded.
	•	Execute Appendix J for the active NO TVOE Host
6	Verify cmha process is running on upgraded	Log into the just-upgraded standby NO, execute the following command to make the NO Active again.
		# ssh root@ <no ip="" xmi=""></no>
		login as: root
		<pre>password: <enter password=""></enter></pre>
		Execute following command on NO:
		[root@NO1 ~]# pl grep "cmha"
		The following output should be generated:
		A 10128 cmha Up 11/20 00:15:58 1
		cmha
		If no output is generated then execute following command:
		<pre>service start_cmha start</pre>

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

4.7.3 Perform Health Check

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

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

S T	This procedure perfo	rms a Health Check.
I E	Check off (\checkmark) each step as it is	s 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.
#	Verify Server Status	Execute the following commands on both the active and standby NOAM servers:
		A Heaview COLL alignet to approach to the unstanded entries (are only not in the vertex).
		ssh < NO XMI IP address >
		login as: root
		password: <enter password=""></enter>
		Note: XMI IP address for the NO server should be available in Table 3.
		# verifyUpgrade
		Examine the output of the above command to determine if any errors were reported.
		Note: It is safe to ignore this error if it appears after upgrade from DSR 4.x to 5.x:
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log)
		reports errors! ERROR: 1347523804::ERROR-{HA::Mgr}: No Clusternode
		found for resource entry, (tklc-ha-active)!
		1347523805::ERROR-{HA::Mgr}: Failed to initialize
		 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)
		Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
		Note : If ALARM ID 32532 is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :
		# alarmMgralarmstatus
		The following output will be raised :
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33
		3. Alarm ID 32532 will be cleared once Procedure 78 is executed to accept the upgrade on each server

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

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

4.7.4 2-Tier Upgrade DA-MP(s)

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

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

S	This procedure upgrad	es the DA-MP(s).
T E	Check off (1) each step as it	is completed. Boxes have been provided for this purpose under each step number.
P #	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.
1	Verify and Record the status of the MP before upgrade	Verify and record the status of each DA-MP Server by going to Status & Manage -> HA and record the hostname of active DA-MP server and standby DA-MP server. Note: Active DA-MP server can be identified by looking out for the VIP. The server with VIP in the row is the active DA-MP.
2	Upgrade the standby DA-MP server (using Upgrade Single Server procedure)	Upgrade the standby DA-MP server using Upgrade Single Server procedure: Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with Step 3 below.
3	Upgrade the active DA- MP server.	Upgrade the active DA-MP server using the Upgrade Single Server procedure. Execute Appendix G Single Server Upgrade Procedure After successfully completing the procedure in Appendix G, return to this point and continue with Step 4 below.
4	Enable global provisioning and configuration.	 Enable provisioning and configuration updates on the entire network: Provisioning and configuration updates may be enabled to the entire network. 1. Log into the Active NOAM GUI using the VIP 2. Select Status & Manage > Database The Database Status screen is displayed.
		 Click Enable Provisioning button. Verify the text of the button changes to Disable Provisioning.
5	Update Max Allowed HA Role for NO	 While logged in to the active NOAM GUI, Go to Status & Manage-> HA screen. Click 'Edit' button. Check the 'Max Allowed HA Role' for the NO. By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. Click 'Ok' button.

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

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

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

S	This procedure perfo	rms a Health Check.
T F	Check off (\checkmark) 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:
		 Log in to the active NOAM GUI using the VIP. Select Status & Manage > Server: the Server Status screen is displayed
		 Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High
		Availability (HA), and Processes (Proc).
		Use your SSH client to connect to the upgraded DA-MP server (ex. ssh, putty): ssh <da-mp address="" ip="" server="" xmi=""></da-mp>
		login as: root
		<pre>password: <enter password=""></enter></pre>
		<pre># verifyUpgrade</pre>
		Examine the output of the above command, and determine if any errors were reported. Contact Tekelec in case of errors.
2	Log all current alarms	Log all current alarms in the system:
		1. Log in to the Active NOAM GUI VIP.
		 Select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed
		Following Alarm ID will be observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
		Note : If ALARM ID 32532 is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm :
		# alarmMgralarmstatus
		Following output shall be raised :
		SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33
		3. Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server
		 Click Report button to generate an Alarms report. Save the report and print the report. Keep these copies for future reference.
3	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade

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

End of maintenance window.

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

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

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

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

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

Procedur e		Elaps	ed Time (Hours: Minute	s)	Procedure Title	Impact
	This Step	Cum.	This Step (with TVOE upgrade)	Cum. (with TVOE upgrade)		
)				

4.8.1 Perform Health Check (Pre-Upgrade of NOAM)

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

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

S	This procedure perfo	orms a Health Check.
T F	Check off (\checkmark) each step as it is	s 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 GUI using the VIP.
		 Select Status & Manage > Server; the Server Status screen isis displayed. Verify all Server Status is Normal (Norm) for Alarm (Alm). Database (DB). High
		Availability (HA), and Processes (Proc).
		4. Do not proceed to upgrade if any of the server statuses displayed is not Norm .
		5. Do not proceed if there are any Major or Critical alarms.
		Note: It is not recommended to continue executing upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
2	Log all current alarms	Log all current alarms in the system:
		1. Select Alarms & Events > View Active; the Alarms & Events > View Active view is
		displayed.
		2. Click Report button to generate an Alarms report.
		3. Save the report and/or print the report. Keep these copies for future reference.
3	Verify that a recent	Verify that a fresh version of the Full DB backup has been performed.
	version of the Full DB	Status and Managa \rightarrow Filos
	performed	Check time stamp on two files:
		Backup.DSR. <hostname>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.ta r.bz2</time_stamp></hostname>
		Backup.DSR. <hostname>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.t ar.bz2</time_stamp></hostname>
		See section 3.3.5 to perform full Backup, if needed.

4.8.2 Upgrade 2-Tier NOAM

Detailed steps are shown in the procedure below.

S	This procedure is used	to upgrade the NOAM(s). This procedure is specific to 2-tier DSR OAM
Т	deployments.	
E		
P	Check off (\mathbf{v}) each step as it	is completed. Boxes have been provided for this purpose under each step number.
#	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.
		Start of maintenance window
1	Disable global	Disable global provisioning and configuration updates on the entire network:
	provisioning and	
	configuration.	Log into the NOAM GUI using the VIP.
		1. Select Status & Manage > Database; The Database Status screen is displayed.
		2. Click Disable Provisioning button.
		3. Confirm the operation by clicking Ok in the popup dialog box.
		4. Verify the button text changes to Enable Provisioning ; a yellow information box should
		also be displayed at the top of the view screen which states: [Warning Code 002] -
		Provisioning is manually disabled.
		5. Active NO server will have the following expected alarm:
		- Alarm ID = 10008 (Provisioning Manually Disabled)
	Inhibit SOAP replication	Record current DSR release number ex: 4 0 2 40 27 3
	(this is typically not	
	required)	ONLY EXECUTE THIS STEP IF ungrading from a release less than DSR
		4.0.0.40.10.0 (most upgrades will not use this step!)
		4.0.0_40.19.0 (most upgrades will not use this step:)
		1 Log into the active NO command prompt :
		1. Log into the active NO command prompt.
		Use your SSH client to connect to the Active NO server (ex. ssh. putty):
		ssh <active address="" ip="" no="" xmi=""></active>
		login as: root
		password: <enter password=""></enter>
		2. Execute the following command to disable SOAP replication :
		<pre># iset -fexcludeTables=' HaNodeLocPref HaVipDef '</pre>
		NodeInfo where "1=1"
		Execute following command to verify if above command successfully updated NodeInfo
		lecolus.
		# igt -F NodeInfo
		# Iqt -E Nodelnio
		Verify that excludeTables field shall include 'HaNodeLocPref HaVipDef' table
		names for each Nodeld present on the setup :
		E,g,
		nodeld=A2823.152 nodeName=NO2 hostName=NO2
		nodeCapability=Stby inhibitRepPlans= siteId=NO_HPC03
		<pre>excludeTables= HaNodeLocPref HaVipDef</pre>
		SUAP replication for HaNodeLocPret and HaVipDet needs to be disabled so that new data
		nom upgraueu NO ubesh i now ubwit to second NO of SO(S)/DA-MP servers.

Inhibit replication to MP	Pecord current release number ex: 1 0 2 10 27 3	
servers (depending on		
upgrade release)	 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 singl server upgrade (Appendix G). In this case, SKIP THIS STEP. 	le
	[Example: DSR 4.0.2_40.27.3 is less than DSR 4.1.0_41.16.0, so th step would be skipped in this example.]	nis
	 IF this release is greater than or equal to DSR 4.1.0_41.16.0, exect the following commands to inhibit A and B level replication on <u>all MP ser</u> of this site: 	ute rvers
	Log into Active NO(if logged out, else ignore this step) :	
	# ssh root@ <active ip="" no="" xmi=""></active>	
	login as: root	
	password: <enter password=""></enter>	
	Execute following command on active NO :	
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne name<br="">the site which is being upgraded>'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done</ne></pre>	fo e o: et
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne name<br="">the site which is being upgraded>'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done Note: NE name of the site can be found out by logging into the Activ GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. Main Menu: Configuration -> Server Groups</ne></pre>	fo e o: et ve NC
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne being="" is="" name="" site="" the="" upgraded="" which="">'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done Note: NE name of the site can be found out by logging into the Activ GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. Main Menu: Configuration -> Server Groups Text </ne></pre>	fo e o: et ve NC
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne name<br="">the site which is being upgraded>'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done Note: NE name of the site can be found out by logging into the Activ GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. Main Menu: Configuration -> Server Groups File - Inter Group Land Funct Functor Screen</ne></pre>	fo e o: et · ve NC
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne name<br="">the site which is being upgraded>'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done Note: NE name of the site can be found out by logging into the Activ GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. Nain Menu: Configuration -> Server Groups Fire ************************************</ne></pre>	fo e o: et · ve NC
	<pre># for i in \$(iqt -p -z -h -fhostName NodeInf where "nodeId like 'C*' and siteId='<ne name<br="">the site which is being upgraded>'"); do ise finhibitRepPlans='A' NodeInfo where "nodeName='\$i'"; done Note: NE name of the site can be found out by logging into the Activ GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. Main Menu: Configuration -> Server Groups Fire Configuration -> Server Groups Fire Configuration => Server Fire Conf</ne></pre>	fo e o: et · ve NC

	1				
	[root@NO1~]# i	qt NodeInfo			
	nodeld	nodeName	hostName	e nodeCapability	inhibitRepPlans
	siteld excludeTal	oles			
	A1386.099	NO1	NO1	Active	
	NO_HPC3				
	B1754.109	SO1	SO1	Active	
	SO_HPC03				
	C2254.131	MP2	MP2	Active	AB
	SO HPC03				
	C2254.233	MP1	MP1	Active	АВ
	SO HPC3				
Inhibit raplication to NO	Inhihit databaaa	realization to th		a in the followin	a ardor.
Inhibit replication to NO	innibit database	replication to th	le NO server	s in the followin	g order:
servers.					
	Note: It is imp	portant to inhib	it the replic	ation of the st	andby server before the
	active server,	to prevent unw	anted HA s	witchovers.	
		-			
	0	Standby NO			
	0	Active NO			
	0				
	a) Select	Status & Manage	e > Database		
	b) The Dr	etabase Status sc	reen isis disp	aved	
	b) The Da			ayeu.	
	c) Select	the appropriate se	erver based o	n the list above.	
	d) Click II	nhibit Replication	n button.		
	e) Verify	the Inhibited text	is displayed f	or server.	
	f) Repea	t the Inhibit subst	tep actions, st	eps a through f. f	or all remaining servers in the
	order s	hown above			
	Ulder 3	snown above.			
Upgrade standby NO					
server (using Upgrade	1. If the TVOE	Host needs to b	e upgraded,	Execute Append	dix J Upgrade TVOE, for the
Single Server	standby NO	, before proceedii	ng with the fol	lowing steps. See	e 6.Appendix D to check
procedure).	TVOE versi	on, if needed.			
	Upgrade the	e standby NO:			
	Execute Ap	pendix G – Upar	ade Single Se	erver procedure	
			5.00	1	
	After successfully	completing the p	procedure in A	ppendix G. return	n to this point and continue
	with step 6 below	/.		,,	
Upgrade 2nd NO TVOF					
server	1 Execute An	nendix I again for	the active NO) if 2nd NO is on	different TVOE blade before
	nroceeding	with the following	stens		
	proceeding	with the following	0.000		

7	Verify cmha process is	1. Log into the just-upgraded standby NO, execute the following command:
	running.	# ssh roota <no ip=""></no>
		login as: root
		password: <enter password=""></enter>
		Execute following command on NO:
		[root@NO1 ~]# pl grep "cmha"
		The following output should be generated:
		A 10128 cmha Up 11/20 00:15:58 1
		cmha
		If no output is generated then execute following command:
		service start_cmha start
8	Upgrade 2nd NO server.	1. Upgrade the 2nd NO server (the mate) using the Upgrade Single Server procedure:
		Execute Appendix G Single Server Upgrade Procedure
		After successfully completing the procedure in Appendix G, return to this point and
		continue with sub-step 4 below.
		Before login to the Upgrade GUI, clear your browser cache. (Note: some gui forms
		<i>may appear incomplete, or may have incorrect</i> behaviors, if the browser cache is not cleared.)
9	Allow replication to NO	Allow database replication to NO servers:
	servers.	1. Select Status & Manage > Database
		2. The Database Status screen isis displayed.
		3. Select the Active NO server.
		 Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for the server. After the Allow action, server HA
		requires time to recover (up to 3 minutes) before "Allowed" text is displayed for that
		 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 Detween Anow Steps.
10	Install NetBackup 7.5 on	Please refer to Appendix I.
	NO (If required).	Note: In DSR 5.0, backup file location is changed from /var/TKLC/db/filemgmt to /var/TKLC/db/filemgmt/backup directory, so configuration in Netbackup server needs to be updated to point to the correct file path. Updating Netbackup server configuration is out of scope of this upgrade document.

4.8.3 Perform Health Check (Post-Upgrade of NOAM)

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

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

S	This procedure performs a Health Check.			
T F	Check off ($\sqrt{2}$) 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.			
T E P # 1	Check off (*) each step as it is SHOULD THIS PROCEDURE Verify Server Status	<pre>completed. Boxes have been provided for this purpose under each step number. FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE. Verify Server Status after NO servers upgraded: 1. Execute following commands on both the active and standby NOAM servers: Use your SSH client to connect to the upgraded NO server (ex. ssh, putty): ssh <no address="" ip="" xmi=""> login as: root password: <enter password=""> Note: The static XMI IP address for each NO server should be available in Table 3 # verifyUpgrade Examine the output of the above command to determine if any errors were reported. Contact Tekelec if any errors are observed.</enter></no></pre> 2. Log in to Active NOAM VIP GUI and select Alarms & Events-> View Active screen to verify alarms. Servers have following expected alarms: Active NO server has: Alarm ID = 10008 (Provisioning Manually Disabled) All other servers might have: Alarm ID = 31113 (Replication Manually Disabled) Observed on all the upgraded servers : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) Note : If ALARM ID 32532 is not raised on any of the upgraded server, then execute following commands on that server to check the existence of alarm : # alarmMgralarmstatus The following output will be raised : SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI331 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33		
		 Contact Tekelec in case above output is not raised. 3. Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server. 		

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

Log all current alarms	Log all current alarms in the system from the already logged in Active NOAM VIP :		
	 Select Alarms & Events > View Active; the Alarms & Events > View Active view isis displayed. Click Penert butten to generate an Alarma report. 		
	2. Click Report buttorn to generate an Alarms report.		
	3. Save the report and/or print the report. Keep these copies for future reference.		
Update Appworks NetworkDeviceOption Table for the configured IPFE Ethernet devices	Note 1: This step is only applicable if the setup includes IPFE servers. This step will handle the possible audit discrepancies which can creep up after upgrading the IPFE servers. We are preparing the Active NO to handle any such discrepancies.		
on the Active NO server	Note 2: To optimize the performance of IPFE Ethernet devices, it is required to execute ipfeNetUpdate.sh script on the IPFE servers after upgrade. Appwork performs audit on the configured IPFE Ethernet devices and will update them with the locally stored information in case of any discrepancies.		
	Note 3: The steps below will update the locally stored information with the performance optimization parameters. This script check for the Ethernet devices on the servers with Function as IPFE and update its locally store information for those devices		
	 Login to Active NO console and execute the following command /usr/TKLC/ipfe/bin/ipfeAppworksUpdate.sh 		
	NOTE: This command may execute without any output if no changes are required (no devices were found to update).		

4.8.4 Upgrade All Active DA-MPs

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

If the DSR being upgraded is running OFCS, ensure that the DA-MPs are upgraded on an enclosure basis: successfully upgrade the DA-MPs in one enclosure first. Then upgrade the DA-MPs in the second enclosure. This approach will ensure that service is not affected. This approach will ensure service is not affected.

Procedure 73 needs to be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 21 must be executed four distinct times.

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

S	This procedure upgrade	es the DA-MP(s).			
Т					
Е	Check off (\mathbf{v}) each step as it	is completed. Boxes have been provided for this purpose under each step number.			
Р	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.			
#					
1	Identify DA-MPs to be upgraded together.	Identify all DA-MPs to be upgraded together.			
		Note: User can choose any number of MP(s) on which upgrade can be executed in parallel, depending upon the configuration.			
2	Upgrade Active MPs	Upgrade the selected DA-MPs, executing the Upgrade Single Server procedure on all selected DA-MPs in parallel.			
		Execute Appendix G Single Server Upgrade Procedure			
		After successfully completing the procedure in Appendix G for all selected DA-MPs, return to this point and continue with Step 3 below.			
3	Update Max Allowed HA				
	Role for NO.	1. Log into the active NOAM GUI using the VIP.			
		2. Go to Status & Manage-> HA screen.			
		3. Click 'Edit' button.			
		 Check the 'Max Allowed HA Role' for all the NO(s). By Default, It should be 'Active'. Else update the 'Max Allowed HA Role' as Active from Drop Down list. 			
		5. Click 'Ok' button.			

4.8.5 Upgrade IPFE(s)

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

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

S	This procedure upgrade	es the IPFE(s).				
Т	Check off (Λ) each step as it is completed. Boxes have been provided for this purpose under each step number					
£	Check off () cuch step us h	Check off (v) each step as it is completed. Boxes have been provided for this purpose under each step number.				
r #	Should this procedure fail, co	ontact the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.				
1	Identify IPFE upgrade	y IPFE upgrade User can choose any number of IPFEs on which upgrade can be executed in parallel				
	order	depending upon traffic conditions. All the IPFE should belong to same enclosure and only after				
		be upgraded.				
2	Upgrade IPFE servers (if exists)	Upgrade IPFEs identified in sub-step 1 in parallel, using Upgrade Single Server procedure.				
		1. Execute Appendix G Single Server Upgrade Procedure				
		2. Upgrade leftover IPFEs of the current site in parallel using Appendix G.				
	Execute ipfeNetUpdate	Execute following steps on each IPFE server just upgraded :				
	server	1. Use ssh client to connect to the IPFE server :				
		ssh <ipfe address="" ip="" xmi=""></ipfe>				
		login as: root				
		<pre>password: <enter password=""></enter></pre>				
		2. Execute following command on the IPFE server :				
		<pre># grep "IPV6_AUTOCONF=no" /etc/sysconfig/network # grep "IPV6FORWARDING=yes" /etc/sysconfig/network</pre>				
		If the outcome of any of the above command is				
		blank then execute the steps below else skip the				
		steps below				
		<pre># /usr/TKLC/ipfe/bin/ipfeNetUpdate.sh # init 6</pre>				
		Note: Command init 6 will cause a reboot of the IPFE server. Best to run the above steps on just one server of the pair, at a time, to reduce traffic impact.				
ļ	Enable global provisioning and	Enable provisioning and configuration updates on the entire network:				
	configuration.	1. Log into the Active Network OAM NE using the VIP.				
		 Select Status & Manage > Database 				
		The Database Status screen is displayed.				
		3. Click Enable Provisioning button.				
		4. Verify the text of the button changes to Disable Provisioning.				

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

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

1 Ioceutie 73. Anow Replication for Opgraded Site

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

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

This includes all DA-MPs and IPFE servers.

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

S This procedure verify Post Upgrade Status (N+0 2-Tier)
 T

 $\frac{1}{E}$ Check off ($\sqrt{2}$) 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.

Procedure	76.	Verify	Post	Ungrade	Status	(N+0 2-Ti	ier)
1 I OCCUUI C	/0.	verny	I USU	Opgraue	Status	(1110 2-1)	u)

#		
	SSH MP Server: Verify Server Status is Normal	<pre>Verify Server Status is Normal: 1. Log in to the active NOAM GUI using the VIP. 2. Select Status & Manage > Server; the Server Status screen is displayed. 3. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). 3. Execute following commands on the upgraded MP servers(both IPFE and DA-MPs): Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <mp address="" ip=""> login as: root password: <enter password=""> # verifyUpgrade Examine the output of the above command, and determine if any errors were reported. Contact Tekelec in case of errors. # alarmMgralarmstatus The following output will be raised , indicating that the upgrade completed. SEQ: 1 UPTIME: 133 BIRTH: 1355953411 TYPE: SET ALARM: TKSPLATMI33 tpdServerUpgradePendingAccept 1.3.6.1.4.1.3 23.5.3.18.3.1.3.33</enter></mp></pre>
2	NO GUI: Log all current alarms	 Log all current alarms in the system: Log in to the Active NOAM GUI VIP and select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed. Following Alarm ID will be observed for all the upgraded servers(DA-MPs and IPFE) : Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) Alarm ID 32532 will be cleared once Procedure 78is executed to accept the upgrade on each server. Click Report button to generate an Alarms report. Save the report and print the report. Keep these copies for future reference.
3	Execute Post Upgrade Overview.	Execute Section 4.9 Post-Upgrade
	E	nd of maintenance window.

4.9 Post-Upgrade Procedures

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

Table 20.	Post-Upgrad	e Procedures	Overview
	- 000 0 pg- 00	• • • • • • • • • • • • • •	0.01.010

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

4.9.1 Perform Post-Upgrade

Procedure 77: Perform Post Upgrade Health Check

C	This was as drive a sufe	mena Daat Urame da Uralth Chad			
5	This procedure perio	rms Post Upgrade Health Check			
Т					
- -	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
E					
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.				
#					
1	Verify Server Status is	Verify Server Status is Normal:			
	Normal	1 Log in to the active NOAM GUI using the VIP			
	Normal	2 Solution and the second			
		2. Select Status & Manage > Server; the Server Status screen is displayed.			
		3. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), High			
		Availability (HA) and Processes (Proc)			
2	Log all current alarms	Log all current alarms in the system:			
	-				
		1 Select Alarms & Events > View Active: the Alarms & Events > View Active view is			
		aispiayea.			
		2. Click Report button to generate an Alarms report.			
		3 Save the report and print the report. Keen these copies for future reference			
		5. Save the report and print the report. Reep these copies for future reference.			

Procedure 77: Perform Post Upgrade Health Check

3	Allow SOAP replication previously inhibited. (If upgrading from DSR release < 40.19.0 and upgrade is already accepted)	<pre>If the upgrade has already been accepted, and the DSR was running a source release older than 4.0.0_40.19.0 prior to the upgrade, execute the following steps, else ignore below mentioned steps : 1. Log into the Active NO command prompt : Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <noam vip=""> login as: root password: <enter password=""> 2. Execute the following command to enable SOAP replication : # iset -fexcludeTables='' NodeInfo where "1=1" Note: This step needs to be executed only if upgraded from any DSR release before 4.0.0_40.19.0.</enter></noam></pre>
4	Check if the setup previously have customer supplied apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	 Verify if the setup had customer supplied apache certificate installed and protected with passphrase before start of upgrade (refer Procedure 4 Step 11) If the certificate was installed and renamed as part of Procedure 4 Step 11 then rename the certificate back to original.

4.9.2 Accept Upgrade

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

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

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

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

S	This procedure accepts a successful upgrade.				
T E	Check off (\checkmark) each step as it is	completed. Boxes have been provided for this purpose under each step number.			
Р	SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.				
#					
1	It is recommended that	Verify that the upgraded system has been stable for 2 weeks or more			
	this procedure is performed 2 weeks after the upgrade.	[It will not be possible to backout after this is procedure is executed.]			

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

gle server	Note: Look a releases, the 1. Select screen	and feel of the e example bel	 Upgrade scree ow provides the 	n has chang snapshot fro	ed between DSR m both the relea	4.x and DSR 5.x ses.
	releases, the 1. Select screen	e example bel	ow provides the	snapshot fro	m both the relea	ses.
	1. Select screen	Administratio				
	screen	Auministratio	on->Software N	anagement	->Upgrade. The	Upgrade Administratio
		displays.				
	2. Select	the first server	r record in the ta	ble.		
	Upgrade sc	reen in DSR	<u>4.x</u> arado" button			
	J. Olick u			···· a d a		
		iu: Administ	ration -> Opy	rade		
	Usstuana	Netv	work Element		Role	Upgrade State
	Hostname	Appl	lication Version		Function	Server Status
	NO1	NO_	HPC03		NETWORK OAM&P	Not Ready
	NOT	4.0.0	0-40.14.1		OAM&P	ETT
	NO2	NO_	_HPC03		NETWORK OAM&P	Not Ready
		4.0.0	0-40.14.1		OAM&P	<u>E</u>
		NO_	HPC03		MP	Not Ready
	MP1	4.0.0	0-40.14.1		(active/standby pair)	Norm
		NO_	HPC03		MP	Not Ready
	MP2	NO_	_HPC03		MP DSR (active/stondby	Not Ready
	MP2 Prepare Upg <u>Upgrade sc</u> 3. Click th	NO_ 4.0.1 Irade Initiate U rreen in DSR 1e "Accept" bu	_HPC03 0-40,14,1 Jpgrade Monitor <u>5.x</u> tton	Jpgrade Co	MP DSR (active/standby *** mplete Upgrade	Not Ready Err Accept Upgrade
	MP2 Prepare Upg <u>Upgrade sc</u> 3. Click th Main Menu: A Fitter Taska	NO_ 4.0.0 rrade Initiate U rreen in DSR 1e "Accept" bu dministration ->	_HPC03 D-40.14.1 Jpgrade Monitor <u>5.x</u> tton > Software Manage	Upgrade Cc :ment -> Upgr	MP DSR (active/standby mplete Upgrade	Not Ready Err Accept Upgrade Fri Nov 15 13:20
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter Taska	NO_ 4.0.1 grade Initiate U creen in DSR = ne "Accept" bu dministration -> s • Sever Status	_HPC03 0-40.14.1 Jpgrade Monitor 5.x tton > Software Manage Server Role Function	Upgrade Cc ement -> Upgr n Upgrade State	MP DSR (active/standby mplete Upgrade	Not Ready Err Accept Upgrade Fri Nev 15 13:20
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter Tasks Hostname	NO_ 4.0.1 grade Initiate U creen in DSR the "Accept" bu dministration -> s • Sever Status OAM Max HA Role Max Allowed	HPC03 0-40,14,1 Jpgrade Monitor 5.x tton > Software Manage Server Role Function Network Element Application Version	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO	MP DSR (active/standby mplete Upgrade . ade Status Message Finish Time	Not Ready Err Accept Upgrade Pri Nov 15 13:20 Mate Server Status
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter • Taska Hostname	NO_ 4.0.1 rrade Initiate U rreen in DSR ine "Accept" bu udministration -> s • Server Status OAM Max HA Role Max Allowed HA Role Norm	HPC03 0-40,14.1 Jpgrade Monitor 5.x tton > Software Manage Server Role Function Network Element Application Version	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO Not Ready	MP DSR (active/standby mplete Upgrade ade Status Message Finish Time	Not Ready
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter - Taska Hostname	NO_ 4.0.1 grade Initiate U creen in DSR the "Accept" bu dministration -> s • Sever Status OAM Max HA Role Max Allowed HA Role Norm Active Active	LHPC03 0-40.14.1 Jpgrade Monitor 5.x tton > Software Manage Server Role Function Network Element Application Version Network CAM&P OAM&F No_DSR_VM 50.0-50.15.1	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO Not Ready	MP DSR (active/standby mplete Upgrade (. ade Status Message Finish Time	Not Ready The server Status No2
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter Tasks Hostname NO1	NO_ 4.0.1 grade Initiate U creen in DSR "Accept" bu udministration -> s • Sever Status OAM Max HA Role Max Allowed HA Role Max Allowed Norm Active Active Standby Active	HPC03 0-40.14.1 Jpgrade Monitor 5.x tton > Software Manage Server Role Function Network Element Application Version Network CAMSP OAMSE No_DSR_VM 5.0.0-50.15.1 Network CAMSP OAMSE No_DSR_VM	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO Not Ready Not Ready	MP DSR (active/standby mplete Upgrade ade Status Message Finish Time	Not Ready
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter Tasks Hostname NO1 NO2 SO2	NO_ 4.0.1 grade Initiate U creen in DSR : the "Accept" bu udministration -> s • S • Server Status OAM Max HA Role Max Allowed HA Role Max Allowed HA Role Max Allowed HA Role Max Max Max Max Max Allowed Norm Active Active Norm Standby Active	LHPC03 0-40.14.1 Jpgrade Monitor 5.x ttton > Software Manage Server Role Function Network Element Application Version Network OAM&P NO_DSR_VM 5.0-50.15.1 Network OAM&P So_DSR_VM So_DSR	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO Not Ready Not Ready Not Ready	MP DSR (active/standby mplete Upgrade ade Status Message Finish Time	Not Ready
	MP2 Prepare Upg Upgrade sc 3. Click th Main Menu: A Filter • Taska Hostname NO1 NO2	NO_ 4.0.1 grade Initiate U creen in DSR ine "Accept" bu idministration -> s • Server Status OAM Max HA Role Max HA	HPC03 0-40.14.1 Jpgrade Monitor 5.x tton Software Manage Server Role Function Network Element Application Version Network CAM&P No_DSR_VM 5.0-50.15.1 Network CAM&P Source	Upgrade Cc ement -> Upgr n Upgrade State Start Time Upgrade ISO Not Ready Not Ready Not Ready	MP DSR (active/standby mplete Upgrade ade Status Message Finish Time	Not Ready

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

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

5. BACKOUT PROCEDURE OVERVIEW

The procedures shown in the following table are executed inside a maintenance window. Backout procedure times are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done. This backout procedure covers all upgrade scenarios and topologies. Note that the elapsed time are for a "Lab Environment", and they might vary on Live Systems.

Procedure	Elapse (Hou Min	ed Time Irs or utes)	Procedure Title	Impact
	This Step	Cum.		
Backout Setup	0:10- 0:30	0:10- 0:30	The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time will vary.	None.
Procedure 79	See Note	See Note	 Back Out Entire Network Note: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures. 	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
	0:01- 0:05	Varies	Perform Health Check (Post-Backout)	None

Table 21. Backout Procedure Overview

5.1 Recovery Procedures

Upgrade procedure recovery issues should be directed to the Tekelec Customer Care Center by referring to Appendix K of this document. Before executing any of these procedures, contact the Tekelec Customer Care Center at 1-888-FOR-TKLC (1-888-367-8552); or 1-919-460-2150 (international). Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of

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. <u>NOTE</u>: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 10.y.z release to the previously installed 10.x.w release). Backout of an initial installation is not supported.

5.2 Backout Setup

Identify IP addresses of all servers that needed to be backout.

- 1. Select Administration->Software Management->Upgrade
- 2. Based on the "Application Version" column, identify all the hostnames that need to be back out.
- 3. Select Configuration > Servers
- 4. Identify the XMI/iLO IP addresses of all the hostnames identified in step 2 from Table 3. These are required to access the server when performing the backout.

The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Backout procedure **WILL** cause traffic loss. Since all possible reasons cannot be predicted ahead of time, contact the Tekelec Customer Care Center as stated in the **Warning** box above.

For DSR 4.x/5.x:

NOTE: Verify that the two backup archive files created using the procedure in section 3.3.5are present on every server that is to be backout. These archive files are located in the /var/TKLC/db/filemgmt directory and have different filenames than other database backup files. The filenames will have the format

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

And

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

5.3 Perform Backout

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

5.3.1 Back Out Entire Network

S T E P	This procedure is used to back out and upgrade of DSR 4.x/5.x application software from multiple servers in the network. Any server requiring backout can be included: NOAMs, SOAMs, DA-MPs, IPFEs, cSBRs, pSBRs, and even TVOE hosts.		
#	Check off (\checkmark) each step as it is	completed. Boxes have been provided for this purpose under each step number.	
1	Identify all servers that require Backout.	Identify all servers that require Backout: 1. Select Administration->Software Management->Upgrade	
		The Upgrade Administration screen is displayed.	
		 Identify the servers with the target release Application Version value. These servers were previously upgraded but now require Backout. Make note of these servers. They have been identified for Backout. 	
2	Disable global provisioning and configuration.	 Disable provisioning and configuration updates on the entire network: Since this step is being executed during a backout procedure, it is likely that Provisioning and Configuration updates are disabled already. If they have not been disabled, Execute the following to disable Provisioning: 1. Log into the NOAM VIP GUI. 2. Select Status & Manage > Database. The Database Status screen is displayed. 3. Click Disable Provisioning button. 4. Confirm the operation by clicking Ok in the popup dialog box. 5. Verify the button text changes to Enable Provisioning; a yellow information box should also be displayed at the top of the view screen which states: [Warning Code 002] - Provisioning is manually disabled. 6. Active NO server will have the following expected alarm: Alarm ID = 10008 (Provisioning Manually Disabled) 	

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

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

16	Back out TVOE if upgraded previously	If the NO/SO server hosts the TVOE software, check if TVOE backout is required (If upgraded previously). If backout is not required then skip to next step.
		Execute following steps for each TVOE blade upgraded previously :
		 Disable all the applications running on TVOE blade: Log into the NOAM GUI using VIP. Select Status & Manage > Server; the Server Status screen is displayed Select all the applications running on current TVOE blade. Click the 'Stop' button. Confirm the operation by clicking Ok in the popup dialog box. 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=""></tvoe>
		login as: root
		<pre>password: <enter password=""></enter></pre>
		# 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 :
		<pre># virsh shutdown <guestname></guestname></pre>
		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.
		 Periodically execute following command until the command displays no entries. This means that all VMs have been properly shut down :
		# virsh list
		Back out TVOE on the blade according to reference [2].

17	Enable virtual guest watchdogs if disabled	 If virtual guest watchdogs were previously disabled for the TVOE blade being backed out, follow procedure 3.12.1 in reference [6] Otherwise execute following sub-steps:
	previously	 a) Log into TVOE host by using following command : # ssh root@<tvoe ip=""></tvoe>
		login as: root
		password: <enter password=""></enter>
		 Execute following command to start the TVOE guests shutdown in step 13 sub- step 3 above (if not already started).
		<pre># virsh start <guestname></guestname></pre>
		 Periodically execute following command until the command displays all the VM guests running.
		# virsh list
		2. Enable all the applications running on backed out TVOE blade :
		a) Log into the NOAM VIP GUI
		 b) Select Status & Manage > Server; the Server Status screen is displayed
		 c) Select all the applications running on current TVOE blade. d) Click the 'Bestart' button
		e) Confirm the operation by clicking Ok in the populo dialog box.
		 f) Verify that the 'Appl State' for all the selected servers is changed to 'Enabled'.
		Note: This step shall be executed only if TVOE is backed out in Step 13.
		Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable).
18	Allow replication to NO servers.	Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps.
18	Allow replication to NO servers.	Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers:
18	Allow replication to NO servers.	Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: 1. Select Status & Manage > Database. The Database Status screen is displayed. 2. Select the active NO server.
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA
18	Allow replication to NO servers.	Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: 1. Select Status & Manage > Database. The Database Status screen is displayed. 2. Select the active NO server. 3. Click Allow Replication button. 4. Verify the Inhibited text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. 5. Repeat sub-steps, 3 and 4, for Standby NO server.
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the Inhibited text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the Inhibited text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the Inhibited text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers:
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps Allow database replication to SO servers: The following steps are to be executed for all SO servers in all Signaling NEs.
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select Status & Manage > Database and the switchover in between Allow steps.
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers: Select Status & Manage > Database. The Database Status screen is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers: The following steps are to be executed for all SO servers in all Signaling NEs. Select Status & Manage > Database. The Database Status screen is displayed. Select the Active SO server. Click Allow Replication button Verify the <i>Inhibited</i> text is not displayed for the server. After the allow action, server
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers: The following steps are to be executed for all SO servers in all Signaling NEs. Select Status & Manage > Database. The Database Status screen is displayed. Select the Active SO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for the server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed.
18	Allow replication to NO servers.	 Execute Steps 16 and 17 again for another TVOE blade hosting NO/SO (as applicable). Note: If major backout from DSR 5.x to DSR 4.x is performed then clear the browser cache before continuing with the following steps. Allow database replication to NO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select the active NO server. Click Allow Replication button. Verify the <i>Inhibited</i> text is not displayed for server. After the allow action, server HA requires time to recover (up to 3 minutes) before "Allowed" text is displayed. Repeat sub-steps, 3 and 4, for Standby NO server. Note: The NO servers intentionally have a sequence of "Allow Active – Allow Standby". This sequence for NOs is necessary to prevent an unwanted HA switchover in between Allow steps. Allow database replication to SO servers: Select Status & Manage > Database. The Database Status screen is displayed. Select Status & Manage > Database. The Database and the switchover in between Allow steps.

20	Allow replication to C-	Allow database replication to all C-level servers:			
	level servers.	The following steps are to be executed for all C-level servers in all Signaling NEs			
		 Select Status & Manage > Database the Database Status screen is displayed. Select the Active MP server. Click Allow Replication button. Verify the <i>Inhibited text</i> is not displayed for the server. After the allow action, server HA requires time to recover (up to 3 minutes) before 'Allowed' text is displayed. Repeat the Allow action for Standby MP server (if dealing with a server pair). While server HA is recovering, monitor Server Status for recovery. Select Status & Manage > Servers The Server Status screen is displayed. Wait for the screen to refresh and show the Server Status fields for the server. 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. Repeat sub steps 1) to 9) for all remaining C-level servers in all Signaling NEs. 			
21	Allow replication for PSBR servers.	Log into the Active NO server and execute following command to allow replication for backed out PSBR servers :-			
		<pre># iset -finhibitRepPlans='' NodeInfo where</pre>			
		"nodeName=' <psbr nodename="" server="">'"</psbr>			
		Note: Execute above command for each of the PSBR server which is currently backed out.			
22	Enable Site Provisioning	Enable Site provisioning :			
		1. Log into the SOAM VIP GUI of the site.			
		 Select Status & Manage > Database the Database Status screen is displayed Olid Final Part - Displayed by the state of the			
		 Click Enable Site Provisioning button. Confirm the operation by clicking Ok in the population box. 			
		 Verify the button text changes to Disable Site Provisioning 			
23	Enable global provisioning and	Enable global provisioning and configuration updates on the entire network:			
	configuration.	1. Select Status & Manage > Database			
		The Database Status screen is displayed. 2. Click Enable Provisioning button			
		3. Verify the button text changes to Disable Provisioning.			
24	Remove 'Ready' state (From Active NO GUI			
24	if exists) for any backed	Hom Active NO GOL			
	out server	 Select Status & Manage > Servers; the Server Status screen is displayed. If the any of the backed-out server's Application Status is 'Disabled', then select the server row and press the Restart button. 			
		 Select Administration > Upgrade (in DSR 4.x) or Administration->Software Management->Upgrade (in DSR 5.x). The Upgrade Administration screen is displayed. 			
		 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 			
		 Click OK. This will now remove the Forced Standby designation for the backed-out server. 			
		Note: Due to Backout being initiated from the command line instead of through the GUI, you may see the following SOAP error in the GUI banner.			
		SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]			
		It is safe to ignore this error message.			
		Verify the Application Version value for servers has been downgraded to the original release version.			

5.3.2 Back Out Single Server

Procedure 80: Back out Single Server

S	This procedure will back out the upgrade of DSR 5.x application software. Any server requiring						-		
Г	Back out can be included: NOAMs, SOAMs, DA-MPs, IPFEs, cSBRs, pSBRs, and even TVOE								
E	hoete								
P	10515.								
#	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
1	Make server ready for	Make the serv	er 'Ready' f	or backout	:				
	backout.	1 Solo	oct Adminic	tration > S	oftwa	ro Managon	ont->Ungrad	• The Upgrade	
		Adn	ninistration s	screen is di	splave	ne manayen ad	ient->0pgrau	e. The Opyrade	
		7.001			50.070				
		2. Sele	ect the serve	er to backou	ut and	check its up	grade state :		
			a) If the	upgrade st	ate is	"Ready" then	n press "Comp	lete" button.	ton
			D) EISE,	Select the s	server		graded and pre	ss the Frepare but	lon.
		The Upg Main Menu	rade [Prepa :: Administratio	are] screen	will ap Manage	ppear. ement -> Upgrad	le [Prepare]		
		Info 🔻			-			Fri Nov 15 13:46:23 :	
		Hostname Actio	n HA St	tatus					
		NO2 Pre	pare • Max	HA Role Active Mate	s	Standby Mat	tes Spare	e Mates	
						Ok Cancel	None		
		3. If th	is is the Sta	ndby serve	er. veri	ifv that the v	alue in the HA	Status field under the	
		Sele	ected Serve	r Status is	Stand	by, otherwis	e it will display	Active.	
		4. CliC	k OK. Setarte the N	Jako Road	vactio	on on the ser	ver Vouwillb	e returned to the	
		Upo	rade Admin	istration sc	reen.				
		5. Wai	t for the scre	een to refre	sh an	d show both	the Upgrade R	Ready State as Ready	/
		and	the Upgrad	le action lin	k to b	e enabled fo	r the server that	at was to be upgraded	d. It
		may	take up to	a minute to	r the l	Jpgrade Rea	ady State to cha	ange to Ready.	
		Main Menu: Adı	ninistration ->	> Software M	anagen	nent -> Upgrad	le		
		Filter - Tasks	•					Fri Nov 15 13:5	0:51 2
			Server Status OAM Max HA Role	Server Role Network Element	Function	Upgrade State Start Time	Status Message Finish Time		
		Hostname	Max Allowed	Application Version		Upgrade ISO		Mate Server Status	
		104	Warn	Network OAM&P	OAM&P	Not Ready			
		NOT	Active	5.0.0-50.15.1					
		NO2	Warn Standby	Network OAM&P NO_DSR_VM	OAM&P	Ready		NOT	
			Standby Norm	5.0.0-50.15.1 System OAM	OAM	Not Ready			
		SO2	Standby Active	SO_DSR_VM 5.0.0-50.15.1				S01	
		SO1	Norm Active	System OAM SO_DSR_VM	OAM	Not Ready		802	
			Active	5.0.0-50.15.1	DSR				
		MP1	Err	MP	(multi- active	Not Ready		MP2 MP3 MP4	
			Standby	SO_DSR_VM	clustery			Land American American	
		Raskup ISO Class	Report	5.0.0-50. 15. I		oeo Roport			
		Duckup 100 Clea		Complet	ALCE				
		Note: If this is	s the Active	e server in	an Ac	ctive-Standl	by pair, the Ma	ake Ready action WI	LL
		cause an HA	switchover	r. The HA s	witch	over is an e	expected outc	ome from the Make	
		Ready action	-						
		Note: The pre	eparation s	teps requi	red to	upgrade a :	server are als	o required when	
		preparing to	back out a	server.					

Procedure 80: Back out Single Server

2	SSH to server	Use your SSH client to connect to the server (ex. ssh, putty):
		Note: You must consult your own software client's documentation to learn how to launch a connection. For example:
		ssh <server address=""></server>
		Note: If you do not have direct access to the IMI or if TVOE is installed on blade, then you must access the target server via a connection through the active NO. SSH to the active NO XMI first. Once you are logged into the NO; from there, SSH to the target server's IMI address.
3	Log in as root	Login as root:
		login as: root password: <enter password=""></enter>
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 " v ".
		······································
5	Backout proceeds	Many informational messages will come across the terminal screen as the backout proceeds:
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.
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. Use your SSH client to connect to the server (ex. ssh, putty):
5	Backout proceeds SSH to server	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot. 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:
5	Backout proceeds SSH to server	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot. 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=""></server>
6	Backout proceeds SSH to server	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot. 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.</server>
5	Backout proceeds SSH to server	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot. 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. Login as root:</server>
5 6 7	Backout proceeds SSH to server Log in as root	Many informational messages will come across the terminal screen as the backout proceeds: Finally, after backout is complete, the server will automatically reboot. 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. Login as root: login as: root</server>

Procedure 80: Back out Single Server

8	Restore the full DB run	Execute the backout_restore utility to restore the full database run environment:				
	chillion nent.	<pre># /var/tmp/backout_restore</pre>				
		NOTE: If you would like to proceed, answer "y".				
		If the restore was successful, the following will be displayed:				
		Success: Full restore of COMCOL run env has completed. Return to the backout procedure document for further instruction.				
		If an error is encountered and reported by the utility, then work with Tekelec Customer Care Center by referring to Appendix K of this document for further instructions.				
9	Verify the backout	1 Examine the output of the following commande to determine if any errors were				
		reported: # verifyUpgrade				
		This command will show the current rev on the server:				
		# appRev				
		2. If the backout was not successful because other errors were recorded in the logs, then contact Tekelec Customer Care Center by referring to Appendix K of this				
		 If the backout was successful (no errors or failures), then continue with the remaining steps. 				
10	Reboot the server	Enter the following command to reboot the server:				
		# init 6				
		This step can take several minutes.				
111	Verify services restart	Verify services have restarted:				
		 You must wait several (approx. 6 minutes) minutes for a reboot to complete before being able to log back into the server. SSH and log back into the server as root. The method is the same as Steps 2 and 3 of Section 5.3.1(this procedure). If this is an NO or SO, verify httpd service is running. Execute the command: 				
		<pre># service httpd status</pre>				
		 Verify expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored): 				
		<pre>httpd <process be="" here="" ids="" listed="" will=""> is running</process></pre>				
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. Contact Tekelec Customer Care Center by referring to Appendix K of this document for further instructions.				
Procedure 80: Back out Single Server

	If the backed out serv	er is Standby NO					
backout (DSR 5.x ->	1. Log into Ac	tive NO :					
DSR 4.X)	login a	s: root					
	passwor	d: <enter pas<="" td=""><td>ssword></td><td></td><td></td><td></td><td></td></enter>	ssword>				
	2. Execute fol # ivi N	lowing commands on co IodeInfo	ommand line :				
	Change the Change the Save the ta	NodeCapability of Active NodeCapability of Star ble.	ve NO to 'Stby ndby NO to 'A	y'. ctive'.			
	VIP and proceed forw	switchover, so it logged ard.	in VIP then it	will be lo	ogged o	ut. Login I	back to
Remove Upgrade Ready status	From the DSR Active 1. Select Statu 2. If the server server row a Main Menu: Status &	NOAM GUI: us & Manage > Server; r just backed-out shows and press the Stop butte Manage -> Server	the Server Sta Application S on.	atus scre Status En	en is di abled, t	splayed. hen selec	t the 0 10:47:47 20
	riller 🔻						
	Network Element	Server Hostname	Appl State	Alm	DB	Reporting Status	Proc
	NO HPC03	N01	Enabled	Warn	Norm	Norm	Norm
	SO HPC03	S01	Enabled	Norm	Norm	Norm	Norm
	SO HPC03	MP1	Enabled	Warn	Norm	Norm	Norm
	SO HPC03				-		
	00_111 000	MF2	Enabled	Warn	Norm	Norm	Norm
	Stop Restart Reboot	MF2	Enabled	Warn	Norm	Norm	Norm
	3. Select Adm Manageme displayed. 4. If the serve select the b	mer inistration > Upgrade int >Upgrade(on DSR so r just backed-out shows acked-out server and p	(on DSR 4.x 5.x GUI); the an Upgrade S ress the Com	GUI) or Upgrade State of ' plete Up	Admini Admini 'Ready" ograde (stration a stration so or "Succe (on DSR •	Pause up Software creen is ess", then 4.x GUI)
	Stop Restart Reboot 3. Select Adm Manageme displayed. 4. If the server select the b or Complet Note: Look and feel or releases, the example	inistration > Upgrade int >Upgrade(on DSR start r just backed-out shows acked-out server and p te (on DSR 5.x GUI) bu f the Upgrade screen ha below provides the sna	(on DSR 4.x 5.x GUI); the an Upgrade 3 ress the Com titon. Otherwis as changed b apshot from b	GUI) or Upgrade State of ⁴ plete Up se, skip t etween E oth the re	Admini Admini 'Ready" ograde (o sub-si DSR 4.x eleases	stration a stration so or "Succe (on DSR 4 tep 6 belo and DSR	Software creen is ess", then 4.x GUI) w. 2.5.x

Procedure 80: Back out Single Server



Procedure 80: Back out Single Server

IS Server Role Network Element Application Version Network OAM&P ND_DSR_VM 5.0.0-50.15.1 Network OAM&P ND_DSR_VM 5.0.0-50.15.1 System OAM	Function OAM&P OAM&P	Upgrade State Start Time Upgrade ISO Not Ready	Status Message Finish Time	Mate Server Status
Noil Network Element Application Versic Network OAM&P NO_DSR_VM 5.050.15.1 Network OAM&P NO_DSR_VM 5.050.15.1 System OAM	n OAM&P OAM&P	Start Time Upgrade ISO Not Ready	Finish Time	Mate Server Status
Application Version Application Version No_DSR_VM 5.0.0-50.15.1 Network 0AM&P No_DSR_VM 5.0.0-50.15.1 System 0AM	n OAM&P OAM&P	Upgrade ISO Not Ready		
Network OAM&P NO_DSR_VM 5.0.0-50.15.1 Network OAM&P Y NO_DSR_VM 5.0.0-50.15.1 System OAM	OAM&P	Not Ready		
NO_DSR_VM 5.0.0-50.15.1 Network OAM&P V NO_DSR_VM 5.0.0-50.15.1 System OAM	OAM&P			,
Network OAM&P NO_DSR_VM 5.0.0-50.15.1 System OAM	OAM&P			NO2
y NO_DSR_VM 5.0.0-50.15.1 System OAM	O/ WIGH	Ready		
5.0.0-50.15.1 System OAM		Reauy		NO1
System OAM				(And and a second s
	OAM	Not Ready		
y SO_DSR_VM				S01
5.0.0-50.15.1				
System OAM	OAM	Not Ready		
SO_DSR_VM				S02
5.0.0-50.15.1				
	DSR (multi-			
MP	active	Not Ready		
	cluster)			MP2 MP3 MP4
SO_DSR_VM				
Software Manager	nent -> Uj	pgrade [Comple	ete]	đ - Fri Nov 15 15:06:53 20
olo Activo Nator	Sta	ndby Mator	Spare Mater	
NO1	No	ne	None	
	Ok Cancel	1		
his will now re backout beir ay see the follo OAP erro ostname=	emove t ng initiat owing S r wh: [frar	ted from the SOAP error	Standby designate e command line in the GUI bann caring upg: b6] ip=[1]	ation for the ba instead of thro er. rade stat 72.16.1.2
gnore this erro	or mess	sage.		
	SO_DSR_VM 5.0.0-50.15.1 MP SO_DSR_VM 5.0.0-50.15.1 e Initiate Comple ete] Screen wi Software Managen Mo his will now re b backout bein ay see the follo OAP erro:	SO_DER_VM SO.0-50.15.1 MP attitute ouster) SO_DER_VM SO.0-50.15.1 e Initiate Complete Accee ete] screen will appe Software Management -> Up Not Not Not OK Cance his will now remove the obackout being initia ay see the following S OAP error wh:	SO_DSR_VM 5.0.0-50.15.1 MP active ousser) SO_DSR_VM 5.0.0-50.15.1 a Initiate Complete Accept Report a Initiate Complete Accept Report a Initiate Complete Accept Report attribution of the second accept a	so_DSR_VM so_0-50.15.1 MP So_0-50.15.1 so_o-50.15.1 s

5.4 Post-Backout Procedures

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

5.4.1 Perform Health Check (Post-Backout)

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

Procedure 8	31:	Perform	Health	Check	(Post-Backout)
-------------	-----	---------	--------	-------	----------------

S	This procedure perfo	rms a Health Check.			
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
- Р #	SHOULD THIS PROCEDURE	FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR <u>UPGRADE ASSISTANCE</u> .			
	Verify Server Status is Normal	 Verify Server Status is Normal: Select Status & Manage > Server; the Server Status screen isis displayed. Verify all Server Status is Normal (Norm) for Alarm (Alm), Database (DB), High Availability (HA), and Processes (Proc). Do not proceed to upgrade if any of the server statuses displayed is not Norm. 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:			
		 Select Alarms & Events > View Active; the Alarms & Events > View Active view is displayed. Click Report button to generate an Alarms report. Save the report and print the report. Keep these copies for future reference. 			
3	Execute optimization script only if backout is done to DSR release less than 4.1.0-41.19.0	Note: Don't execute following steps for PSBR/PDRA servers. Use your SSH client to connect to the upgraded server (ex. ssh, putty): ssh <server address=""> login as: root password: <enter password=""> Execute following commands :- # /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage force # sleep 20 # prod.start # pm.sanity Note: Execute optimization script for all the servers backed out to DSR release less than 4.1.0-41.19.0 in the setup.</enter></server>			

6. APPENDIXES

APPENDIX A. COMMAND OUTPUTS

Not applicable.

APPENDIX B. SWOPS SIGN OFF.

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

Discrepancy List

APPENDIX C. CUSTOMER SIGN OFF

Sign-Off Record

*** Please This is to certify that all steps requir	review this entire document. *** ed for the upgrade successfully completed wit	hout failure.
Sign your name, showing approval of this proc	edure, and fax this page and the SWOPS Sign FAX # 919-460-3669.	Off matrix to Tekelec,
Customer: Company Name:	Date:	
Site: Location:		
Customer:(Print)	Phone:	
	Fax:	
Start Date:	Completion Date:	
This procedure has been approved by the under both Tekelec and the customer representative. The SWOPS supervisor will also maintain a sig	signed. Any deviations from this procedure n A copy of this page should be given to the cus and copy of this completion for future referen	nust be approved by tomer for their records. ce.
Tekelec Signature:	Date:	
Customer Signature:	Date:	
909-2277-001 Revision A, March 2014	Version 4.0	223 of 252

APPENDIX D. SECTION DELETED

APPENDIX E. DETERMINE IF TVOE UPGRADE IS REQUIRED

When upgrading a server that exists as a virtual guest on a TVOE host, it is first necessary to determine whether the TVOE host (i.e. the "bare-metal") server must first be upgraded to a newer release of TVOE.

NOAM and SOAM servers are often implemented as TVOE guests in C-class deployments, and so the TVOE upgrade check is necessary. DA-MPs are not implemented as TVOE guests in C-class deployments, so the TVOE upgrade check is not necessary when upgrading C-class DA-MPs.

When DSR is deployed on Rack Mounted Servers (RMSes), all servers are virtual guests, and the TVOE upgrade check is always required. However, DA-MPs are often deployed as guests on the same TVOE host as the OAM server(s), and so by the time the DA-MP servers are being upgraded, TVOE has already been upgraded and there is no need to do so again.

Procedure 82: Determine if TVOE Upgrade is Required

S	This procedure check	s if TVOE upgrade is required.
Т Е Р #	Check off (√) each step as it is SHOULD THIS PROCEDURE	completed. Boxes have been provided for this purpose under each step number. FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR <u>UPGRADE ASSISTANCE</u> .
	Determine the version of TVOE already running on the bare-metal server that hosts the virtual guest you are currently upgrading.	 Log into the host server on which TVOE is installed. Execute the following command to get the current TVOE installed version : [root@dsrTVOEblade2 ~]# appRev Install Time: Tue Aug 7 08:17:52 2012 Product Name: TVOE Product Release: 2.0.0_80.16.0 Part Number ISO: 872-2290-104 Part Number USB: 872-2290-104 Base Distro Product: TPD Base Distro Release: 6.0.0_80.16.0 Base Distro ISO: TPD.install-6.0.0_80.16.0- CentOS6.2-x86_64.iso OS: CentOS 6.2
2	Check the TVOE release version required for target DSR release	Please contact Tekelec customer by referring to Appendix K of this document to get support for the same.
3	If the release in Step 1 is less than what is required in Step 2 then upgrade of TVOE is required	The procedure to upgrade TVOE on the host server is given in Appendix J.

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

If the ISO image is delivered on optical media, or USB device, continue with step 1 of this appendix, otherwise if the ISO image was delivered to the PM&C using sftp continue with step 5.

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

VM Info Software Network Media Attached Image Path Attached Image Path Detach /var/TKLC/tvoe/mapping-isos/vm-pmacdev6.iso Detach /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Detach /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Image Path Attach Label Image Path Attach Label Image Path Attach tkic_000-0000-000_Rev_A_80.16 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Attach tkic_000-0000-000_Rev_A_80.17 /var/TKLC/upgrade/TPD.install-6.0.0_80.17.0-CentOS6.2-x86_64.iso	Name: vr Host: fe	n-pmacdev6 80::461e:a1ff:	fe06:484			Current Po	wer State:	Running
Attached Image Path Detach /var/TKLC/tvoe/mapping-isos/vm-pmacdev6.iso Detach /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Attach Label Image Path Attach Label /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Attach Label Image Path Attach Label /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Attach tkic_000-0000-000_Rev_A_80.16 //media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Attach tkic_000-0000-000_Rev_A_80.17 //media/sdb1/000-0000-000-6.0.0_80.17.0-CentOS6.2-x86_64.iso	VM Info	Software	Network	Media				
Detach /var/TKLC/tvoe/mapping-isos/vm-pmacdev6.iso Detach /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Available Media Attach Label Image Path Attach tklc_000-0000-000_Rev_A_80.16 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS- 6.2-x86_64.iso Attach tklc_000-0000-000_Rev_A_80.17 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS- 6.2-x86_64.iso Attach tklc_000-0000-000_Rev_A_80.17 /media/sdb1/000-0000-000-6.0.0_80.17.0- CentOS6.2-x86_64.iso	Attached	d Media Image Path	ALL ALL	AL-K	and the second	- Ale	No. 15	
Detach /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS-6.2-x86_64.iso Available Media Attach Label Image Path Attach tklc_000-0000-000_Rev_A_80.16 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS- 6.2-x86_64.iso Attach tklc_000-0000-000_Rev_A_80.17 /mar/TKLC/upgrade/TPD.install-6.0.0_80.17.0- CentOS6.2-x86_64.iso	Detach	Nar/TKLC/tv	oe/mapping	-isos/vm-pm	acdev6.iso			
Available Media Image Path Attach Label Image Path Attach tklc_000-0000-000_Rev_A_80.16 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS- 6.2-x86_64.iso Attach tklc_000-0000-000_Rev_A_80.17 /var/TKLC/upgrade/TPD.install-6.0.0_80.17.0- CentOS6.2-x86_64.iso	Detach	/media/sdb	1/000-0000-1	000-6.0.0 80	16.0-CentOS-6.	2-x86 64.iso		and the second
Attach tklc_000-0000_Rev_A_80.16 /media/sdb1/000-0000-000-6.0.0_80.16.0-CentOS- 6.2-x86_64.iso Attach tklc_000-0000-000_Rev_A_80.17 /var/TKLC/upgrade/TPD.install-6.0.0_80.17.0- CentOS6.2-x86_64.iso	1-1		54	4	51		1	
Attach tklc_000-0000-000_Rev_A_80.17 /var/TKLC/upgrade/TPD.install-6.0.0_80.17.0- CentOS6.2-x86_64.iso	Available Attach	e Media Label	1	Im	age Path		1	
AN	Available Attach Attach	e Media Label tkic_000-00	00-000_Rev	Im A_80.16 ^{/m} 6.2	age Path edia/sdb1/000-0 -x86_64.iso	000-000-6.0.0	_80.16.0-Ce	entOS-
	Available Attach Attach Attach	e Media Label tkic_000-00 tkic_000-00	00-000_Rev 00-000_Rev	Im _A_80.16 ^{/m} _A_80.17 ^{Na} Ce	age Path edia/sdb1/000-0 -x86_64.iso r/TKLC/upgrade. ntOS6.2-x86_64	1000-000-6.0.0 /TPD.install-6.1	_80.16.0-Ce 0.0_80.17.0-	entOS-

- 3. PM&C GUI: Navigate to Manage Software Images Navigate to Main Menu ➤ Software ➤ Manage Software Images
 - Main Menu
 Hardware
 Software
 Software Inventory
 Manage Software Images
 Storage
 Administration
 Task Monitoring
 Logout
- 4. **PM&C GUI:**Add image Press the **Add Image** button .

Manage Software Images

Tasks 🔻					
	Incore Manua	Turne	Anabitaatuus	Description	
	image Name	туре	Architecture	Description	
	PMAC4.0.0_40.11.0872-2291-101i386	Upgrade	i386		
	PMAC4.0.0_40.15.0872-2291-101i386	Upgrade	i386		
	TPD5.0.0_72.28.0x86_64	Bootable	x86_64		
	TPD5.0.0_72.24.0i386	Bootable	i386		
	PMAC4.0.0_40.14.1872-2291-101i386	Upgrade	i386		
	Add Image	Edit Image	Delete Ir	nage	

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.

Add Soft	ware Image	⊘ _Help
Images may	v be added from any of these sources:	
Tekel	lec-provided media in the PM&C host's CD/DVD drive (See Not	e)
• USB	media attached to the PM&C's host (See Note)	
Extern	nal mounts. Prefix the directory with "extfile://".	
• These	e local search paths:	
Nar Nar	r/TKLC/upgrade/*.iso r/TKLC/smac/image/isoimages/home/smacftpusr/*.iso	
Note: CD and	d USB images mounted on PM&C's VM host must first be mad	le accessible to the PM&C VM guest. To do
this, go to the	e Media tab of the PM&C guest's View VM Guest page.	
Path:	/var/TKLC/smac/image/isoimages/home/smacftpusr/872-229	90-104-2 🔻
Description:	/var/TKLC/smac/image/isoimages/home/smactpusr/872-229 var/TKLC/smac/image/isoimages/home/smactpusr/872-244 /var/TKLC/smac/image/isoimages/home/smactpusr/872-244 device://dev/sr0 device://dev/sr1 device://dev/sr2 device://dev/sr3	90-104-2.0.0 80.14.0-TVOE-x86_64.iso 41-101-5.0.0_50.6.0-PMAC-x86_64.iso 64-101-5.0.0_50.10.0-ALEXA-x86_64.iso
	Add New Image	

6. PM&C GUI Monitor the Add Image status

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

Manage Software Images

Thu Nov 17 18:28:11 2011 UTC • Info Tasks 💌 Info 8 Software image /var/TKLC/upgrade/872-2290-101-1.0.0_72.24.0-TVOE-x86_64.iso will be added in the background. • 1 The ID number for this task is: 5. TPD--5.0.0_72.28.0--X80_04 B00(able x80_04 TPD--5.0.0_72.24.0--i386 Bootable i386 PMAC--4.0.0_40.14.1--872-2291-101--i386 Upgrade i386 Delete Image Add Image Edit Image

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:

lelp

🤌 Help

Manage Software Images

						18:31:19 201
· • []	Tasks	Y				
	Tasks					
	ID	Task	Target	Status	Start Time	Progress
E	5	Add Image		Done: 872-2290-101-1.0.0_72.24.0- TVOE-x86_64	2011-11-17 13:31:19	100%
- 1						

8. **PM&C GUI:** Detach the image from the PM&C guest

If the image was supplied on CD or USB, return to the PM&C guest's "**Media**" tab used in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use. Remove the CD or USB device from the Management Server.

APPENDIX G. UPGRADE SINGLE SERVER – UPGRADE ADMINISTRATION

This Appendix provides the procedure for upgrading a DSR single server of any type (NO, SO, MP, etc).

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

S	This procedure executes the Upgrade Single Server – Upgrade Administration steps.
T E	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 the Tekelec Customer Care Center and ask for UPGRADE ASSISTANCE.

NO GUI – Upgrade Administration: View the pre-upgrade status of Servers	From the A Select Upg (DSR 4.x: DSR 5.x: ⁴ The Upgrad	Active NO Irade Adn "Adminis " Adminis de Adminis	GUI: tration > U tration -> stration scr	n form pgrac Softv een is	le" vare Manag displayed	gement -> Upgr (example below)	ade")
	Note: Look releases, th <u>Upgrade S</u>	and feel one procedu	of the Upgraure below p DSR 4.x	ade so provide	creen has c es the snap	hanged betweer shot from both th	n DSR 4.x and DSR 5.x ne releases.
			Network Elem	ent		Role	Upgrade State
	Hostname		Application Ve	ersion		Function	Server Status
	NOL		NO_HPC03			NETWORK OAI	M&P Not Ready
	1101		4.0.0-40.14.1			OAM&P	<u></u>
	NO2		NO_HPC03 4.0.0-40.14.1			NETWORK OAI OAM&P	M&P Not Ready Norm
	MP1		NO_HPC03			MP DSR (active/standby	Not Ready Norm
	MP2		NO_HPC03			DSR (active/standby	Not Ready
	Upgrade S Hostname	Creen in Server Status OAM Max HA Ro Max Allowed HA Role Norm	DSR 5.x Server Role Network Element Application Version Network OAM&P	Function	Upgrade State Start Time Upgrade ISO Not Ready	Status Message Finish Time	Mate Server Status
	Viper-NO1	Active Active Norm	NO_Viper 5.0.0-50.15.1 Network OAM&P	OAM&P	Not Ready		[Viper-NO2]
	Viper-NO2	Standby Active	NO_Viper 5.0.0-50.15.1				Viper-NO1
	Viper-SO1-A	Norm Active Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-B
	Viper-SO1-B	Norm Standby Active	System OAM SO1_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO1-A
	Viper-SO2-A	Norm Active Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-B
	Viper-SO2-B	Norm Standby Active	System OAM SO2_Viper 5.0.0-50.15.1	OAM	Not Ready		Viper-SO2-A
	Viper-MP05	Norm	MP	DSR (multi- active cluster)	Not Ready		Viper-MP06
		Active Active	SO1_Viper 5.0.0-50.15.1				
	The follow Active NO s Alarm ID	Active Active ing statu server will = 10008	son_Viper 5.0.0-50.15.1 Is may be of have the for (Provisionin	expec ollowir ng Ma	t ed: ng expected nually Disa	d alarm: bled)	
	Servers wit Alarm ID Alarm ID have been Alarm ID	h replicati = 31113 = 10075 manually = 31228	on disabled (Replication (The server stopped (re (High Avail	d may n Man r is no esult o ability	have the fo ually Disab longer pro f make rea Server fail	ollowing expected led) viding services b dy) ed to receive ma	d alarms: ecause application process te heartbeats)

2	NO GUI – Upgrade	For the server to be upgraded:
	Administration: Verify status of Server to	1. Identify server NO, SO, MP, etc)(record name)
	be upgraded	2. Verify the Application Version value is the expected source software release version.
		3. Verify the Upgrade State is Not Ready .
		at Step 7
3	Identify key info for	Before executing this procedure, document the following information for this server upgrade:
	the server to be	For the cite:
	upgraueu	Is the source upgrade release {less than, greater than or equal to} DSR 4.1.0_41.16.0? Is the DA-MP redundancy for this site {(1+1), (N+0)}? Is the site 3-Tier or 2-Tier OAM?
		For this server: Is the server {3-tier NO, 2-Tier NO, SO, MP or other C level server} ? Is the server {Standby, Active}?
		You must have clear answers to these questions to proceed.
		NOTE: if the server is part of an Active/Standby pair, the following Make Ready step will cause a failover, and the server will become Standby.

Prepare Upgrade		ver to be u	pgraded.				
(step I)	On the Upg upgraded a	grade form and,	, make the s	server 'Upgrad	de Ready', by sele	ecting the serve	r to be
	Select: Pre	pare Upgr pare (lf D	ade (if DSR SR 5.x)	8 4.x)			
	(In this exa	mple, NO	with name "	NO2" will be r	nade ready for Up	ograde)	
	Note: Look	and feel o	f the Upgrad	de screen has	changed betwee	n DSR 4.x and	DSR 5.x
	Upgrade S	creen in C	SR 4.x	DVIDES THE SHA	ipsnot from dotn t	ne releases.	
	Hostnar	ne	Network Elem Application Ve	ent rsion	Role Function	Upgrade State Server Status	
	NOT		NO_HPC03		NETWORK OAM6P	Not Ready	
	1402		NO_HPC03		NETWORK OAM&P	Not Ready	
	1402		4.0.0-40.14.1		OAM&P	Norm	
	MP1		4.0.0-40.14.1		DSR (active/standby pair)	Norm	
			NO_HPC03		MP	Not Ready	
	MP2		4.0.0-40.14.1		OSR (active/standby pair)	30	
	Prepar	e Upgrade	liate Upgrade	Monitor Upgrade	Complete Upgrade	o+o Accept Upgrade	
	Prepar Upgrade S	e Upgrade	late Upgrade	Monitor Upgrade	Complete Upgrade	eee Accept Upgrade	
	Prepar Upgrade S	e Upgrade Screen in D Server Status OAM Max NA Role	DSR 5.x Server fielde Network Element	Monifor Upgrade sction Upgrade State Start Time	Complete Upgrade	o++ Accept Upgrade	
	Prepar Upgrade S Hostname	e Upgrade Screen in D Server Status OAM Max NA Role Max Allowed Max Object	Liste Upgrade. DSR 5.x Server Role Network Element Application Version	Monflor Upgrade Stati Start Time Upgrade ISO	Complete Upgrade Status Message Finish Time	oee Accept Upgrade	
	Prepar Upgrade S Hostname NO1	e Upgrade Screen in L OAM Max HA Role Max Allowed MA Role Norm Active	DIST DISTRICT DIST DISTRICT Server Role Fur Network Clement Application Version Network OMMSP DUST N DUST N DU	Nontior Upgrade State Start Time Upgrade ISO M&P Not Ready	Complete Upgrade	eee Accept Upgrade	
	Prepar Upgrade S Hostname NO1 NO2	e Upgrade Server Status OM Max HA Role Max Allowed Max Role Norm Active Active Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Active Standby Standby Active Standby Active Standby Standby Standby Standby Standby Standby Standby Standby Standby Active Standby Active Standby Standb	DIST Diggrade	Monitor Upgrade State Start Time Upgrade ISO W&P Not Ready M&P Not Ready	Complete Upgrade	eee Accept Upgrade	
	Prepar Upgrade S Hostname NO1 NO2 SO2	Screen in Li Server Status OAM Max HA Role Max Alowed HA Role Norm Active Active Active Active Norm Standby Active Norm Norm Standby Active Norm	Server Role Fur Server Role Fur Network Element Application Version No. DSR. VM 50.0-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151 Solo-50151	Monitor Upgrade State Start Time Upgrade ISO Ubgrade ISO W&P Not Ready W&P Not Ready M Not Ready	Complete Upgrade	o++o Accept Upgrade late Server Status 1022 1011	
	Prepar Upgrade S Hostname NO1 NO2 SO2 SO1	e Upgrade Server Status OAM Max HA Role Max Adoved Max Adoved Addve Addve Addve Standby Addve Norm Standby Addve Norm Addve Norm Addve Norm Addve Norm	Application Version Network Element Application Version Network CoMAPP 0.05,07,01 0.05,015,1 Solution Version No.05,015,1 Solution Version Solution Version Solution Solution Version Solution So	Monitor Upgrade State Start Time Upgrade State Start Time Upgrade ISO M&P Not Ready M& Not Ready M Not Ready R	Status Message Pinish Time P	Accept Upgrade	
	Viostname No1 No2 SO1 MP1	E Upgrade Screeen in E Server Status OAM Max HA Role Max Alove Max Alove Max Alove Adive Adive Adive Norm Adive Adive Norm Adive Adive Norm Adive Adive Stantby Adive Norm	Server Role Fur Server Role Fur Network Element Applradion Version Network Server Role Not Notor SAMS OAI Notorio CMASP OAI Solo-Soi 151 Server Role Solo-Soi 151 OAI	Monitor Upgrade State Start Time Upgrade ISO Upgrade State Upgrade State Upgrade ISO Upgrade ISO ISO Upgrade ISO Upgrade ISO ISO Upgrade ISO ISO Upgrade ISO ISO ISO ISO ISO ISO ISO ISO ISO ISO	Status Message Finish Time I	•••• Accept Upgrade Iate Server Status V02] 001] 001] 001] 001] 002]	
	Prepar Upgrade S Hostname NO1 NO2 SO2 SO1 MP1 MP2	E Upgrade Server Status OM Max HA Role Max Allowed Max Allowed Max Allowed Active Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Active Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Standby Active Norm Active Norm Standby Active Norm Active Norm Norm Active Norm Standby Active Norm Active Active Norm Active Active Active Norm Standby Active Norm Active Active Norm Active Active Norm Active Norm Norm Active Norm Active Norm Active Norm Active Norm Norm Active Norm Norm Active Norm Norm Active Norm	Intel Upgrade Server Role Fur Network Element Application Version Application Version OA So.D.SR_VM So.D.So.15.1 Network Count OA So.D.SR_VM So.D.So.15.1 System OAM OA So.D.SS.VM So.D.So.15.1 So.D.SS.VM So.D.SS.VM	Upgrade State Start Time Upgrade ISO Upgrade ISO MSP Not Ready Mash Not Ready	Status Message Finish Ture I	•••• Accept Upgrade Iate Server Status ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••01 ••02 ••02 ••01 ••02 ••02 ••02 ••02 ••02 ••02 ••02 ••02 ••01 ••02 ••02 ••02 ••02 ••02 ••02 ••03 ••04 ••05 ••05 ••05 ••05 ••05 ••05 ••05 ••05	
	VDggrade S Hostname N01 N02 S02 S01 MP1	Screen in LC Server Status OM Max HA Role Max Alove Max Alove Max Alove Active Active Active Active Norm Active Active Norm Active Active Norm Active Active Active Norm Active A	Anto Upgrade Server Role Server Role Server Role Retwork Element Application Version NO_DSR_VM 50.050151 Network CMARP OJSR_VM 50.050151 Sratem OAM S0.050151 Sratem OAM S0.050151 MP MP MP MP MP MP MP MP MP MP	Monitor Upgrade State Start Time Upgrade State Start Time Upgrade ISO MSP Not Ready MAP Not Ready Main Not Ready R Not Ready R R R Not Ready	Complete Upgrade	•••• Accept Upgrade Iate Server Status V02 001 001 001 002 001 001 001 001 001 001 001 001 001 001 001 001 001 001 001 001 002 001 002 001 002 001 002 001 002 001 002 001 002 003 004 005 005 005 005 005 005 005 005 005 005 005	

NO GUI – Upgrade Administration:	Upgrade form is displayed (see example below)
Prepare Upgrade	Note: Look and feel of the Lingrade screen has changed between DSR 4 x and DSR 5 x
(step 2)	releases, the procedure below provides the snapshot from both the releases.
	English Marchie Date
	For the Max Ha Kole:
	Active) (this will depend on the server being upgraded)
	2. IF the condition of the Server to be upgraded is as expected, then: Select: \mathbf{OK}
	Upgrade Screen in DSR 4.x
	Mon Oct 08 08:02+
	Selecting 'CK' will result in the selected server's Max HA Capability being set to 'Standby', 'Observer' for query servers, and its applications being disabled.
	Helecited Servert NU2
	Ok Cencel
	Upgrade Ready Criteria Selected Server Status Mate Status
	Max HA Role Standby Active
	Critical Alarms 0
	Minor Alams 0 0
	Database Server Status Norm Norm
	HA Server Status Norm Norm
	Process Server Status Norm Norm
	Apprication state Enabled Enabled
	Ok Cancel
	Upgrade Screen in DSR 5.x Main Menu: Administration -> Software Management -> Upgrade [Prepare]
	Hoteans Action IIA Status
	Max HA Role Active Mates Standby Mates Spare Mates
	NO2 Prepare V Standby NO1 None None
	Ok Cancel
	Note: If this is the active server in an active/standby pair, the Make Ready action
	WILL cause an HA switchover.
	If the server being upgraded is the active NOAM, the HA switchover will cause the
	GUI session to be automatically logged out. You can log back into the GUI using the NOAM VIP.
	For 2 tier Active-Standby Setup, the Make Ready action on DA-MP server MAY
	cause the value in the HA Status field under the Selected Server Status be shown
1	as 'Active' for both the DA-MP(s). This is OK. Please proceed with upgrade.

Upgrade Status =	READY (This may take a r	ninute)	
Hostname	Network Element	Role	Upgrade State
N01	Application Version NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Not Ready
N02	NO_HPC03 4.0.0-40.14.1	NETWORK OAM&P OAM&P	Ready Warn
MP1	NO_HPC03 4.0.8-40.14.1	MP DSR (active/standby pair)	Not Ready Norm
MP2	NO_HPC03 4.0.0-40.14.1	MP DSR (active/standby pair)	Not Ready
Depending on the Servers may have all alarms: Alarm ID = 1000 Alarm ID = 1007 have been manua	40.040.141 server being upgraded, ne a combination of the follov 08 (Provisioning Manually I 75 (The server is no longer Ily stopped)	(active/standby pair) w alarms may occur. ving expected alarms Disabled) providing services be	Note: Not all servers ecause application proc
	Hostname N01 N02 MP1 MP2 Depending on the Servers may have all alarms: Alarm ID = 1000 Alarm ID = 1000 bave been manua	Hostname Network Element Application Version N01 N0_HPC03 400-40.14.1 N02 4.00-40.14.1 N02 4.00-40.14.1 N0_HPC03 MP1 4.00-40.14.1 MP2 4.00-40.14.1 MP2 4.00-40.14.1 Depending on the server being upgraded, net Servers may have a combination of the follow all alarms: Alarm ID = 10008 (Provisioning Manually I Alarm ID = 10075 (The server is no longer base been manually stopped)	Notwork Element Role Application Version Function N01 N0_HPC03 NETWORK 0AM8P N01 4.0.0-40.14.1 0AM8P N02 N0_HPC03 NETWORK 0AM8P N02 N0_HPC03 NETWORK 0AM8P N02 N0_HPC03 NETWORK 0AM8P N02 N0_HPC03 MP MP1 4.0.0-40.14.1 OAM8P MP1 4.0.0-40.14.1 DSR (active/standby pair) MP2 4.0.0-40.14.1 DSR (active/standby pair) Depending on the server being upgraded, new alarms may occur. Servers may have a combination of the following expected alarms all alarms: Alarm ID = 10008 (Provisioning Manually Disabled) Alarm ID = 10075 (The server is no longer providing services be have been manually stopped)

NO GUI – Upgrade Administration : Initiate Upgrade on the server: Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x Initiate Upgrade (initiate) releases, the procedure below provides the snapshot from both the releases (part 1) Upgrade Screen in DSR 4.x While viewing the Upgrade Administration screen, select the server to be upgraded 1. Ensure that the "Initiate Upgrade" button is enabled for the server to be upgraded. 2. Click "Initiate Upgrade" button. 3. Network Element Upgrade State Role Hostname Application Version Function Server Status NO_HPC03 NETWORK OAM&P Not Ready N01 4.0.0-40.14.1 OAM8P Em NO_HPC03 NETWORK OAM&P Ready N02 4.0.0-40.14.1 OAM&P NO_HPC03 MP Not Ready DSR MP1 4.0.0-40.14.1 (active/standby Norm pair) NO_HPC03 MP Not Ready < 040 Monitor Upgrade Prepare Upgrade Initiate Upgrade Complete Upgrade Accept Upgrade Upgrade Screen in DSR 5.x While viewing the Upgrade Administration screen, select the server to be upgraded 1. Ensure that the "Initiate" button is enabled for the server to be upgraded. 2. 3. Click "Initiate" button. Server Status Server Role Function Upgrade State Status Message OAM Max HA Role Network Element Start Time Finish Time Mate Server Status Max Allowed HA Role Application Version Upgrade ISO Network OAM&P OAM&P Not Ready NO1 NO_DSR_VM NO2 Active 5.0.0-50.15.1 Network OAM&P OAM&P Ready NO2 NO_DSR_VM 5.0.0-50.15.1 System OAM OAM Not Ready S02 SO_DSR_VM Standb 5.0.0-50.15.1 Norm System OAM OAM Not Ready **SO1** SO_DSR_VM 5.0.0-50.15.1 DSR (multi-active cluster) Norm MP Not Ready MP2 MP3 MP4 MP1 SO_DSR_VM Standby 5.0.0-50.15.1 Backup ISO Cleanup Prepare Initiate Complete Accept Report

NO GUI – Upgrade Administration : Initiate Upgrade (part 2) – Select ISO form	The Initial [DSR 4.x: DSR 5.x: / The target Group and	Upgrade form w Administration Administration server is identif application ver	vill be displayed: • > Upgrade [In -> Software Ma fied with its asso sion)	itiate], anagement -> ociated data (H	• Upgrade [Initiate] lostname, Network E	lement, Server
	1. I	From the pick lisupgrade.	st at the lower le	ft of the form,	select the ISO to use	e in the server
	2. (t	Click the Start U the Upgrade Ad	Jpgrade button; Iministration so	the upgrade creen.	will begin and you wil	ll be returned to
					-	in victualitie
		Hostname	Network Element	Server Group	Application Version	
		N02	NO_HPC03	SGN01	4.0.0-40.14.1	
	872-2438	+110-40.0_40.141-DSR-x86	.64iso y Cancel Star	tUbgrade		

9	View In-Progress Status	View Upg	grade	Adminis	tration form	:						
		Note: Loo	ok an	d feel of	the Upgrad	e screen has	s chai	nged betweer	DSR 4.x	and DS	SR 5.x	
		Teleases,	uie k	JIOCEUUI	e below pro		apsno		le lelease	5.		
		Upgrade	Scre	en in DS	<u>SR 4.x</u> Upgrada S	toto of the e	onior	of interact				
		2.	For click	more det the Mor	tailed status	s of the upgra	ade fo	or a given ser	ver select	the ser	ver, and	
				2								
				Hostname	1	letwork Element		Role		Upgrade	State	
				1770 Societadoren 14	,	Application Version	1	Fund	tion	Server S	tatus	
				N01	1	NO_HPC03		NET	WORK OAM&P	Not Read	W.	
					4	1.0.0-40.14.1		CAM	8P	<u> </u>		
				N02	1	NO_HPC03		NET	WORK OAM8P	Upgradin	9	
				1402	1	10.0-40.14.1		OAM	8P	Nan		
					1	NO_HPC03		MP		Not Read	W	
				MP1				DSR	6	_		
						4.0.0-40.14.1		(act) pair)	ve/standby	Wan		
					1	NO_HPC03		MP		Not Read	¥	
				<								
						1	-	~	040			
				Prepare U	pgrade Initial	te Upgrade 🤇 Mo	onitor Up	grade Complet	e Upgrade 👘	Accept Upg	pade	
								/				
				The Ad	ministratio	n > Monitor	· Upgi	rade screen is	s displayed	l, and ι	upgrade	
		2	Wai	progres	s data is pr	esented.	· · ·	arada Stata	" under the	"Soru	or Stotuo"	
		З.	colu	mn will s	how "Succ	ess". This st	ep wi	Il take around	15-20 mir	nutes.	er Status	
			•									
		Upgrade 1.	Obs	erve the	<u>SR 5.x</u> Upgrade S	tate of the s	erver	of interest. U	pgrade sta	atus wil	lbe	
			disp	layed un	der the colu	umn "Status	Mess	age"	Status Massaga			
			Hostna	me	OAM Max HA Role	Network Element	uncuon	Start Time	Finish Time		Mate Server Status	
					HA Role	Application Version		Upgrade ISO				
			NO1		Active Active	NO_DSR_VM 5.0.0-50.15.1	JAWIGE	NorReady			NOZ	
			N02		Warn	Network OAM&P	DAM&P	Upgrading	state for IP: 192.168 IN_PROGRESS_ST	IPD task 1.1.12 is ATE	NO1	
					Standby Standby	NO_DSR_VM 5.0.0-50.15.1		2013-11-14 18:49:57 872-2526-101-5.0.0_50	15.1-DSR-x86_64.is	0		
			SO2		Warn Standby Active	System OAM C SO_DSR_VM 5.0.0-50.15.1	MAC	Not Ready			501	
			SO1		Warn Active	System OAM C SO_DSR_VM	MAC	Not Ready			<mark>502</mark>	
					Active	5.0.0-50.15.1						
		This step	Wait will t	for the u ake arou	ipgrade to o nd 15-20 m	complete. Th iinutes.	ie "Up	ograde State	' column w	ill shov	v "Success".	
		See ston	helov	N for inet	ructions if t	he l Ingrade (faile	or execution f	ime evcee	ds 30 r	ninutes	
		Note: If the	he up	grade pro	ocessing er	ne opgrade i ncounters a p	proble	em, it may att	empt to R	OLL BA	CK to the	
		original s	oftwa	re releas	se. In this c	ase, the Upg	grade	will be shown	n as "FAILI	ED".	le where	
		there was	s a pr	oblem.	y De SHOITE	i or ionger, c	lepen	ung on the p		upgrad		
			•									

10	Optional : View In-	Optional method to view Upgrade progress from a command line:
	command line of server	In case the user wants to view the detailed progress of the upgrade – Access the server command line (via ssh or Console), and:
		<pre># tail -f /var/TKLC/log/upgrade/upgrade.log</pre>
		Once the server has upgraded, it will re-boot, and then it will take a couple of minutes for the DSR Application processes to start up.
		This command will show the current rev on the server:
		<pre># appRev Install Time: Mon Oct 7 03:00:14 2013 Product Name: DSR Product Release: 5.0.0_50.12.5 Part Number ISO: 872-2526-101 Part Number USB: 872-2526-101 Base Distro Product: TPD Base Distro Release: 6.5.0_82.24.0 Base Distro ISO: TPD.install-6.5.0_82.24.0-CentOS6.4-x86_64.iso OS: CentOS 6.4</pre>
11	IF Upgrade Fails:	Access the server command line (via ssh or Console), and collect the following files:
		/var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log
		Contact Tekelec Customer Care by referring to Appendix K of this document and provide these files.
12	If upgraded server is: 2-Tier NO Server and	Execute following commands IF:
	(N+0) DA MP configuration	 SOURCE UPGRADE RELEASE is less than DSR 4.1.0_41.16.0
		Note: The following steps will inhibit replication to C level servers
		Log into upgraded NO server :
		# ssh root@ <standby ip="" no=""></standby>
		login as: root
		password: <enter password=""></enter>
		Note: Take the backup of TableDef table. We will be requiring this data to enable the replication once this site is successfully upgraded
		Execute following commands::
		<pre># iqt -Iarchiver -N TableDef > /var/TKLC/db/filemgmt/\$(hostname).TableDef_backup.xml</pre>
		Note: Re-verify if the backup file gets created in the /var/TKLC/db/filemgmt directory by executing the following command.
		<pre># ls -ltr /var/TKLC/db/filemgmt/\$(hostname).TableDef.backup</pre>
		Inhibit the A to C level replication

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

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

If upgraded server is:	SKIP THIS STEP I	F SOURCE UP	GRADE REL	EASE is less that	n DSR 4.1.0_41.16.0	
MP Server (or any C	Execute following o	ommande IE:				
level server)	Server is	MP or other C	level server			
	AND					
	SOURCE	UPGRADE R	ELEASE is g i	reater than or equ	ual to DSR 4.1.0_41.16.0	
	Note: The follo	wing steps	will allow	' 'A and B' lev	el replication to	
	upgraded C le	vel servers	i		•	
	Logisto Activo NO	(aithar 2 tion	ar 2 tian).			
	Log Into Active NO	(either 2-tier (or 3-tier):			
	# ssh root@	<active n<="" th=""><th>0 IP></th><th></th><th></th><th></th></active>	0 IP>			
	login as: :	root				
	password:	<enter pa<="" th=""><th>ssword></th><th></th><th></th><th></th></enter>	ssword>			
	Execute following c	ommand , whe	re the <serve< b=""></serve<>	e r name> is the na	me of the upgraded MP (or	
	other C level server	r:				
	<pre># iset -finl</pre>	hibitRepP	lans=' '	NodeInfo w	here	
	"nodeName='	<server n<="" th=""><th>ame>'"</th><th></th><th></th><th></th></server>	ame>'"			
	Notes After evenue	ing alarma ata	na ta anakia		D(a) na indiaatian an CUU	
	would be raised. \ Nodelnfo output.	ling above ste /erification of hibitRepPlan	ps to enable replication enable is field for all	nabling on MPs of the MP servers s	an be done by analyzing shall be empty:	
	[root@NO1 ~]# iqt	Nodelnfo	hostNom	o nodoConobility	inhihitPonPlana	
	siteld excludeTable	s	nostinam	enouecapability	IIIIIDIINEPFIAIIS	
	A1386.099	NO1	NO1	Active		
	NO_HPC3	SO1	SO1	Active		
	SO_HPC03	301	301	ACTIVE		
	C2254.131	MP2	MP2	Active		
	SO_HPC03	MD4		Activo		
	SO_HPC3	MP1	WP1	Active		
	NT . (C C 1	1.101	1	
	Note: This allow	s AB Replica	tion for the	upgraded C leve	a server, which was	
	inhibited during	the upgrade o	t the NOAN	4.		
If upgraded server is:						
MP server (or any C lever server)	IF the server be the following sto	ing upgraded eps must be	d is a MP (a executed o	ny C level serve nce the Upgrad	er), le State is "Success":	
Allow replication	From the estimation					
	From the active I					
	1. Select Status 2 Select the MP	& Manage > D	atabase. The	e Database Status	screen is displayed.	
	3. Click Allow R	eplication butto	on only if rep	olication is Inhibit	ed, Else move to next step.	

		•								
Network	< Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Statu
NO_HPC	C03	N01	Network OAM&P	Active	005	Normal	0	Normal	NotApplicable	Allowed
NO_HPC	C03	N02	Network OAM&P	Standby	00S	Normal	0	Normal	NotApplicable	Allowed
NO_HPO	C03	MP1	MP	Standby	Standby	Minor	0	Normal	Failed	Inhibited
NO HPO	C03	MP2	MP	Active	Active	Normal	0	Normal	Failed	Allowed
Disable	s Presidencias	Haw Doullockap Dador	Compose	000						Pause upd
Disable	e Provisioning Report	(Allow Replication) Backup	. Compare R	oto estore						Pause upd

Take the upgraded server out of the upgrade SUCCESS	Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type.								
<i>sta</i> te. (part 1)	Note : Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases								
	1. Se (D: DS 2. Ve sol 3. Ve 4. Ve <u>Upgrade Sc</u> 5. Ve 6. Cli	lect Upgrac SR4.x: "Adr R5.x: " Adr rify the App ftware relea rify status: rify the Upg reen in DSI rify the Cor ck Comple	le Adminis ninistratior ninistratior Dication V Ise version grade Stat R 4.x nplete Upgrad	tration h > Upg h -> So /ersior e of the grade e butto	screen grade" ftware Mana a value for th e server that button is ena on.	gement is serve was up abled for	-> Upgra r has bee graded is r the serv	ade") en update s Succes ver that w	ed to the target s . as upgraded
		Network	k Element		Role	Role Upgrade S		tate	
	Hostname	Applicat	tion Version		Function		Server Stat	us	
	N01	NO_HP	C03		NETWO	RK OAM&P	Not Ready		
		NO_HP	C03		NETWO	RK OAM&P	Not Ready	TO Not Ready	
	N02	4.0.0-40	1.14.1		OAM6P		Norm		
	MP1	NO_HP	NO_HPC03 4.0.0-40.14.1			MP Su DSR (active/standby 22		\$\$	
		NO_HP	C03		MP		Not Ready	8	
	<								
	<u>Upgrade Scr</u> 5. Ve 6. Cli	rify the Cor ck Comple Server Status	<u>R 5.x</u> nplete but te button. ^{Server Role}	ton is e	enabled for th	TE SEIVE	er that wa	as upgrad	led
	Hostname	OAM Max HA Role Max Allowed	Network Element Application Version	n	Start Time Upgrade ISO	Finish Time		Mate Server S	tatus
	NO1	Warn Active Active	Network OAM&P NO_DSR_VM 5.0.0-50.15.1	OAM&P	Not Ready			NO2	
	NO2	Warn Standby	Network OAM&P	OAM&P	Success 2013-11-14 18:49:57	Upgrade: Ta 192.168.1.1 indicating no 2013-11-14	sk result for IP: 2 is INVALID, ot needed. 18:52:32	NO1	
	SO2	Norm Standby Active	System OAM SO_DSR_VM 5.0.0-50.15.1	OAM	Not Ready	v. 19. 1-Dort-X8	04.130	S01	E
	S01	Norm Active	System OAM SO_DSR_VM	OAM	Not Ready			S02	
	Backup ISO Clear	Prepare .	Initiate Comple	te Acce	Pt Report				
	Take the upgraded server out of the upgrade SUCCESS state. (part 1)	Take the upgraded server out of the upgrade SUCCESS state. (part 1) Take the upgrades of regardless of Note: Look a releases, the releases, the releases, the 1. Se (D) 25. 1. Se (D) 25. Se (D) 25. 2. Ve (SO) 3. Ve (A) Ve (B) 25. Ve (B) 25. 3. Ve (A) Ve (B) 25. Ve (B) 25. 4. Ve (B) 2007ade Sc (S) Ve (B) 2007ade Sc (S)	Take the upgraded server out of the upgrade SUCCESS state. (part 1) Take the upgraded server regardless of type. Note: Look and feel of the releases, the procedure 1. Select Upgrad (DSR4.x: "Adr DSR5.x: "Adr 2. Verify the Upg software relea 3. Verify the Upg software Upg	Take the upgraded server out of the regardless of type. Upgrade SUCCESS state. (part 1) Take the upgraded server out of the regardless of type. Note: Look and feel of the Upgrade Administration DSR4.x: "Administration DSR5.x: "Administration 0. Verify the Application V 2. Verify the Upgrade State Upgrade Screen in DSR 4.x 5. Verify the Complete Upgrade No1 No_JPC03 No1 No_JPC03 No1 No_JPC03 MP1 40.040141 NO2 NO_JPC03 NO3 NO_JPC0	Take the upgraded server out of the upgrade server out of the upg	Take the upgraded server out of the upgrade ready st regardless of type. Note: Look and feel of the Upgrade screen has chang releases, the procedure below provides the snapshot (DSR4.: "Administration > Upgrade" DSR5.: "Administration > Upgrade " DSR5.: "Administration > Upgrade" DSR5.: "Administration > Upgrade " DSR5.: "Administration > Upgrade button is ena 6. Click Complete Upgrade button is ena 6. Click Complete Upgrade button is ena 6. Click Complete Upgrade button is ena 7. Upgrade <u>DSR111</u> 002 000-0111 002 000-0111 000 000 000 000 000 0000 0000	Take the upgraded server out of the upgrade ready state. Thi regardless of type. Wote: Look and feel of the Upgrade screen has changed betwere teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases, the procedure below provides the snapshot from bother teases were since. 3. Verify the Application Version value for this serve software felase version. 3. Verify the Upgrade State of the server that was up Upgrade State . (both is enabled for 6. Click Complete Upgrade button is enabled for 6. Click Complete Upgrade button. Note: Complete Upgrade Note: Complete Upgrade Note: Complete Upgrade Note: Complete Upgrade Note: Click Complete Dutton Note: Click Complete Duton . Not: Note: Complete Duton Note: Click Complete Duton Note: Click Complete Duton Note: Click Complete Duton . Not: Note: Complete Duton Note: Note	Take the upgraded server out of the upgrade ready state. This step and regardless of type. Note: Look and feel of the Upgrade screen has changed between DSI releases, the procedure below provides the snapshot from both the rel (DSR5,x: "Administration > Upgrade") DSR5,x: "Administration > Upgrade" DSR5,x: "Administration > Software Management > Upgrade Software release version. 3. Verify the Upgrade State of the server that was upgraded is Upgrade Screen in DSR 4,x 5. Verify the Upgrade State of the server that was upgraded for the server 6. Click Complete Upgrade button is enabled for the server 6. Click Complete Upgrade button is enabled for the server 6. Click Complete Upgrade button is enabled for the server 6. Click Complete Upgrade button is enabled for the server 7. Verify the Complete Upgrade button is enabled for the server 7. Verify the Complete Upgrade button is enabled for the server 7. Verify the Complete Upgrade button is enabled for the server 7. Verify the Complete Upgrade button 7. Verify the Complete button 7	Take the upgraded server out of the upgrade ready state. This step applies to a server out of the upgrade SUCCESS state. (part 1) Take the upgraded server out of the upgrade screen has changed between DSR 4.x and releases, the procedure below provides the snapshot from both the releases. 1. Select Upgrade Administration > Software Management > Upgrade") 2. Verify the Application Version value for this server has been updrate software release version. 2. Verify the Application Version value for this server has been updrate software release version. 3. Verify status: 4. Verify the Oupgrade State of the server that was upgraded is Success Upgrade Screen in DSR 4.x 5. Verify the Complete Upgrade button is enabled for the server that we 6. Click Complete Upgrade button is enabled for the server that we 7. Software Version

Talaa dha san maada d	Nata Laska		reen nas cna	nged between Da	SR 4.X and DSR 5.X			
Take the upgraded server out of the upgrade SUCCESS <i>sta</i> te. (part 2)	releases, the	Note: Look and feel of the Upgrade screen has changed between DSR 4.x and DSR 5.x releases, the procedure below provides the snapshot from both the releases						
	Upgrade Scr	een in DSR 4.x						
	The Upgrade [Remove Ready] screen is displayed							
	• Selecting 'Ok	K will result in the selected server's application being en	bled and the Max HA Capabil	ity of 'Active' set. 'Observer' is set for qu	ery servers.			
	Selected Server: NP1							
	Ok Cancel]						
	Upgrade Ready Criteria Sele Max HA Role Stan	ected Server Status Mate Status hdby Active						
	Critical Alarms 0 Major Alarms 0	0						
	Minor Alarms 2	4 m Warn						
	HA Server Status Nor	m Norm						
	Application State Disa	abled Enabled						
	Ok Cancel	1						
	Ungrade Scr	een in DSR 5 x						
	The Upgrade	[Complete] screen is dis	played					
	Hostname Action	HA Status Max HA Role Active Mates	Stan	ndby Mates	Spare Mates			
	NO2 Complete	Standby NO1	Nor	ne	None			
			Ok Cancel					
	 Click OF The Upg Wait for Upgrade minutes 	C. This completes the Reigrade Administration scree the screen to refresh and action link is disabled for for the Upgrade Ready S reen in DSR 4.x	nove Ready a en is displaye show the Up or the server the tate to chang	action on the serv ed. ograde Ready Sta hat was upgraded le to Not Ready .	rer. te is Not Ready and th d. It may take up to 2			
	 Click OF The Upg Wait for Upgrade minutes 	C. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x	nove Ready a en is displaye show the Up or the server ti tate to chang	action on the served. Ingrade Ready Sta hat was upgraded le to Not Ready .	rer. te is Not Ready and th d. It may take up to 2			
	 Click OF The Upg Wait for Upgrade minutes 	K. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element	nove Ready a en is displaye I show the Up or the server the tate to chang	action on the served. Igrade Ready Sta hat was upgraded le to Not Ready .	rer. te is Not Ready and th d. It may take up to 2 Upgrade State			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname 	K. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version	nove Ready a en is displaye I show the Up or the server th tate to chang	action on the served. Igrade Ready Stathat was upgraded to Not Ready. Role Function	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 	C. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03	nove Ready a en is displaye show the Up or the server ti tate to chang	Role Function Network OAMSP	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname No1 	C. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1 NO_HPC03	nove Ready a en is displaye show the Up or the server the tate to chang	Role Function NETWORK CAMEP NETWORK CAMEP	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 	K. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready Streen in DSR 4.x Network Element Application Version NO_HPC03 4.0.040.14.1	nove Ready a en is displaye I show the Up or the server th tate to chang	Role Function NETWORK OAMSP OAMSP	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready Norm			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 	K. This completes the Rep grade Administration scre the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40.14.1 NO_HPC03	nove Ready a en is displaye I show the Up or the server th tate to chang	Role Function NETWORK OAMSP OAMSP MP NETWORK OAMSP OAMSP MP NETWORK OAMSP OAMSP	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready Norm Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 	C. This completes the Reigrade Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4 0.0-40141 NO_HPC03 4 0.0-40141	nove Ready a en is displaye show the Up or the server to tate to chang	Action on the served. In the	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not Ready Not Ready Norm			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 	K. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready S Teen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40141 NO_HPC03 4.0.40141 NO_HPC03	nove Ready a en is displaye I show the Up or the server th tate to chang	Action on the served. In grade Ready State hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP	te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not Ready Not Ready Not Ready Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 	K. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready Streen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.40.14.1	nove Ready a en is displaye I show the Up or the server th tate to chang	Action on the served. Igrade Ready Stathat was upgraded hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby (active/standby)	Vpgrade State Server Status Not Ready Not Ready Not Ready Not Ready Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade 	C. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready Streen in DSR 4.x Network Element Application Version No_HPC03 4.0.40.14.1 No_HPC03 4.0.40.14.1 No_HPC03 4.0.40.14.1 No_HPC03 4.0.040.14.1 No_HPC03 4.0	nove Ready a en is displaye I show the Up or the server ti tate to chang	Role Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP	ver. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready Norm Not Ready TT Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade 	A. This completes the Reprode Administration scree the screen to refresh and e action link is disabled for the Upgrade Ready Streen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1	nove Ready a en is displayed show the Up or the server to tate to chang	Action on the served. Agrade Ready Stathat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP DSR (active/standby pail) MP DSR (active/standby emotione Upgrade	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready Not Ready Not Ready Not Ready Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr 	C. This completes the Reprode Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S Ceen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1 NO_HPC03	nove Ready a en is displayed show the Up or the server the tate to change a Upgrade	Action on the served. Agrade Ready State hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) OSR (active/standby Cather/standby Cather/standby Cather/standby Cather/Standby	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not Ready Not Ready Not Ready Not Ready Not Ready			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr Hostname 	A. This completes the Reprode Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.040.14.1 NO_HPC03 4.0.40.14.1 NO_HPC03	nove Ready a en is displayed show the Up or the server the tate to chang	Action on the served. In a se	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not Ready Not Ready Not Ready Not Ready TT Not Ready TT Not Ready Not Ready TT			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr Hostname 	A. This completes the Reprode Administration scree the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.0.40.14.1 N	nove Ready a en is displayed show the Up or the server that tate to chang	Action on the served. In grade Ready State hat was upgrader to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP DSR (active/standby Concluse Upgrader Status Message Finish Time	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready Not Ready Norm Not Ready Not Ready Norm Not Ready Mate Server Status			
	 Click OF The Upg Wait for Upgrade minutes Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr Hostname NO1 	C. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready S Ceen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1 NO_HPC03	nove Ready a en is displayed show the Up or the server the tate to chang or Upgrade State Start Time Upgrade ISO P Not Ready	Action on the served. Agrade Ready State hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP DSR (active/standby omplete Upgrade Status Message Finish Time	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not Ready Not Ready Worm Not Ready Not Ready Worm Not Ready Worm Not Ready Worm Not Ready Worm Not Ready Worm Not Ready Not Ready Not Ready Not Ready			
	2. Click OF 3. The Upg 4. Wait for Upgrade Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr Hostname NO1	A. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1 NO_HPC03	nove Ready a en is displayed show the Up or the server that tate to chang by Upgrade State Start Time Upgrade ISO P Not Ready P Not Ready	Action on the served. In grade Ready State hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP DSR (active/standby Complete Opgrade Status Message Finish Time	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready Not			
	2. Click OF 3. The Upg 4. Wait for Upgrade Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrade Upgrade Scr Hostname NO1 NO2	A. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready Streen in DSR 4.x Network Element Application Version NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.40.14.1 NO_HPC03 4.0.0.40.14.1 NO_HPC03 4.0.0.40.14 NO_HPC03 4.0.	nove Ready a en is displayed show the Up or the server to tate to chang or Upgrade State Start Time Upgrade ISO P Not Ready P Not Ready	Action on the served. In grade Ready State hat was upgrader to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby Cative/standby	eer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready 10 Not Ready			
	2. Click OF 3. The Upg 4. Wait for Upgrade Scr Hostname NO1 NO2 MP1 MP2 Prepare Upgrad Upgrade Scr Hostname NO1 NO2 S02	A. This completes the Reigrade Administration scrept the screen to refresh and e action link is disabled for for the Upgrade Ready S reen in DSR 4.x Network Element Application Version NO_HPC03 4.0.0-40.14.1 NO_HPC03	nove Ready a en is displayed show the Up or the server that tate to chang or Upgrade State Start Time Upgrade ISO P Not Ready P Not Ready	Action on the served. Ingrade Ready State hat was upgraded to Not Ready. Role Function NETWORK OAMSP OAMSP NETWORK OAMSP OAMSP MP DSR (active/standby pair) MP DSR (active/standby Cather/standby Cather/Sta	rer. te is Not Ready and th d. It may take up to 2 Upgrade State Server Status Not Ready TT Not Ready TOT Not Ready TT Not Ready TT TT Not Ready TT TT Not Ready TT TT Not Ready TT TT Not Ready TT TT TT TT TT TT TT TT TT T			

10	View Boot Llagrada	View Dest Upgrade Statue of the conver
10	Statua	view rost-opyrade Status of the server.
	Status.	
		1. Active NO(or SO for 3 – Tier setup) server will have some or all the following expected
		alarm(s):
		Alarm ID = 10075 (The server is no longer providing services because application processes
		have been manually stopped)
		Or
		Alarm ID = 31000 (Program impaired by S/W Fault)
		Alarm ID - 10008 (Provisioning Manually Disabled)
		Alarm $D = 10000$ (Stateful database not yet synchronized with mate database)
		Alarm $D = 20522$ (Server Lbgrade Dending Accent/Deject)
		Alam $D = 32332$ (Server Opgrade Fending Accept Reject)
		NOTE: Do Not Accept upgrade at this time. This alarm is OK.
		Servers that still have replication disabled will have the following expected alarm:
		Alarm ID = 31113 (Replication Manually Disabled)
10		
19	Procedure Complete.	I he single server upgrade is now complete.
		Return BACK to the overall DSR upgrade procedure step that directed you to execute
		Appendix G.
		11

APPENDIX H. UPGRADE FIRMWARE

Firmware Upgrade procedures are not included in this document. See Tekelec Customer Care by referring to Appendix K of this document for the latest info on Firmware upgrades.

APPENDIX I. NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

NOTE: Execute the following procedure to switch/migrate to having NetBackup installed via NBAutoInstall (Push Configuration) instead of manual installation using platcfg

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed and then complete TPD related tasks that are needed for effective Netbackup Client operation. With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *Netbackup Client Install/Upgrade with platcfg*.

Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

Prerequisites:

• Application server platform installation has been completed.

• Site survey has been performed to determine the network requirements for the application server and interfaces have been configured.

- NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server.
- Filesystem for Netbackup client software has been created (Create LV and Filesystem for Netbackup Client Software)

• Contact Tekelec to determine if the version of Netbackup Client being installed requires workarounds.

- Follow Tekelec Provided Workarounds Follow tekelec provided procedures to prepare the server for Netbackup Client install using nbAutoInstall.
- 2. **Application server iLO:** Login and launch the integrated remote console SSH to the application Server (PM&C or NOAM) as root using the management network for the PM&C or XMI network for the NOAM.
- 3. Enable nbAutoInstall:

Execute the following command: # /usr/TKLC/plat/bin/nbAutoInstall --enable The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly. At any time, the customer may now push and install a new version of Netbackup Client.

4. Return to calling procedure if applicable.

APPENDIX J. UPGRADE TVOE PLATFORM

This Appendix gives the procedure for upgrading TVOE on a host server that supports one or more DSR virtual guests.

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

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

Procedure 84: Upgrade TVOE

S	This procedure upgrades TVOE.					
T E	Check off (\checkmark) each step as it is completed. Boxes have been provided for this purpose under each step number.					
Е Р	SHOLU D THIS PROCEDURE FAIL CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR LIPCRADE ASSISTANCE					
#	SHOULD THIS PROCEDURE FAIL, CONTACT TERELEC TECHNICAL SERVICES AND ASK FOR UPGRADE ASSISTANCE.					
1	Disable all the	1. Log into the NOAM VIP GUI				
	applications running on current TVOF blade.	2. Select Status & Manage > Server ; the Server Status screen isis displayed				
		 Identify the NO of SO (virtual) servers that are running on the TVOE environment to be upgraded, and select these. 				
		4. Click the 'Stop' button.				
		5. Confirm the operation by clicking Ok in the popup dialog box.				
		6. Verify that the 'Appl State' for all the selected servers is changed to 'Disabled'.				
2	Find out the guests	1. Find out the guests running on TVOE host by using following command :				
	running on TVOE host.	# ssh root@ <tvoe ip=""></tvoe>				
		login as: root				
		password: <enter password=""></enter>				
		# virsh listall				
		Note: the output of above command will list all the guests running on current TVOE host.				
3	Shutdown each guest running on TVOE host.	1. Execute the following command for each guest identified in Step 2 :				
	· · · · · · · · · · · · · · · · · · ·	<pre># virsh shutdown <guestname></guestname></pre>				
4	Upgrade TVOE	1. Periodically execute following command until the command displays no entries. This				
		means that all VMs have been properly shut down :				
		# virsh list				
		2. Once all VMs have been properly shut down:				
		Ungrode TVOE using "DMAC Aided TVOE Ungrode Descedure" from Deference [0]				
		<i>TVOE 2.5 upgrade Document. 909-2276-001. V 1.0 or greater</i>				
		[If the "PMAC Aided TVOE Upgrade" procedure is not possible, it is also possible to upgrade TVOE using the alternate procedure provided in Reference [2].]				
		Note: If Active NO is hosted on the TVOE blade which is being ungraded, then VIP may				
		be lost till TVOE is successfully upgraded.				
5	After completed					
		After TVOE upgrade is completed on the Host Server, the Application(s) may not be started				
		automationity.				
		Proceed as below to restore service.				

Procedure 84: Upgrade TVOE

6	Verify Enable Virtual Guest Watchdog is set for VM	From PMAC VM Management form, verify that the "Enable Virtual Watchdog" is checked.					
		Virtual Machine Management					
		Tasks ▼ VM Entities to ⊙ — ■ Enc: 101 Bay: 8F Name: minilab BMAC					
		Enc: 101 Bay: 10F Host; fe80::7ae7:d1ff:feec:9540					
		Iminilab-PMAC-TVOE VM Info Software Network Media					
		Immilab-PMAC Num vCPUs: 1 Memory (MBs): 2,048 Enc: 101 Bay: 9F Memory (MBs): 2,048 Enable Virtual Watchdog:					
		Enc: 101 Bay: 1F Virtual Disks Prim Size (MB) Host Pool Host Vol Name Guest Dev Name Volume Guest Dev Name Volume Guest Dev Name 10240 vgguests minilab-PMAC_mg PRIMARY PMAC_logs img logs					
		Virtual NICs Host Bridge Guest Dev Name MAC Addr control control 52:54:00:b0:72:8d management management 52:54:00:a7:a3:05					
		Edit Delete Install OS Clone Guest Upgrade Regenerate Device Mapping ISO					
6	Start guests on TVOE host.	Execute following steps : a) Log into upgraded TVOE host by using following command : # ssh root @ <tvoe ip=""></tvoe>					
		login as: root					
		password: <enter password=""></enter>					
		 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></guestname> 					
		c) Periodically execute following command until the command displays all the VM guests running.					
		# virsh list					
7	Enable all the	Enable all the applications running on current TVOE blade:					
	step1	a) Select Status & Manage > Server; the Server Status screen isis displayed					
		 b) Select all the applications (NO(s)/SO(s)) running on current TVOE blade, excluding the server which is in upgrade 'Ready' state. Upgrade State can be verified from Administration->Upgrade screen. 					
		c) Click the 'Restart' button.					
		 Confirm the operation by clicking Ok in the popup dialog box. Verify that the 'Appl State' for all the selected servers is changed to 'Enabled'. 					

APPENDIX K. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A Representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request. The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

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

Tekelec – Global

Email (All Regions): support@tekelec.com

USA and Canada

Phone:

1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)
1-919-460-2150 (outside continental USA and Canada)
TAC Regional Support Office Hours:
8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

Caribbean and Latin America (CALA)

Phone:

+1-919-460-2150

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays • Argentina

Phone:

0-800-555-5246 (toll-free)

• Brazil

Phone: 0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

Chile

Phone:

1230-020-555-5468

- Colombia
 - Phone:

01-800-912-0537

- Dominican Republic
 - Phone:

1-888-367-8552

Mexico

Phone:

001-888-367-8552

• Peru

Phone: 0800-53-087

909-2277-001 Revision A, March 2014

 Puerto Rico Phone: 1-888-367-8552 (1-888-FOR-TKLC) Venezuela Phone: 0800-176-6497 • Europe, Middle East, and Africa **Regional Office Hours:** 8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays Signaling Phone: +44 1784 467 804 (within UK) Software Solutions Phone: +33 3 89 33 54 00Asia • India Phone: +91-124-465-5098 or +1-919-460-2150 TAC Regional Support Office Hours: 10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays Singapore Phone: +65 6796 2288 TAC Regional Support Office Hours: 9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays