Oracle® Communications

Diameter Signaling Router

DSR Cloud Software Upgrade Guide

Release 8.3

E93221-01

September 2018

ORACLE

Oracle® Communications Diameter Signaling Router, Cloud Software Upgrade User's Guide, Release 8.3

Copyright © 2011, 2018 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, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

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

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

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

See more information on My Oracle Support (MOS).

Table of Contents

1. Introduction ... 11
1.1 Purpose and Scope ... 11
1.1.1 What is Not Covered by this Document ... 11
1.2 References ... 11
1.3 Acronyms ... 11
1.4 Terminology ... 13
1.5 How to Use this Document ... 14
1.5.1 Executing Procedures ... 15
1.6 Recommendations ... 15
1.6.1 Frequency of Health Checks ... 15
1.6.2 Large Installation Support ... 15
1.6.3 Logging of Upgrade Activities ... 15
1.7 Warnings, Cautions, and Notes ... 16
1.7.1 Signaling Firewall ... 16
1.7.2 NetBackup 7.7 Support ... 16
1.7.3 Network IDIH Compatibility ... 16
1.7.4 Review Release Notes ... 17
1.7.5 Upgrade Check ... 17
2. General Description ... 17
2.1 Supported Upgrade Paths to 8.3 ... 17
2.2 Geo-Diverse Site (Active/Standby/Spare PCA Configuration) ... 19
2.3 Traffic Management During Upgrade ... 19
2.4 Automated Site Upgrade ... 19
2.4.1 Site Upgrade Execution ... 21
2.4.2 Minimum Server Availability ... 25
2.4.3 Site Upgrade Options ... 26
2.4.4 Cancel and Restart Auto Site Upgrade ... 27
2.5 Automated Server Group Upgrade ... 30
2.5.1 Cancel and Restart Automated Server Group Upgrade ... 30
2.5.2 Site Accept ... 31
3. Upgrade Planning and Pre-Upgrade Procedures ... 32
3.1 Required Materials and Information ... 32
3.1.1 Application ISO Image File/Media ... 33
3.1.2 Logins, Passwords and Server IP Addresses ... 33
3.2 Plan Upgrade Maintenance Windows ... 36

3.2.1 Calculating Maintenance Windows Required 37
3.3 Site Upgrade Methodology Selection 37
3.3.1 DA-MP Upgrade Planning 39
3.3.2 Pre-upgrade validation to avoid Comcol inter-connectivity issue between MPs 41
3.3.3 Maintenance Window 1 (NOAM Site Upgrades) 42
3.3.4 Maintenance Window 2 and Beyond (SOAM Site Upgrades) 42
3.4 Prerequisite Procedures 45
3.4.1 Required Materials Check 46
3.4.2 DSR ISO Administration 47
3.4.3 Data Collection — Verification of Global and Site Configuration Data 51
3.4.4 ISO Link Correction 61
3.4.5 Back Up TKLCConfigData Files 63
3.4.6 Full Backup of DB Run Environment at Each Server 64
3.4.7 IDIH Pre-Upgrade 67
3.5 Software Upgrade Execution Overview 68
3.5.1 Accepting the Upgrade 69
4. NOAM Upgrade Execution 69
4.1 NOAM Pre-Upgrade Checks and Backup 70
4.1.1 NOAM Health Check for Source Release 7.3, 7.4 71
4.1.2 NOAM Health Check for Source Release 8.0 and Later 74
4.1.3 NOAM Pre-Upgrade Backup 77
4.2 Disable Global Provisioning 78
4.3 NOAM Upgrade 79
4.4 Verify NOAM Post Upgrade Status 80
4.5 Allow Provisioning (Post NOAM Upgrade) 82
5. Site Upgrade Execution 83
5.1 Site Pre-Upgrade Activities 83
5.1.1 Site Pre-Upgrade Backups 84
5.1.2 Site Pre-Upgrade Health Checks 87
5.1.3 Site Upgrade Options Check 94
5.1.4 Disable Site Provisioning 95
5.2 Automated Site Upgrade 96
5.2.1 Site Upgrade Pre-Checks 96
5.2.2 Initiate Automated Site Upgrade 97
5.2.3 Rearrange Automated Site Upgrade Cycles 101
5.3 Automated Server Group/Manual Upgrade Overview 104
5.3.1 Site Upgrade Planning 106

5.3.2 SOAM Upgrade Overview 108
5.3.3 Upgrade SOAMs 109
5.3.4 Upgrade Iteration 3 111
5.3.5 Upgrade Iteration 4 125
5.3.6 Upgrade Iteration 5 132
5.4 Site Post-Upgrade Procedures 134
5.4.1 Allow Site Provisioning 134
5.4.2 Site Post-Upgrade Health Checks 134
5.4.3 Post-Upgrade Procedures 140
6. Backout Procedure Overview 141
6.1 Recovery Procedures 143
6.2 Backout Health Check 143
6.3 Disable Global Provisioning 147
6.4 Perform Emergency Backout 147
6.4.1 Emergency Site Backout 147
6.4.2 Emergency NOAM Backout 149
6.5 Perform Normal Backout 151
6.5.1 Normal Site Backout 151
6.5.2 Normal NOAM Backout 155
6.6 Back Out Single Server 156
6.7 Back Out Multiple Servers 161
6.8 Post-Backout Health Check 169
6.9 IDIH Backout 169
6.9.1 Oracle Server Backout 169
6.9.2 Mediation and Application Server Backout 169
Appendix A. Post Upgrade Procedures 170
Appendix A.1. Accept Upgrade 170
Appendix A.2. Undeploy ISO 172
Appendix A.3. Post Upgrade Accept Procedures 173
Appendix B. Increase Maximum Number of Open Files 174
Appendix C. Upgrade Single Server – DSR 8.x 177
Appendix D. Upgrade Single Server – Pre-DSR 8.0 183
Appendix E. Upgrade Multiple Servers – Upgrade Administration 190
Appendix F. IDIH Upgrade at a Site 198
Appendix F.1. Upgrade Oracle Guest 199
Appendix F.2. Upgrade the Mediation and Application Guests 202
Appendix G. Alternate Server Upgrade Procedures 202

Appendix G.1. Alternate Pre-Upgrade Backup 203
Appendix G.2. Server Upgrade Using platcfg 205
Appendix G.3. Manual DA-MP (N+0) Upgrade Procedure 208
Appendix G.4. ASG SBR Upgrade Procedure 209
Appendix G.5. Manual SBR Upgrade Procedure 209
Appendix H. Expired Password Workaround Procedure 213
Appendix H.1. Inhibit Password Aging 213
Appendix H.2. Enable Password Aging 215
Appendix H.3. Password Reset 216
Appendix I. Network IDIH Compatibility Procedures 217
Appendix J. Recover From a Failed Upgrade 218
Appendix K. Critical and Major Alarms Analysis 223
Appendix L. Additional Backout Steps 234
Appendix M. Additional Post-Backout Steps 237
Appendix N. Manual Completion of Server Upgrade 239
Appendix O. Identify the DC server 243
Appendix P. Limitations of Automated Server Group and Automated Site Upgrade 245
Appendix Q. Advanced Health Check Procedure 247
Appendix R. Workaround to Resolve DB Site Replication Alarms 250
Appendix S. Workaround to Resolve the Server HA Switchover Issue 251
Appendix T. Workaround to Resolve Device Deployment Failed Alarm 252
Appendix U. Workaround to Resolve syscheck Error for CPU Failure 254
Appendix V. Create a Link for ComAgent 255
Appendix W. Change SOAM VM Profile for Increased MP Capacity 256
Appendix X. My Oracle Support (MOS) 258
Appendix Y. Reset the SOAP Password 260

List of Tables

Table 1: Acronyms 11
Table 2: Terminology 13
Table 3. Server Selection vs. Server Group Function 24
Table 4. Site Upgrade Availability vs. Server Group Function 25
Table 5: Logins, Passwords, and Server IP Addresses 33
Table 6. Traffic Analysis Checklist 37
Table 7. DA-MP Upgrade Planning Sheet 40
Table 8. Prerequisite Procedures Overview 45

Table 9. Release Specific Data Collection Procedures 52
Table 10. IDIH Upgrade Preparation Overview 67
Table 11. NOAM Upgrade Execution Overview 69
Table 12. Site Upgrade Execution Overview 83
Table 13. Non-PCA/PDRA Site Upgrade Plan 105
Table 14. Two-Site Redundancy PCA Site Upgrade Plan 105
Table 15. Three-Site Redundancy PCA Site Upgrade Plan 105
Table 16. Site Upgrade Planning Sheet 106
Table 17. Site Upgrade Execution Overview 108
Table 18. SOAM Upgrade Execution Overview 109
Table 19. Iteration 3 Upgrade Execution Overview 111
Table 20. Iteration 4 Upgrade Execution Overview. 125
Table 21. Iteration 5 Upgrade Execution Overview 132
Table 22. Emergency Backout Procedure Overview 141
Table 23. Normal Backout Procedure Overview 142
Table 24. IDIH Upgrade Execution Overview 198
Table 25. High Impact Alarms 224
Table 26. Medium Impact Alarms 228

List of Figures

Figure 1. Example Procedure Steps Used in This Document 15
Figure 2. DSR 8.3.x Supported Upgrade Paths 19
Figure 3. Upgrade Perspective of DSR "Site" Topology 20
Figure 4. Site Upgrade – NOAM View 21
Figure 5. Site Upgrade - Entire Site View 22
Figure 6. Site Upgrade - Site Initiate Screen 23
Figure 7. Site Upgrade Monitoring 24
Figure 8. Server Group Upgrade Monitoring 25
Figure 9. Auto Site Upgrade General Options 26
Figure 10. Site Upgrade Active Tasks 27
Figure 11. Canceled Site Upgrade Tasks 28
Figure 12. Partially Upgraded Site 28
Figure 13. Restarting Site Upgrade 29
Figure 14. Active Tasks Screen 30
Figure 15. Site Accept Button 31
Figure 16. Site Accept Screen 31

Figure 17. Upgrade Maintenance Windows for 3-Tier Upgrade 36
Figure 18. Specialized Fixed Diameter Connections 245
Figure 19. Specialized Floating Diameter Connections 246
Figure 20. Specialized Distribution of DSR Features 246

List of Procedures

Procedure 1. Required Materials Check 46
Procedure 2. DSR ISO Administration 47
Procedure 3. Verification of Configuration Data 51
Procedure 4. Data Collection for Source Release 7.3, 7.4 52
Procedure 5. Data Collection for Source Release 8.0 and Later 57
Procedure 6. ISO Link Correction 61
Procedure 7. TKLCConfigData backup 63
Procedure 8. Full Backup of DB Run Environment for Release 7.3.x and Later 65
Procedure 9. IDIH Upgrade Preparation 68
Procedure 10. NOAM Health Check for Source Release 7.3, 7.4 71
Procedure 11. NOAM Health Check for Source Release 8.0 or Later 74
Procedure 12. NOAM Pre-Upgrade Backup 77
Procedure 13. Disable Global Provisioning 78
Procedure 14. NOAM Upgrade 79
Procedure 15. Verify NOAM Post Upgrade Status 80
Procedure 16. Allow Provisioning (Post NOAM Upgrade) 82
Procedure 17. Site Pre-Upgrade Backups 84
Procedure 18. Site Pre-Upgrade Health Check for Release 8.0 and Later 88
Procedure 19. Site Pre-Upgrade Health Check for Release 7.x 91
Procedure 20. Site Upgrade Options Check 94
Procedure 21. Disable Site Provisioning 95
Procedure 22. Site Upgrade Pre-Checks 96
Procedure 23. Automated Site Upgrade 97
Procedure 24. Rearrangement of upgrade cycles for Automated Site Upgrade 101
Procedure 25. SOAM Upgrade Pre-Checks 109
Procedure 26. Automated SOAM Upgrade (Active/Standby) 110
Procedure 27. Manual SOAM Upgrade (Active/Standby/Spare) 110
Procedure 28. Upgrade Iteration 3 112
Procedure 29. Upgrade Iteration 4 125
Procedure 30. Upgrade Iteration 5 132

Procedure 31. Allow Site Provisioning 134
Procedure 32. Site Post-Upgrade Health Check 135
Procedure 33. Alternate SOAM Post-Upgrade Health Check 138
Procedure 34. Post-Upgrade Procedures 140
Procedure 35. Backout Health Check 143
Procedure 36. Disable Global Provisioning 147
Procedure 37. Emergency Site Backout 148
Procedure 38. Emergency NOAM Backout 149
Procedure 39. Normal Site Backout 151
Procedure 40. Normal NOAM Backout 155
Procedure 41. Back Out Single Server 156
Procedure 42. Back Out Multiple Servers 161
Procedure 43. Post-Backout Health Check 169
Procedure 44. Accept Upgrade 170
Procedure 45. Undeploy ISO 172
Procedure 46. Post Upgrade Accept Procedure. 173
Procedure 47. Increase Maximum Number of Open Files 174
Procedure 48. Upgrade Single Server – Upgrade Administration – DSR 8.x 177
Procedure 49. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x 183
Procedure 50. Upgrade Multiple Servers – Upgrade Administration 190
Procedure 51. Upgrade Oracle Guest 199
Procedure 52. Upgrade the Mediation and Application Guests 202
Procedure 53. Alternate Pre-Upgrade Backup 203
Procedure 54. Server Upgrade Using Platcfg 205
Procedure 55. Manual DA-MP (N+0) Upgrade Procedure 208
Procedure 56. ASG SBR Upgrade 209
Procedure 57. Manual SBR Upgrade Procedure 209
Procedure 58. Expired Password Workaround Procedure 214
Procedure 59. Expired Password Workaround Removal Procedure 215
Procedure 60. Expired Password Reset Procedure 216
Procedure 61. Enable IDIH 8.x Compatibility 217
Procedure 62. Disable IDIH 8.x Compatibility 217
Procedure 63. Recover from a Failed Upgrade 218
Procedure 64. Verify Critical and Major Alarms in the System Before the Upgrade 223
Procedure 65. Additional Backout Steps for NOAM, SOAM, and SBR Server(s) 234
Procedure 66. Additional Post Backout Steps for NOAM, SOAM, and SBR Server(s) 237
Procedure 67. Manual Completion of Server Upgrade 239

Procedure 68. Identification of the DC server 243
Procedure 69. Firewall Check for DNS Port 53 247
Procedure 70. Workaround to Resolve DB Site Replication Alarms 250
Procedure 71. Resolve the HA Switchover Issue on Affected Server(s) 251
Procedure 72. Resolve Device Deployment Failed Alarm 252
Procedure 73. Workaround to Resolve syscheck Error for CPU Failure 254
Procedure 74. Create a Link for ComAgent 255
Procedure 75. Change SOAM VM Profile for Increased MP Capacity 256
Procedure 76. Reset the SOAP Password 260

1. Introduction

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform the following upgrades:

- Major upgrade from DSR 7.3, 7.4, 8.0, 8.1.x, 8.2.x to 8.3
- Incremental upgrade from an earlier DSR 8.2 build to a later 8.2 build

The upgrade of cloud deployments is covered by this document. The audience for this document includes Oracle customers as well as following internal groups: Software Development, Quality Assurance, Information Development, and Consulting Services including NPx. This document provides instructions to execute any incremental or major cloud software upgrade.

The execution of this procedure assumes that the target DSR 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.

Note: To understand the capacity/performance impact of this software release, refer to the [8] DSR 8.3 Cloud Benchmarking document.

1.1.1 What is Not Covered by this Document

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

- Distribution of DSR 7.x/8.x software loads. It is recommended to contact MOS for the software loads as described in Appendix X.
- Initial installation of DSR software. Refer to [1].
- SDS installation. Refer to [2].

1.2 References

[1] DSR 8.3 Cloud Installation Guide

[2] SDS Cloud Installation document

[3] Maintenance Window Analysis Tool CGBU_010314

[4] Fast Deployment and Configuration Tool Technical Reference, CGBU_ENG_24_2353

[5] Cloud DSR 8.2 Disaster Recovery Guide

[6] Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) In DSR 7.3 By Enabling SCTP AUTH Extensions By Default, OSD 2019141.1

[7] DSR Alarms and KPIs Reference

[8] DSR 8.3 Cloud Benchmarking document

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1: Acronyms

Acronym	Meaning
ASG	Automated Server Group upgrade

Acronym	Meaning
ASU	Automated Site Upgrade
CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
DA	Diameter Agent
DA MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
DSR DR NOAM	Disaster Recovery DSR NOAM
FABR	Full Address Based Resolution
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
HA	High Availability
IDIH	Integrated Diameter Intelligence Hub
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
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent
SBR	Session Binding Repository
SDS	Subscriber Database Server

Acronym	Meaning
SOAM	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
XSI	External Signaling Interface
vSTP	Virtual Signaling Transfer Point

1.4 Terminology

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

Table 2: Terminology

Term	Definition
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 8.0 to 8.2.
Incremental Upgrade	An upgrade within a given DSR release e.g. 8.2.x to 8.2.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Source Release	Software release to upgrade from
Target Release	Software release to upgrade to
Single Server Upgrade	The process of converting a DSR 8.2 server from its current release to a newer release.
Backout	The process of converting a single DSR 8.2 server to a prior version. This could be performed due to failure in Single Server Upgrade or the upgrade cannot be accepted for some other reason. Backout is a user initiated process.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.
Primary NOAM Network Element	The network element that contains the active and standby NOAM servers in a DSR.
Signaling Network Element	Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. Each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element.
Site	Physical location where one or more network elements reside. The site is defined by the SOAM.

Term	Definition
Geographic Site	A Geographic Site is defined as the physical location of a SOAM and its co-located children, as well as its non-preferred spare SOAM(s). In this document, a Geographic Site is designated as **GSite**.
Topological Site	A Topological Site is defined as a SOAM Server Group and all C-level Server Groups that are children of the SOAM. All servers within a server group belong to the server group's site, regardless of the physical location of the server. Thus, for upgrade, a Topological Site does not correlate to a 'network element' or a 'place'. In this document, a Topological Site is designated as **TSite**.
Health Check	Procedure used to determine the health and status of the DSR's internal network. This includes status displayed from the DSR GUI and PM&C GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
Upgrade Ready	State that allows for graceful upgrade of a server without degradation of service. It is a state that a server is required to be in before upgrading a server. The state is defined by the following attributes: • Server is Forced Standby • Server is Application Disabled (signaling servers do 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.
N+0	Set up with N active DA-MP(s), but no standby DA-MP.
NOAM	Network OAM for DSR.
SOAM	System OAM for DSR.
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (active/standby) policy to N+ 0 (multiple active) policies.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

1.5 How to Use this Document

1. When executing the procedures in this document, there are a few key points which help to ensure that the user understands procedure convention. These points are: Before beginning a procedure, completely read the instructional text (it displays 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. It is recommended to contact for assistance, before attempting to continue.

1.5.1 Executing Procedures

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- 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 step has a checkbox the user should check to keep track of the progress of the procedure.

The Title column describes the operations to perform during that step.

Each command the user enters, and any response output, is formatted in 10-point `Courier` font.

	Title/Instructions	Directive/Result Steps
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 1. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.6 Recommendations

This section provides some recommendations to consider when preparing to execute the procedures in this document.

1.6.1 Frequency of Health Checks

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

1.6.2 Large Installation Support

For large systems containing multiple Signaling Network Elements, it is impossible to upgrade multi-site systems in a single 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.

1.7 Warnings, Cautions, and Notes

This section presents notices of warnings and cautions that directly relate to the success of the upgrade. It is imperative that each of these notices be read and understood before continuing with the upgrade. If there are any conflicts, issues, or questions related to these notices, it is recommended to contact before starting the upgrade.

1.7.1 Signaling Firewall

Signaling firewall remains disabled when upgrade is done from Pre 8.x release to 8.x release. If there is need to enable the signaling firewall after upgrade to 8.x release, then there are some limitations.

!!WARNING!! After the upgrade to release 8.2, signaling firewall cannot be enabled when there is at least one SCTP multi-homed connection is enabled.

A **Cannot enable Signaling Firewall** error message displays when there is at least on SCTP multi-homed connection.

Also, if the signaling firewall is enabled after the upgrade, the SCTP multi-homed connections cannot be enabled.

A **SCTP Multi-homed connections cannot be enabled when Signaling Firewall is administratively enable** error message displays.

!!WARNING!! After the upgrade to release 8.2, SCTP multi-homed connection cannot be enabled if signaling firewall is already enabled.

1.7.2 NetBackup 7.7 Support

NetBackup 7.7 requires additional disk space that is not available prior to DSR release 8.2. Thus, the DSR must be upgraded to Release 8.0 or later before upgrading to NetBackup 7.7.

!!WARNING!! Upgrade DSR to release 8.2 before upgrading to NetBackup 7.7.

1.7.3 Network IDIH Compatibility

Upgrading an IDIH site to release 8.2 makes it incompatible for viewing network trace data contained in remote IDIH sites that are running a prior release. The incompatibility is removed once all Network IDIH systems have been upgraded to release 8.2.

To view network traces for a network of IDIH systems where there is a mix of systems running release 8.2 and systems running a prior release, Procedure 61 in Appendix I must be executed to prepare the systems running IDIH release 8.2 to support IDIH systems running the prior release. After executing Procedure 61, network traces should be viewed only from an IDIH system running the prior IDIH release. Viewing a network trace from an IDIH 8.2 results in a visualization that is incomplete because the IDIH 8.2 system fails to retrieve Trace Transaction Records (TTRs) from IDIH systems running the prior IDIH release.

When all IDIH systems have been upgraded to release 8.2, Procedure 62 should be executed on each IDIH system where Procedure 61 was previously executed to ensure that no errors occur when viewing network traces.

1.7.4 Review Release Notes

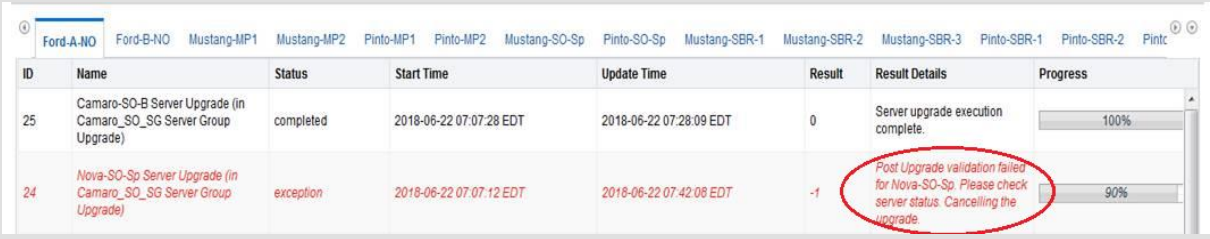
Before starting the upgrade, it is recommended to review the Release Notes for the target release to understand the functional differences and possible traffic impacts of the upgrade.

1.7.5 Upgrade Check

!!WARNING!!

If this error displays, contact .

```
"Post Ugrade validation failed for <server_name>.  Please check server status.  Cancelling the upgrade."
```



CAUTION If your deployment includes both FABR and PCA, then upgrade the DSR nodes first before upgrading the SDS nodes.

2. General Description

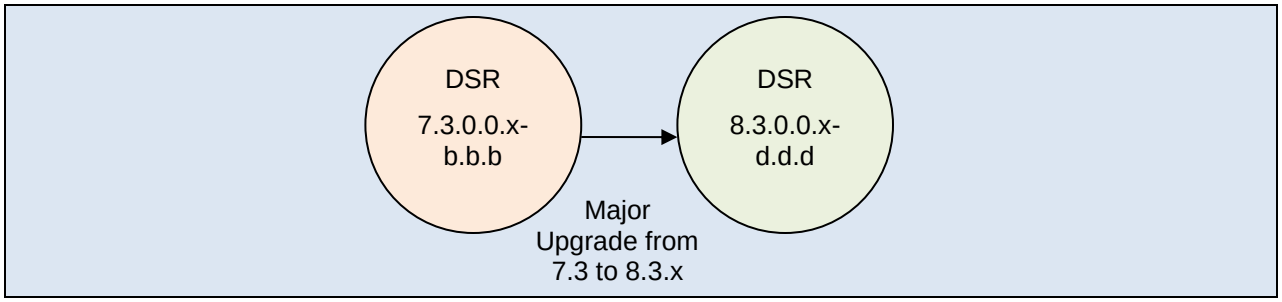
This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 7.x to target release 8.2. An incremental upgrade advances the DSR from an earlier DSR 8.2 source release to a more recent 8.2 target release.

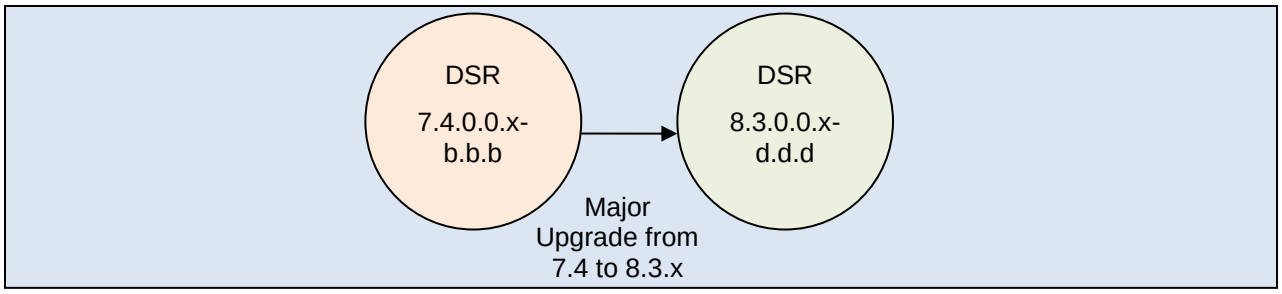
Note: With any incremental upgrade, the source and target releases must have the same value of **x**. For example, advancing a DSR from 8.2.0.0.0-82.3.0 to 8.2.0.0.0-82.4.0 is an incremental upgrade. But, advancing a DSR running a 7.2 release to an 8.2 target release constitutes a major upgrade.

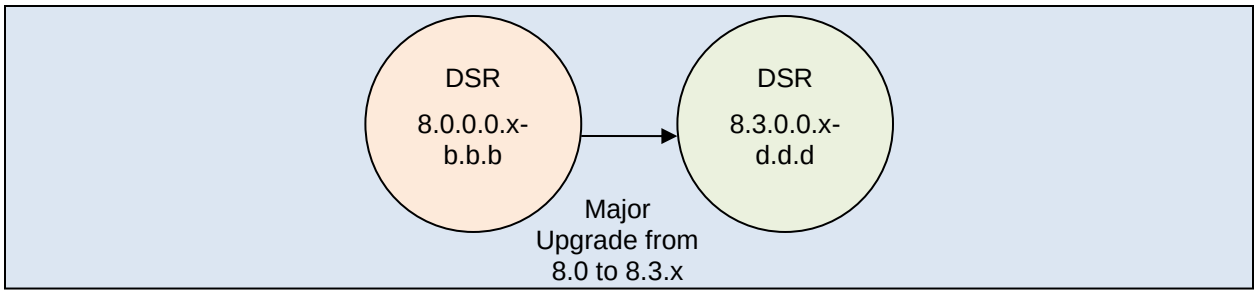
2.1 Supported Upgrade Paths to 8.3

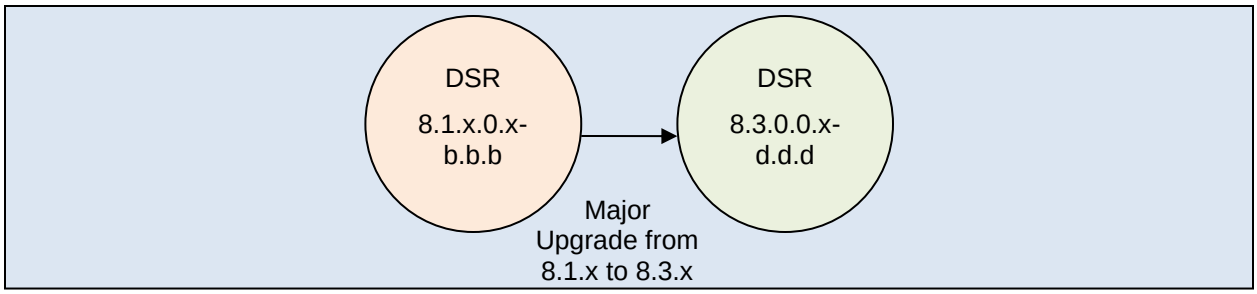
The supported paths to upgrade to a DSR 8.3 target release are shown in Figure 2.

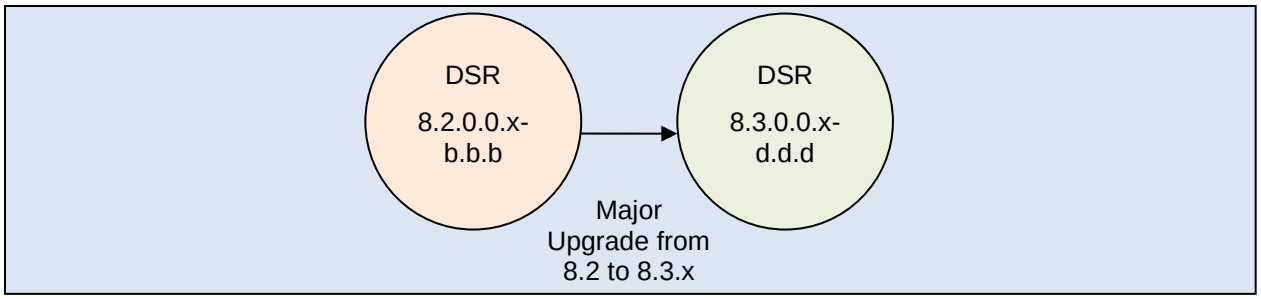
Note: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.


DSR
7.3.0.0.x-
b.b.b
DSR
8.3.0.0.x-
d.d.d
Major
Upgrade from
7.3 to 8.3.x


DSR
7.4.0.0.x-
b.b.b
DSR
8.3.0.0.x-
d.d.d
Major
Upgrade from
7.4 to 8.3.x


DSR
8.0.0.0.x-
b.b.b
DSR
8.3.0.0.x-
d.d.d
Major
Upgrade from
8.0 to 8.3.x


DSR
8.1.x.0.x-
b.b.b
DSR
8.3.0.0.x-
d.d.d
Major
Upgrade from
8.1.x to 8.3.x


DSR
8.2.0.0.x-
b.b.b
DSR
8.3.0.0.x-
d.d.d
Major
Upgrade from
8.2 to 8.3.x

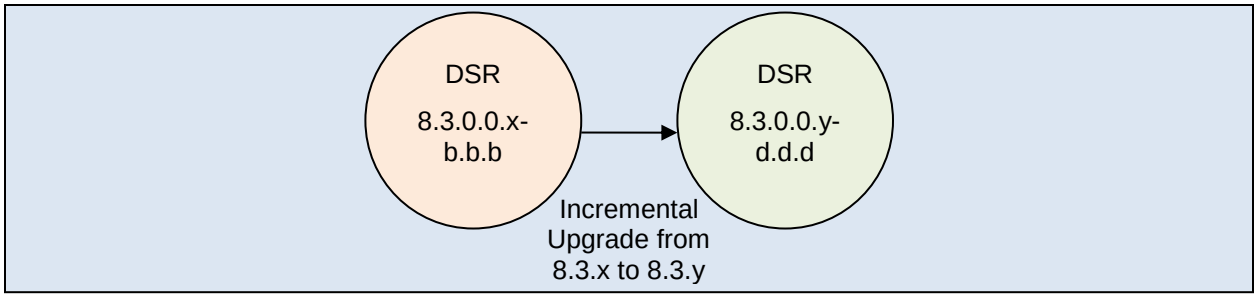


Figure 2. DSR 8.3.x Supported Upgrade Paths

2.2 Geo-Diverse Site (Active/Standby/Spare PCA Configuration)

With a geo-diverse site, the upgrade of the SOAM active/standby servers must also include an upgrade of the spare SOAM at the geo-redundant site, in the same maintenance window.

2.3 Traffic Management During Upgrade

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

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

!!WARNING!! SCTP Datagram Transport Layer Security change.

Oracle introduced SCTP Datagram Transport Layer Security (DTLS) in DSR 7.3 by enabling SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced in [6]. It is highly recommended that customers upgrading to Release 8.2 should prepare clients before the DSR is upgraded. This ensures the DSR-to-Client SCTP connection establishes with DTLS with SCTP AUTH extensions enabled.

If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices DO NOT restore after the DSR is upgraded to DSR 8.2. In the event that the SCTP connections do not re-establish after the upgrade, follow the Disable/Enable DTLS procedure in [1].

2.4 Automated Site Upgrade

There are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature upgrades an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade automatically prepares the server(s), performs the upgrade, and sequences to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity.

Automated Site Upgrade can be used to upgrade the DSR servers. However, Auto Site Upgrade cannot be used to upgrade IDIH servers at a site.

An important definition with regard to a site upgrade is the **site**. For the purposes of DSR site upgrade, a **site** is defined as a SOAM server group plus all subtending servers of that server group, **regardless of physical location**. To demonstrate this definition, Figure 3 shows three physical locations, labeled **TSite 1**, **TSite 2**, and **TSite 3**. Each site contains a SOAM server group and an MP server group. Each SOAM server group has a spare SOAM that, although physically located at another site, is a member of

the site that “owns” the server group. With site upgrade, SOA-Sp is upgraded with the Site 1 SOA server group, and SOB-sp is upgraded with the Site 2 SOB server group. The MP server groups are upgraded in the same maintenance window as their respective site SOAMs. These sites conform to the Topological Site definition of Table 2: Terminology.

1. With this feature, a site upgrade can be initiated on SO-A SG and all of its children (in this example, MP1 SG) using a minimum of GUI selections. The upgrade performs the following actions: Upgrade SOA-1, SOA-2, and SOA-sp.
2. Upgrade the servers in MP1 SG based on an availability setting and HA roles.
3. Immediately begin the upgrade of any other server groups which are also children of SO-A SG (not shown). These upgrades begin in parallel with step 2.

Server groups that span sites (e.g., SOAMs and SBRs) are upgraded with the server group to which the server belongs. This results in upgrading spare servers that physically reside at another site, but belong to a server group in the SOAM that is targeted for site upgrade.

Note: Automated Site Upgrade does not automatically initiate the upgrade of TSite 2 in parallel with TSite 1. However, the feature does allow the user to initiate Auto Site Upgrade of multiple sites in parallel **manually**.

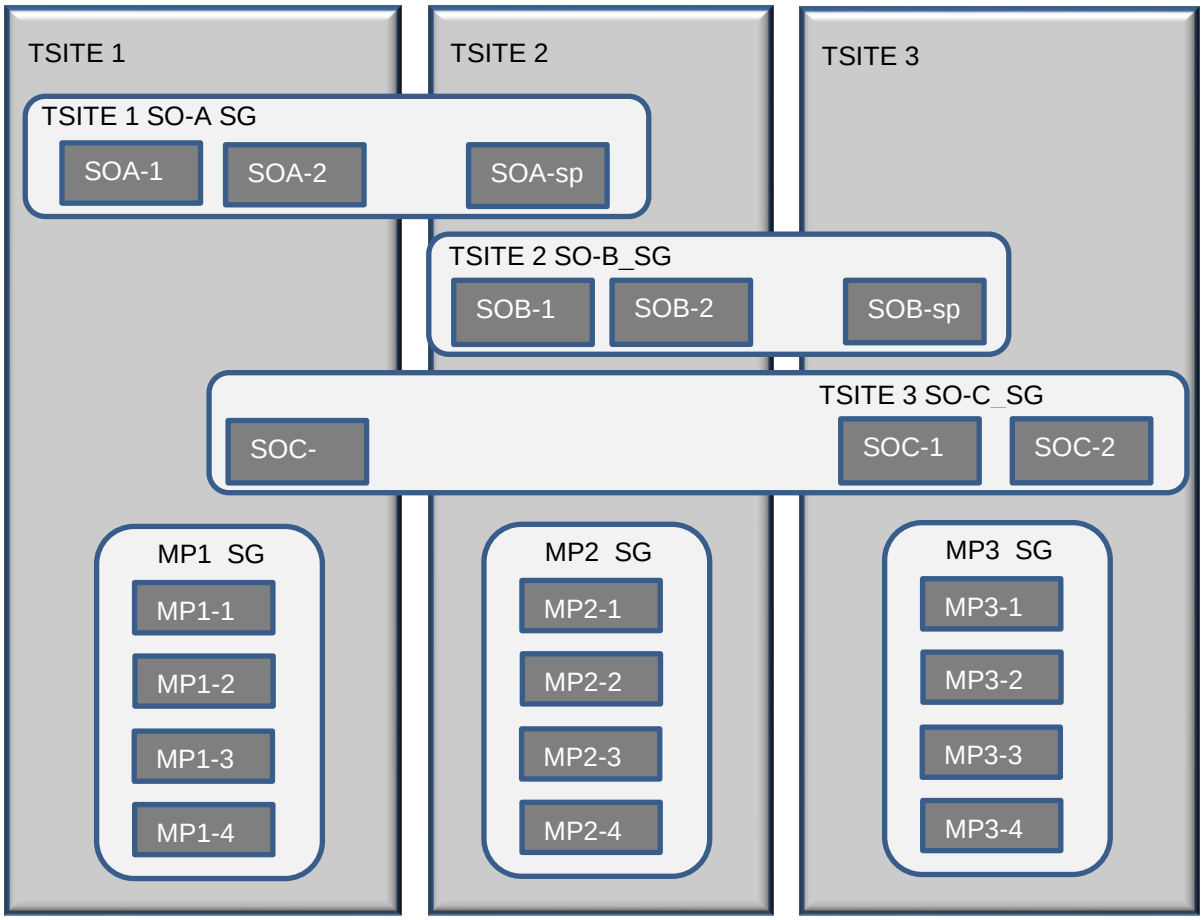


Figure 3. Upgrade Perspective of DSR "Site" Topology

CAUTION

Automated Site Upgrade and Options

Limitations in Appendix U for Automated Site Upgrade can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles then in that case manual upgrade section 5.3 method should be used

2.4.1 Site Upgrade Execution

With Auto Site Upgrade, the upgrade is initiated from the **Administration > Software Management > Upgrade** GUI. Upon initial entry to this screen, the user is presented with a tabbed display of the NOAM server group and SOAM sites (Figure 4). When the NOAM server group tab is selected (as shown in Figure 4), this screen is largely unchanged from the upgrade screen of previous releases. The NOAM server group servers are displayed with the usual assortment of buttons. On this screen, **Auto Upgrade** refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature becomes available once a SOAM server group tab is selected. The SOAM server group tabs correspond to the topological sites (TSites).

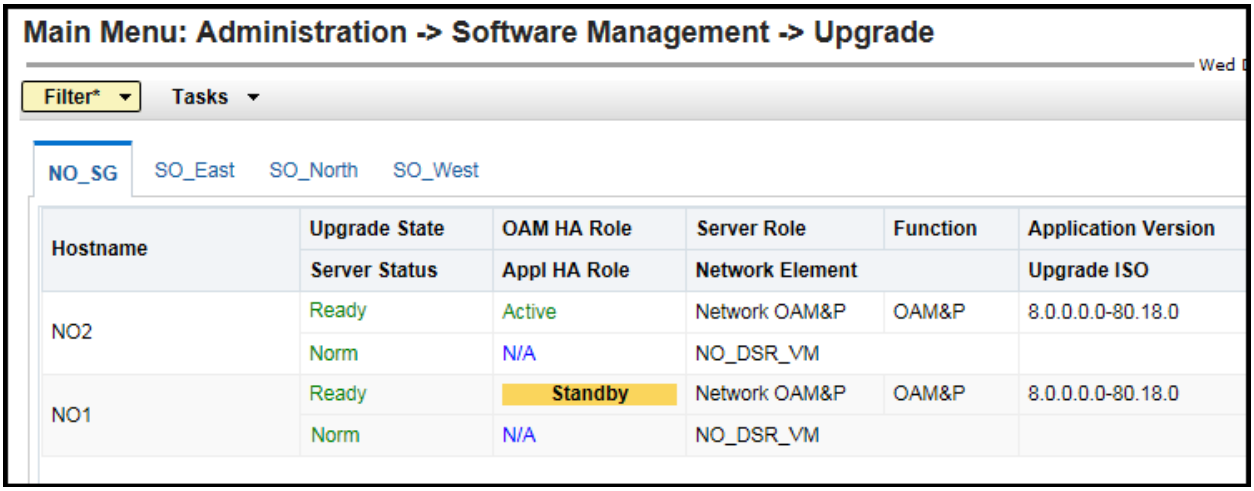


Figure 4. Site Upgrade – NOAM View

After selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen is displayed (Figure 5). Just below the row of NOAM and SOAM tabs is a row of links related to the selected SOAM site. The first link on the site summary screen displays the Entire Site view. In the entire site view, all of the server groups for the site are displayed in table form, with each server group populating one row. An upgrade summary of the server groups is provided in the table columns:

- The Upgrade Method column shows how the server group is upgraded. The upgrade method is derived from the server group function and the bulk availability option (see Section 2.4.3 for additional details on bulk availability).
- The Server Upgrade States column groups the servers by state, indicating the number of servers in the server group that are in each state.
- The Server Application Versions column indicates the current application version, indicating the number of servers in the server group that are at each version.

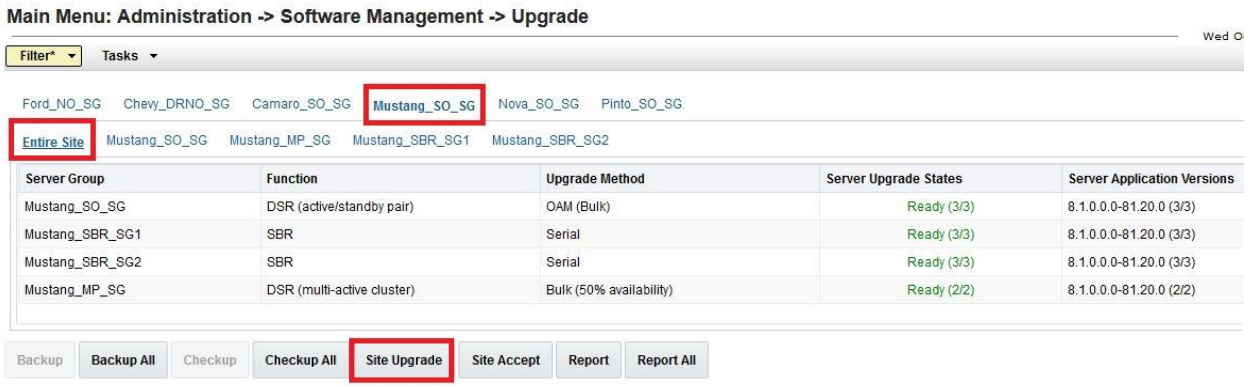


Figure 5. Site Upgrade - Entire Site View

For a server to be considered “Ready” for upgrade, the following conditions must hold true:

- Server has not been upgraded yet
- The FullDBParts and FullRunEnv backup files exist in the filemgmt area

A site is eligible for Automated Site Upgrade when at least one server in the site is upgrade-ready.

Click **Site Upgrade** from the **Entire Site** screen to display the Upgrade Site Initiate screen (Figure 6). The **Site Initiate** screen presents the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 6, Cycle 1 upgrades the spare and standby SOAMs in parallel.

Note: This scenario assumes default settings for the site upgrade options. These options are described in Section 2.4.3.) The specific servers to be upgraded in each cycle are identified in the **Servers** column of the **Site Initiate** display. Cycle 1 is an atomic operation, meaning that Cycle 2 cannot begin until Cycle 1 is complete. Once the spare and standby SOAMs are in **Accept or Reject** state, the upgrade sequences to Cycle 2 to upgrade the active SOAM. Cycle 2 is also atomic - Cycle 3 does not begin until Cycle 2 is complete.

Note: IPFE servers require special handling for upgrade, because IPFE servers are clustered into Target Sets and assigned an IP address, it is called Target Set Assignment (TSA). While upgrading IPFE servers, Auto Site Upgrade makes sure that there is no service outage for IPFE while upgrade is in progress, that is, IPFE servers in same TSA are not upgraded in same cycle. If IPFE server address is not configured on **IPFE -> Configuration -> Options** screen on active SOAM GUI, that IPFE server are not included in the Upgrade Cycle; therefore, are not considered for upgrade using Automated Site Upgrade.

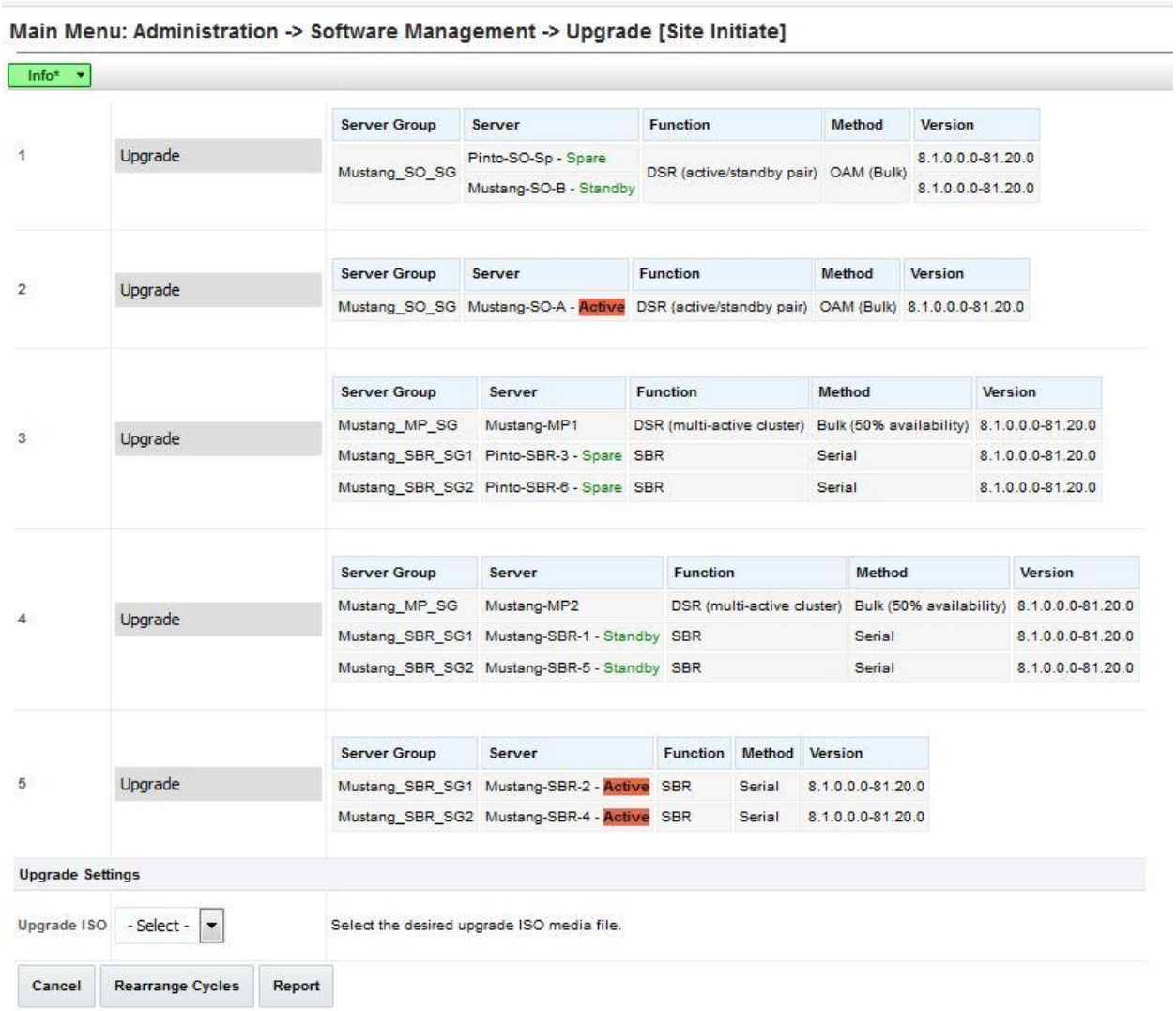


Figure 6. Site Upgrade - Site Initiate Screen

Cycles 3 through 5 upgrade all of the C-level servers for the site. These cycles are **not** atomic.

In Figure 6, Cycle 3 consists of IPFE1, IPFE3, MP1, MP4, and SBR3. Because some servers can take longer to upgrade than others, there may be some overlap in Cycle 3 and Cycle 4. For example, if IPFEs 1 and 3 complete the upgrade before SBR3 is finished (all are in Cycle 3), the upgrade allows IPFEs 2 and 4 to begin, even though they are part of Cycle 4. This is to maximize Maintenance Window efficiency. The primary factor for upgrading the C-level servers is the upgrade method for the server group function (for example, bulk by HA, serial, etc.).

The site upgrade is complete when every server in the site is in the **Accept or Reject** state.

In selecting the servers that are included with each upgrade cycle, particularly the C-level, consideration is given to the server group function, the upgrade availability option, and the HA designation. Table 3 describes the server selection considerations for each server group function.

Note: The minimum availability option is a central component of the server selections for site upgrade. The effect of this option on server availability is described in detail in Section 2.4.2.

Table 3. Server Selection vs. Server Group Function

SG Function	Selection Considerations
DSR (multi-active cluster) (for example, DA-MP)	The selection of servers is based primarily on the minimum server availability option. Servers are divided equally (to the extent possible) among the number of cycles required to enforce minimum availability. For DA-MPs, an additional consideration is given to the MP Leader. The MP with the Leader designation is the last DA-MP to be upgraded to minimize leader changes[1].
DSR (active/standby pair) (for example, SOAM)	The SOAM upgrade method is dependent on the Site SOAM Upgrade option on the General Options page. See section 2.4.3.
SBR	SBRs are always upgraded serially, thus the primary consideration for selection is the HA designation. The upgrade order is spare – spare – standby – active.
IP Front End	IPFEs require special treatment during upgrade. One consideration for selection is the minimum server availability, but the primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2. If minimum availability permits, IPFE A1 can be upgraded with IPFE B1, and IPFE A2 can be upgraded with B2.

[1] In the event of a leader change while upgrades are in progress, the MP Leader may not be the last MP to be upgraded.

To initiate the site upgrade, a target ISO is selected from the ISO picklist in the **Upgrade Settings** section of the **Site Initiate** screen (Figure 6). Once the **OK** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 7). With the **Entire Site** link selected, a summary of the upgrade status for the selected site is displayed. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. This view can be used to monitor the upgrade status of the overall site. More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.

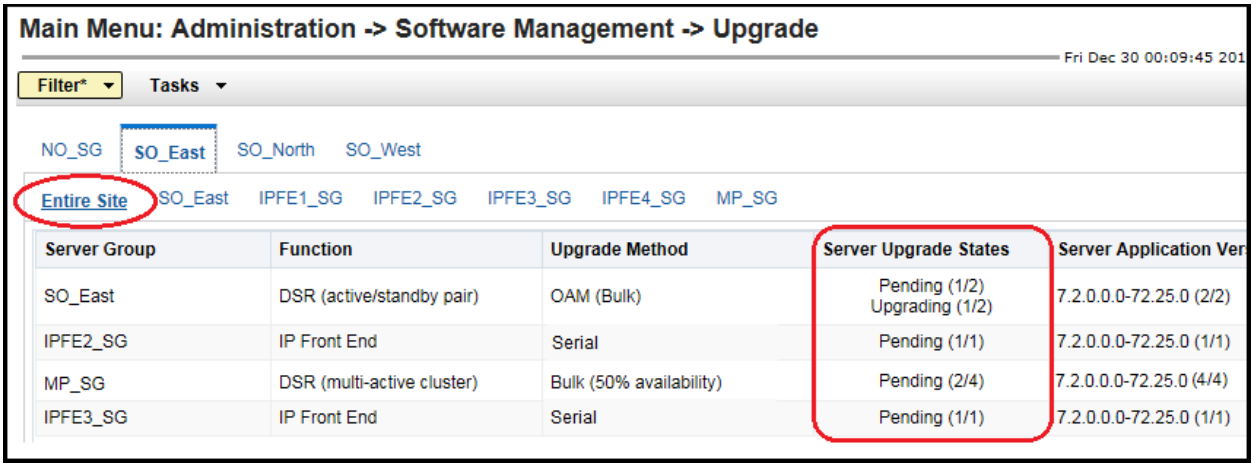


Figure 7. Site Upgrade Monitoring

When a server group link is selected on the upgrade administration screen, the table rows are populated with the upgrade details of the individual servers within that server group (Figure 8).

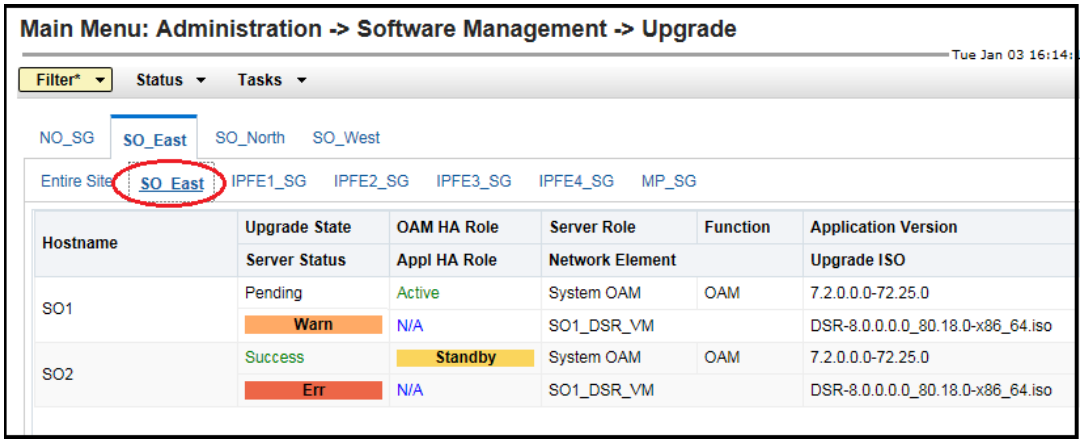


Figure 8. Server Group Upgrade Monitoring

Upon completion of a successful upgrade, every server in the site is in the **Accept** or **Reject** state. See Section 2.4.4 for a description of canceling and restarting the Automated Site Upgrade.

2.4.2 Minimum Server Availability

The concept of Minimum Server Availability plays a key role during an upgrade using Automated Site Upgrade. The goal of server availability is to ensure that at least a specified percentage of servers (of any given type) remain in service to process traffic and handle administrative functions while other servers are upgrading.

For example, if the specified minimum availability is 50% and there are eight servers of type X, then four remain in service while four upgrade. However, if there are nine server of type X, then the minimum availability requires that five remain in service while four upgrade. The minimum availability calculation automatically rounds up in the event of a non-zero fractional remainder.

To meet the needs of a wide-ranging customer base, the minimum availability percentage is a user-configurable option. The option allows for settings of 50%, 66%, and 75% minimum availability. There is also a setting of 0% for lab upgrade support. This option is described in detail in Section 2.4.3.

The application of minimum server availability differs for the various server group functions. For some function types, it is a straight calculation of a percentage. However, for others, minimum availability does not apply due to overriding operational considerations. Table 4 describes the application of availability for the various server group functions.

Table 4. Site Upgrade Availability vs. Server Group Function

Server Group Function	Server Availability
DSR (multi-active cluster)	In a multi-active cluster, the availability percentage applies to all of the servers in the server group. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.
SBR	Availability percentage does not apply to SBR server groups. SBRs are upgraded in a very specific order: spare – spare – standby – active
IP Front End	IPFEs require special treatment during upgrade. The primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2.

When calculating the number of servers required to satisfy the minimum server availability, all servers in the server group (or server group cluster) are considered. Servers that are OOS or otherwise unable to perform their intended function, are included, as are servers that have already been upgraded. For

example, consider a DA-MP server group with 10 servers; four have already been upgraded, one is OOS, and five are ready for upgrade. With a 50% minimum availability, only four of the servers that are ready for upgrade, can be upgraded in parallel. The four servers that have already been upgraded count toward the five that are needed to satisfy minimum availability. The OOS server cannot be used to satisfy minimum availability, so one of the upgrade-ready servers must remain in-service for minimum availability, thus leaving four servers to be upgraded together. Upgrading the last server would require an additional upgrade cycle.

2.4.3 Site Upgrade Options

To minimize user interactions, the automated site upgrade makes use of a pair of pre-set options to control certain aspects of the sequence. These options control how many servers remain in service while others are upgrading and are located on the **Administration > General Options** screen (Figure 9). The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

Site Upgrade Bulk Availability *	1	Site based upgrade availability for bulk upgrade of MP groups. (0 = none, 1 = 50%, 2 = 66%, 3 = 75%). **** Cannot be changed while any site upgrade is running. **** [Default = 1; Range = 0-3] [A value is required.]
Site Upgrade SOAM Method *	1	Site based upgrade SOAM method. (0 = serial, 1 = bulk). *Note: Bulk upgrade will upgrade all non-active SOAM servers together.* **** Cannot be changed while any site upgrade is running. **** [Default = 1; Range = 0-1] [A value is required.]

Figure 9. Auto Site Upgrade General Options

The first option that affects the upgrade sequence is the **Site Upgrade SOAM Method**. This option determines the sequence in which the SOAMs are upgraded. The default value of 1 considers the OAM HA role of the SOAMs to determine the upgrade order. In this mode, all non-active SOAM servers are upgraded first (in parallel), followed by the active SOAM. This upgrade method requires at most two upgrade cycles to upgrade all of the SOAMs, regardless of how many are present. If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

Changing the Site Upgrade SOAM Method setting to **0** causes the standby SOAM and the spare SOAM(s) to be upgraded serially. With this mode, the SOAM upgrade could take as many as four cycles to complete (that is, spare – spare – standby – active). If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

Regardless of the SOAM upgrade method, the active SOAM is always upgraded after the standby and spare SOAMs.

The second option that affects the upgrade sequence is the **Site Upgrade Bulk Availability** setting. This setting determines the number of C-level servers that remain in service during the upgrade. The default setting of “1” equates to 50% availability, meaning that a minimum of one-half of the servers stay in service during the upgrade. The default setting is the most aggressive setting for upgrading the site, requiring the minimum number of cycles, thus the least amount of time. The settings of 66% and 75% increase the number of servers that remain in service during the upgrade.

Note: Increasing the availability percentage may increase the overall length of the upgrade.

A setting of “0” for the bulk availability option allows all of the DA-MPs to be upgraded at once. This setting is not recommended for live production systems.

The application of minimum server availability varies for the different types of C-level servers. For example, for a multi-active DA-MP server group, the minimum availability applies to all of the DA-MPs within the server group. This same setup applies to IPFEs as well. Table 4 defines how the Site Upgrade Bulk Availability setting on the General Options page affects the various server group function types.

The Site Upgrade General Options cannot be changed while a site upgrade is in progress. Attempting to change either option while a site upgrade is in progress results in:

```
[Error Code xxx] - Option cannot be changed because one or more automated
site upgrades are in progress
```

2.4.4 Cancel and Restart Auto Site Upgrade

When an Auto Site Upgrade is initiated, several tasks are created to manage the upgrade of the individual server groups as well as the servers within the server groups. These tasks can be monitored and managed via the Active Task screen (**Status & Manage > Tasks > Active Tasks**).

The main site upgrade controller task is identified by the naming convention **<site_name> Site Upgrade**. In Figure 10, the main task is task ID 22. This task is controlling the server group upgrade task (task ID 23), which in turn is controlling the server upgrade task (task ID 24).

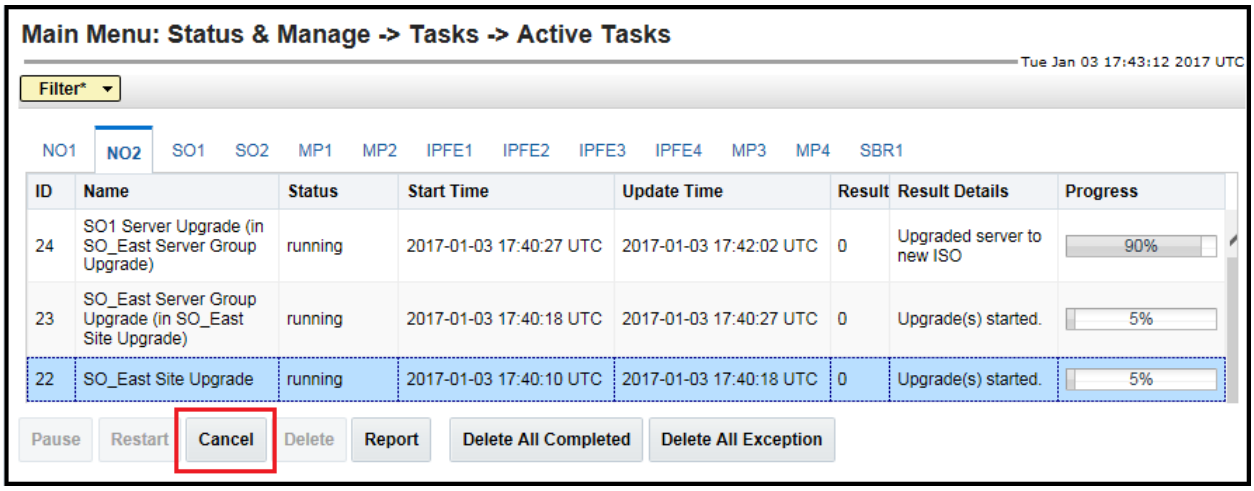


Figure 10. Site Upgrade Active Tasks

To cancel the site upgrade, select the site upgrade task and click **Cancel**. A screen requests confirmation of the cancel operation. The status changes from **running** to **completed**. The Results Details column updates to display **Site upgrade task cancelled by user**. All server group upgrade tasks that are under the control of the main site upgrade task immediately transition to **completed** state. However the site upgrade cancellation has no effect on the individual server upgrade tasks that are in progress. These tasks continue until completion. Figure 11 shows the Active Task screen after a site upgrade has been canceled.

Once the site upgrade task is canceled, it cannot be restarted. However, a new site upgrade can be started via the Upgrade Administration screen.

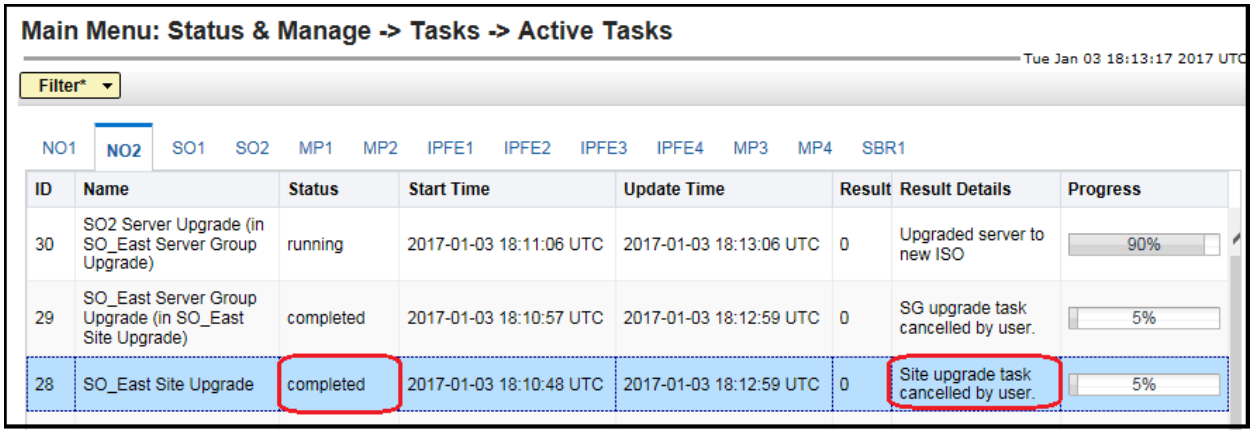


Figure 11. Canceled Site Upgrade Tasks

Figure 12 is representative of a site upgrade that was canceled before the site was completely upgraded. The servers that were in progress when the upgrade was canceled continued to upgrade to the target release. These servers are now in the Accept or Reject state. The servers that were pending when the upgrade was canceled are now in the Ready state, ready to be upgraded.

To restart the upgrade, verify the **Entire Site** link is selected and click **Site Upgrade**. The Upgrade Site Initiate screen displays.

Figure 12. Partially Upgraded Site

On the Upgrade Site Initiate screen, the servers that have not yet been upgraded are grouped into the number of cycles that are required to complete the site upgrade. For the upgrade that was canceled in Figure 11, only a single cycle is needed since the availability requirements can be met by the servers that have already been upgraded. Once an ISO is selected and **OK** is clicked, the site upgrade continues normally.

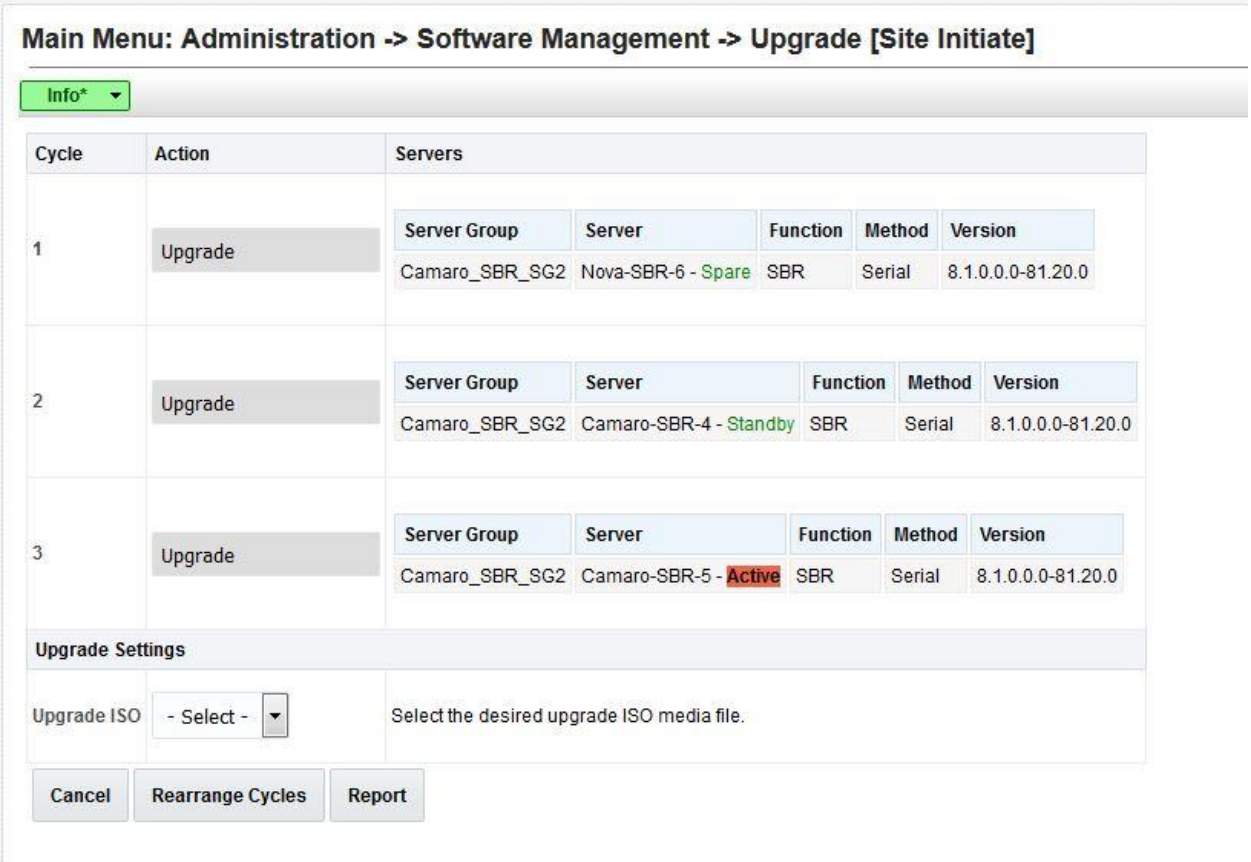


Figure 13. Restarting Site Upgrade

2.5 Automated Server Group Upgrade

The Automated Server Group (ASG) upgrade feature allows the user to upgrade all of the servers in a server group automatically by specifying a set of controlling parameters.

The purpose of ASG is to simplify and automate segments of the DSR upgrade. The DSR has long supported the ability to select multiple servers for upgrade. In doing so however, it was incumbent on the user to determine ahead of time which servers could be upgraded in parallel, considering traffic impact. If the servers were not carefully chosen, the upgrade could adversely impact system operations.

When a server group is selected for upgrade, ASG upgrades each of the servers serially, or in parallel, or a combination of both, while enforcing minimum service availability. The number of servers in the server group that are upgraded in parallel is user selectable. The procedures in this document provide the detailed steps specifying when to use ASG, as well as the appropriate parameters that should be selected for each server group type.

ASG is the default upgrade method for most server group types associated with the DSR. However, there are some instances in which the manual upgrade method is utilized. In all cases where ASG is used, procedures for a manual upgrade are also provided.

Note: To use ASG on a server group, no servers in that server group can be already upgraded – either by ASG or manually.

DSR continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

2.5.1 Cancel and Restart Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be manually canceled from the **Status & Manage > Active Tasks** screen (Figure 14) if necessary. Once the task is cancelled, it cannot be restarted. However, a new ASG task can be restarted via the Upgrade Administration screen.

For example, in Figure 14, task ID #1 (SO_SG Server Group Upgrade) is an ASG task, while task ID #2 is the corresponding individual server upgrade task. When the ASG task is selected (highlighted in green), the **Cancel** button is enabled. Canceling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tasks that were started by the ASG task (that is task ID #2 in Figure 14). Because the ASG task is canceled, no new server upgrades are initiated by the task.

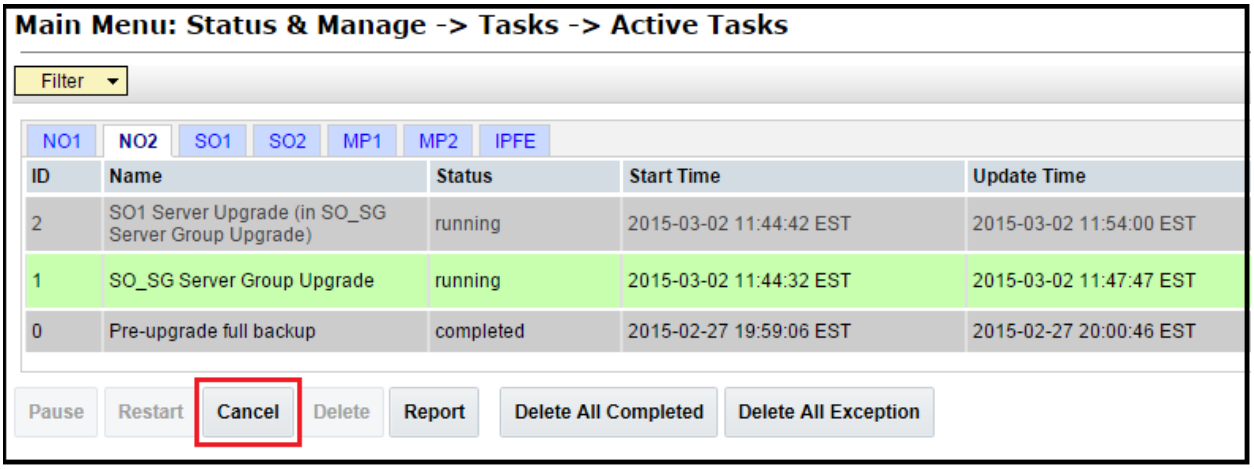


Figure 14. Active Tasks Screen

In the event that a server fails upgrade, that server automatically rolls back to the previous release in preparation for backout_restore and fault isolation. Any other servers in that server group that are in the process of upgrading continue to upgrade to completion. However, the ASG task itself is automatically cancelled and no other servers in that server group are upgraded. Cancelling the ASG task provides an opportunity for troubleshooting to correct the problem. Once the problem is corrected, the server group upgrade can be restarted by initiating a new server group upgrade on the upgrade screen.

2.5.2 Site Accept

The **Site Accept** button on the upgrade GUI (Figure 15) provides the capability to nearly simultaneously accept the upgrade of some or all servers for a given site. When the button is clicked, a subsequent screen (Figure 16) displays the servers that are ready for the Accept action.

Figure 15. Site Accept Button

A checkbox on the Upgrade Site Accept screen allows for the selective application of the Accept action. However, normal procedure calls for the Accept to be applied to all of the servers at a site only after the upgrade to the new release is stable and the back out option is no longer needed. After verifying that the information presented is accurate, clicking **OK** results in a screen that requires confirmation of the intended action. Confirming the action causes the server upgrades to be accepted.

The Accept command is issued to the site servers at a rate of approximately one server every second. The command takes approximately 10 seconds per server to complete. As the commands are completed, the server status on the Upgrade Administration screen transitions to **Backup Needed**.

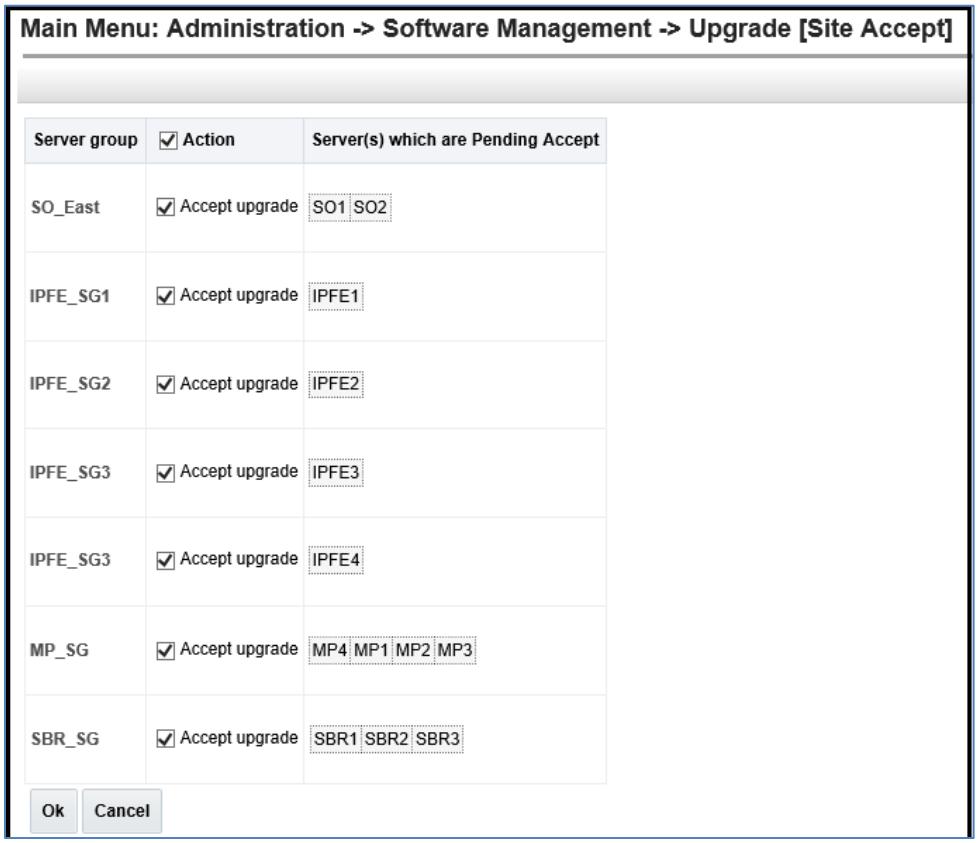


Figure 16. Site Accept Screen

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 document that help plan the upgrade and estimate how long it takes to perform various actions. The stated time durations for each step or group of steps **are estimates only**. Do not use the overview tables to execute any actions on the system. Only the procedures should be used when performing upgrade actions, beginning with Procedure 1.

!!WARNING!! For vSTP-related deployments, it is not allowed to do any adding/updating/deleting of configuration until the upgrade is completed on all sites and the upgrade is accepted.

Note: While planning an upgrade, be aware that once the upgrade is started and OAM level servers are on different releases than servers on different sites, OAM level provisioning data is not replicated to sites that have not been upgraded.

Once servers at the site are upgraded, replication from OAM level serves is restored and upgraded servers start receiving provisioning data.

Read 2.4 Automated Site Upgrade for details and limitations/solutions while planning upgrade cycles.

There are some limitations with upgrading the DC server in a C-level server group that are upgraded in a group of servers, for example DA-MP, vSTP MP(s). So, while manually upgrading, make sure the DC server is not upgraded in the first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix O Identify the DC server.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader** = **Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

   The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**.

2. Use the **/vstp/mpleader** MO.

   The result is the hostname of the MP leader server.

Note: If the **31149 - DB Late Write Nonactive** displays, ignore it. This alarm does not have any effect on functionality.

3.1 Required Materials and Information

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

- Target-release application ISO image file or target-release application media.
- The capability to log into the network OAM servers with administrator privileges.

  Note: All logins into the DSR NOAM servers are made using the external management VIP unless otherwise stated.

- User logins, passwords, IP addresses and other administration information. See [Table 5].

- VPN access to the customer's network is required if that is the only method to log into the OAM servers.

3.1.1 Application ISO Image File/Media

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

The DSR ISO image file name is in the following format (version changes from release to release):

```
DSR-8.3.0.0.0_83.xx.0-x86_64.iso
```

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

The ISO is deployed as part of the pre-upgrade activities in Section 3.4.

3.1.2 Logins, Passwords and Server IP Addresses

Table 5 identifies the information that is called out in the upgrade procedures, such as server IP addresses and login credentials. For convenience, space is provided in Table 5 for recording the values, or the information can be obtained by other means. This step ensures that the necessary administration information is available before an upgrade.

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

Table 5: Logins, Passwords, and Server IP Addresses

Item	Description	Recorded Value
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username[1]	
	GUI Admin Password	
	DSR admusr Password[2]	
	DSR Root Password[2]	
VPN Access Details	Customer VPN information (if needed)	

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

[2] This is the password for the server login. This is not the same login as the GUI Administrator. The admusr password is required if recovery procedures are needed. If the admusr password is not the same on all other servers, then all those servers' admusr passwords must also be recorded; use additional space at the bottom of this table.

Item	Description	Recorded Value
NOAM	XMI VIP address[3]	
	NOAM 1 XMI IP Address	
	NOAM 2 XMI IP Address	
SOAM	XMI VIP address	
	SOAM 1 XMI IP Address (Site 1)	
	SOAM 2 XMI IP Address (Site 1)	
	PCA (DSR) Spare System OAM&P server – Site 1 Spare in Site 2, XMI IP Address	
	SOAM 1 XMI IP Address (Site 2)	
	SOAM 2 XMI IP Address (Site 2)	
	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 1)	
	Binding SBR SR2 Server Group Servers (Site 1)	
	Binding SBR SR3 Server Group Servers (Site 1)	
	Binding SBR SR4 Server Group Servers (Site 1)	
PCA MP Server Group	PCA MP Server Group Servers (Site 1)	
	PCA MP Server Group Servers (Site 1)	
IPFE Server Groups(For PDRA)	PCA IPFE A1 Server Group Server (Site 1)	
	PCA IPFE A 2 Server Group Server (Site 1)	
	PCA IPFE B 1 Server Group Server (Site 1)	
	PCA IPFE B 2 Server Group Server (Site 1)	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 2)	
	Binding SBR SR2 Server Group Servers (Site 2)	
	Binding SBR SR3 Server Group Servers (Site 2)	
	Binding SBR SR4 Server Group Servers (Site 2)	
PCA MP Server Group	PCA MP Server Group Servers (Site 2)	

[3] All logins into the NOAM servers are made via the External Management VIP unless otherwise stated.

Item	Description	Recorded Value
IPFE Server Groups (For PCA)	PCA IPFE A1 Server Group Server (Site 2)	
	PCA IPFE A 2 Server Group Server (Site 2)	
	PCA IPFE B 1 Server Group Server (Site 2)	
	PCA IPFE B 2 Server Group Server (Site 2)	
vSTP MP Server Group	vSTP MP server(s)	
Software	Target Release Number	
	ISO Image (.iso) file name	
Misc.[4]	Miscellaneous additional data	

[4] As instructed by Oracle CGBU Customer Service.

3.2 Plan Upgrade Maintenance Windows

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

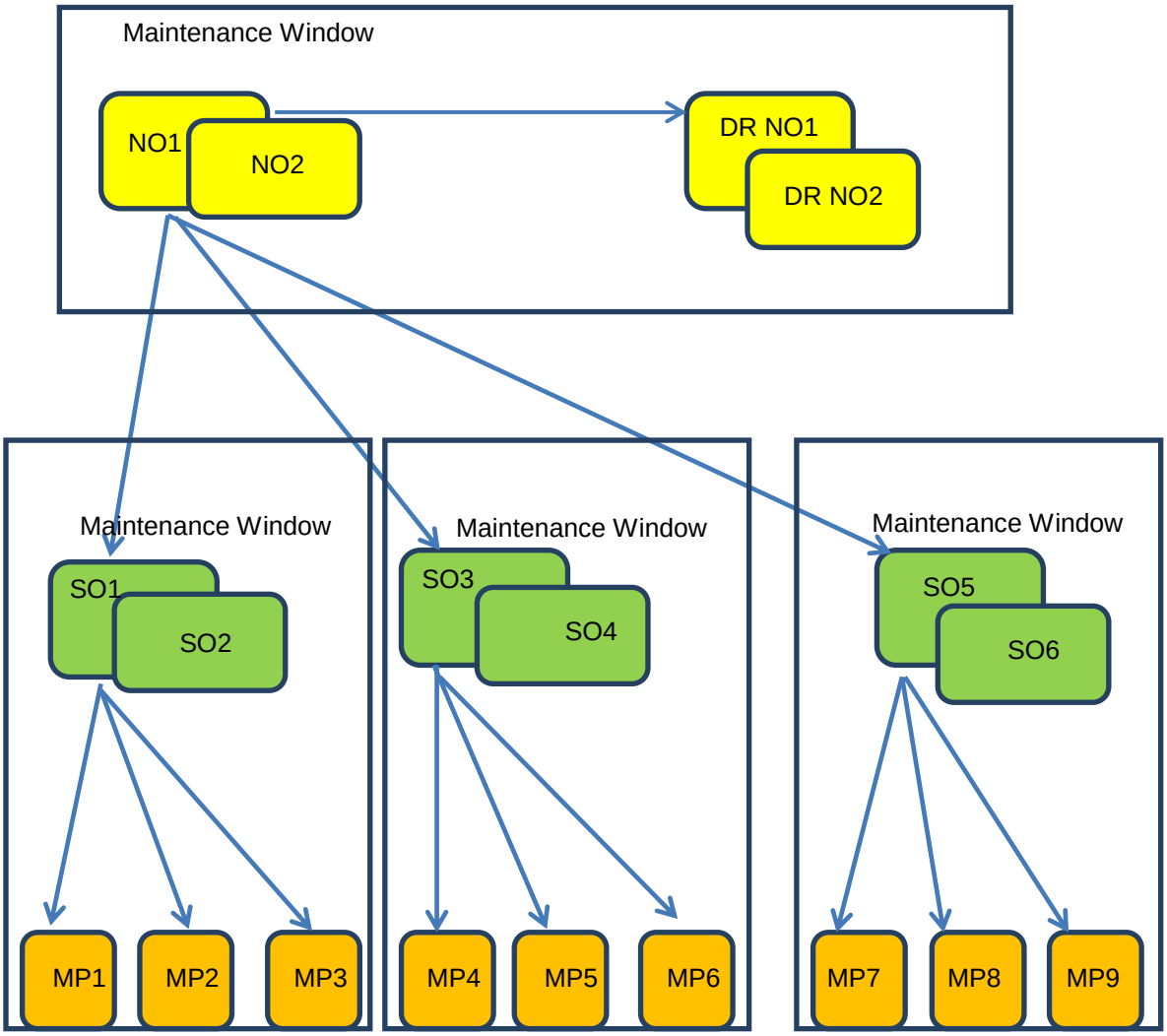


Figure 17. Upgrade Maintenance Windows for 3-Tier Upgrade

!!WARNING!! Mated SOAM sites must be upgraded in separate maintenance windows.

3.2.1 Calculating Maintenance Windows Required

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see ref [3]).

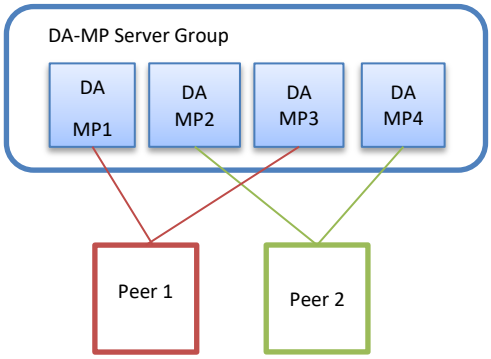
This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. The spreadsheet also specifies, in detail, which servers need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in Reference [3]. Please see the instructions tab of the spreadsheet for more information and details.

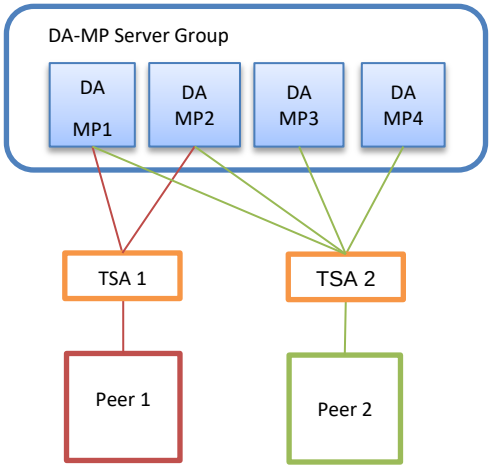
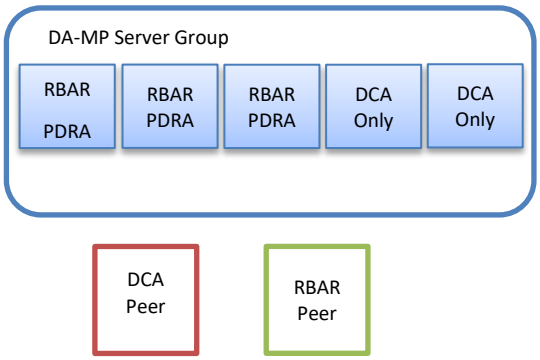
3.3 Site Upgrade Methodology Selection

There are three primary methods for upgrading a DSR site: Auto Site Upgrade, Auto Server Group Upgrade, and manual upgrade. The Auto Site Upgrade is the easiest and most efficient site upgrade method; however, it is not suitable for all customers or all configurations. The Auto Server Group upgrade incorporates many of the conveniences of Auto Site Upgrade, but allows for more customer control of the upgrade process. Again, Auto Server Group upgrade is not for all customers or all configurations. The manual upgrade method gives maximum control to the customer and can be used for all configurations. A combination of upgrade methods can be utilized to upgrade a given site to maximize efficiency with customer peace-of-mind.

Table 6 is a worksheet for determining which upgrade method meets the needs of the customer while ensuring compatibility with the DSR configuration. Upon completion of the worksheet, a recommended upgrade method is identified.

Table 6. Traffic Analysis Checklist

	Criteria	Yes	No	Notes
1.	Do any of the site's DA-MPs have fixed diameter connections to any peer node, similar to this depiction?  	☐	☐	Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider fixed peer connections when selecting servers to upgrade. It is possible that all DA-MPs servicing a given peer (such as DA-MPs 1 and 3) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given peer are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for a manual upgrade. If no, continue with step 2.

	Criteria	Yes	No	Notes
2.	If peer nodes are configured via IPFE TSAs, are there any TSAs that are not distributed across all DA-MPs, similar to this depiction?  	☐	☐	Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider non-uniformly distributed TSAs when selecting servers to upgrade. It is possible that all DA-MPs servicing a given TSA (such as DA-MPs 1 and 2) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given TSA are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for a manual upgrade. If no, continue with step 3.
3.	Do any of the site's DA-MPs have specialized distribution of DSR features, similar to this depiction?  	☐	☐	Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider non-uniform distribution of features when selecting servers to upgrade. It is possible that all DA-MPs hosting a given feature (such as DCA) could be upgraded simultaneously, thereby eliminating service functionality. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs hosting a given feature are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for manual upgrade. If no, continue with step 4.

	Criteria	Yes	No	Notes
4.	Automated Site Upgrade is a candidate for this system. Automated Site Upgrade supports 50% minimum server availability by default. A general option allows availability percentage settings of 66% or 75%. Is 50%, 66%, or 75% server availability during upgrade acceptable to the customer?	☐	☐	In general, a higher minimum availability setting increases the time required to upgrade a site. On the other hand, a lower minimum availability may reduce operational redundancy during the upgrade. If none of the minimum availability options are acceptable, Automated Site Upgrade should not be used to upgrade the site. If yes, continue with step 6. If no, proceed to step 7.
5.	Is the customer comfortable with minimum user intervention (that is, user input) during the upgrade?	☐	☐	Once initiated, Automated Site Upgrade requires no additional user input to complete the upgrade. User control is limited to canceling the site upgrade task. If yes, Automated Site Upgrade is the recommended upgrade method. If no, proceed to step 7.
6.	Automated Server Group Upgrade is a candidate for this system. Is the customer comfortable with the level of control afforded by the Automated Server Group upgrade?	☐	☐	Auto Server Group upgrade allows the user to initiate the upgrade of each server group, while the individual servers within the server group upgrade automatically. If yes, Auto Server Group upgrade is the recommended upgrade method. If no, proceed to step 8.
7.	A manual upgrade affords the maximum level of control over upgrade sequencing. With this method, the upgrade of each server is individually initiated, allowing the user to control the level of parallelism and speed of the upgrade. ***Note***: A site upgrade can include a combination of Automated Server Group upgrade and manual upgrades to improve efficiency. For example, SBRs can be upgraded with Automated Server Group upgrade, while the DA-MPs may be upgraded manually to control the order of upgrade for traffic continuity.	☐	☐	A manual upgrade is the recommended upgrade method.

3.3.1 DA-MP Upgrade Planning

If a manual upgrade is recommended by the Table 6 worksheet, additional planning is required to ensure a successful upgrade of the DA-MP server group. A manual upgrade is typically required/recommended when the DA-MPs are configured in a way such that an upgrade could result in a traffic outage. Pre-planning the upgrade of the DA-MPs is key to avoiding an outage.

Table 7 is an aid to laying out the sequence of the DA-MP upgrades, taking into consideration configuration and traffic continuity. **This worksheet must be completed by the customer and**

provided to Oracle if Oracle personnel are performing the upgrade. It is highly recommended that the worksheet be completed for customer-driven upgrades as well.

Customer: Perform an analysis of the Diameter application and connection configurations to assess any potential traffic loss due to the DA-MP upgrade. Complete the worksheet, specifying the order in which the DA-MPs will be upgraded, and which MPs, if any, can be upgraded in parallel.

The worksheet is divided into four upgrade **Cycles**. Each cycle represents an upgrade period during which one or more servers are upgraded. Distributing the DA-MPs servers over two or more cycles, takes advantage of parallels, thereby reducing the time required to upgrade the entire server group.

To achieve 50% server availability, half of hostnames would be listed in Cycle 1 while the other half would be listed in Cycle 2, requiring two upgrade cycles. Similarly, 75% availability can be achieved by spreading the hostname over all four cycles.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader** = **Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

   The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**.

2. Use the **/vstp/mpleader** MO.

   The result is the hostname of the MP leader server.

Note: If desired, the DA-MPs can be upgrade serially, in which case, all hostnames would be listed in cycle 1. List the DA-MPs in the order in which they will be upgraded.

Table 7. DA-MP Upgrade Planning Sheet

	Hostnames			
Upgrade Cycle 1 or Serial Upgrade				
	Hostnames			
Upgrade Cycle 2				
	Hostnames			
Upgrade Cycle 3				

	Hostnames			
Upgrade Cycle 4				
DA-MP Leader:				

3.3.2 Pre-upgrade validation to avoid Comcol inter-connectivity issue between MPs

The HA framework enhancements cause the inter-connectivity issue between the old-DC and non-DC MP nodes during upgrade scenario.

Note: This procedure provides solution to resolve the inter-connectivity issue between the old-DC and non-DC MP at the time of upgrade for the BUG 27428669.

To overcome the inter-connectivity issue:

1. Check the Designated Coordinator (DC) node in the system by using the command:

   ```
   ssh admusr@<MP_server>

   $ ha.info -d
   ```

   Example output:

   ```
   Node ID:     HDBDBGTGCHBDRA54TK
   Report Time: 01/07/2018 03:48:43.299

   ***
   ** Election Mgr: C2939 (4b2799)
   ***

   DC: HDBDBGTGCHBDRA54TK  Generation: 1  State: DC
     Elected: 01/07/2018 02:14:40.822
     Other Non-DC Group Members:
       HDBDBGTGCHBDRA53TK
       HDBDBGTGCHBDRA5BTK
       HDBDBGTGCHBDRA5CTK

   DC Group Candidates: <none>
   ```

2. Before starting the MP server upgrade, disable the DSR application on current DC node, using command:
   a. On Active SOAM - Go to **Server** under **Status & Manage** option.
   b. Disable the DSR application by selecting the MP (DC Node) and click **Stop**.
3. Select an MP to be upgraded:
   Note: The MP Leader Node should be the last server to be upgraded.
   a. Case where there existing IPFE based floating (Diameter) connections, choose an MP from TSA having more than 2 MPs.
      Note: If there exists a TSA with just two MPs, and one having DC role. We should avoid using other MP (non-DC) in this TSA for upgrade at this step.
   b. Case where there are MP based (Diameter) connection, select any MP except the MP having DC role.
4. After upgrade, one of the upgraded MP with new release takes over the new-DC role.
5. The DSR application remains disabled on the old-DC node, as performed in step 2.

6. The old-DC is upgraded in the next upgrade cycle.
7. Once the upgrade is completed, from Active SOAM - Go to **Server** under **Status & Manage** GUI screen and check if the DSR application is ENABLED on MP node (old-DC). If not then ENABLE it by restart button.

3.3.3 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded.

Maintenance Window 1 (NOAM Sites) **Date**: _____ ***Note***: The NE Name may be viewed from the DSR NOAM GUI under **Configuration -> Network Elements**.	Record the Site **NE Name** of the DSR NOAM 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. ☐ DR Standby NOAM (Guest): _____ ☐ DR Active NOAM (Guest): _____ ☐ Primary Standby NOAM (Guest): _____ ☐ Primary Active NOAM (Guest): _____

3.3.4 Maintenance Window 2 and Beyond (SOAM Site Upgrades)

During Maintenance Window 2, all servers associated with the first SOAM site are upgraded. All servers associated with the second SOAM site are upgraded during Maintenance Window 3.

For DSRs configured with multiple mated-pair sites, or DSRs having multiple, distinct sites (e.g., geo-redundant PCA installations), copy and use the following form for the subsequent SOAM site upgrades.

From release 8.1, vSTP MP support is available. While upgrading from pre 8.1 releases, vSTP MP server will not be in the system. So, after major upgrade is completed. In case vSTP MP server is required, it is freshly installed on 8.1 release using reference [1]. For release 8.1, planning should be done for vSTP MP incremental upgrades.

Note: In release 8.1, there can be only one vSTP MP server in the STP server group and one server in one site. This means whenever the vSTP MP server is upgraded, there is traffic loss on that vSTP MP server.

!!WARNING!! Mated SOAM sites must be upgraded in separate maintenance windows.

Maintenance Window SOAM Sites **Date**: _____	1. Record the site NE Name of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided. 2. Mark the associated checkbox as each server upgrade is completed. SOAM Site: _____ ☐ Spare SOAM1 (Guest): _____ (If equipped) ☐ Spare SOAM2 (Guest): _____ (If equipped) ☐ Standby SOAM (Guest): _____ ☐ Active SOAM (Guest): _____

	☐ DA-MP1: _____ ☐ DA-MP2: _____ ☐ DA-MP3: _____ ☐ DA-MP4: _____ ☐ DA-MP5: _____ ☐ DA-MP6: _____ ☐ DA-MP7: _____ ☐ DA-MP8: _____ ☐ DA-MP9: _____ ☐ DA-MP10: _____ ☐ DA-MP11: _____ ☐ DA-MP12: _____ ☐ DA-MP13: _____ ☐ DA-MP14: _____ ☐ DA-MP15: _____ ☐ DA-MP16: _____
	☐ IPFE1: _____ ☐ IPFE2: _____ ☐ IPFE3: _____ ☐ IPFE4: _____
	Binding Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 2 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ _____ _____ ☐ Spare SBR2 (Mate): _____ (If equipped)

	Binding Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Binding Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped)
	Session Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 2 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____

	☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped) Session Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 (Mate): _____ ☐ Spare SBR2 (Mate): _____ (If equipped)
	vSTP MP Server Group ☐ vSTP MP(s): _____ (If equipped)

3.4 Prerequisite Procedures

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

Table 8. Prerequisite Procedures Overview

Procedure	Elapsed Time (hr:min)		Procedure Title
	This Step	Cum.	
Procedure 1	0:10-0:30	0:10-0:30	Procedure 1

Procedure	Elapsed Time (hr:min)		Procedure Title
	This Step	Cum.	
Procedure 2	0:15-0:30	0:25-1:00	Procedure 2
Procedure 3	0:20-0:30	0:55-1:30	Procedure 3
Procedure 4 or Procedure 5	0:15-0:20 0:15-0:20	1:10-1:50 1:10-1:50	Procedure 4 Procedure 5
Procedure 6	0:05	1:15-2:35	Procedure 6
Procedure 7	0:15-0:30	1:30-3:05	Procedure 7
Procedure 8	0:10-2:00	1:40-5:05	Procedure 8**Error! Reference source not found.**

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

3.4.1 Required Materials Check

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

Procedure 1. Required Materials Check

Step #	Procedure	Description
This procedure verifies all required materials are present. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Verify all required materials are present	Materials are listed in Section 3.1: Required Materials. Verify required materials are present.
2. ☐	Verify all administration data needed during upgrade	Double-check that all information in Section 3.2 is filled-in and accurate.
3. ☐	Contact My Oracle Support (MOS)	It is recommended to contact My Oracle Support (MOS) and inform them of plans to upgrade this system. See Appendix V for these instructions. ***Note***: Obtaining a new online support account can take up to 48 hours.

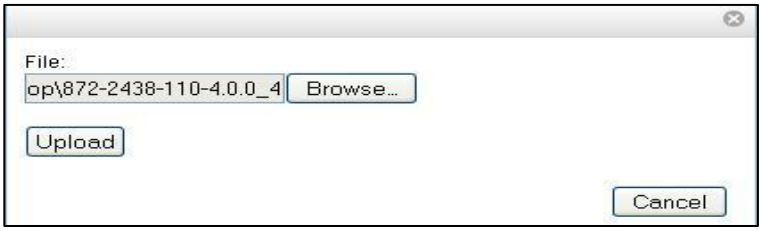
3.4.2 DSR ISO Administration

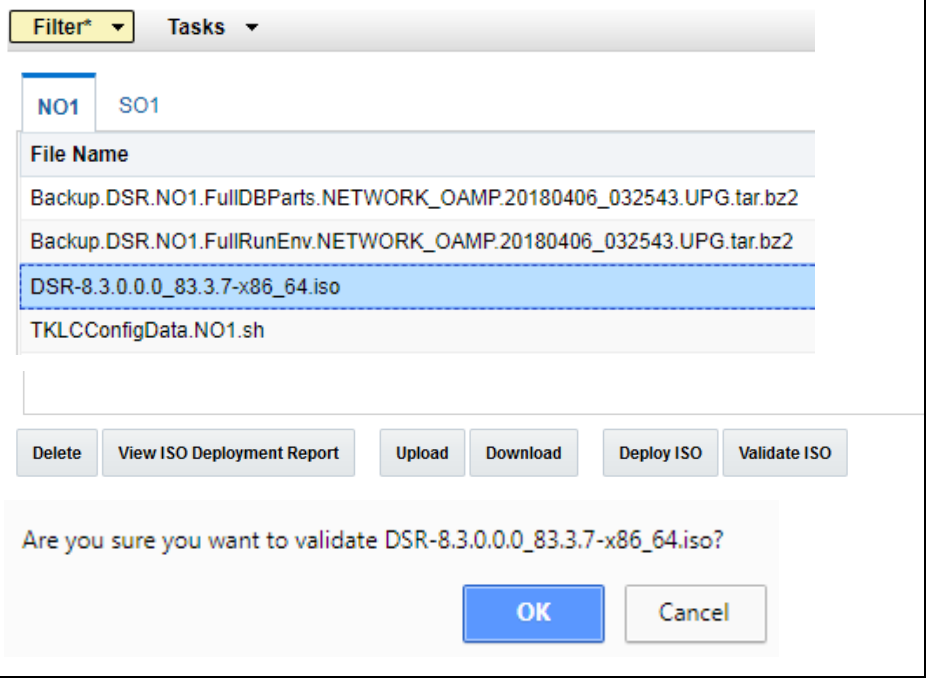
This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

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

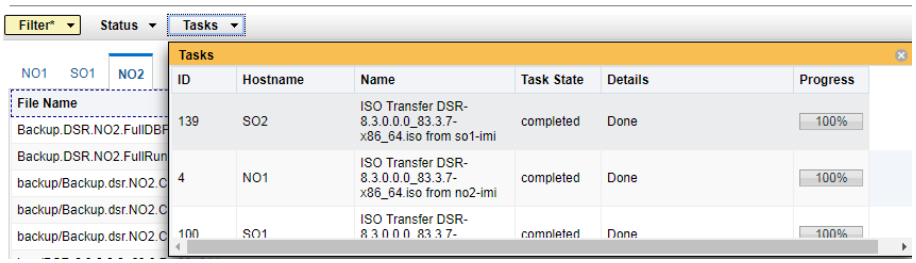
Procedure 2. DSR ISO Administration

Step #	Procedure	Description
This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Transfer via NOAM GUI	Use the NOAM GUI upload function for ISO file transfer over the network. Upload the target release ISO image file to the File Management Area of the active NOAM server: 1. Log into the active NOAM GUI. 2. Navigate to **Status & Manage > Files**. 3. Click the active NOAM server in the network to display all files stored in the file management storage area of this server. 4. Ensure that this is actually the active NOAM server in the network by comparing the hostname in the screen title vs. the hostname in the session banner in the GUI. Verify they are the same and the status is **Active** in the session banner. 5. Click **Upload**. ***Note***: Actual screens may vary from those shown depending on the browser and browser version used.

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**	1. Click **Browse** to select the file to upload. 2. Select the target release ISO image file and click **Open**. 3. Click **Upload**.  The ISO file begins uploading to the file management storage area. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This usually takes between 2 to 10 minutes, but more if the network upload speed is slow.
3. ☐	**Active NOAM CLI**: Change Permission of ISO	Log into the Active NOAM CLI and execute the following command: `sudo chmod 644 /var/TKLC/db/filemgmt/<DSR_ISO_Filename>`

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Using NOAM GUI, deploy ISO to all servers to be upgraded.	1. Navigate to **Status & Manage > Files**. 2. Click the active NOAM server tab. All files stored in the file management storage area of this server display on the screen. 3. Select the target release ISO, and click **View ISO Deployment Report**. 4. In the resulting report, determine if the ISO has been deployed to all servers in the system. 5. If the ISO has been deployed to all servers, this procedure is complete. Proceed to the next procedure per Table 8. 6. If the ISO has not been deployed, select the target release DSR ISO in the file list, and click **Validate ISO**. Click **OK** on the confirmation screen. 7. Verify the ISO status is valid. If the ISO is not valid, repeat this procedure beginning with step 1. If the ISO fails validation more than once, it is recommended to contact . 8. If the ISO is valid, select the ISO, and click **Deploy ISO**. Click **OK** on the confirmation screen. **Main Menu: Status & Manage -> Files** 

Step #	Procedure	Description

5.
☐
	Active NOAM VIP: Monitor ISO deployment	The deployment progress can be monitored by viewing the **Tasks** options on the **Status & Manage > Files** screen.
		 
		
		Select the target release ISO, and click **View ISO Deployment Report**. Verify the ISO has been deployed to all servers in the system.
		Main Menu: Status & Manage -> Files [View]
		`Main Menu: Status & Manage -> Files [View]`
		`Tue Apr 10 01:35:34 2018 EDT`
		`Deployment report for DSR-8.3.0.0.0_83.3.7-x86_64.iso:`
		`Deployed on 4/4 servers.`
		`NO1: Deployed`
		`SO1: Deployed`
		`NO2: Deployed`
		`SO2: Deployed`

3.4.3 Data Collection — Verification of Global and Site Configuration Data

The procedures in this section are part of software upgrade preparation and are used to collect data required for network analysis, disaster recovery, and upgrade verification. Data is collected from both the active NOAM and various other servers at each site.

3.4.3.1 Verification of Configuration Data

This procedure checks the configuration data of the system and servers to ensure a successful upgrade.

Procedure 3. Verification of Configuration Data

Step #	Procedure	Description
This procedure checks the configuration data and server status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Verify application version	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the upgrade path to the target release is supported as documented in Section 2.1 (Supported Upgrade Paths). 3. Select the NOAM Server Group and verify the Application Version. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Tasks ▾ NOSG SOSG Hostname / Upgrade State / OAM HA Role / Server Role / Function / Application Version Server Status / Appl HA Role / Network Element / Upgrade ISO NO2: Ready / Active / Network OAM&P / OAM&P / 8.0.0.0.0-80.25.0 Norm / N/A / NE_NO NO1: Ready / Standby / Network OAM&P / OAM&P / 8.0.0.0.0-80.25.0 Norm / N/A / NE_NO

Step #	Procedure	Description

2.
☐
	Active NOAM CLI: Check if the setup has customer supplied Apache certificate installed and protected with a passphrase	1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active NOAM
		`ssh admusr@<NOAM_VIP>`
		`password:  <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. cd to **/etc/httpd/conf.d** and open the file named **ssl.conf**.
		3. Locate the line beginning with the phrase **SSLCertificateFile**.
		4. The path that follows **SSLCertificateFile** is the location of the Apache certificate. If the path is **/usr/TKLC/appworks/etc/ssl/server.crt**, then the certificate is supplied by Oracle and no further action is required. Continue with the next step.
		5. If the path is anything other than **/usr/TKLC/appworks/etc/ssl/server.crt**, then a customer-supplied Apache certificate is likely installed. Rename the certificate, but note the original certificate pathname for use in Section 4.4.

The following data collection procedures collect similar data; however, the collection method varies depending on the source release. Only one of the following procedures is to be executed for the pre-upgrade data collection. Refer to Table 9 for guidance on which procedure to use.

Table 9. Release Specific Data Collection Procedures

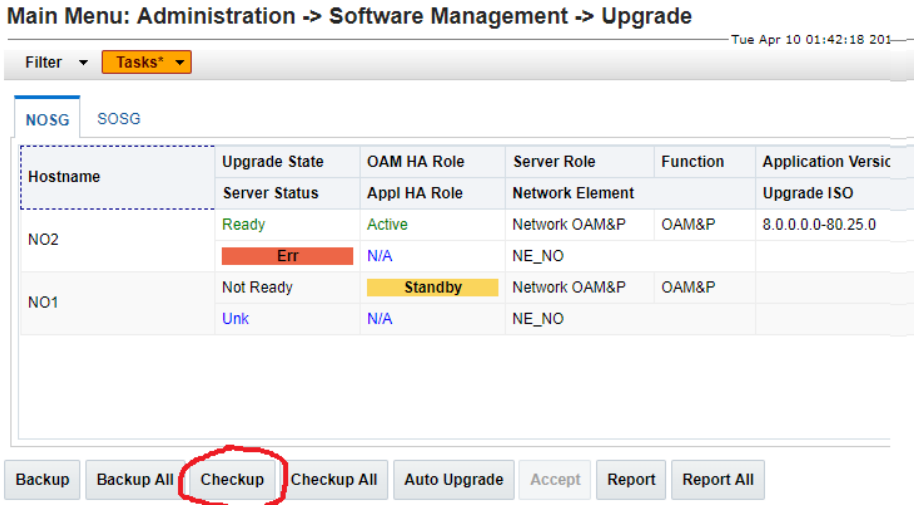
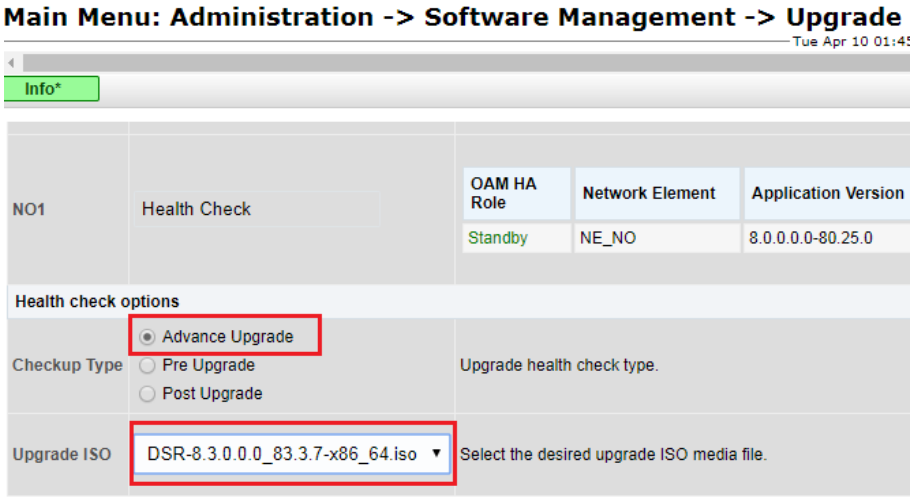
If the Source Release is	Use This Pre-Upgrade Data Collection Procedure
7.3, or 7.4	Procedure 4
8.0 and later	Procedure 5

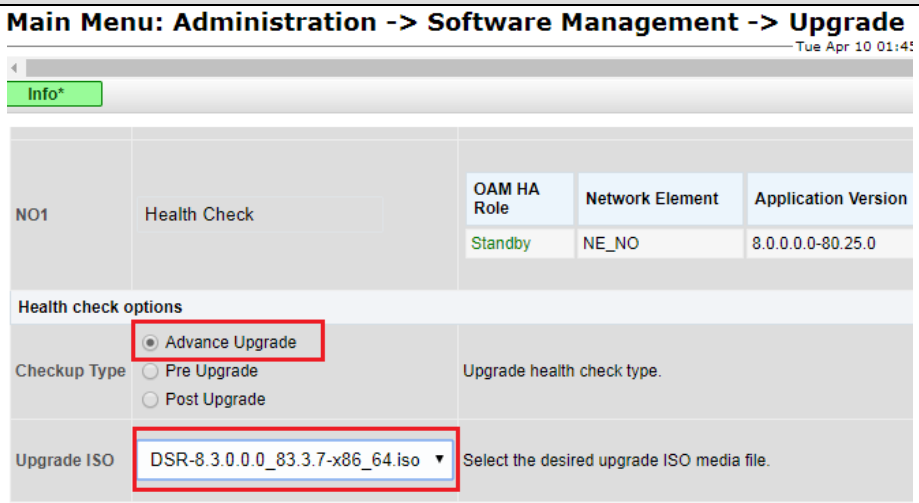
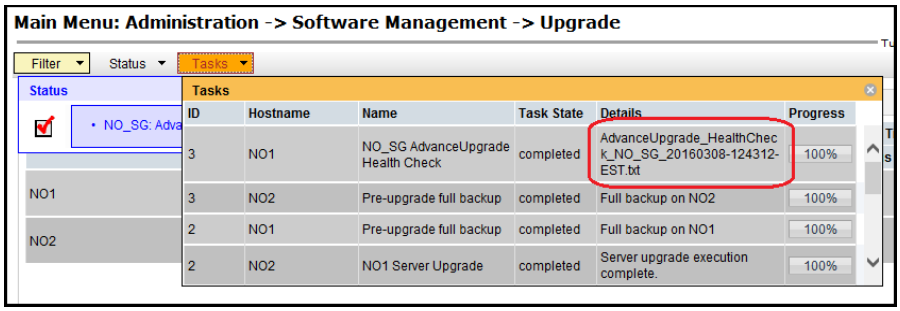
3.4.3.2 Data Collection for Source Release 7.3, 7.4

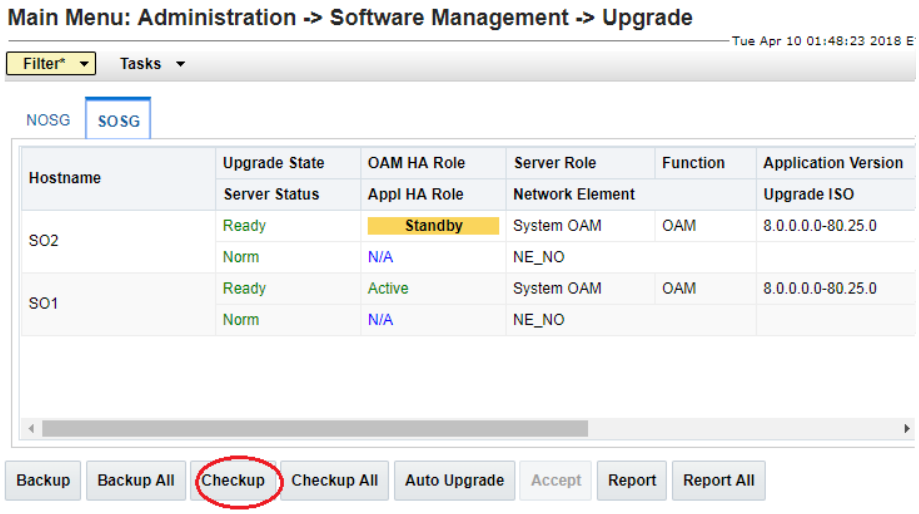
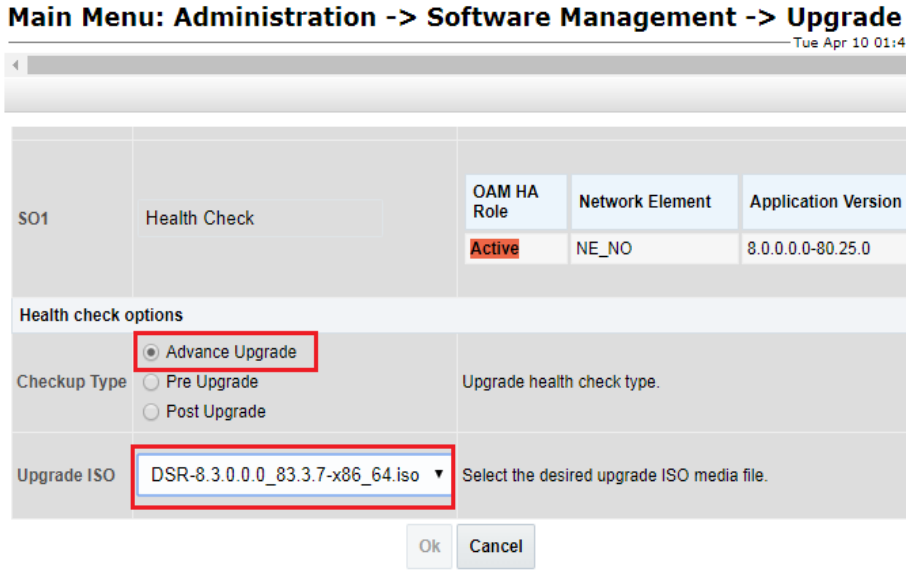
This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.3, or 7.4.

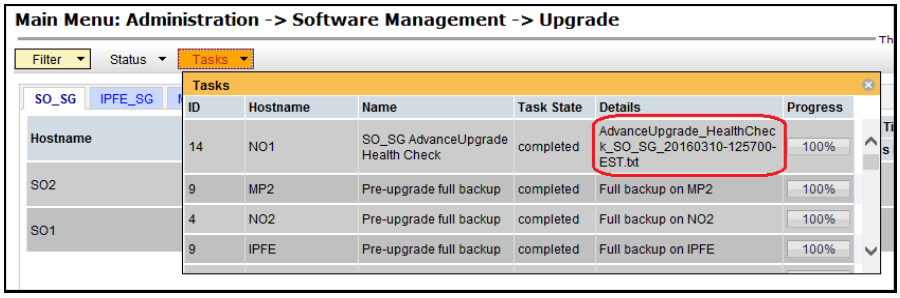
Procedure 4. Data Collection for Source Release 7.3, 7.4

Step #	Procedure	Description
This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Run the automated health checks on the active NOAM	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the active NOAM.

Step #	Procedure	Description
		  3. Click **Checkup**. 4. In the Health check options section, select the **Advance Upgrade** option. 5. If the ISO Administration procedure has already been performed for the target ISO, select the **target release ISO** from the Upgrade ISO option. Otherwise, do not select an ISO. 6. Click **OK**. Control returns to the Upgrade screen.

Step #	Procedure	Description
		
2. ☐	**Active NOAM VIP**: Monitor health check progress	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as **<NOServerGroup> AdvanceUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze any health check failures	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the **UpgradeHealthCheck.log** file and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance.

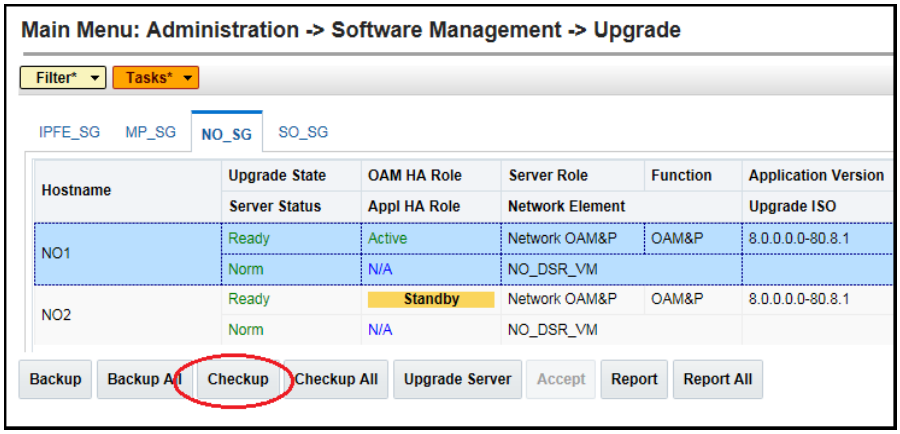
Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Initiate SOAM health check	This procedure runs the automated health checks on the active SOAM. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM server group tab. 3. Select the active SOAM.  4. Click **Checkup**. 5. In the Health check options section, select the **Advance Upgrade** option. 6. For a major upgrade, select the **target release ISO** from the Upgrade ISO option. Do not select an ISO for an incremental upgrade. 7. Click **OK**. Control returns to the Upgrade screen. 

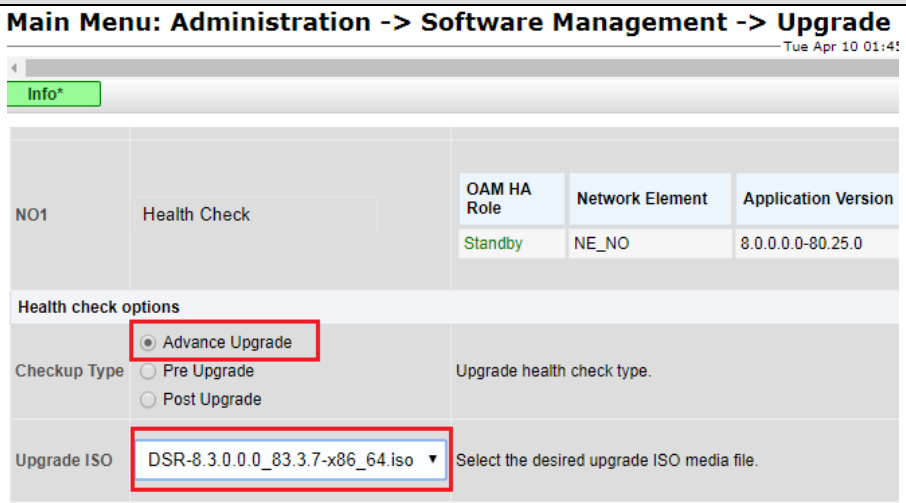
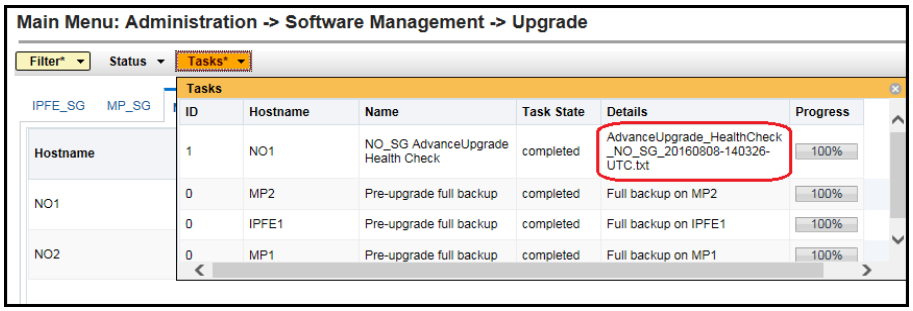
Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Monitor health check progress	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <SOServerGroup> **AdvanceUpgrade Health Check**. 2. Monitor the health check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
6. ☐	**Active NOAM VIP**: Analyze health check failures	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the active SOAM tab. 3. Select the **UpgradeHealthCheck.log** file and click **View**. 4. Locate the log entries for the most recent health check. 5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance. If the health check log contains the **Unable to execute Health Check on <Active SOAM hostname>** message, perform health checks in accordance with Procedure 4.
7. ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA that are out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.4.3.1 and steps 1 through 6 of this procedure. The Health Check reports from steps 3 and 6 can be found in **Status & Manage > Files** on the active SOAM. 2. It is recommended to plan for MP upgrades by consulting to assess the impact of out-of-service MP servers 3. Determine the manner in which the MP servers are upgraded: Manually or Automated Server Group Upgrade. If the MPs are upgraded manually, determine the exact sequence in which MP servers are upgraded for each site.

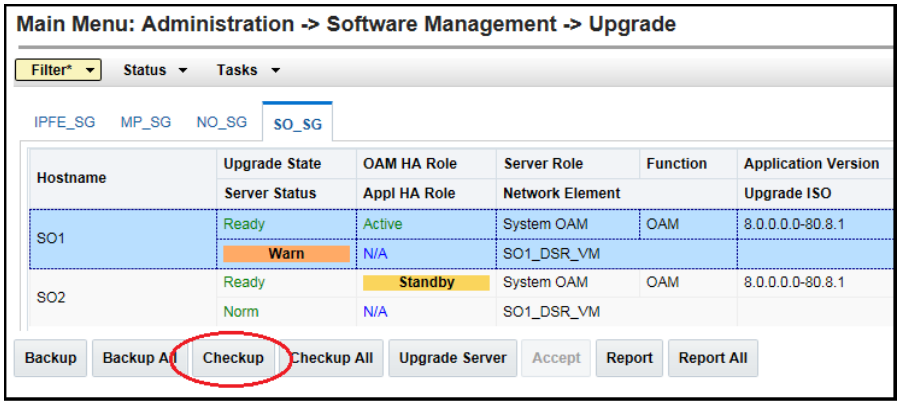
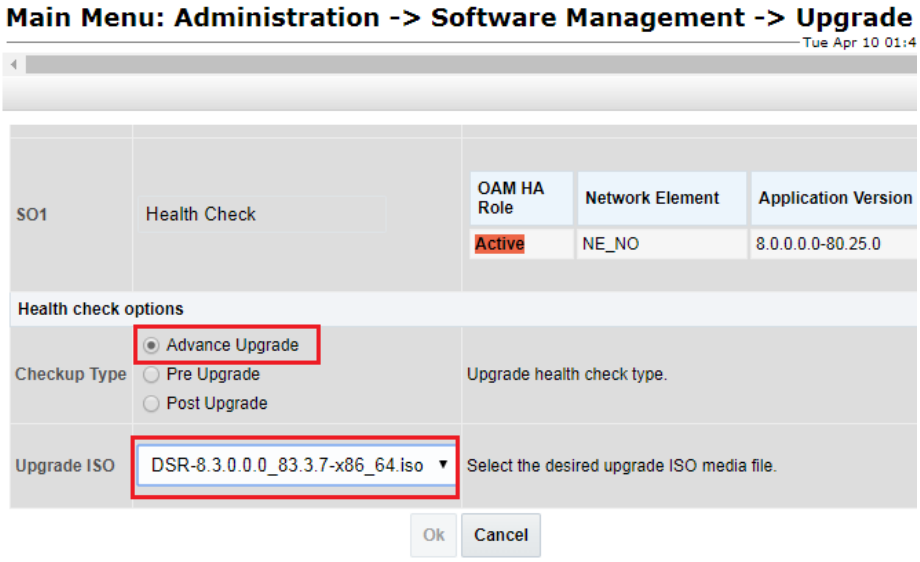
3.4.3.3 Data Collection for Source Release 8.0 and Later

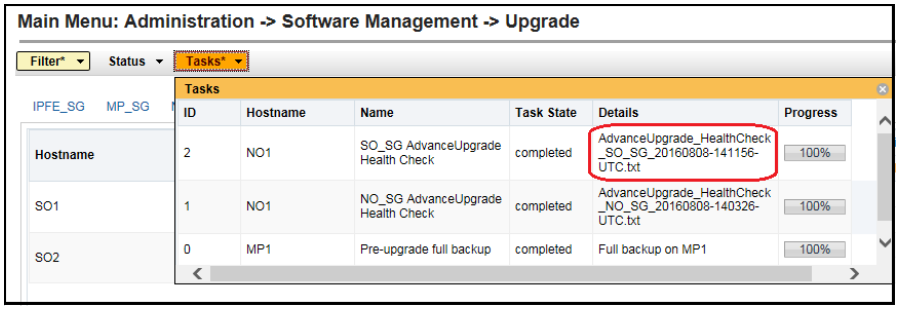
This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 8.0 and later.

Procedure 5. Data Collection for Source Release 8.0 and Later

Step #	Procedure	Description
This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Run the automated health checks on the active NOAM	4. Navigate to **Administration > Software Management > Upgrade**. 5. Select the active NOAM.  6. Click **Checkup**. 7. In the Health check options section, select the **Advance Upgrade** option. 8. If the ISO Administration procedure has already been performed for the target ISO, select the **target release ISO** from the Upgrade ISO option. Otherwise, do not select an ISO. 9. Click **OK**. Control returns to the Upgrade screen.

Step #	Procedure	Description
		
2. ☐	**Active NOAM VIP**: Monitor health check progress	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **AdvanceUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze any health check failure	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the **UpgradeHealthCheck.log** file and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance.

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Initiate SOAM health check	This procedure runs the automated health checks on the active SOAM. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM server group tab. 3. Select the active SOAM.  4. Click **Checkup**. 5. In the Health check options section, select the **Advance Upgrade** option. 6. For a major upgrade, select the **target release ISO** from the Upgrade ISO option. Do not select an ISO for an incremental upgrade. 7. Click **OK**. Control returns to the Upgrade screen. 

Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Monitor health check progress	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <SOServerGroup> **AdvanceUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
6. ☐	**Active NOAM VIP**: Analyze health check failure	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the active SOAM tab. 3. Select the **UpgradeHealthCheck.log** file and click **View**. 4. Locate the log entries for the most recent health check. 5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance. If the health check log contains the **Unable to execute Health Check on <Active SOAM hostname>** message, perform health checks in accordance with Procedure 4.
7. ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA which are out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.4.3.1 and steps 1. through 6. of this procedure. The Health Check reports from steps 3. and 6. can be found in **Status & Manage > Files** on the active SOAM. 2. It is recommended to plan for MP upgrades by consulting My Oracle Support (MOS) to assess the impact of out-of-service MP servers. 3. Determine the manner in which the MP servers are upgraded: Manually or Automated Server Group Upgrade. If the MPs are upgraded manually, determine the exact sequence in which MP servers are upgraded for each site.

3.4.4 ISO Link Correction

This procedure is required when upgrading from Release 7.1, 7.2, 7.3, or 7.4 to DSR 8.2 and later. In DSR 7.x, the ISO image management was changed to put a symlink in the **/var/TKLC/upgrade** directory to the actual file in the **/var/TKLC/db/filemgmt** directory. However, in order to support the Storage Reclamation feature used in DSR 8.0, the symlinks to the ISO image in the /var/TKLC/db/filemgmt/isos directory must be removed and replaced with direct copies of the ISO image in the **/var/TKLC/upgrade** directory.

This must be executed after the application ISO has been deployed but before the software upgrade in Section 4. This may be done in a maintenance window before the actual upgrade maintenance window.

This procedure is not required if the source release is 8.x.

Procedure 6. ISO Link Correction

Step #	Procedure	Description
This procedure performs the ISO symlink correction. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Verify this procedure should be run	• Is the topology of servers to be upgraded currently running DSR release 7.1, 7.2, 7.3, or 7.4? • Has the new DSR 8.2 ISO been deployed? If **Yes**, then proceed to next step. If **No**, this procedure is complete.
2. ☐	**Active NOAM GUI**: Undeploy all unneeded ISO images	Remove all unneeded old ISO images from the **/var/TKLC/upgrade** directory. Keep deployed the ISO image file being used for this upgrade. This saves space in the **/var/TKLC/upgrade** directory. 1. Navigate to **Status & Manage > Files**. 2. Select the ISOs to be undeployed and click **Undeploy ISO**. 3. Click **OK** to confirm the ISO undeployment. This launches the ISO un-deployment to the entire topology. This function removes the symlink in **/var/TKLC/upgrade** to the ISO in the isos directory. The **Tasks** option at the top of the Files page displays the status of the undeployment for each server. In addition, an ISO Deployment report can be viewed by selecting the ISO and clicking **View ISO Deployment Report**.
3. ☐	**Active NOAM CLI**: Log into the active NOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM: `ssh admusr@<NOAM_VIP>`
4. ☐	**Active NOAM CLI**: Mount the DSR 8.2 ISO image	The following example uses a DSR ISO image name as an example. Use the appropriate application ISO image name. `$ sudo mount -o loop /var/TKLC/db/filemgmt/isos/DSR-8.3.0.0.0_83.x.y-x86_64.iso /mnt/upgrade`

Step #	Procedure	Description
5. ☐	**Active NOAM CLI**: Copy the script from the mounted ISO to /var/tmp	`$ cp /mnt/upgrade/upgrade/bin/changeLinksToFiles.php /var/tmp`
6. ☐	**Active NOAM CLI**: Unmount the DSR 8.2 ISO image	`$ sudo umount /mnt/upgrade`

7. ☐	**Active NOAM CLI**: Verify the script is executable	`$ chmod +x /var/tmp/changeLinksToFiles.php`
		`$ ls -l /var/tmp/changeLinksToFiles.php`
		`-r-x------ 1 admusr admgrp 2652 Dec  2 14:07 /var/tmp/changeLinksToFiles.php`
		In the above example, the **x** is present for admusr, indicating that the script is indeed executable for the user.

Step #	Procedure	Description

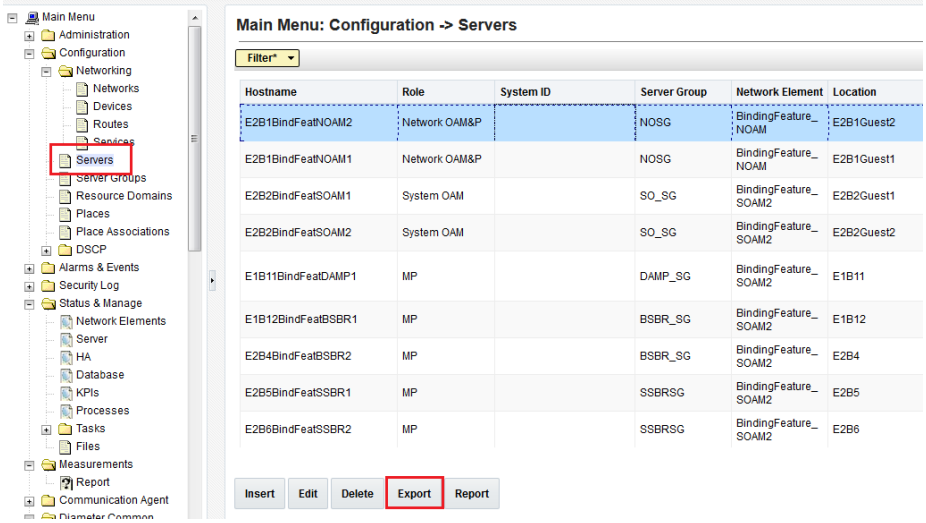
8.
☐
	Active NOAM CLI: Execute the script to change the symlink into a copy of the ISO image file	***Note***: Make sure user is **admusr** and not root. Do not use sudo before of this script.
		`$ /var/tmp/changeLinksToFiles.php`
		The script uses SSH to contact all the servers in the topology and convert any link to an ISO images in **/var/TKLC/upgrade** into a copy of the ISO image file.
		Output similar to the following occurs for each server in the entire topology.
		`$ /var/tmp/changeLinksToFiles.php`
		`server: NO1`
		`hostname alias based on service: no1-internalimi`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi, 192.168.1.11' (RSA) to the list of known hosts.`
		`found link /var/TKLC/upgrade/DSR-8.3.0.0.0_83.3.7-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi, 192.168.1.11' (RSA) to the list of known hosts.`
		`Remove command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/DSR-8.3.0.0.0_83.3.7-x86_64.iso`
		`FIPS integrity verification test failed.`
		`Warning: Permanently added 'no1-internalimi, 192.168.1.11' (RSA) to the list of known hosts.`
		`Copy command succeeded! host: no1-internalimi, file: /var/TKLC/upgrade/DSR-8.3.0.0.0_83.3.7-x86_64.iso`
		The following expected messages can be ignored:
		`FIPS integrity verification test failed.`
		`Warning: Permanently added '<host>-internalimi,<IP address>' (RSA) to the list of known hosts.`
		If any unexpected failure messages occur, it is recommended to contact for guidance.

3.4.5 Back Up TKLCConfigData Files

This procedure helps to restore networking and server-related information in some cases. For example, disaster recovery when it needs to be performed on servers in case a server is lost during an upgrade.

Procedure 7. TKLCConfigData backup

Step #	Procedure	Description
This procedure backs up the **TKLCConfigData** file on all servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Active **NOAM GUI**: Login	Use the VIP address to access the primary NOAM GUI

Step #	Procedure	Description
2. ☐	Primary DSR NOAM VIP (GUI): Export configuration data for each server	1. Navigate to **Configuration > Servers**. 2. Select each server in the topology and click **Export**.  4. Repeat this for all servers.

3. ☐	**Primary SDS NOAM Server**: Back up TKLCConfig data	1. Access the primary DSR NOAM server command line using ssh or a console.
		`ssh admusr@<NOAM_VIP>`
		2. Transfer the TKLCConfigData files for all servers in the /var/TKLC/db/filemgmt directory to a remote location.
		`$ cd /var/TKLC/db/filemgmt`
		`$ scp TKLCConfigData.<Sever Hostname>.sh <username>@<remote-server>:<directory>`
		Example:
		`scp TKLCConfigData.DSRNO1.sh <username>@<remote-server>:<directory>`
		Remember to back up the TKLCConfig data file for **all** servers.

3.4.6 Full Backup of DB Run Environment at Each Server

The procedures in this section are part of software upgrade preparation and are used to conduct a full backup of the run environment on each server, to be used in the event of a back out of the new software release. The backup procedure to be executed is dependent on the software release that is running on the active NOAM.

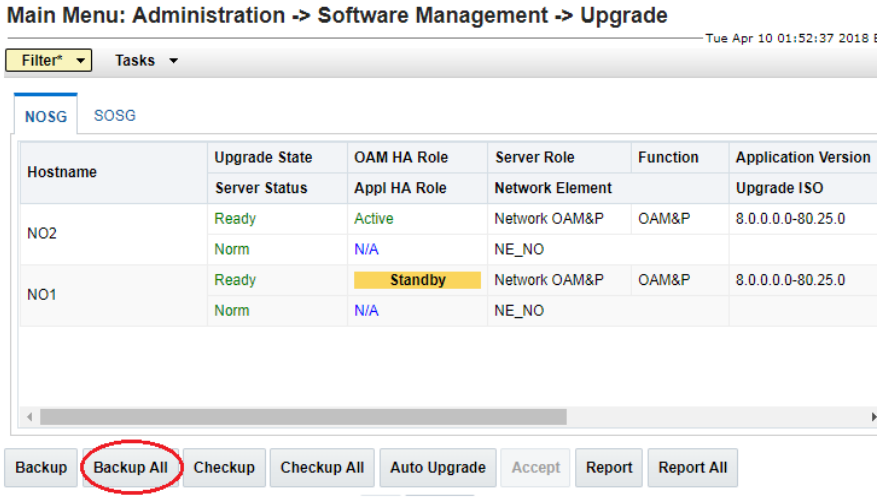
Note: Do not perform this procedure until the ISO deployment is completed to all servers in the topology. Failure to complete the ISO may disrupt ISO deployment/undeployment in the event of a partial backout (for example, backout of one site).

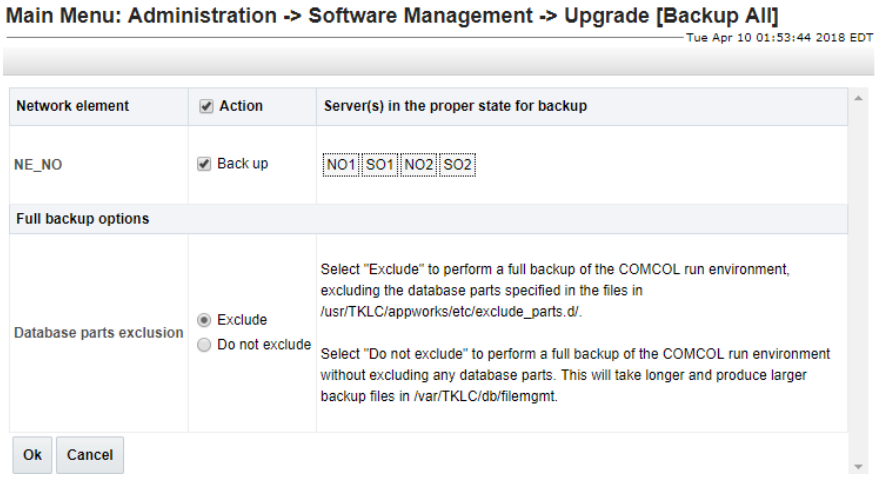
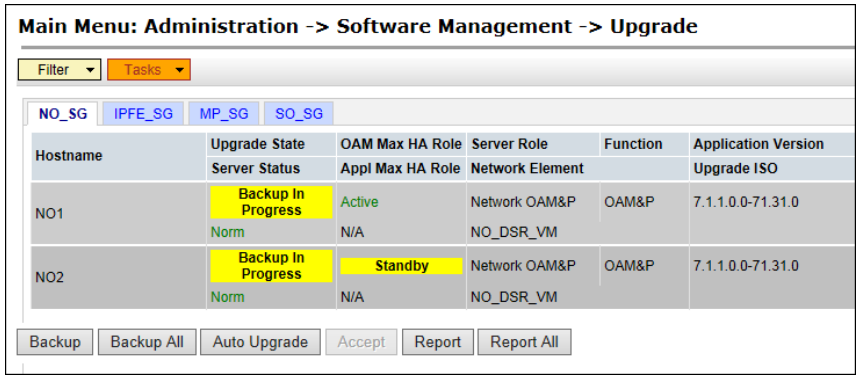
!!WARNING!! If back out is needed, any configuration changes made after the DB is backed up at each server is lost.

3.4.6.1 Full Backup of DB Run Environment for Release 7.3.x and Later

This procedure backs up the DB run environment when the active NOAM is on release 7.3.x and later.

Procedure 8. Full Backup of DB Run Environment for Release 7.3.x and Later

Step #	Procedure	Description
This procedure (executed from the active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Start backup of all servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Click **Backup All**. 

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Select network elements to backup	The Upgrade Backup All screen displays the various network elements and identifies which servers are ready for backup. 1. In the **Action** column, mark the **Back up** checkbox for each network element. 2. Ensure the **Exclude** option is selected. 3. Click **OK**. This initiates a full back up on each eligible server. 
3. ☐	**Active NOAM VIP**: Monitor backup progress	Select each server group tab and verify each server transitions from **Backup in Progress** to **Ready**. 

Step #	Procedure	Description

4. ☐	**ALTERNATIVE METHOD** (Optional)
	Server CLI: If needed, the alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script
		ALTERNATIVE: A manual backup can be executed on each server individually, rather than using the GUI method. To do this, log into each server in the site individually, and execute this command to generate a full back up on that server manually:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following indicates successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

5. ☐	**Active NOAM VIP**: Verify backup files are present on each server	1. Log into the active NOAM.
		2. Navigate to **Status & Manage > Files**.
		3. Click on each server tab.
		4. For each server, verify the following 2 files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

3.4.7 IDIH Pre-Upgrade

If IDIH is a component of a Network Element, it should be upgraded only after the DSR. However, it should be noted that certain compatibility limitations may exist while the two components (DSR and IDIH) are not on the compatible release.

The IDIH upgrade procedures are provided in Appendix F and may be performed at any time after Section 3.4.7.1 has been completed.

Table 10. IDIH Upgrade Preparation Overview

Procedure	Elapsed Time (hr:min)		Procedure Title
	This Step	Cum.	
Procedure 9	0:15-0:30	0:15-0:30	Procedure 9

3.4.7.1 IDIH Upgrade Preparation

Procedure 9. IDIH Upgrade Preparation

Step #	Procedure	Description
This procedure prepares the Mediation and Application guests for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Place the Mediation and Application OVAs in the cloud repository	Follow the hypervisor's instructions to add the Mediation and Application OVAs to the cloud repository.

3.5 Software Upgrade Execution Overview

It is recommended to contact before executing this upgrade to ensure that the proper media are available for use.

Before upgrading, users must perform data collection and system health check procedures in section 3.4. This ensures 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 an upgrade can proceed with alarms.

!!WARNING!!

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

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

Please read the following notes on upgrade procedures:

- All procedure completion times shown in this document are estimates. Times may vary due to differences in database size, user experience, and user preparation.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
  - Session banner information such as **time** and **date**.
  - System-specific configuration information such as **hardware locations**, **IP addresses** and **hostnames.**
  - ANY information marked with **XXXX** or **YYYY**. Where appropriate, instructions are provided to determine what output should be expected in place of **XXXX** or **YYYY**.
  - Aesthetic differences unrelated to functionality such as **browser attributes: window size**, **colors**, **toolbars,** and **button layouts**.

- After completing each step, and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A checkbox is provided. For procedures which are executed multiple times, the checkbox 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 a representative is not present during the upgrade.
- Answer these questions, and record:

  What is the DSR Application version to be upgraded? _____

  What is the DSR Application new version to be applied? _____

  Is this a Major or Incremental Upgrade? _____

  Are there IPFE servers to upgrade? _____

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

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

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

3.5.1 Accepting the Upgrade

After the upgrade of ALL Servers in the topology has been completed, and following an appropriate soak time, the Post-Upgrade procedures in Section 5.4 are performed in a separate Maintenance Window to finalize the upgrade. Procedure 44 accepts the upgrade and performs a final Health Check of the system to monitor alarms and server status. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4. NOAM Upgrade Execution

NOAM UPGRADE

The NOAM upgrade section is common to all topologies. This section must be completed before executing the site upgrade procedures.

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

Global Provisioning is disabled before upgrading the NOAM servers. Provisioning activities at the NOAM and SOAM servers have certain limitations during the period where the NOAMs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in Table 11 specifies the time to upgrade the DSR application. All times are estimates.

Table 11. NOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 10 or Procedure 11	0:20-0:30 0:20-0:30	0:20-0:30 0:20-0:30	Procedure 10 Procedure 11	None None
Procedure 12	0:05-0:10	0:25-0:55	Procedure 12	None
Procedure 13	0:01-0:05	0:26-1:00	Procedure 13	Global Provisioning Disabled
Procedure 14	0:40-1:20	1:06-2:20	Procedure 14	No Traffic Impact
Procedure 15	0:06-0:20	1:12-2:40	Procedure 15	None
Procedure 16	0:05-0:10	1:17-2:50	Procedure 16	Global Provisioning Enabled

4.1 NOAM Pre-Upgrade Checks and Backup

The procedures in this section perform health checks and backups to prepare the NOAM NE for upgrade. These procedures must be executed on the active NOAM.

Note: These procedures may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 14.

Note: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE:: No record in alarm table for FAILURE!**, see Procedure 73.

!!WARNING!!

Increase the Maximum Number of Open Files

As the number of servers in the topology grows, so does the need for additional files to handle merging data to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files.

See Appendix B to increase the maximum number of open files.

4.1.1 NOAM Health Check for Source Release 7.3, 7.4

This procedure is used to determine the health and status of the network and servers when the NOAM is on release 7.3, or 7.4. This procedure must be executed on the active NOAM.

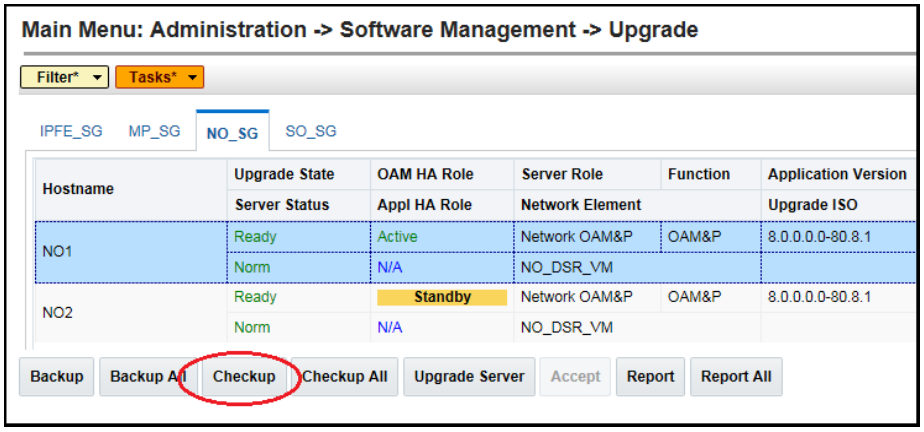
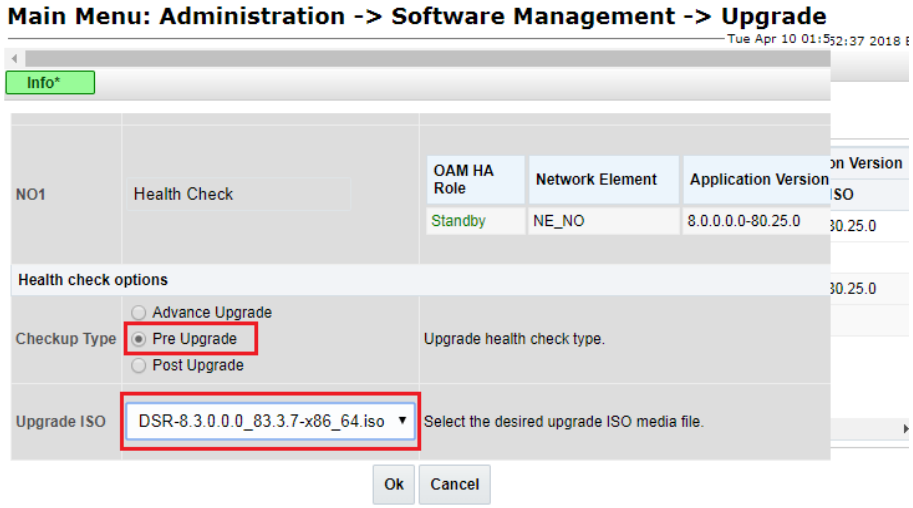
Note: This procedure may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 14.

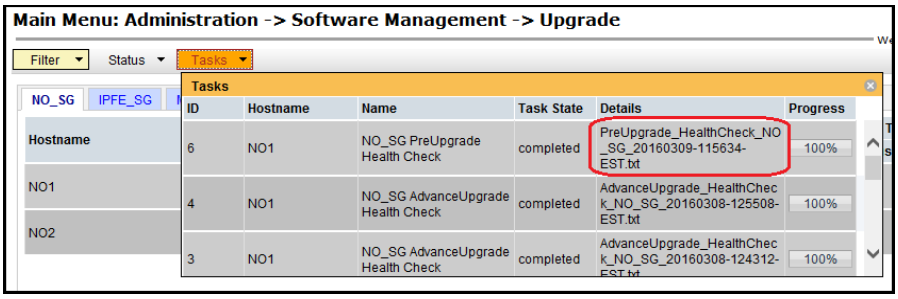
Procedure 10. NOAM Health Check for Source Release 7.3, 7.4

Step #	Procedure	Description
This procedure performs a Health Check on the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active NOAM VIP: Verify upgrade DSR ISO has been transferred to all servers	5. Navigate to **Status & Manage > Files**.
		6. Select the target release DSR ISO and click **View ISO Deployment Report**.
		7. Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.3.0.0_83.4.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

2. ☐	**Active NOAM VIP**: Export and archive the Diameter configuration data	1. Navigate to **Diameter Common > Export**. 2. Capture and archive the Diameter data by selecting the **ALL** option for the Export Application. 3. Verify the requested data is exported by clicking **Tasks** at the top of the screen. 4. Navigate to **Status & Manage > Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Initiate NOAM health checks	This procedure runs the automated pre-upgrade health checks. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the active NOAM.  3. Click **Checkup**. 4. Under Health check options, select the **Pre Upgrade** option. 5. From the Upgrade ISO option, select the target release ISO. 6. Click **OK**. Control returns to the Upgrade screen. 

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Monitor health check progress for completion	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> PreUpgrade Health Check. 2. Monitor the Health Check task until the **Task State** is completed. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
5. ☐	**Active NOAM VIP**: Analyze health check results	Analyze health check report for failures. If the Health Check report status is anything other than **Pass**, analyze the Health Check logs to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the **PreUpgrade_HealthCheck_<NOAM SG>_<TIMESTMP>.txt** file and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. 5. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance as described in Appendix X. If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform health checks in accordance with Procedure 10.

4.1.2 NOAM Health Check for Source Release 8.0 and Later

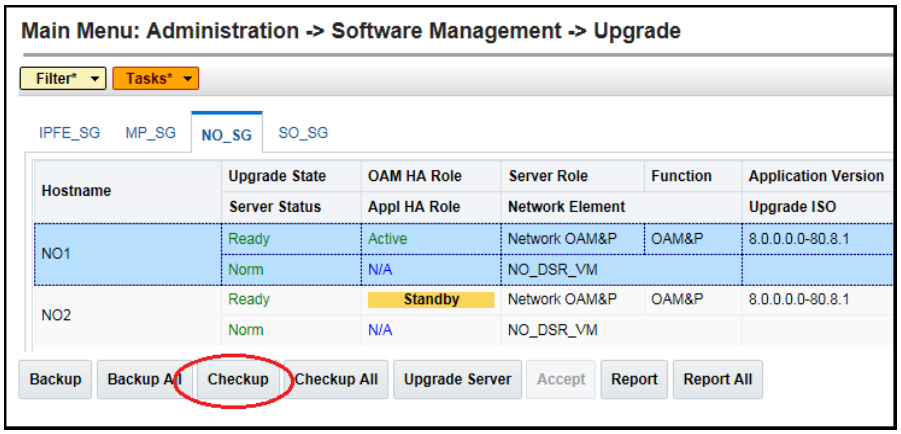
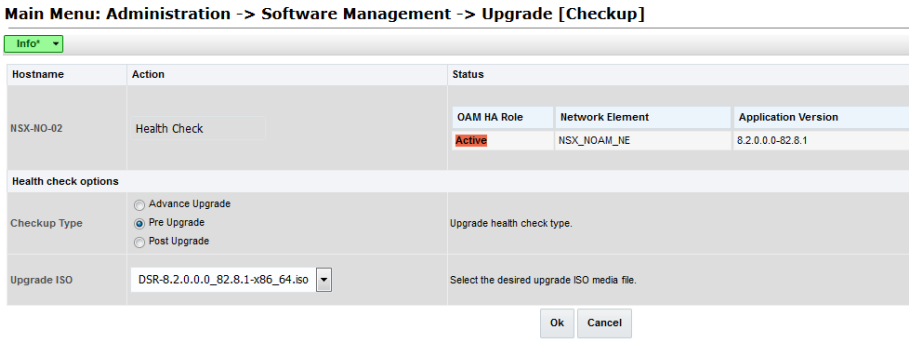
This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 8.0 or later. This procedure must be executed on the active NOAM.

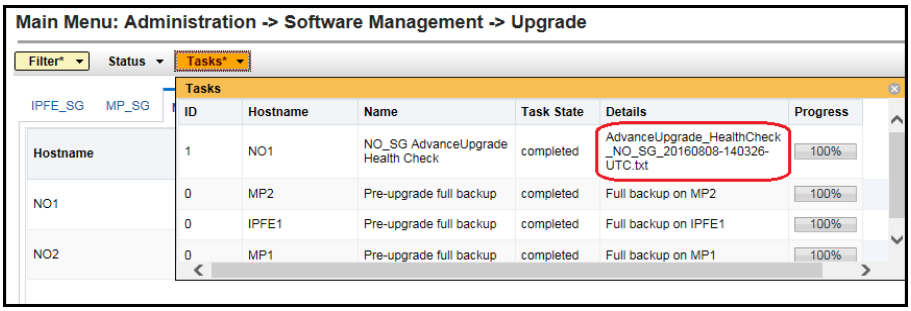
Procedure 11. NOAM Health Check for Source Release 8.0 or Later

Step #	Procedure	Description
This procedure performs a Health Check of the system before upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active NOAM VIP: Verify upgrade DSR ISO has been transferred to all servers	6. Navigate to **Status & Manage > Files**.
		7. Select the target release DSR ISO and click **View ISO Deployment Report**.
		8. Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.3.0.0.0_83.3.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

2. ☐	**Active NOAM VIP**: Export and archive the Diameter configuration data	1. Navigate to **Diameter Common > Export**. 2. Capture and archive the Diameter data by selecting the **ALL** option for the Export Application. 3. Verify the requested data is exported by clicking **Tasks** at the top of the screen. 4. Navigate to **Status & Manage > Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Initiate NOAM health checks	This procedure runs the automated pre-upgrade health checks. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the active NOAM.  3. Click **Checkup**. 4. Under Health Check options, select the **Pre Upgrade** option. 5. From the Upgrade ISO option, select the target release ISO. 6. Click **OK**. Control returns to the Upgrade screen. 

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Monitor health check progress for completion	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> PreUpgrade Health Check. 2. Monitor the Health Check task until the **Task State** is completed. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
5. ☐	**Active NOAM VIP**: Analyze health check results	Analyze health check report for failures. If the Health Check report status is anything other than **Pass**, analyze the Health Check logs to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the **AdvancedUpgrade_HealthCheck_<NOAM SG>_<TIMESTMP>.txt** file and click View. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. 5. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact . If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform health checks in accordance with Procedure 10 or Procedure 11.

4.1.3 NOAM Pre-Upgrade Backup

This procedure takes a backup of the NOAM servers just prior to the upgrade.

Procedure 12. NOAM Pre-Upgrade Backup

Step #	Procedure	Description
This procedure takes a backup of the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Backup all global configuration databases for NOAM ***Important***: Required for disaster recovery	6. Navigate to **Status & Manage > Database** to return to the Database Status screen. 7. Click to highlight the active NOAM server and click **Backup**. ***Note***: **Backup** is only enabled when the active server is selected. 8. Mark the **Configuration** checkbox. 9. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 10. Enter **Comments** (optional). 11. Click **OK**. ***Note***: On the **Status & Manage >Database** screen, the active NOAM server displays the word **Active** in the OAM Max HA Role column.
2. ☐	**Active NOAM VIP**: Download/Save database files backups for NOAM ***Important***: Required for disaster recovery	1. Navigate to **Status & Manage > Files**. 2. Click on the active NOAM server tab. 3. Select the configuration database backup file and click **Download**. 4. If a confirmation window displays, click **Save**. 5. If the Choose File screen displays, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a Download Complete confirmation displays, click **Close**.

4.2 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures no changes are made to the database while the NOAMs are upgraded. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 13. Disable Global Provisioning

Step #	Procedure	Description
This procedure disables provisioning for the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Disable global provisioning and configuration updates on the entire network	1. Log into the active NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Disable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Enable Provisioning**; a yellow information box should also display at the top of the view screen that states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: **Alarm ID = 10008 (Provisioning Manually Disabled)**

4.3 NOAM Upgrade

This procedure is used to upgrade the NOAM and DR NOAM servers.

Procedure 14. NOAM Upgrade

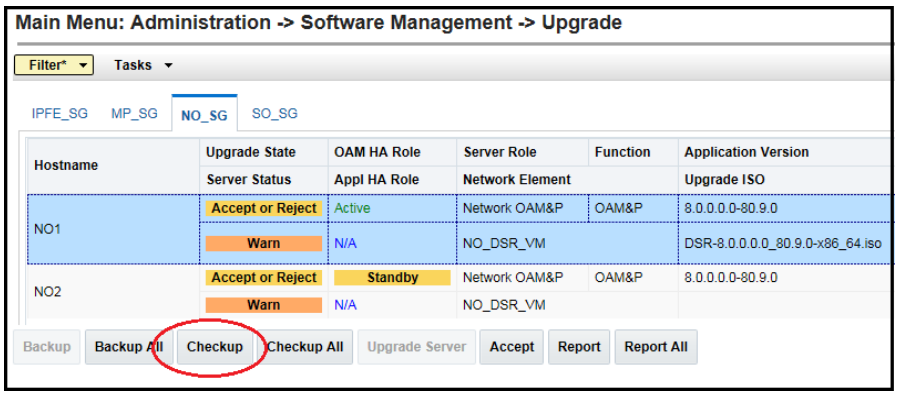
Step #	Procedure	Description
This procedure upgrades the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Upgrade primary DSR standby NOAM	1. Upgrade the primary DSR standby NOAM server using Upgrade Single Server procedure: **If the active NOAM is on DSR 8.x**: Execute Appendix C -- Upgrade Single Server – DSR 8.x. **Otherwise**: Execute Appendix D - Upgrade Single Server – Pre-DSR 8.0. 2. After successfully completing the procedure in Appendix C or Appendix D, return to this point and continue with the next step. The active NOAM server may have some or all of the following expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31225 (HA Service Start Failure)** **Alarm ID = 31226 (HA Availability Status Degraded)** **Alarm ID = 31233 (HA Path Down)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action. If the active NOAM is on release 7.1.1 or later, proceed to step 3.
2. ☐	Upgrade second DSR NOAM	Upgrade the second DSR NOAM server using the Upgrade Single Server procedure: Execute Appendix C -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.
3. ☐	Upgrade standby DR NOAM	Upgrade the standby DR NOAM server using the Upgrade Single Server procedure: Execute Appendix C -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.

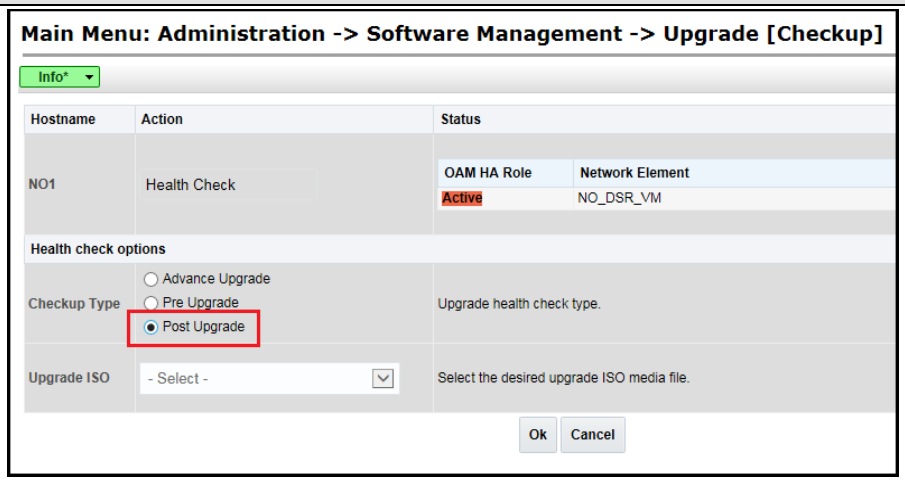
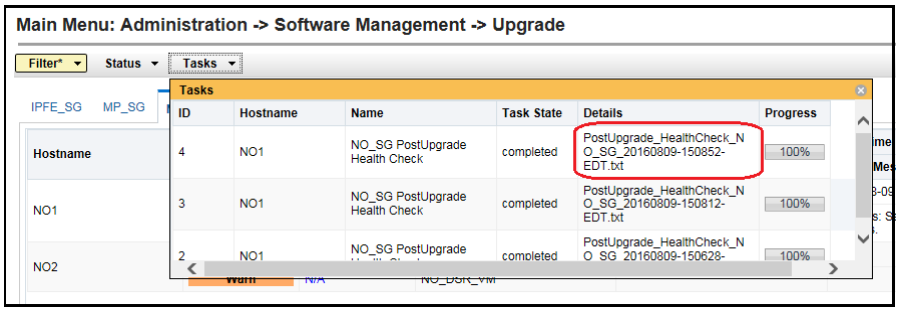
Step #	Procedure	Description
4. ☐	Upgrade active DR NOAM	Upgrade the active DR NOAM server using the Upgrade Single Server procedure: Execute Appendix C -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next procedure per Table 11.

4.4 Verify NOAM Post Upgrade Status

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

Procedure 15. Verify NOAM Post Upgrade Status

Step #	Procedure	Description
This procedure verifies post upgrade status for NOAM upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Post-upgrade health checks	This procedure runs the automated post-upgrade health checks. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the active NOAM.  3. Click **Checkup**. 4. Under Health check options, select the **Post Upgrade** option. 5. Click **OK**. Control returns to the Upgrade screen.

Step #	Procedure	Description
		
2. ☐	**Active NOAM VIP**: Monitor health check progress	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **PostUpgrade Health Check**. 2. Monitor the health check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze health check failures	If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the file named **UpgradeHealthCheck.log** and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance.

4.5 Allow Provisioning (Post NOAM Upgrade)

The following procedure enables Global Provisioning after the NOAM upgrade.

CAUTION Any network-wide provisioning changes made at the NOAM site before the upgrade is accepted are lost if the upgrade is backed out.

Procedure 16. Allow Provisioning (Post NOAM Upgrade)

Step #	Procedure	Description
This procedure enables provisioning for the NOAM and DR NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Enable global provisioning and configuration updates on the entire network	1. Log into the active NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Disable Provisioning.**
	Note: After enabling provisioning at the NOAM, the SOAM GUI(s) may display a banner indicating that global provisioning is disabled. This message can be ignored – global provisioning is enabled. This is a display issue only and is corrected when the SOAMs are upgraded.	
2. ☐	**Active NOAM VIP**: Add new network element (if required)	**Perform this step only if the addition of a new network element is required at this time.** If a new network element is to be added, start this procedure now. The addition of the new network element requires a separate maintenance window. The servers in the new network element must be installed with the same DSR release as that of the upgraded NOAM(s). Follow the release specific installation procedures from reference [1] to install the software on the new servers and add the new network element under the existing NOAM(s). Skip the sections of the installation procedure related to installing and configuring the NOAM(s). This adds a new DSR SOAM site under the existing NOAM(s).

5. Site Upgrade Execution

This section contains the procedures for upgrading an entire site - starting with the pre-upgrade activities, upgrading the SOAMs and C-level servers, and finishing with verifying the upgrade.

To maximize the Maintenance Window usage, the procedures in this section make full use of the parallel upgrade capabilities of the DSR, while ensuring traffic continuity and redundancy to the fullest extent possible.

CAUTION Read 2.4 Automated Site Upgrade for details and limitations/solutions while doing planning of upgrade cycles.

The Automated Site Upgrade procedures are in section 5.2: Automated Site Upgrade. Use the procedures in this section if the Automated Site Upgrade was recommended in section 3.3 Site Upgrade Methodology Selection. See section 5.2.3 for more details for rearranging cycles, if needed.

The manual site upgrade procedures are in section 5.3. Use the procedures in this section if the manual upgrade was recommended in section 3.3 Site Upgrade Methodology Selection.

5.1 Site Pre-Upgrade Activities

SITE UPGRADE: Pre-Upgrade Activities

Use this section to execute pre-upgrade planning, pre-upgrade backups, pre-upgrade health checks, and to disable site provisioning.

This section contains the procedures for site upgrade planning, pre-upgrade backups, health checks, and disabling site provisioning.

Table 12 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 12 as a guide for determining the order in which the procedures are to be executed.

Table 12. Site Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 17	0:10-0:20	0:10-0:20	Procedure 17	None
Procedure 20 or Procedure 19	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:35	0 Procedure 19	None None
Procedure 20	0:03	0:18-0:38	Procedure 20	None
Procedure 21	0:01-0:05	0:19-0:48	Procedure 21	Site Provisioning Disabled, No Traffic Impact
Procedure 22	0:05-0:10	0:24-0:58	Procedure 22	None

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 23	2:40-4:00	3:04-4:58	Procedure 23	Traffic is not serviced by servers that are actively upgrading.
Procedure 24	0:02	3:06-5:00	Procedure 24	Site Provisioning Enabled, No Traffic Impact
Procedure 25	0:10-0:15	3:26-5:15	Procedure 25	None

5.1.1 Site Pre-Upgrade Backups

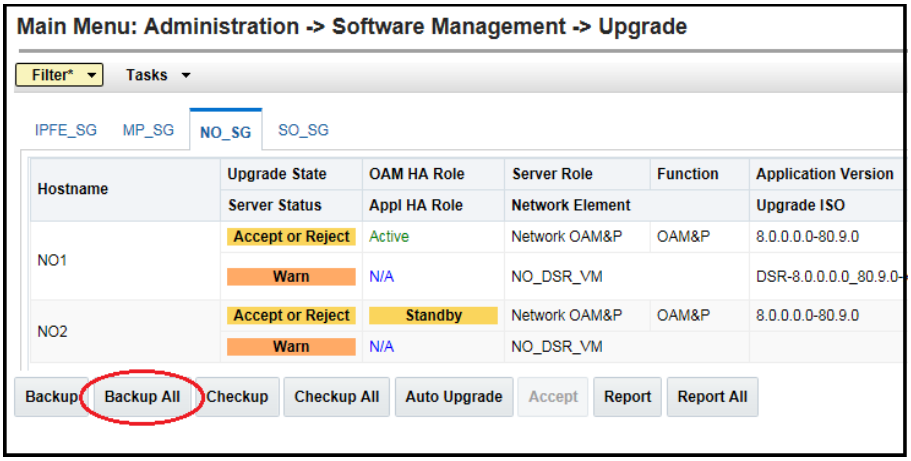
This procedure is non-intrusive and is used to perform a backup of all servers associated with the SOAM Site(s) being upgraded. It is recommended that this procedure be executed no earlier than 36 hours prior to the start of the upgrade.

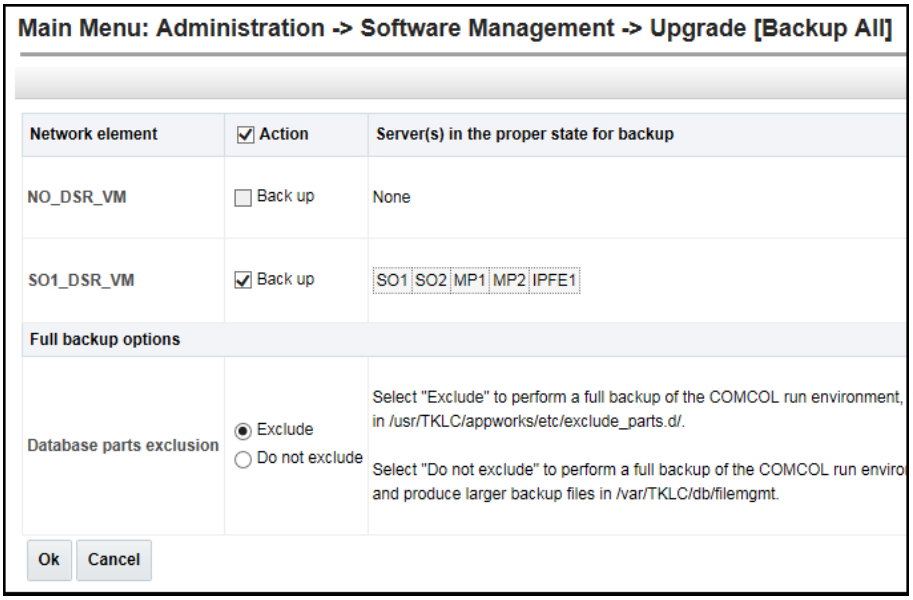
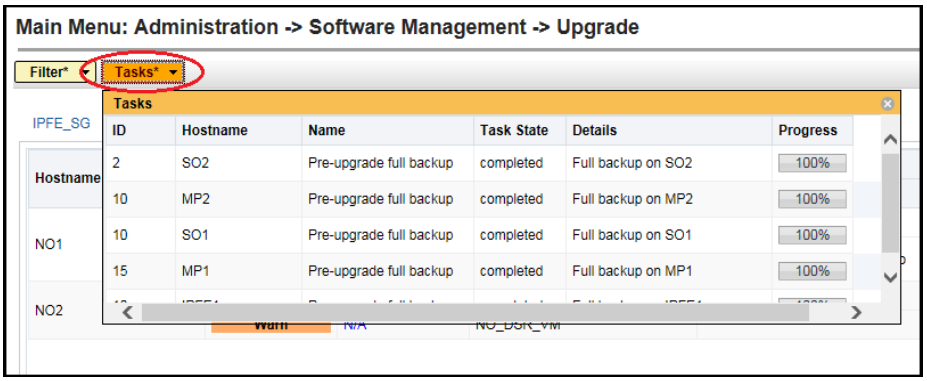
Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 17 is an alternate procedure that can be used to backup a site using the command line. Procedure 17 should only be used by direction of .

Procedure 17. Site Pre-Upgrade Backups

Step #	Procedure	Description
This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM VIP**: Back up site configuration data ***Important***: Required for disaster recovery	1. Log into the SOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database** to return to the Database Status screen. 3. Click to highlight the **Active SOAM** server, and click **Backup.** ***Note***: **Backup** is only enabled when the active server is selected. 4. Mark the **Configuration** checkbox. 5. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 6. Enter **Comments** (optional). 7. Click **OK**. ***Note***: The active SOAM can be determined by navigating to **Status & Manage > HA** and noting which server is currently assigned the VIP in the **Active VIPs** field. The server having VIP assigned is the **Active**.

Step #	Procedure	Description
2. ☐	**Active SOAM VIP**: Download/Save database backup files ***Important***: Required for disaster recovery	1. Navigate to **Status & Manage > Files**. 2. Click on the active SOAM server tab. 3. Select the configuration database backup file and click **Download**. 4. If a confirmation window displays, click **Save**. 5. If the Choose File window displays, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a download complete confirmation displays, click **Close**.
3. ☐	**Active NOAM VIP**: Upgrade/Back up DB run environment for site	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Click **Backup All**. 

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Set backup parameters	The Upgrade Backup All screen displays the various network elements and identifies which servers are ready for backup. 1. In the Action column, mark the **Back up** checkbox for each network element. 2. Verify the **NOAM server group** checkbox is **NOT** marked. ***Note***: Backing up the NOAM servers at this point overwrites the pre-upgrade backup files needed for backing out the target release. Do NOT back up the NOAM servers. 3. In the Full Backup Options section, verify the **Exclude** option is selected. 4. Click **OK**. This initiates a full backup on each eligible server. 
5. ☐	**Active NOAM VIP**: Monitor tasks for backup completion	1. From the Upgrade screen, click the **Tasks** option. 2. Monitor the progress of the backups until the network element(s) selected in step 4 are complete. 

Step #	Procedure	Description

6.
☐
	Active NOAM VIP: Verify backup files are present on each server.	1. Log into the active NOAM or SOAM GUI.
		2. Navigate to **Status & Manage > Files**.
		3. Click on each server tab.
		4. For each server, verify the following 2 files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		5. Repeat sub-steps 1 through 4 for each site being upgraded.

5.1.2 Site Pre-Upgrade Health Checks

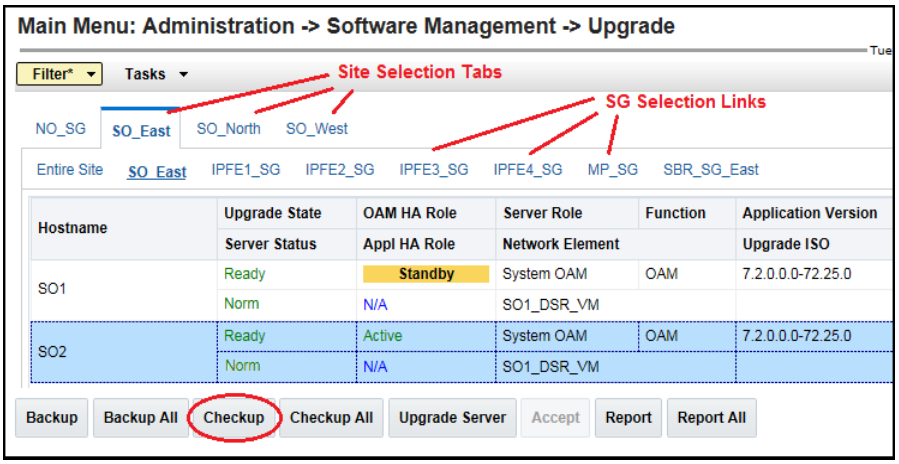
This section provides procedures to verify the health of the SOAM site prior to upgrade. 0 is the primary procedure to be executed when the active NOAM is on release 8.0 and later. Alternate release-specific procedures are also provided, to be used as directed.

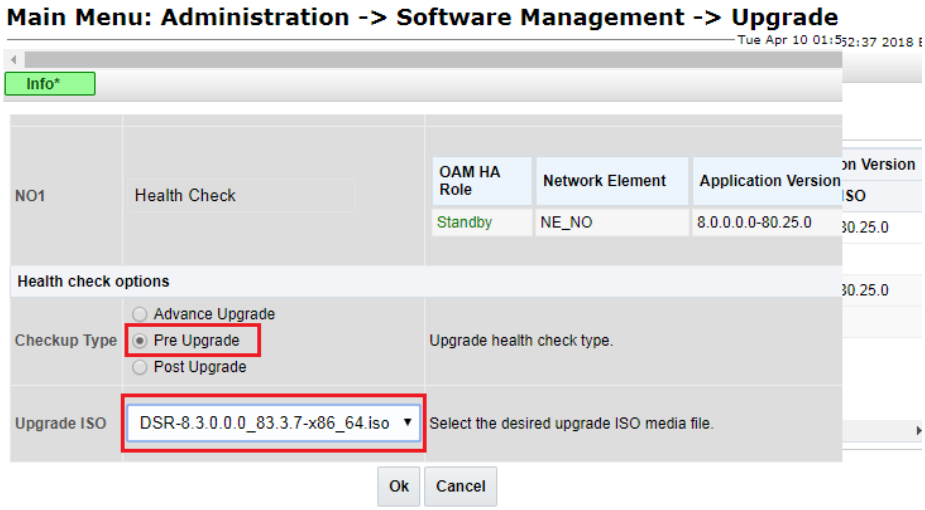
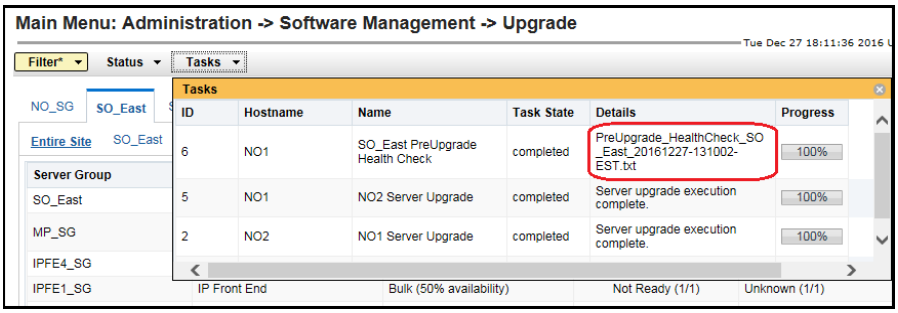
5.1.2.1 Site Pre-Upgrade Health Check for Release 8.0 and Later

This procedure is used when the NOAMs are on release 8.0 and later. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

Note: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE:: No record in alarm table for FAILURE!**, see Procedure 73.**Error! Reference source not found.**.

Procedure 18. Site Pre-Upgrade Health Check for Release 8.0 and Later

Step #	Procedure	Description
This procedure performs a health check before upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Run site health checks (part 1)	Select the SOAM on which health checks are run. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the tab of the site to be upgraded. 3. Select the SOAM server group link. 4. Select the active SOAM. 5. Click **Checkup**. 

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Run site health checks (part 2)	Initiate the health checks. 1. Click **Checkup**. 2. In the Health check options section, select the **Pre Upgrade** option. 3. Use the **Upgrade ISO** option to select the target release ISO. 4. Click **OK** to initiate the health check. Control returns to the Upgrade Administration screen. 
3. ☐	**Active SOAM VIP**: Monitor health check progress for completion	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PreUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 

Step #	Procedure	Description
4. ☐	**Active SOAM VIP**: Analyze any health check failures	If the Health Check report status is anything other than **Pass**, the Health Check logs must be analyzed to determine if the upgrade can proceed. The Health Check log is located in the File Management area of the active SOAM. Select the active SOAM tab to see the Health Check log. 1. Navigate to **Status & Manage > Files**. 2. Select the active SOAM tab. 3. Select the **UpgradeHealthCheck.log** file and click **View**. 4. Locate the log entries for the most recent health check. 5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance. If the health check log contains the **Unable to execute Health Check on <Active SOAM hostname>** message, perform an alternate health check procedure as follows: **If the active SOAM release is 7.x/8.0/8.1:** Execute Procedure 19.
5. ☐	**Active SOAM VIP**: Export and archive the Diameter configuration data on active SOAM GUI	1. Navigate to **Diameter Common > Export**. 2. Capture and archive the Diameter data by selecting the **ALL** option for the Export Application. 3. Click **OK**. 4. Verify the requested data is exported by clicking **Tasks** at the top of the screen. 5. Click **File Management** to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.
6. ☐	Capture data for each SOAM site	Repeat this procedure for each configured SOAM site to be upgraded.

5.1.2.2 SOAM Pre-Upgrade Health Check for Release 7.x

This procedure is an alternate health check that is used when upgrading to release 8.2 and the active SOAM is on release 7.x. The procedure is non-intrusive and performs a health check of the site before upgrading. Do not perform this procedure unless directed in Procedure 19, step 4.

Procedure 19. Site Pre-Upgrade Health Check for Release 7.x

Step #	Procedure	Description
This procedure performs a health check before upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active SOAM CLI: Perform health checks. Verify SOAM pre-upgrade status	1. Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		This command creates three files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If any alarms are present in the system:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		3. If the Server <hostname> needs operator attention before upgrade message displays, inspect the Server Status Report to determine the reason for the message. If the Server <hostname> has no alarm with DB State as Normal and Process state as Kill message displays in the Server Status Report, the alert can be ignored.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact for guidance.
		4. Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

Step #	Procedure	Description
2. ☐	**Active SOAM CLI**: Capture Diameter maintenance status	Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command outputs a series of messages, providing Diameter Maintenance status. Capture this output and save for later use. ***Note***: The output is also captured in **/var/TKLC/db/filemgmt/UpgradeHealthCheck.log**. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
3. ☐	**Active SOAM CLI**: Capture/View DA-MP status	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available. 3. Note the number of Total Connections Established _____
4. ☐	**Active SOAM VIP**: Capture/Export Diameter configuration on active SOAM GUI	1. Navigate to **Diameter Common > Export**. 2. Capture and archive the Diameter data by selecting the **ALL** option for the Export Application. 3. Click **OK**. 4. Verify the requested data is exported by clicking **Tasks** at the top of the screen. 5. Click **File Management** to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.

Step #	Procedure	Description
5. ☐	**Active SOAM VIP**: Capture measurements data	DSR 8.0 introduces **Alarm 22077 – Excessive Request Reroute Threshold Exceeded**. This alarm indicates the request reroutes due to Answer response and/or Answer timeout has exceeded the configured threshold on a DA-MP server. During the upgrade, this threshold is set to 100%, effectively disabling the alarm. Before upgrading a site, measurement statistics are collected from the DA-MPs to serve as a baseline for post-upgrade comparisons. 1. Navigate to **Measurements > Report**. 2. Click **Go** to export. 3. On the Report Export screen, make the following selections: • Report Scope => <Site SOAM NE> • Report Groups => Diameter Rerouting • Time Interval => Fifteen Minute • Time Range => 1 Day • Export Frequency => Once • Task Name => leave as is 4. Click **OK** to initiate the export. 5. When the export task is complete, navigate to **Status & Manage > Files**. 6. Locate the measurements file generated by the export task, and download the file to the local workstation. Save this file for later use in the Post Upgrade Procedures section of this document.
6. ☐	Capture data for each SOAM site	Repeat this procedure for each configured SOAM site to be upgraded.

5.1.3 Site Upgrade Options Check

Automated Site Upgrade provides user-configurable options that control certain upgrade behaviors. These options are found on the active NOAM's **Administration > General Options** screen and are described in detail in Section 2.4.3. Before initiating a site upgrade, review these options to verify the current settings are correct, or to modify the settings to meet customer requirements/preferences.

This procedure is applicable only to Auto Site Upgrade. The options have no effect on manual upgrades or Automated Server Group upgrades.

Procedure 20. Site Upgrade Options Check

Step #	Procedure	Description
This procedure is used to review the site upgrade options and make changes as necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: View auto site upgrade options	1. Log into the active NOAM GUI. 2. Navigate to **Administration > General Options**. 3. Scroll down to the Site Upgrade Bulk Availability option. 4. Review the existing value of this option and determine if changes are needed. If the option is changed, click **OK** to save the change. 5. Scroll down to the **Site Upgrade SOAM Method** option. 6. Review the existing value of this option and determine if changes are needed. If the option is changed, click **OK** to save the change.

5.1.4 Disable Site Provisioning

This procedure disables Site Provisioning in preparation for upgrading the site.

!!WARNING!! This procedure may only be performed in the maintenance window immediately before the start of the SOAM site upgrade.

Procedure 21. Disable Site Provisioning

Step #	Procedure	Description
This procedure disables provisioning for the SOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM VIP**: Disable site provisioning	1. Log into the SOAM GUI of the site to be upgraded. 2. Navigate to **Status & Manage > Database**. 3. Click **Disable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Enable Provisioning**. A yellow information box also displays at the top of the view screen that states: **[Warning Code 004] – Site provisioning has been manually disabled**. The active SOAM server has the following expected alarm: **Alarm ID = 10008 (Provisioning Manually Disabled)**
2. ☐	Repeat for each SOAM site	Repeat this procedure for each configured SOAM site to be upgraded.

5.2 Automated Site Upgrade

!!WARNING!!

The following procedures must be completed before the start of automated site upgrade: Procedure 17; [0 or Procedure 19]; Procedure 20; Procedure 21; and Procedure 22.

Read 2.4 Automated Site Upgrade for details.

Upgrade cycles are created when using the Automated Site Upgrade. Limitations in Appendix P for Automated Site Upgrade can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles, then manually upgrade using section 5.3.

5.2.1 Site Upgrade Pre-Checks

This procedure verifies that the system is prepared for Automated Site Upgrade.

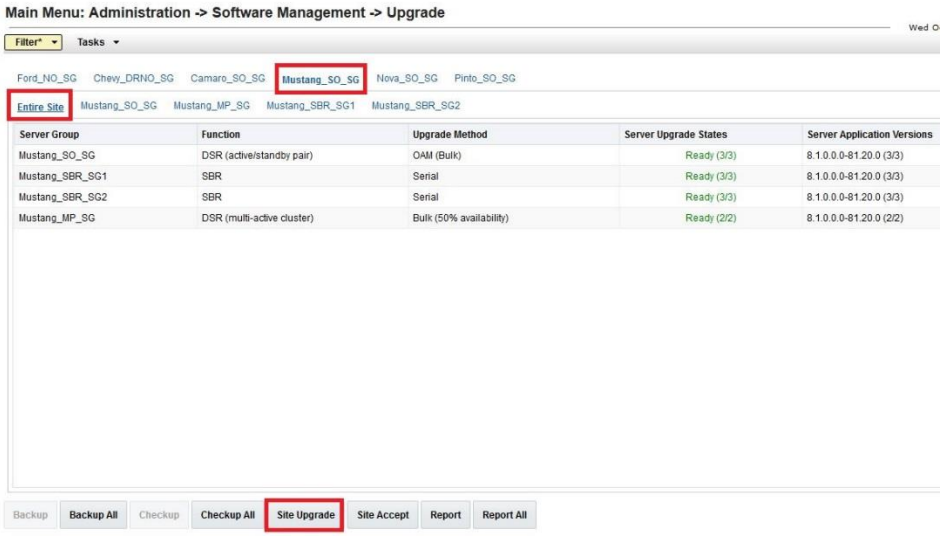
Procedure 22. Site Upgrade Pre-Checks

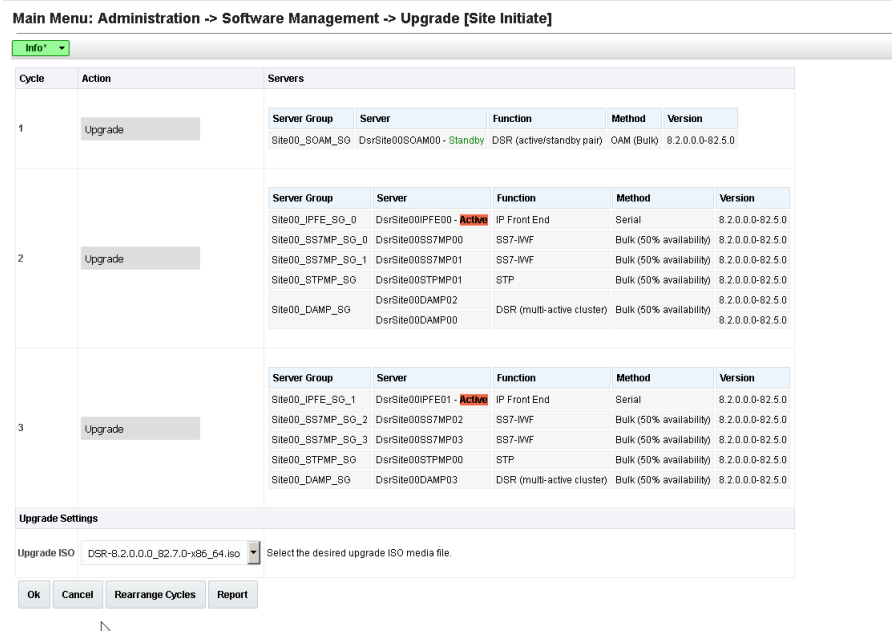
Step #	Procedure	Description
This procedure verifies traffic status, and verifies that Site Provisioning is disabled, in preparation for upgrading the site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM VIP**: View KPIs to verify traffic status	1. Log into the active SOAM GUI using the VIP. 2. Navigate to **Status & Manage > KPIs**. 3. Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	**Active SOAM VIP**: Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 21. In the GUI status bar, where it says **Connected using …**, check for the message **Site Provisioning disabled**. If the message is present, continue with the next procedure per Table 12; otherwise, execute Procedure 21.

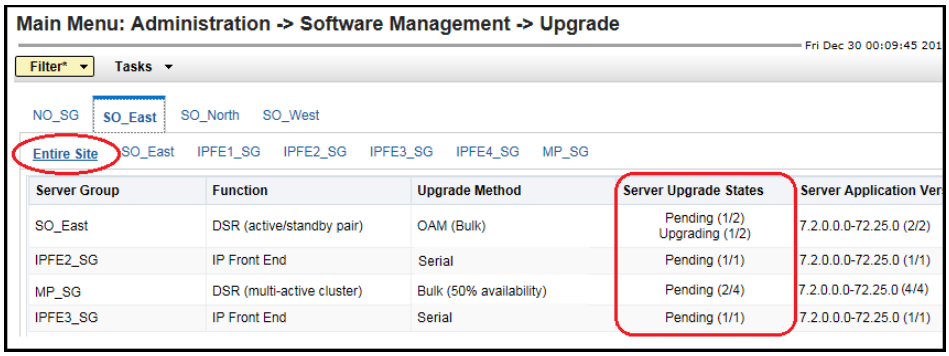
5.2.2 Initiate Automated Site Upgrade

This procedure initiates the Automated Site Upgrade sequence.

Procedure 23. Automated Site Upgrade

Step #	Procedure	Description
This procedure upgrades an entire site using the Automated Site Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Review site upgrade plan and site readiness	Review the site upgrade plan created in Section 3.2. This step verifies that the servers and server groups to be upgraded are in the proper state. 1. Log into the NOAM GUI using the VIP. 2. Select **Administration > Software Management > Upgrade**. 3. Select the SOAM tab of the site to be upgraded. 4. Verify the **Entire Site** link is selected. The Entire Site screen provides a summary of the server states and upgrade readiness. More detailed server status is available by selecting a specific server group link.  Server Group: Mustang_SO_SG, Mustang_SBR_SG1, Mustang_SBR_SG2, Mustang_MP_SG Function: DSR (active/standby pair), SBR, SBR, DSR (multi-active cluster) Upgrade Method: OAM (Bulk), Serial, Serial, Bulk (50% availability) Server Upgrade States: Ready (3/3), Ready (3/3), Ready (3/3), Ready (2/2) Server Application Versions: 8.1.0.0.0-81.20.0 (3/3), 8.1.0.0.0-81.20.0 (3/3), 8.1.0.0.0-81.20.0 (3/3), 8.1.0.0.0-81.20.0 (2/2) ***Note***: The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including **Accept or Reject**, **Ready**, **Backup Needed**, **Failed**, or **Not Ready**. Only the servers in the **Ready** or **Failed** state are upgrade eligible.
2. ☐	**Active NOAM VIP**: Initiate site upgrade	1. Verify no server groups are selected on the upgrade administration screen. The Site Upgrade button is not available if a server group is selected. 2. Click **Site Upgrade**. 3. Review the upgrade plan as presented on the Site Initiate screen. This plan represents an approximation of how the servers are upgraded.

Step #	Procedure	Description
		Due to the dynamic nature of the upgrade, some servers (typically only C-level) may be upgraded in a different cycle than displayed here.  **Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]** Info* Cycle / Action / Servers 1 — Upgrade Server Group: Site00_SOAM_SG; Server: DsrSite00SOAM00 - Standby; Function: DSR (active/standby pair); Method: OAM (Bulk); Version: 8.2.0.0.0-82.5.0 2 — Upgrade Server Group: Site00_IPFE_SG_0; Server: DsrSite00IPFE00 - Active; Function: IP Front End; Method: Serial; Version: 8.2.0.0.0-82.5.0 Site00_SS7MP_SG_0; DsrSite00SS7MP00; SS7-IWF; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_SS7MP_SG_1; DsrSite00SS7MP01; SS7-IWF; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_STPMP_SG; DsrSite00STPMP01; STP; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_DAMP_SG; DsrSite00DAMP02; DSR (multi-active cluster); Bulk (50% availability); 8.2.0.0.0-82.5.0 DsrSite00DAMP00; 8.2.0.0.0-82.5.0 3 — Upgrade Server Group: Site00_IPFE_SG_1; Server: DsrSite00IPFE01 - Active; Function: IP Front End; Method: Serial; Version: 8.2.0.0.0-82.5.0 Site00_SS7MP_SG_2; DsrSite00SS7MP02; SS7-IWF; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_SS7MP_SG_3; DsrSite00SS7MP03; SS7-IWF; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_STPMP_SG; DsrSite00STPMP00; STP; Bulk (50% availability); 8.2.0.0.0-82.5.0 Site00_DAMP_SG; DsrSite00DAMP03; DSR (multi-active cluster); Bulk (50% availability); 8.2.0.0.0-82.5.0 Upgrade Settings Upgrade ISO: DSR-8.2.0.0.0_82.7.0-x86_64.iso — Select the desired upgrade ISO media file. Ok	Cancel	Rearrange Cycles	Report ***Note***: Review the upgrade plan again and ensure all concerns noted in Table 6 have been addressed with the upgrade plan shown on the screen. If you need to rearrange the upgrade cycle, see section 5.2.3 to do it; otherwise, continue with the next step. There are some limitations with upgrading the DC server during its server group upgrade, which are upgraded in a group of servers. This is applicable for all upgrade options, for example DA-MP, vSTP MP(s). So, make sure the DC server is not upgraded in first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix O Identify the DC server. If the DC server displays by default in the first upgrade cycle of its server group, then rearrange the upgrade cycles using section 5.2.3 such that the DC server is not upgraded in the first upgrade cycle of its server group. vSTP MPs should be divided in cycles to avoid a network outage. In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade. The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader** = **Yes**. Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI. 4. From the MMI command using the REST Client for the vSTP configuration. The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**. 5. Use the **/vstp/mpleader** MO. The result is the hostname of the MP leader server.

Step #	Procedure	Description
		6. In the Upgrade Settings section of the form, use the **Upgrade ISO** options to select the target ISO. Click **OK** to start the upgrade sequence. Control returns to the Upgrade Administration screen.
3. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	See step 4. for instructions if the upgrade fails, or if execution time exceeds 60 minutes. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. With the **Entire Site** link selected, a summary of the upgrade status for the selected site displays. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrading, and the number of servers that are pending upgrade. Use this view to monitor the upgrade status of the overall site.  More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group. During the upgrade, the servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 32515 (Server HA Failover Inhibited)**

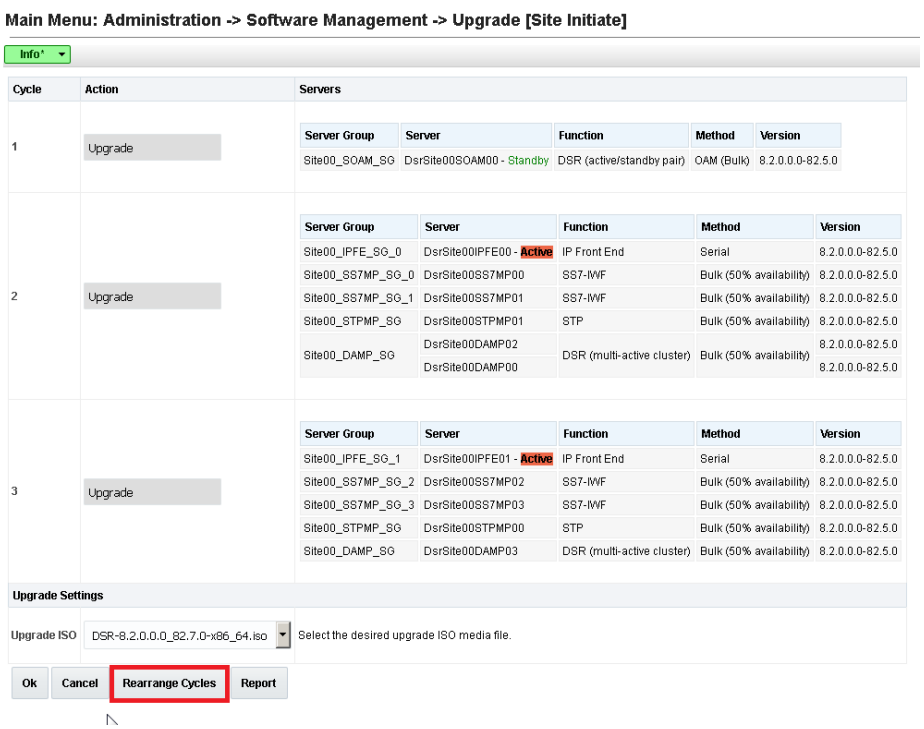
Step #	Procedure	Description
		Alarm ID = 31114 (DB Replication over SOAP has failed) **Alarm ID = 31225 (HA Service Start Failure)** **Alarm ID = 31149 (DB Late Write Nonactive)** ***Note***: Do not accept any upgrades at this time. ***Note***: In the unlikely event that after the upgrade, if the **Upgrade State** of server is **Backout Ready** and the **Status Message** displays **Server could not restart the application to complete the upgrade**, then perform Appendix N Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade. Perform Appendix V to create a link of Comagent. If the upgrade fails, do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.
4. ☐	**Server CLI**: If the upgrade of a server fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/platcfg.log It is recommended to contact by referring to Appendix V of this document and provide these files. Refer to Appendix J for failed server recovery procedures. When upgrade failure issue is identified and resolved, then Auto Site upgrade can be started again without executing any failed server recovery procedure.
5. ☐	Post upgrade verification	Proceed to section 5.4 Site Post-Upgrade Procedures for post upgrade verification procedures.

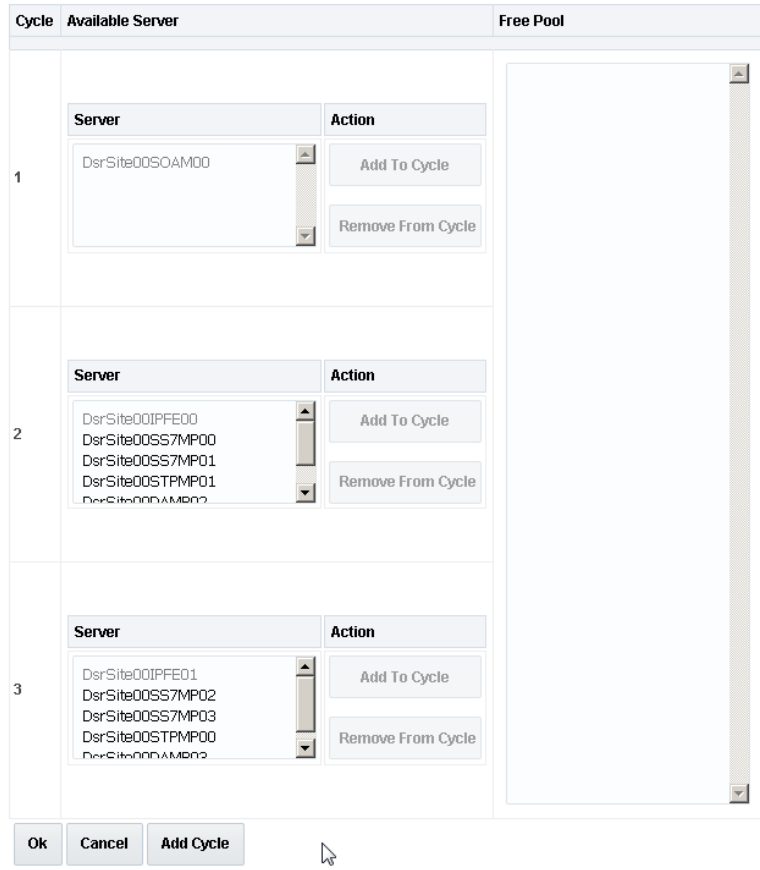
5.2.3 Rearrange Automated Site Upgrade Cycles

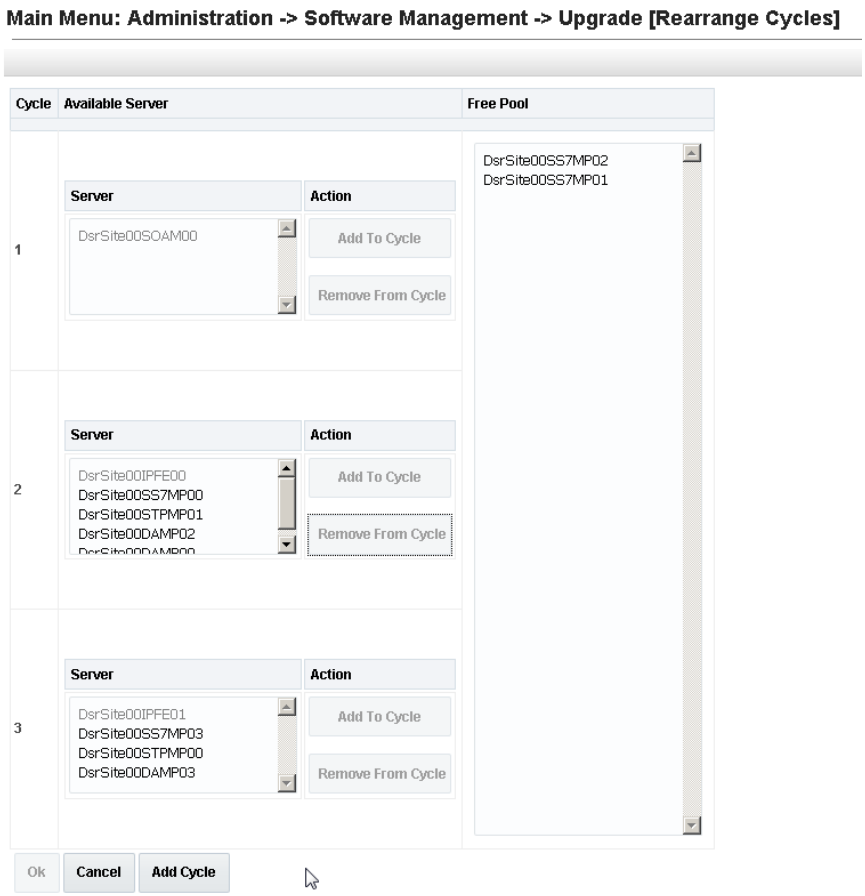
This procedure provide details to rearrange the Automated Site Upgrade cycles if required.

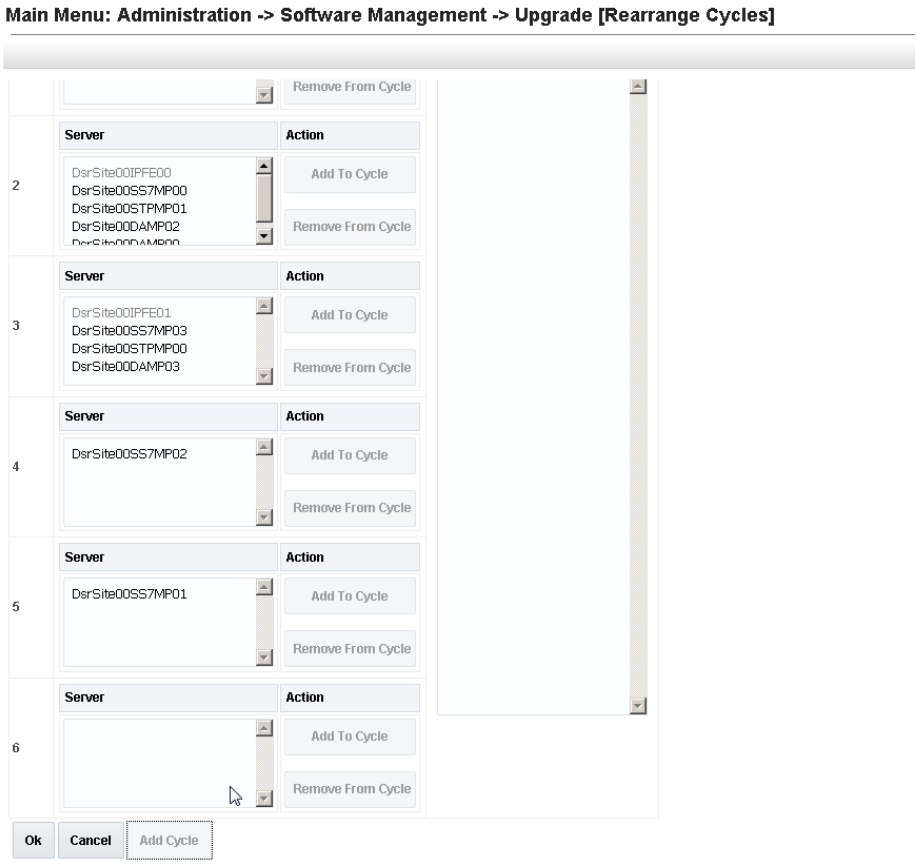
Automated Site Upgrade provides an option to rearrange servers in the cycles thus eliminating the risks of a potential network outage. ASU provides the flexibility to user to order the servers within the cycles without breaking the Minimum Availability and DA-MP Leader/vSTP MP leader criteria.

Procedure 24. Rearrangement of upgrade cycles for Automated Site Upgrade

Step #	Procedure	Description
This procedure provides option to rearrange the upgrade cycles for Automated Site Upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: Rearrange the upgrade cycle as needed	Click **Rearrange Cycles**. 
2. ☐	**Active NOAM VIP**: Rearrangement of Servers in cycles	1. Automated Site Upgrade Cycles across the sites. ***Note***: Only DA-MPs, and vSTPs, can be re-arranged. Re-arranging SBR and IPFE servers is restricted.

Step #	Procedure	Description
		Main Menu: Administration -> Software Management -> Upgrade [Rearrange Cycles]  2. When a server needs to be removed from cycle and needs to be added in an existing cycle or a new cycle, do this: 1. Select the desired server in the list and click **Remove from Cycle**. The server Moves to the Free Pool on the right side.

Step #	Procedure	Description
		 2. Add the servers in Free Pool to another existing cycle or new cycle. The next step describes how to add a new cycle, if required 3. If there is no need to add a new cycle, then steps to rearrange the cycle are complete. Return to the section 5.2.2 step that pointed to this procedure.

Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Add new cycle (If required)	1. Click **Add Cycle**.  After adding new cycle, servers available in free pool can be added in new cycle. 2. Click **OK**.

5.3 Automated Server Group/Manual Upgrade Overview

This section contains alternative site upgrade procedures that can be used when Automated Site Upgrade does not meet the needs or concerns of the customer. These procedures use a combination of Automated Server Group upgrade and manual server upgrades to upgrade a specific site.

Table 13 details the site upgrade plan for a non-PCA/PDRA site, which divides the upgrade into four cycles. A cycle is defined as the complete upgrade of one or more servers, from initiate upgrade to success or failure. The first two cycles consist of upgrading the SOAMs - the first cycle upgrades the standby SOAM, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, vSTP MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions in-service to process traffic. The fourth cycle upgrades the second half of the DA-MPs, and IPFEs to complete the site upgrade.

Table 13. Non-PCA/PDRA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4
Standby SOAM	Active SOAM		
		½ DA-MPs	½ DA-MPs
		½ IPFEs	½ IPFEs
		½ vSTP MPs	½ vSTP MPs

Table 14 details the site upgrade plan for a PCA/PDRA system with two-site redundancy. This upgrade plan is divided into five cycles. The first two cycles consist of upgrading the SOAMs - the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, IPFEs, and vSTP servers are upgraded in parallel with all of the spare SBRs. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the standby SBRs.

The fifth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 14. Two-Site Redundancy PCA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5
Standby SOAM, Spare SOAM	Active SOAM			
		½ DA-MPs	½ DA-MPs	
		½ IPFEs	½ IPFEs	
		Spare SBR(s)	Standby SBR(s)	Active SBR(s)

Table 15 details the site upgrade plan for a PCA/PDRA system with three-site redundancy. This upgrade plan is divided into six cycles.

Note: It is mandatory to follow the mentioned division and execution order of the cycles. This ensures the OAM controllers are always upgraded before any C-level servers.

For C-level servers, the division of servers can be planned in different cycles depending on customer requirements, which means SBR and DA-MPs can be upgraded in different cycles. **But, as mentioned, spare, standby, and active SBRs should be upgraded in different cycles.**

The first two cycles consist of upgrading the SOAMs – the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. **This ensures the OAM controllers are always upgraded before any C-level servers.**

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, and IPFEs are upgraded in parallel with one spare SBR. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the second spare SBR.

The fifth cycle upgrades the standby SBR(s), and the sixth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 15. Three-Site Redundancy PCA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5	Cycle 6
Standby SOAM, Spare SOAM	Active SOAM				
		½ DA-MPs	½ DA-MPs		
		½ IPFEs	½ IPFEs		
		Spare SBR(s)	Spare SBR(s)	Standby SBR(s)	Active SBR(s)

5.3.1 Site Upgrade Planning

The upgrade of the site servers consists of a mixture of automated upgrades using the Automated Server Group upgrade feature, along with "manual" upgrades that are a little less automated.

Table 16 should be used to plan the upgrade of each site. For the server groups that are upgraded using ASG, the only planning necessary is to record the server group name. ASG automatically selects the individual servers to upgrade. The IPFE, and vSTP (if equipped) server groups must be upgraded manually since there is only one server per server group. Planning is necessary for these server groups to ensure traffic continuity. Record the hostname of the servers to be upgraded in each iteration. vSTP MPs should be divided in cycles to avoid a network outage.

While choosing ASG and Manual upgrades for multi-active MP servers, see the limitations in Appendix P for the Automated Server Group upgrade option.

If your network aligns with any of the scenarios listed in Appendix P**,** then do NOT use the Automated Server Group. This avoids risks of a potential network outage.

There are some limitations with upgrading the DC server in a C-level server group, which are upgraded in a group of servers, for example, DA-MP, vSTP MP(s). So, make sure the DC server is not upgraded in first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix O Identify the DC server.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader** = **Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

   The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**.

2. Use the **/vstp/mpleader** MO.

   The result is the hostname of the MP leader server.

Table 16. Site Upgrade Planning Sheet

Iteration 1		Notes
Standby SOAM Hostname Spare SOAM Hostname		If a spare SOAM exists, the spare and standby SOAMs are upgraded manually. Otherwise, the SOAMs are upgraded with ASG.

Iteration 2		**Notes**
Active SOAM		The active SOAM is upgraded in iteration 2, either manually or by ASG.
Iteration 3		**Notes**
DA-MP Group 1		ASG automatically selects DA-MPs for upgrade
IPFE 1 Hostname		Manual upgrade
IPFE 3 Hostname		Manual upgrade
Spare SBR(s)		ASG automatically selects the spare SBR(s) for upgrade
Iteration 4		**Notes**
DA-MP Group 2		ASG automatically selects DA-MPs for upgrade
IPFE 2 Hostname		Manual upgrade
IPFE 4 Hostname		Manual upgrade
Standby SBR(s)		ASG automatically selects the standby SBR(s) for upgrade
Iteration 5		**Notes**
Active SBR(s)		ASG automatically selects the active SBR(s) for upgrade

Table 17 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 17 as a guide for determining the order in which the procedures are to be executed.

Table 17. Site Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 17	0:10-0:20	0:10-0:20	Procedure 17	None
Procedure 20 or Procedure 19	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:25	Site Upgrade Options Check Site Pre-Upgrade Health Check for Release 7.x	None None
Procedure 20	0:01-0:05	0:16-0:35	Site Upgrade Options Check	Site Provisioning Disabled, No Traffic Impact
Procedure 25	0:01-0:05	0:17-0:40	SOAM Upgrade Pre-Checks	No Traffic Impact
Iteration 1	0:40-1:00	0:57-1:40	Standby SOAM, Spare SOAM (if equipped)	Refer to Section 5.3.2 for details
Iteration 2	0:40-1:00	1:37-2:40	Active SOAM	Refer to Section 5.3.2 for details
Iteration 3	0:40-1:00	2:17-3:40	½ DA-MPs, ½ IPFEs, Spare SBR(s), ½ vSTP MPs	Refer to Section 5.3.4 for details
Iteration 4	0:40-1:00	2:57-4:40	½ DA-MPs, ½ IPFEs, Standby SBR(s), ½ vSTP MPs	Refer to Section 5.3.5 for details
Iteration 5	0:00-1:00	2:57-5:40	Active SBR(s)	Refer to Section 5.3.6 for details
Procedure 31	0:02	2:59-5:42	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 32	0:10-0:15	3:09-5:57	Site Post-Upgrade Health Check	None

5.3.2 SOAM Upgrade Overview

This section contains the steps required to perform a major or incremental upgrade of the SOAMs for a DSR site.

During the site upgrade (SOAMs plus all C-level servers), site provisioning is disabled. Provisioning is re-enabled at the completion of the site upgrade.

For each site in the DSR, the SOAM(s) and associated MPs and IPFEs should be upgraded within a single maintenance window.

Table 18 shows the estimated execution times for the SOAM upgrade. Procedure 27 is the recommended procedure for upgrading the SOAMs when there is no spare SOAM. ASG automatically upgrades the standby SOAM followed by the active SOAM.

If the site does have a spare SOAM, Procedure 27 is the recommended procedure. The manual upgrade procedure upgrades the standby and spare SOAMs in parallel, followed by the active SOAM.

Note: For information on SOAM VM profile for increased MP Capacity, refer to Appendix W.

Table 18. SOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Iteration 1 & 2 Procedure 26 or Procedure 27	1:20-2:40	1:20-2:40	Procedure 26 Procedure 27	No traffic impact

5.3.3 Upgrade SOAMs

!!WARNING!! The following procedures must be completed before the start of SOAM upgrade: Procedure 17; [0 or Procedure 19]; Procedure 21.

This section provides the procedures to upgrade the SOAMs. The SOAMs can be upgraded manually under user control, or automatically using the Automated Server Group Upgrade option. The recommended method for SOAM upgrade depends on the existence of a spare SOAM. If the site includes a spare SOAM, then the SOAMs are upgraded manually so that the spare and standby can be upgraded concurrently. This reduces the time required to upgrade the SOAMs.

Regardless of which SOAM upgrade option is used, Procedure 25**Error! Reference source not found.** is required to ensure site provisioning is disabled.

If the site does **not** include a spare SOAM, use the automated SOAM upgrade in Procedure 26.

If the site does include a spare SOAM, use the manual SOAM upgrade in Procedure 27.

Procedure 25. SOAM Upgrade Pre-Checks

Step #	Procedure	Description
This procedure verifies traffic status, and verifies that Site Provisioning is disabled, in preparation for upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM VIP**: View KPIs to verify traffic status	1. Log into the active SOAM GUI using the VIP. 2. Navigate to **Status & Manage > KPIs**. 3. Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	**Active SOAM VIP**: Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 21. In the GUI status bar, where it says **Connected using …**, check for the message **Site Provisioning disabled**. If the message is present, continue with the next procedure per Table 17; otherwise, execute Procedure 21.

5.3.3.1 Automated SOAM Upgrade (Active/Standby)

Procedure 26 is the recommended method for upgrading the SOAMs if the site does not include a spare SOAM. If the site has a spare SOAM, upgrade using Procedure 27. Upon completion of this procedure, proceed to Section 5.3.4 Upgrade Iteration 3.

Procedure 26. Automated SOAM Upgrade (Active/Standby)

Step #	Procedure	Description
This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Upgrade SOAM Server Group	Upgrade the SOAM server group using the Upgrade Multiple Servers procedure with the following options: • Use the Automated Server Group Upgrade option • Select the Serial upgrade mode Execute Appendix E Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix E, return to this point and proceed to section 5.3.4 Upgrade Iteration 3.

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored using disaster recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

5.3.3.2 Manual SOAM Upgrade (Active/Standby/Spare)

Procedure 27 upgrades the SOAM server group if the site includes a spare SOAM. If the SOAM server group was upgraded using Procedure 26, then do not execute this procedure; proceed to section 5.3.4 Upgrade Iteration 3.

Procedure 27. Manual SOAM Upgrade (Active/Standby/Spare)

Step #	Procedure	Description
This procedure upgrades the SOAMs in a DSR manually. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Upgrade standby and spare SOAMs in parallel using the Upgrade Multiple Servers procedure	Execute Appendix E Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix E, return to this point and continue with the next step.

Step #	Procedure	Description
2. ☐	Upgrade active SOAM using Upgrade Single Server procedure	Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and proceed to section 5.3.4 Upgrade Iteration 3.

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored using disaster recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

5.3.4 Upgrade Iteration 3

Upgrade iteration 3 begins the upgrade of the site C-level servers. As shown in Table 16, iteration 3 consists of upgrading the DA-MPs, IPFEs, spare SBR(s), and vSTP MP server, if equipped. The C-level components are upgraded in parallel to maximize Maintenance Window usage.

Table 19 shows the estimated time required to upgrade the C-level servers for iteration 3.

Table 19. Iteration 3 Upgrade Execution Overview

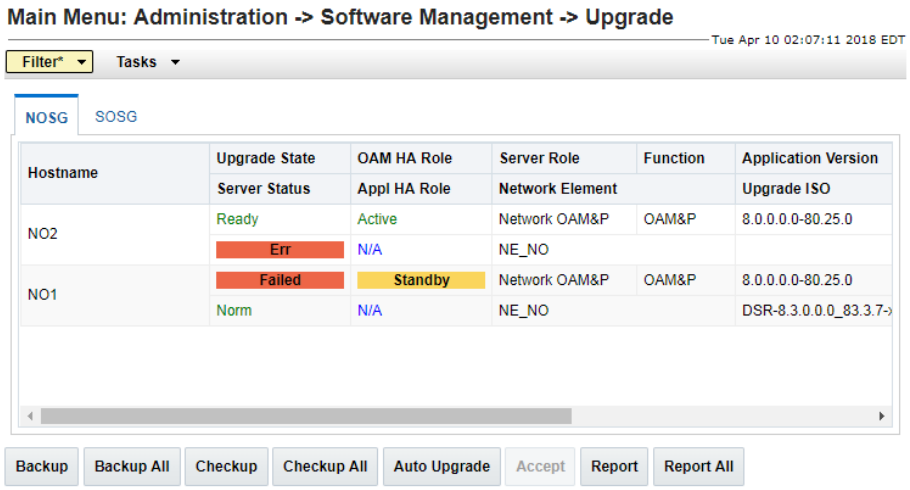
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 28	0:40-1:00	0:40-1:00	Procedure 28	½ DA-MPs, ½ IPFEs, spare SBR(s), ½ vSTPs servers will be offline

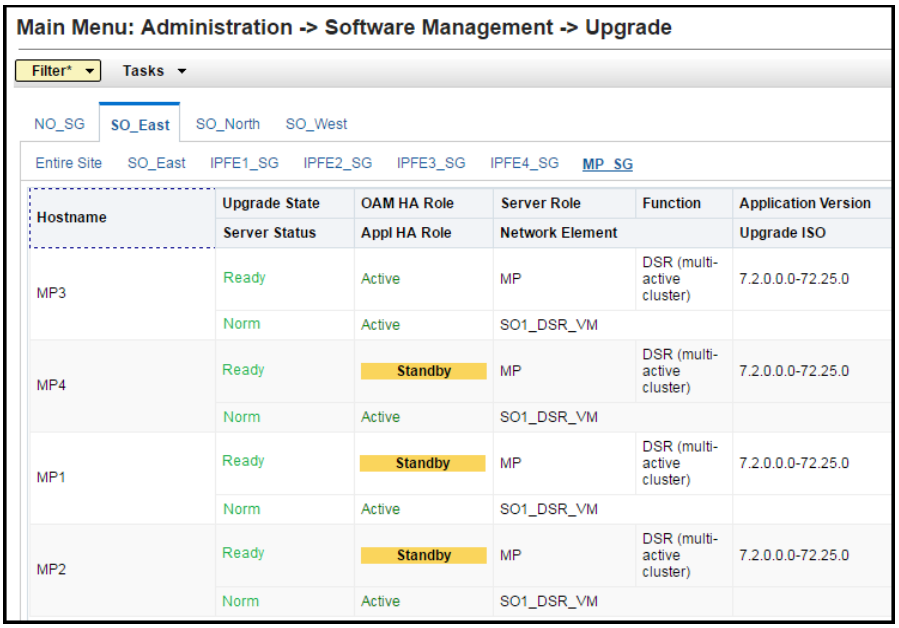
CAUTION

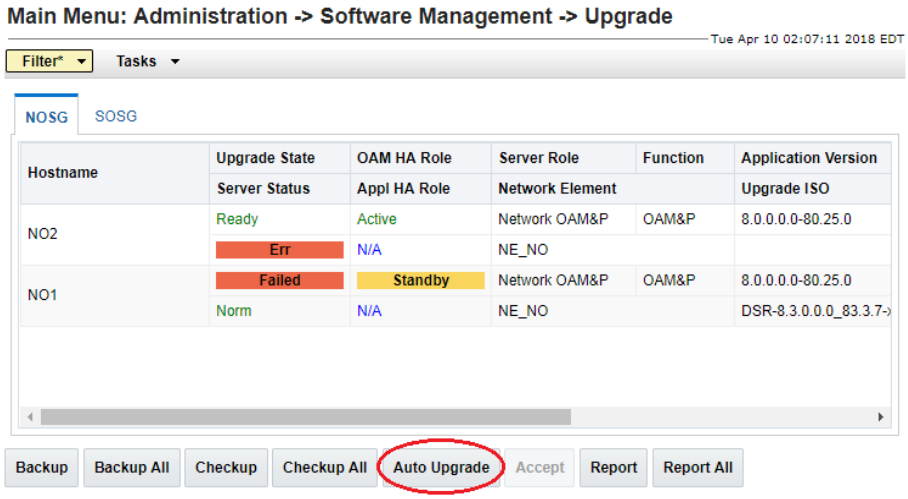
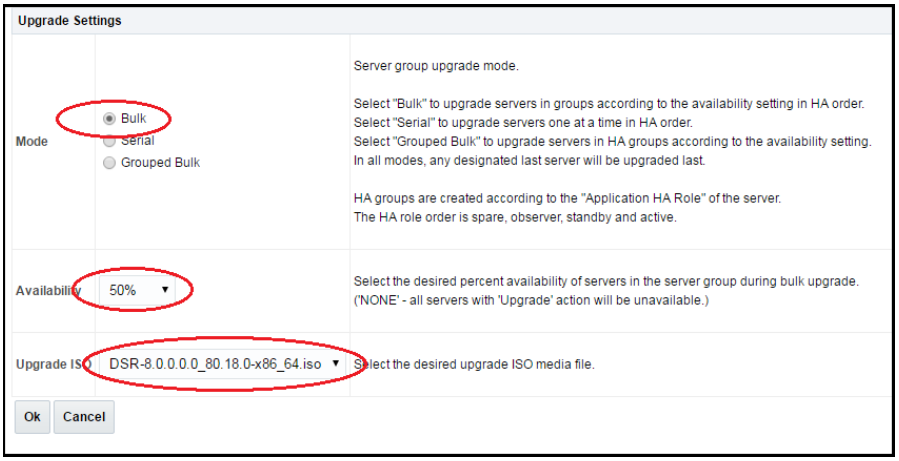
ASG does not allow the operator to specify the upgrade order of the DA-MP servers. If a manual upgrade was recommended in section 3.3, do not use ASG to upgrade the DA-MPS in this iteration. Alternate upgrade procedures are provided Appendix G.3.

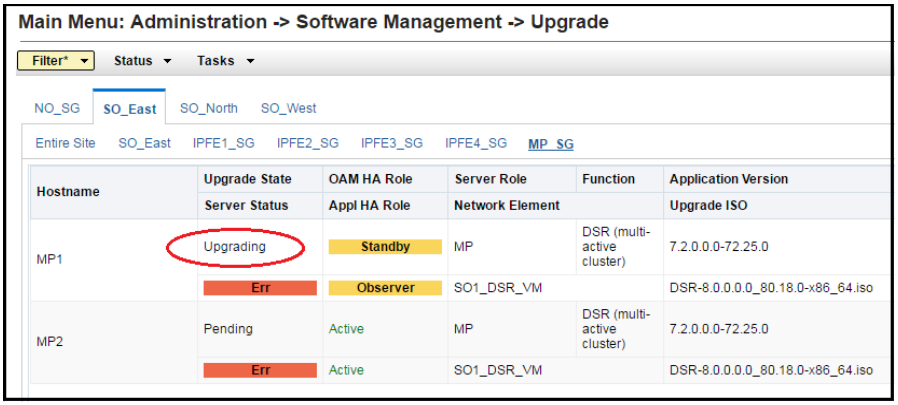
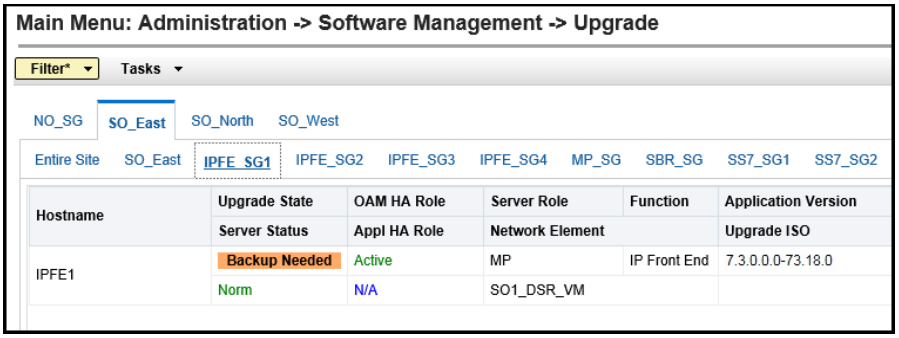
Procedure 28 upgrades ½ of the DA-MPs, ½ of the IPFEs, ½ of the vSTPs, and the spare SBR(s). Refer to Table 16 for the hostnames of the servers to be upgraded in this iteration.

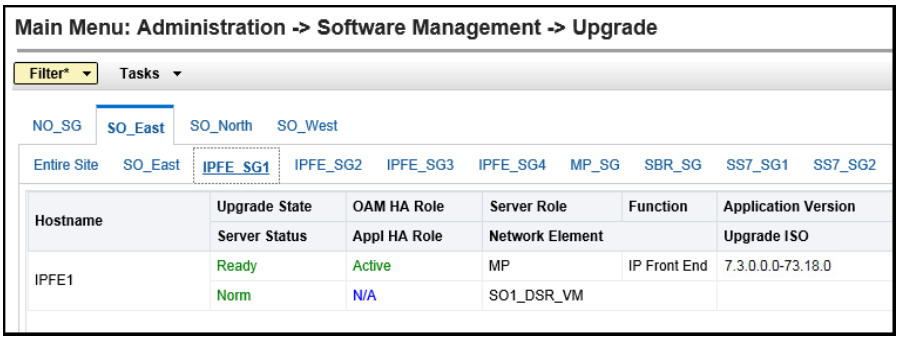
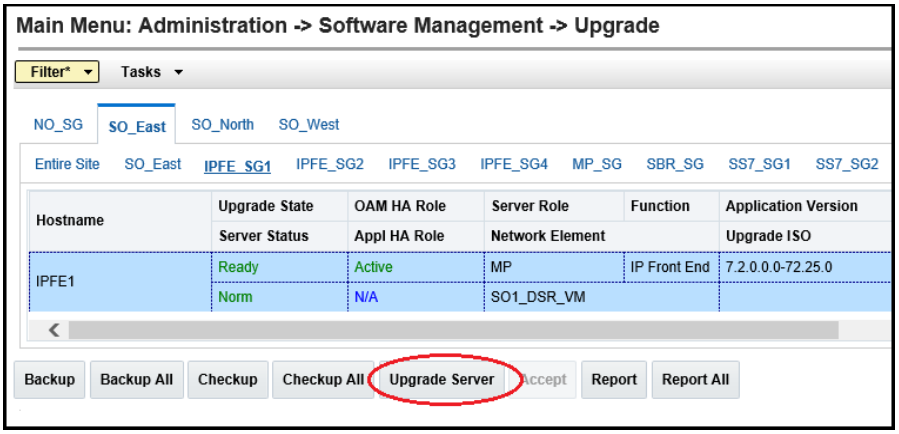
Procedure 28. Upgrade Iteration 3

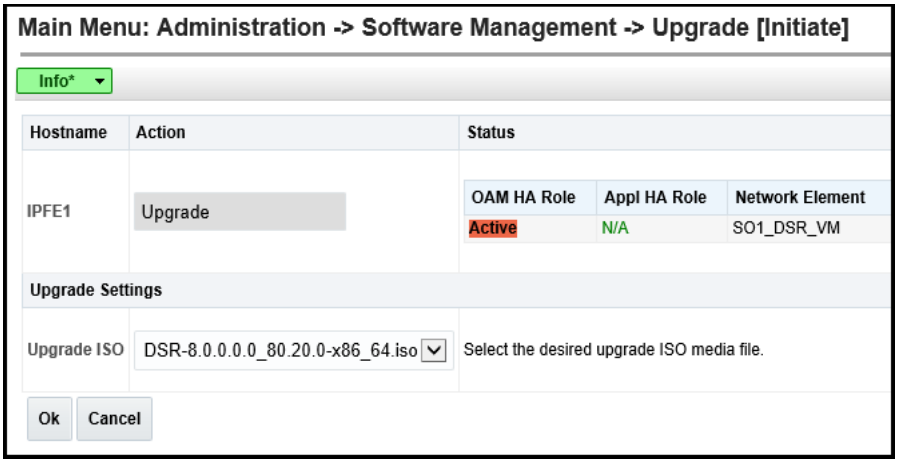
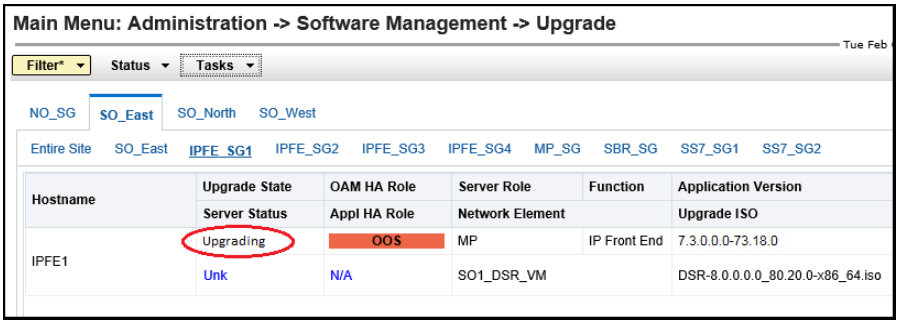
Step #	Procedure	Description
This procedure upgrades a portion of the C-level servers for iteration 3. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Select the DA-MP server group to view pre-upgrade status of DA-MPs	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Select the SOAM tab of the site being upgraded. 4. Select the DA-MP Server Group link. 5. For the DA-MP servers to be upgraded in iteration 3, verify the application version value is the expected source software release version.
2. ☐	**Active NOAM VIP**: View pre-upgrade status of DA-MP servers	1. If the servers are in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 2. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded. 

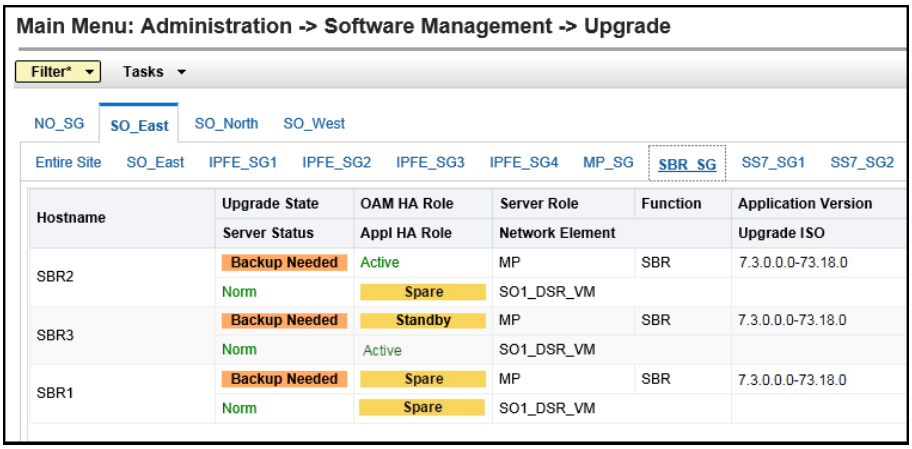
Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the DA-MP server group of the site being upgraded.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_East SO_North SO_West Entire Site SO_East IPFE1_SG IPFE2_SG IPFE3_SG IPFE4_SG MP_SG Hostname / Upgrade State / Server Status / OAM HA Role / Appl HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO MP3: Ready, Active, MP, DSR (multi-active cluster), 7.2.0.0.0-72.25.0; Norm, Active, SO1_DSR_VM MP4: Ready, Standby, MP, DSR (multi-active cluster), 7.2.0.0.0-72.25.0; Norm, Active, SO1_DSR_VM MP1: Ready, Standby, MP, DSR (multi-active cluster), 7.2.0.0.0-72.25.0; Norm, Active, SO1_DSR_VM MP2: Ready, Standby, MP, DSR (multi-active cluster), 7.2.0.0.0-72.25.0; Norm, Active, SO1_DSR_VM Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**

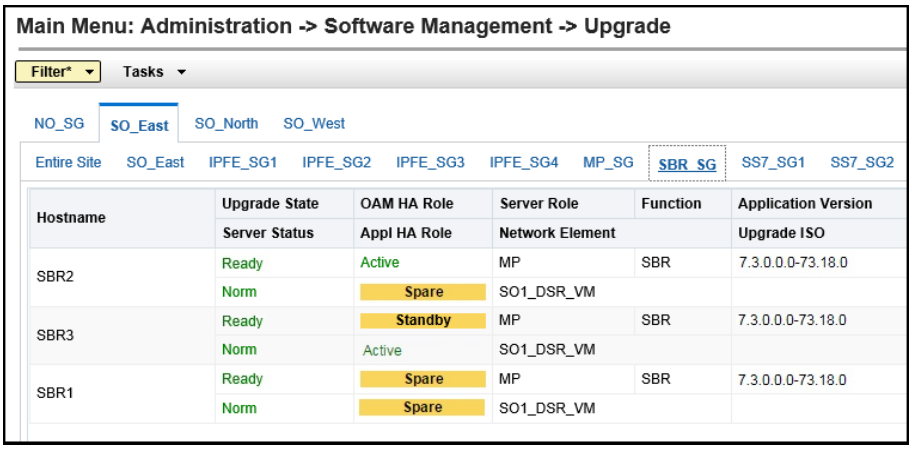
Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Initiate the Automated Server Group upgrade of the DA-MP servers (part 1)	1. To use the Automated Server Group upgrade option, verify no servers in the server group are selected. 2. Click **Auto Upgrade**. 
5. ☐	**Active NOAM VIP**: Initiate the Automated Server Group upgrade of the DA-MP server (part 2)	1. The **Upgrade Settings** section of the Initiate screen controls the behavior of the server group upgrade. Select **Bulk** Mode. 2. Select **50%** for the **Availability** setting. 3. Select the appropriate ISO from the **Upgrade ISO** options. 4. Click **OK** to start the upgrade. 

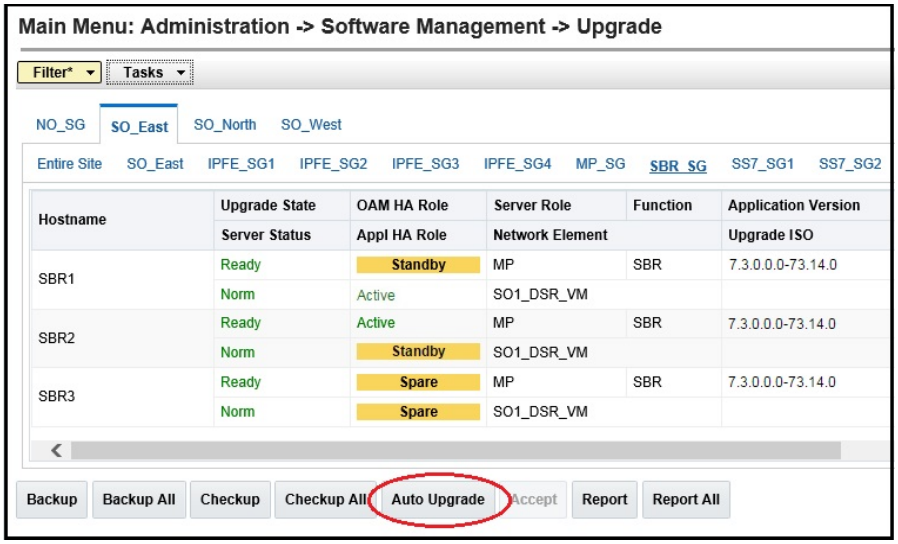
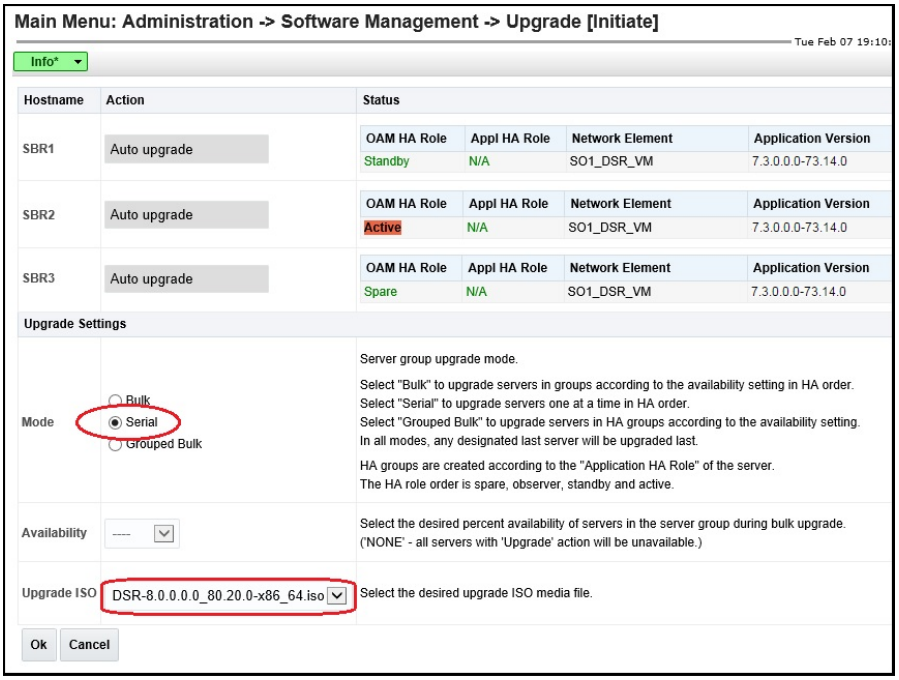
Step #	Procedure	Description
6. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the upgrade state of the DA-MP servers. Upgrade status displays under the Status Message column.  While the DA-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
7. ☐	Identify the IPFE server group(s) to upgrade	From the data captured in Table 16, identify the IPFE server group(s) to upgrade in iteration 3.
8. ☐	**Active NOAM VIP**: View pre-upgrade status of IPFEs	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the link for each IPFE server group to upgrade. 4. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. 5. If a server is in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 6. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded. 

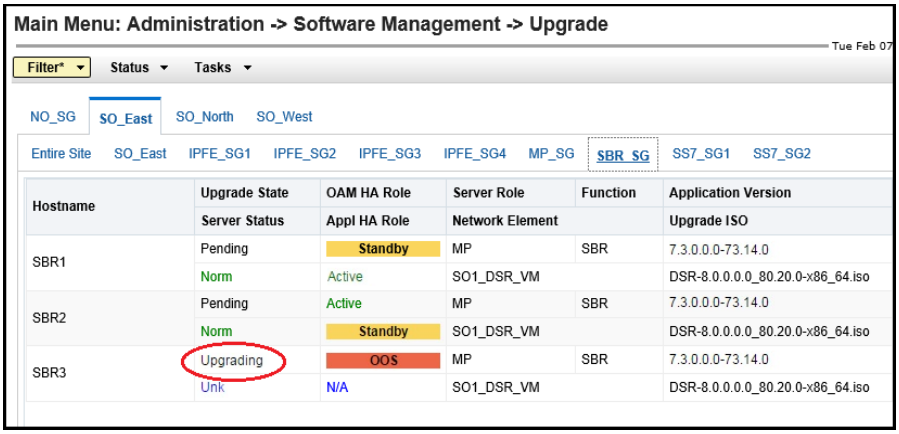
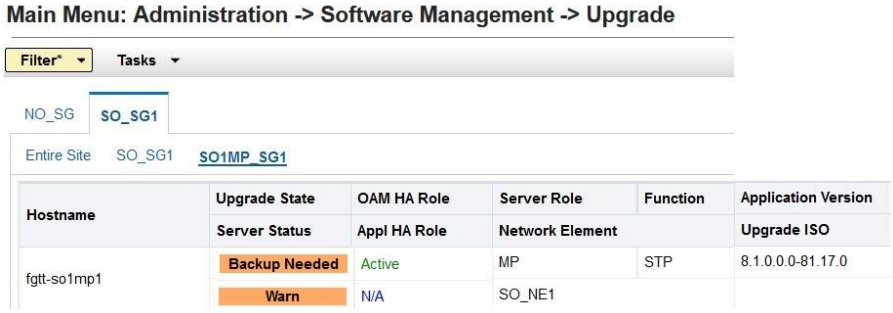
Step #	Procedure	Description
9. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the IPFE server group being upgraded.  Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**
10. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 1)	Select the Upgrade Server method. 1. From the Upgrade Administration screen, select the server to upgrade. 2. Click **Upgrade Server**. 

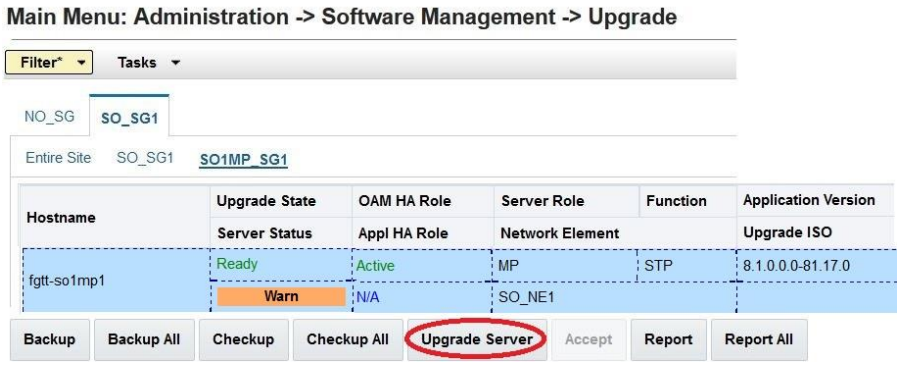
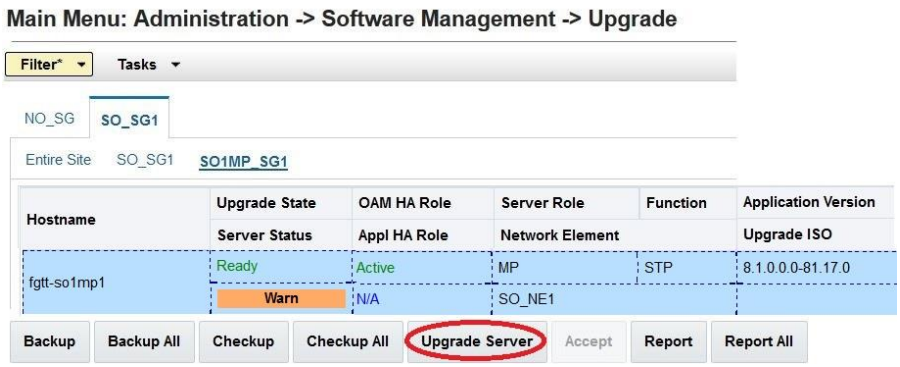
Step #	Procedure	Description
11. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 2)	Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click **OK** to start the upgrade. 
12. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the upgrade state of the IPFE server. Upgrade status displays under the Status Message column. 
13. ☐	Repeat for each IPFE	Repeat steps 7. through 12. for the next IPFE to be upgraded in this iteration per Table 16.
14. ☐	Identify the SBR server group(s) to upgrade	From the data captured in Table 16, identify the SBR server group(s) to upgrade in iteration 3. ASG steps (Auto Upgrade), mentioned in the next steps, do not provide any liberty to the operator to verify observations during the upgrade. If a manual upgrade was recommended for the SBR upgrade, do not use ASG to upgrade all the SBR servers from the same server group in this single iteration. Alternate upgrade procedures are provided in Procedure 57. Spare SBR server(s) need to be upgraded. If the Manual Upgrade is used, skip ASG steps 15. to 19.

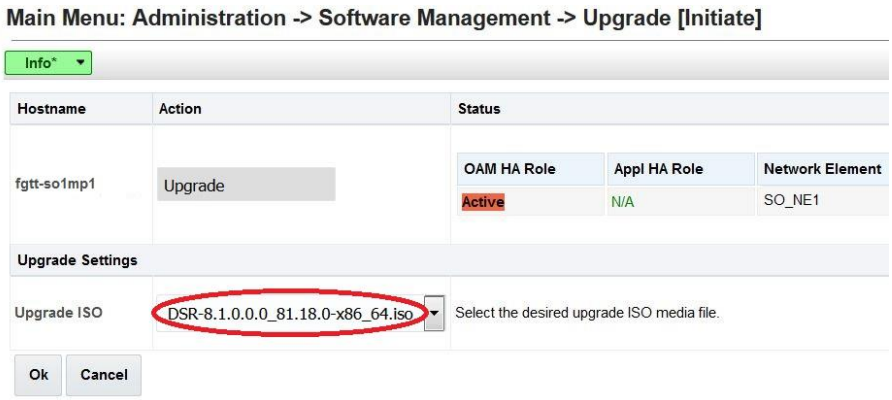
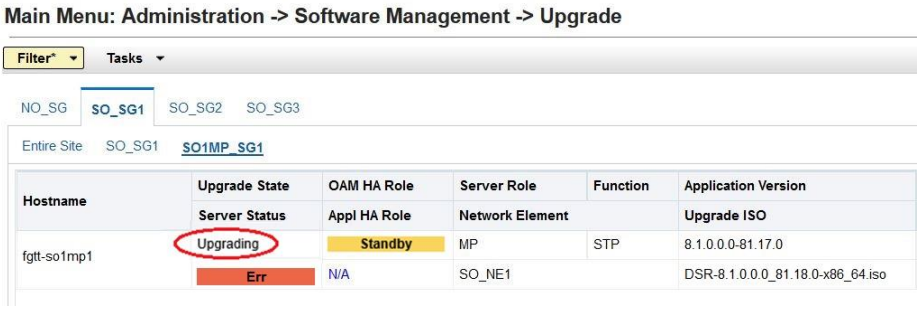
Step #	Procedure	Description
15. ☐	**Active NOAM VIP**: View pre-upgrade status of SBRs to upgrade	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the link for each SBR server group to upgrade. 4. For the SBR servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. 5. If the server is in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 6. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_East SO_North SO_West Entire Site SO_East IPFE_SG1 IPFE_SG2 IPFE_SG3 IPFE_SG4 MP_SG SBR_SG SS7_SG1 SS7_SG2 Hostname / Upgrade State / Server Status / OAM HA Role / Appl HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO SBR2: Backup Needed, Norm, Active, Spare, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0 SBR3: Backup Needed, Norm, Standby, Active, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0 SBR1: Backup Needed, Norm, Spare, Spare, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0

Step #	Procedure	Description
16. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the SBR server group being upgraded.  Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks NO_SG SO_East SO_North SO_West Entire Site SO_East IPFE_SG1 IPFE_SG2 IPFE_SG3 IPFE_SG4 MP_SG SBR_SG SS7_SG1 SS7_SG2 Hostname / Upgrade State / Server Status / OAM HA Role / Appl HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO SBR2: Ready, Norm, Active, Spare, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0 SBR3: Ready, Norm, Standby, Active, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0 SBR1: Ready, Norm, Spare, Spare, MP, SO1_DSR_VM, SBR, 7.3.0.0.0-73.18.0 Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**

Step #	Procedure	Description
17. ☐	**Active NOAM VIP**: Initiate SBR upgrade (part 1)	Select the Auto Upgrade method. 1. To use the Automated Server Group upgrade option, select the SBR server group to upgrade. 2. Verify no servers in the server group are selected. 3. Click **Auto Upgrade**. 
18. ☐	**Active NOAM VIP**: Initiate SBR upgrade (part 2)	Set upgrade options and start the Automated Server Group Upgrade. 1. The Upgrade Settings section of the Initiate screen controls the behavior of the automated upgrade. Select **Serial** mode. 2. Select the appropriate ISO from the **Upgrade ISO** options. 3. Click **OK** to start the upgrade. 

Step #	Procedure	Description
19. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the **Upgrade State** of the SBR server group. Upgrade status displays under the Status Message column (not shown). 
20. ☐	Repeat for each SBR server group	Repeat steps 14. through 19. for the next SBR server group to be upgraded per Table 16.
21. ☐	Identify the STP server group(s) to upgrade	From the data captured in Table 16, identify the STP server group(s) to upgrade in iteration 3.
22. ☐	**Active NOAM VIP**: View pre-upgrade status of vSTP MP servers	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the link for each vSTP server group to upgrade. 4. For the vSTP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version. 5. If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 6. Verify the **OAM Max Ha Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

Step #	Procedure	Description
23. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the vSTP MP server group being upgraded.  Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**
24. ☐	**Active NOAM VIP**: Initiate vSTP MP upgrade (part 1)	Select the Upgrade Server upgrade method. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click **Upgrade Server**. 

Step #	Procedure	Description
25. ☐	**Active NOAM VIP**: Initiate vSTP upgrade (part 2)	Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click **OK** to initiate the upgrade. 
26. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the **Upgrade State** of the vSTP MP server. Upgrade status displays under the Status Message column. 
27. ☐	Repeat for each vSTP server(s).	Repeat steps 22. through 26. for the next vSTP servers to be upgraded per Table 16.
28. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	See step 29. for instructions if the upgrade fails, or if execution time exceeds 60 minutes. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Sequence through the server group links for the server groups being upgraded. Observe the Upgrade State of the servers of interest. Upgrade status displays under the Status Message column. During the upgrade, the servers may have a combination of the following expected alarms.

Step #	Procedure	Description
		Note: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)** Database (DB) replication failure alarms may display during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix P resolve this issue. 4. Half of the DA-MP and SBR server groups are upgraded in iteration 3. ASG automatically sequences to iteration 4 to upgrade the remaining servers. Periodically monitor these servers for failures. 5. For the IPFE servers being upgraded, wait for the upgrades to complete. The Status Message column displays **Success** after approximately 20 to 50 minutes. Do not proceed to iteration 4 until the IPFE servers have completed upgrade. ***Note***: Do not accept any upgrades at this time. **If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.**

29.
☐
	Server CLI: If the upgrade of a server fails	If the upgrade of a server fails, access the server command line (using ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		It is recommended to contact and provide these files. Refer to Appendix J for failed server recovery procedures.

5.3.5 Upgrade Iteration 4

Upgrade iteration 4 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 4 consists of upgrading the second half of the DA-MPs, vSTPs, and IPFEs, as well as the standby SBR(s), if equipped.

Table 20 shows the estimated time required to upgrade the C-level servers for iteration 4.

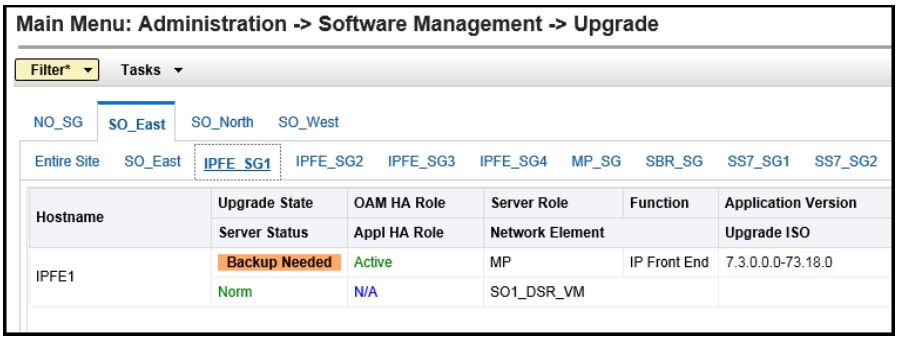
Table 20. Iteration 4 Upgrade Execution Overview.

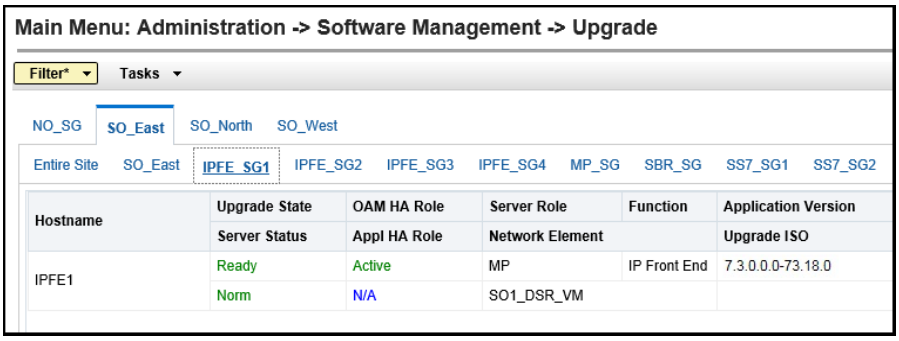
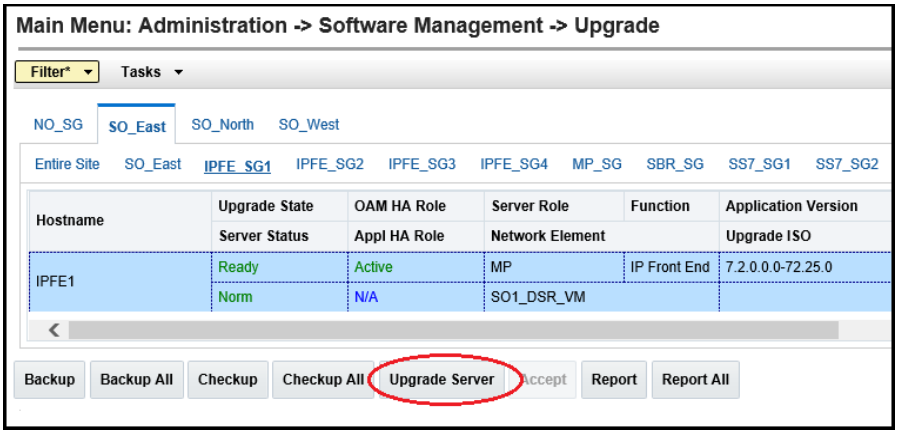
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 29	0:40-1:00	0:40-1:00	Procedure 29	½ DA-MPs, ½ IPFEs, standby SBR(s), ½ vSTP servers are offline

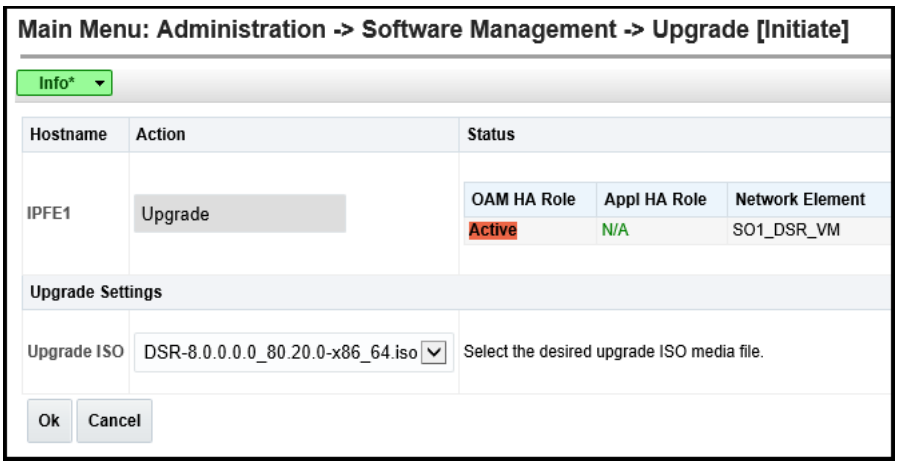
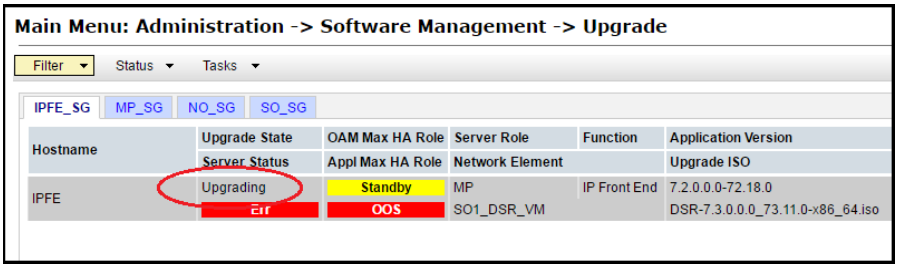
Procedure 29 provides the steps to upgrade, ½ of the vSTPs servers and ½ of the IPFEs. ASG automatically upgrades the DA-MPs and SBRs.

Procedure 29. Upgrade Iteration 4

Step #	Procedure	Description
This procedure upgrades a portion of the C-level servers for iteration 4. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Identify the IPFE server group(s) to upgrade	From the data captured in Table 16, identify the IPFE server group(s) to upgrade in iteration 4.

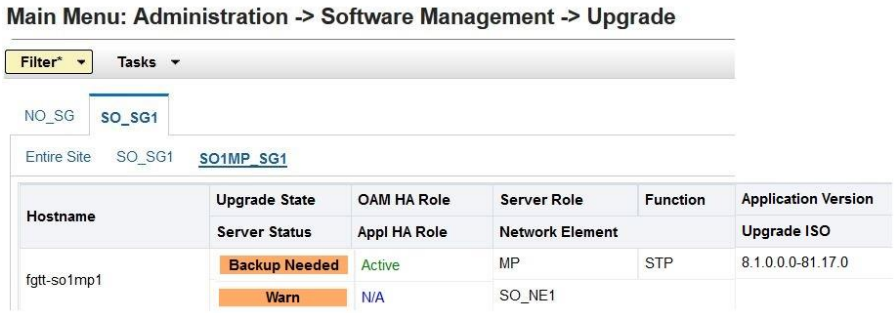
Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: View pre-upgrade status of IPFEs	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the link of each IPFE server group to be upgraded. 4. For the IPFE servers to be upgraded in iteration 4, verify the application version value is the expected source software release version. 5. If a server is in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 6. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded. 

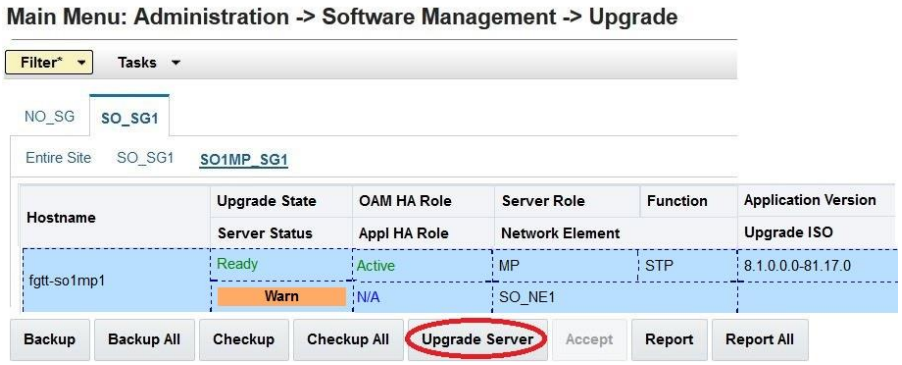
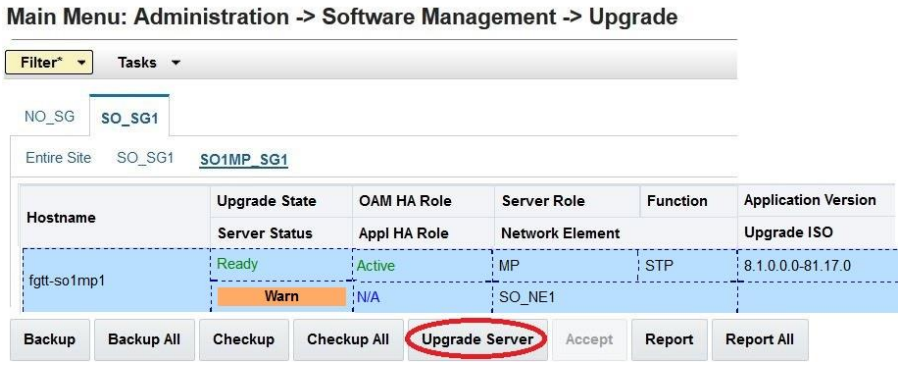
Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the IPFE server group being upgraded.  Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**
4. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 1)	Select the Upgrade Server method. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click **Upgrade Server**. 

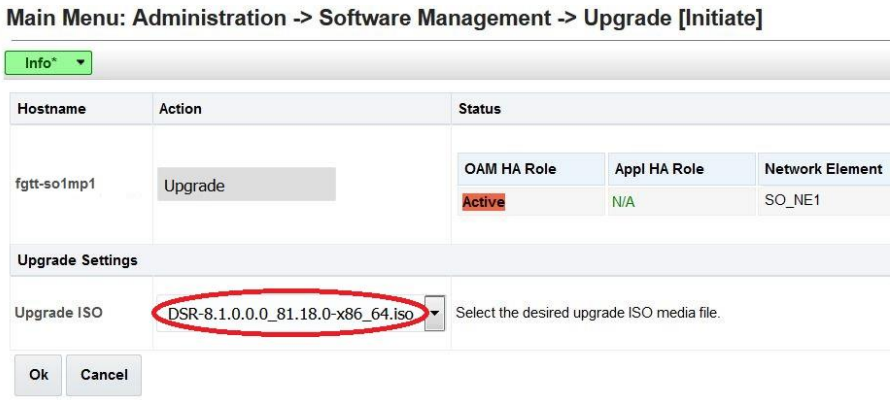
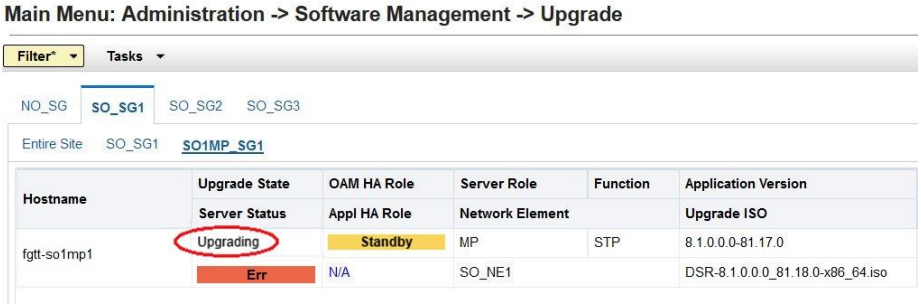
Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Initiate IPFE upgrade (part 2)	Select target ISO. 1. On the **Upgrade Initiate** screen, select the target ISO from the Upgrade ISO options. 2. Click **OK** to initiate the upgrade. 
6. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the Upgrade State of the IPFE server. Upgrade status displays under the Status Message column. 
7. ☐	Repeat for each IPFE	Repeat steps 1. through 6. for the next IPFE to be upgraded per Table 16.

8. ☐	**Server CLI**: If the upgrade of a server fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

9. ☐	Identify the STP server group(s) to upgrade	From the data captured in Table 16, identify the STP server group(s) to upgrade in iteration 4.

Step #	Procedure	Description
10. ☐	**Active NOAM VIP**: View pre-upgrade status of vSTP MP servers	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the link for each vSTP server group to upgrade. 4. For the vSTP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version. 5. If a server is in **Backup Needed** state, select the server and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 6. Verify the **OAM Max Ha Role** is the expected condition (either standby or active). This depends on the server being upgraded. 

Step #	Procedure	Description
11. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** for the server to be upgraded	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the vSTP MP server group being upgraded.  Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)**
12. ☐	**Active NOAM VIP**: Initiate vSTP MP upgrade (part 1)	Select the Upgrade Server upgrade method. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click **Upgrade Server**. 

Step #	Procedure	Description
13. ☐	**Active NOAM VIP**: Initiate vSTP upgrade (part 2)	Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click **OK** to initiate the upgrade. 
14. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the **Upgrade State** of the vSTP MP server. Upgrade status displays under the Status Message column. 
15. ☐	Repeat for each vSTP server(s).	Repeat steps 10. through 14. for the next vSTP servers to be upgraded per Table 16.
16. ☐	Identify the Standby SBR server(s) to upgrade	From the data captured in Table 16, identify the SBR server (s) to upgrade in iteration 4. If ASG was used in Upgrade Iteration 3, then the standby SBR server(s) is already upgraded and this step is not required. If a manual upgrade was recommended, use the alternate upgrade procedures provided in Procedure 57 for Standby SBR Server (s) upgrade.

5.3.6 Upgrade Iteration 5

Upgrade iteration 5 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 5 consists of upgrading the active SBR(s).

Table 21 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

Table 21. Iteration 5 Upgrade Execution Overview

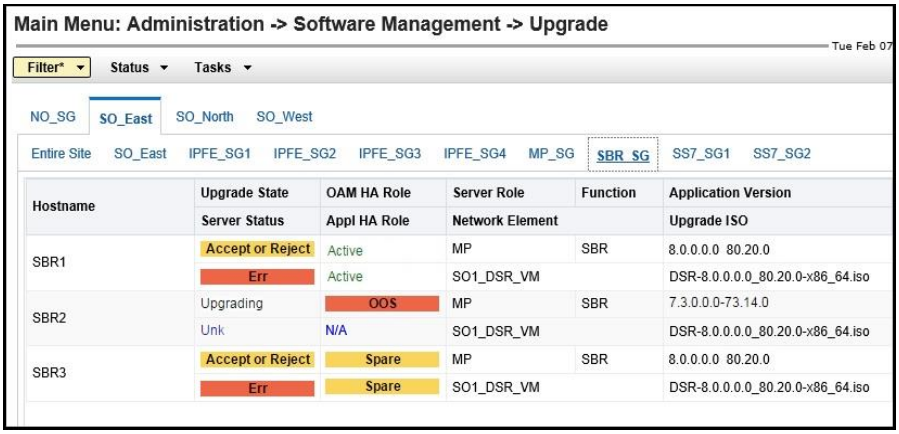
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 30	0:40-1:00	0:40-1:00	Procedure 30	Standby SBR becomes active; previously active SBR is offline for upgrade

CAUTION

If ASG was used in Upgrade Iteration 3, then the standby SBR server(s) is already upgraded and this step is not required.

If a manual upgrade was recommended, use the alternate upgrade procedures provided in Procedure 57 for Standby SBR Server (s) upgrade.

Procedure 30. Upgrade Iteration 5

Step #	Procedure	Description
This procedure upgrades the active SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Iteration 5	At iteration 5, the active SBR is upgraded, causing the standby to become active. 
2. ☐	**Active NOAM VIP**: View the upgrade	See step 3 for instructions if the upgrade fails, or if execution time exceeds 60 minutes.

Step #	Procedure	Description
	administration form to monitor upgrade progress	***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Sequence through the server group links for the server groups being upgraded. Observe the upgrade state of the servers of interest. Upgrade status displays under the Status Message column. During the upgrade, the servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)** Database (DB) replication failure alarms may display during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix P to resolve this issue. Wait for the SBR upgrades to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes.

3.
☐
	Server CLI: If the upgrade of a server fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

5.4 Site Post-Upgrade Procedures

The following procedures must be executed at the completion of each SOAM site upgrade:

- Procedure 31 Allow Site Provisioning
- Procedure 32 Site Post-Upgrade Health Check

After all SOAM sites in the topology have completed upgrade, the upgrade may be accepted using the following procedure:

- Procedure 44 Accept Upgrade

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

5.4.1 Allow Site Provisioning

This procedure enables Site Provisioning for the site just upgraded.

CAUTION Any provisioning changes made to this site before the upgrade is accepted are lost if the upgrade is backed out.

Procedure 31. Allow Site Provisioning

Step #	Procedure	Description
This procedure allows provisioning for SOAM and MP servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM VIP**: Enable site provisioning	1. Log into the SOAM GUI of the site just upgraded using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Site Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Disable Site Provisioning**.

5.4.2 Site Post-Upgrade Health Checks

This section provides procedures to verify the validity and health of the site upgrade.

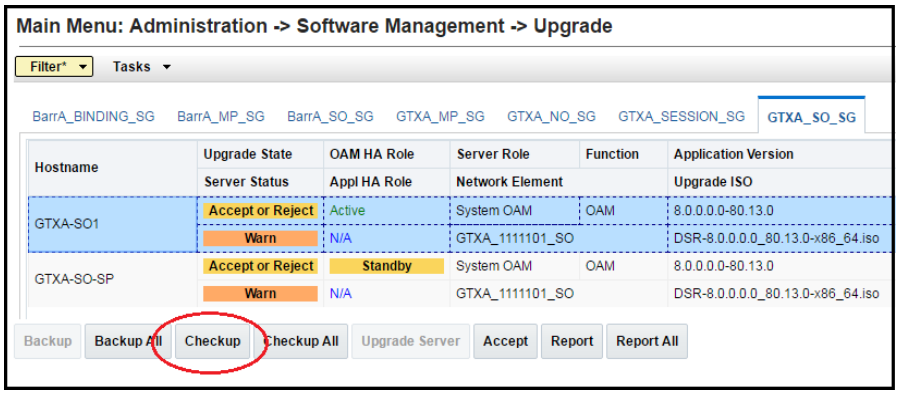
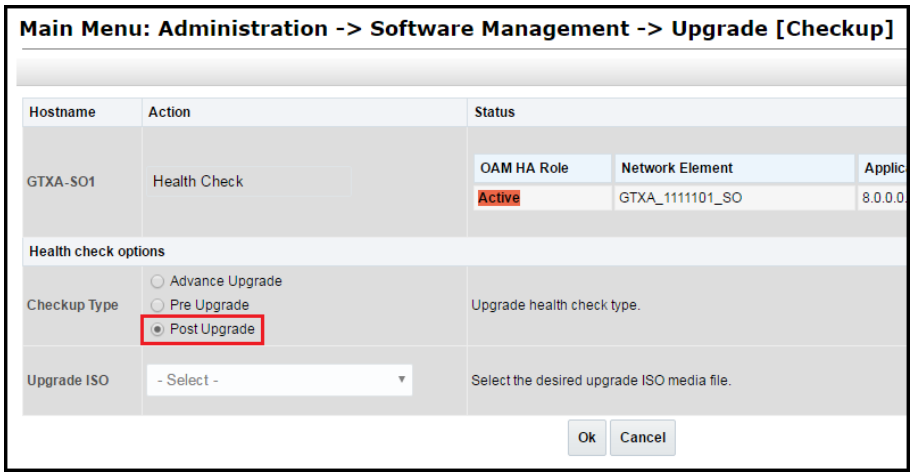
5.4.2.1 Site Post-Upgrade Health Check

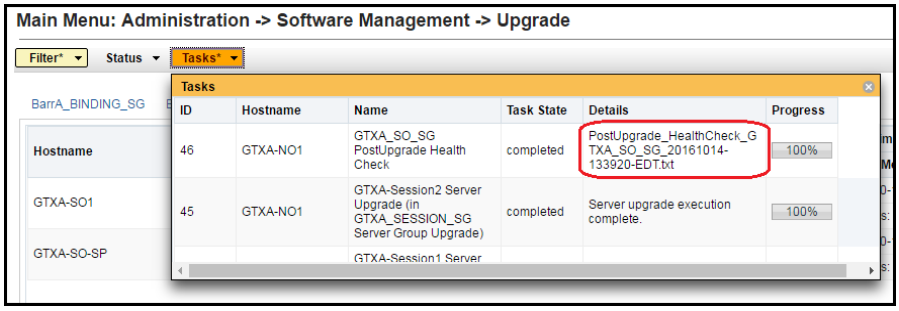
This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

If the **10054 - Device Deployment Failed** alarm displays after the upgrade for any server, see for Appendix T Workaround to Resolve Device Deployment Failed Alarm corrective steps.

Note: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE:: No record in alarm table for FAILURE!**, see Procedure 73.

Procedure 32. Site Post-Upgrade Health Check

Step #	Procedure	Description
This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Run automated post-upgrade health checks	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being upgraded. 3. Select the SOAM server group link for the site being upgraded. 4. Select the active SOAM.  5. Click **Checkup**. 6. Under Health check options, select **Post Upgrade**. 7. Click **OK**. **Control returns to the Upgrade screen.** 

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Monitor health check progress for completion	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze health check results	Analyze Health Check failure. If the Health Check report status is anything other than "Pass", the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the active SOAM tab. 3. Select the **UpgradeHealthCheck.log** file and click **View**. 4. Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance. If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform the health checks in Procedure 33.
4. ☐	**Active SOAM VIP**: Export and archive the Diameter configuration data	1. Navigate to **Diameter Common > Export**. 2. Capture and archive the Diameter data by selecting the **ALL** option for the Export Application. 3. Verify the requested data is exported by clicking **Tasks** at the top of the screen. 4. Navigate to **Status & Manage > Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine. 5. Navigate to **Diameter > Maintenance > Applications**. 6. Verify Operational Status is **Available** for all applications.

Step #	Procedure	Description
5. ☐	**Active SOAM Server**: Check if the setup previously has a customer supplied Apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade	If the setup had a customer-supplied Apache certificate installed and protected with passphrase before the start of the upgrade (refer to Procedure 3 and rename the certificate back to the original name.
6. ☐	Compare data to the pre-upgrade health check to verify if the system has degraded after the second maintenance window	Verify that the health check status of the upgraded site as collected from Steps 1 through 4 is the same as the pre-upgrade health checks taken in Section 5.1.2. If system operation is degraded, it is recommended to contact .

5.4.2.2 Alternate SOAM Post-Upgrade Health Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers. This procedure is an alternative to the normal post upgrade health check in Procedure 34.

Procedure 33. Alternate SOAM Post-Upgrade Health Check

Step #	Procedure	Description
This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

1.
☐
	Active SOAM CLI: Run/verify SOAM post-upgrade health check status	1. Use an SSH client to connect to the active SOAM:
		`ssh admusr@<SOAM XMI IP address>`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter the command:
		`$ upgradeHealthCheck postUpgradeHealthCheckOnSoam`
		This command creates two files in **/var/TKLC/db/filemgmt/ UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If any alarms are present in the system:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		3. If the Server <hostname> needs operator attention before upgrade message displays, inspect the Server Status Report to determine the reason for the message. If the Server <hostname> has no alarm with DB State as Normal and Process state as Kill message displays in the Server Status Report, the alert can be ignored.
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact My Oracle Support (MOS) for guidance.
		4. Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

Step #	Procedure	Description
2. ☐	**Active SOAM CLI**: Capture Diameter maintenance status	Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command displays a series of messages providing Diameter Maintenance status. Capture this output and save for later use. ***Note***: The output is also captured in **/var/TKLC/db/filemgmt/UpgradeHealthCheck.log**. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
3. ☐	**Active SOAM CLI**: View DA-MP status	1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. ***Note***: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all peer MPs are available. 3. Note the number of Total Connections Established _____
4. ☐	Compare data to the pre-upgrade health check to verify if the system has degraded after the second maintenance window	Verify the health check status of the upgraded site as collected in this procedure is the same as the pre-upgrade health checks taken in section 5.1.2. If system operation is degraded, it is recommended to report it to My Oracle Support (MOS).

Note: If another site is to be upgraded, all procedures specified by Table 12 must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.

5.4.3 Post-Upgrade Procedures

The procedures in this section are to be executed after the site upgrade is verified to be valid and healthy. These procedures should be executed in the maintenance window.

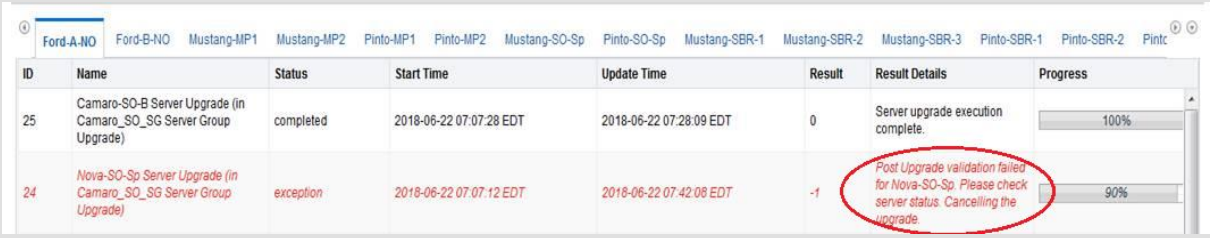
Procedure 34. Post-Upgrade Procedures

Step #	Procedure	Description
This procedure performs additional actions that are required after the upgrade is successfully completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active SOAM VIP**: Enable the signaling firewall for the upgraded site	The firewall enables the DSR to dynamically determine and customize the Linux firewall on each DA-MP server in the DSR Signaling node to allow only the essential network traffic pertaining to the active signaling configuration. There are some limitations related to enabling of signaling firewall in DSR 8.2 releases. See section 1.7.3 for more details. 1. Navigate to **Diameter > Maintenance > Signaling Firewall**. 2. Select the Signaling Node that was just upgraded. 3. Click **Enable**. 4. Click **OK** to confirm the action. 5. Verify the Admin State changes to **Enabled**. ***Note***: There may be a short delay while the firewall is enabled on the site.

!!WARNING!!

If this error displays, contact .

```
"Post Ugrade validation failed for <server_name>.  Please check server
status.  Cancelling the upgrade."
```



6. Backout Procedure Overview

The procedures provided in this section return the individual servers and the overall DSR system to the source release after an upgrade is aborted. The backout procedures support two options for restoring the source release:

- Emergency backout
- Normal backout

The emergency backout overview is provided in Table 22. These procedures back out the target release software in the fastest possible manner, without regard to traffic impact.

The normal backout overview is provided in Table 23. These procedures back out the target release software in a more controlled manner, sustaining traffic to the extent possible.

All backout procedures are executed inside a maintenance window.

The backout procedure times provided in Table 22 and Table 23 are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done.

Note: While not specifically covered by this procedure, it may be necessary to re-apply patches to the source release after the backout. If patches are applicable to the source release, verify all patches are on-hand before completing the backout procedures.

Table 22. Emergency Backout Procedure Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 35	0:10-0:30	0:10-0:30	Procedure 35 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 varies.	None.
Procedure 36	0:01	0:11-0:31	Procedure 36	Disables global provisioning
Procedure 37	See Note	See Note	Procedure 37 ***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 cause traffic loss.
Procedure 42	See Note	See Note	Procedure 42 ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 38	See Note	See Note	Procedure 38 ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures cause traffic loss.
Procedure 43	0:01-0:05	Varies	Procedure 43	None

Table 23. Normal Backout Procedure Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum		
Procedure 35	0:10-0:30	0:10-0:30	Procedure 35 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 varies.	None
Procedure 36	0:01	0:11-0:31	Procedure 36	Disables global provisioning
Procedure 39	See Note	See Note	Procedure 39 ***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 cause traffic loss.
Procedure 42	See Note	See Note	Procedure 42 ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 40	See Note	See Note	Procedure 40 ***Note***: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 43	0:01-0:05	Varies	Procedure 43	None

6.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to . Before executing any of these procedures, it is recommended to contact .

Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.

!!WARNING!!

Before attempting to perform these backout procedures, it is recommended to first contact My Oracle Support (MOS) as described in Appendix V.

Backout procedures cause traffic loss.

Note: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 8.2 release to the previously installed 7.1.w release). Backout of an initial installation is not supported.

During the backout, servers may have the following expected alarms until the server is completely backed out. The servers may have some or all of the following expected alarms, but are not limited to event IDs:

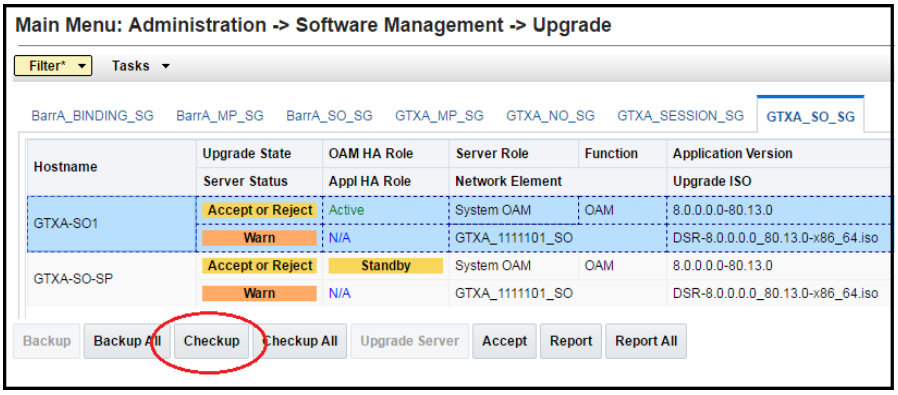
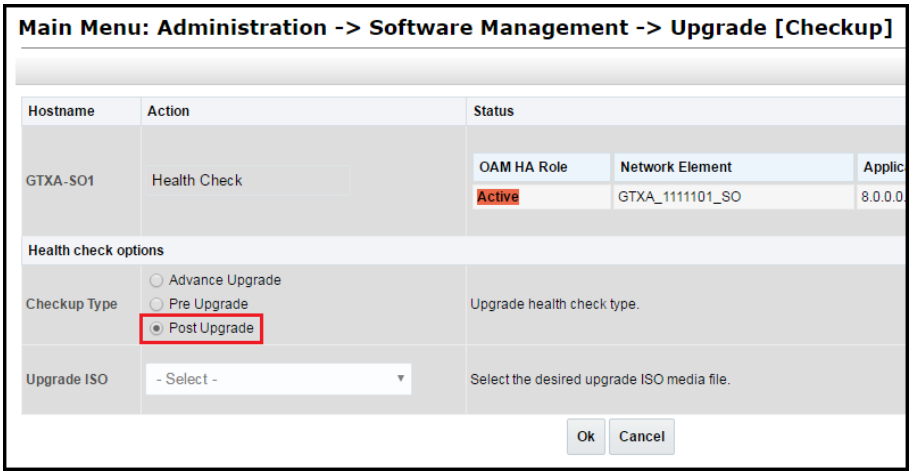
- Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
- Alarm ID = 31109 (Topology config error)
- Alarm ID = 31114 (DB Replication over SOAP has failed)
- Alarm ID = 31106 (DB Merge To Parent Failure)
- Alarm ID = 31134 (DB replication to slave failure)
- Alarm ID = 31102 (DB replication from master failure)
- Alarm ID = 31282 (HA management fault)

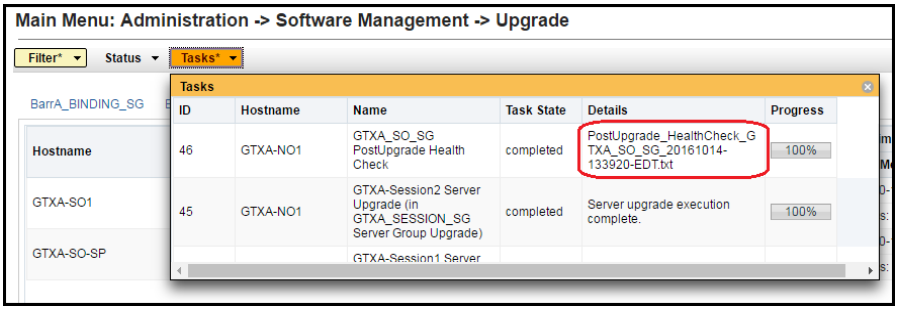
6.2 Backout Health Check

This section provides the procedure to verify that the DSR is ready for backout. The site post-upgrade Health Check is used to perform the backout Health Check.

Procedure 35. Backout Health Check

Step #	Procedure	Description
This procedure performs a Health Check on the site prior to backing out the upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

Step #	Procedure	Description
1. ☐	**Active NOAM VIP**: Run the automated post-upgrade health checks for backout	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being backed out. 3. Select the SOAM server group link for the site being backed out. 4. Select the active SOAM.  5. Click **Checkup**. 6. Under Health check options, click **Post Upgrade**. 7. Click **OK**. Control returns to the Upgrade screen. 

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Monitor health check progress for completion	1. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. 4. Open the report and review the results. 
3. ☐	**Active NOAM VIP**: Analyze health check results	Analyze health check report for failures. If the Health Check report status is anything other than **Pass**, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to **Status & Manage > Files**. 2. Select the active SOAM tab. 3. Select the **UpgradeHealthCheck.log** file and click **View**. 4. Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact for guidance.
4. ☐	**Active NOAM VIP**: Identify IP addresses of servers to be backed out	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being backed out. 3. Select each server group link, making note of the application version of each server. 4. Based on the Application Version column, identify all the hostnames that need to be backed out. 5. Navigate to **Configuration > Servers**. 6. Using the data recorded in Table 5, note the XMI/iLO/LOM IP addresses of all the hostnames to be backed out. These are required to access the server when performing the backout. The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended to contact My Oracle Support (MOS) as stated in the **Warning** box.

Step #	Procedure	Description

5.
☐
	Active NOAM VIP: Verify backup archive files	1. Navigate to **Status & Manage > Files**.
		2. For each server to be backed out, select the server tab on the Files screen. Verify the two backup archive files, created in section 3.4.5, are present on every server that is to be backed out. These archive files have the format:
		`Backup.<application>.<server>.FullDBParts.<role>.<date_time>.UPG.tar.bz2`
		`Backup.<application>.<server>.FullRunEnv.<role>.<date_time>.UPG.tar.bz2`

6.
☐
	Active NOAM CLI: Verify disk usage	Starting with the active SOAM, log into each server to be backed out to verify the disk usage is within acceptable limits.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM.
		`ssh admusr@<server IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Enter the command:
		`[admusr@EVO-NO-1 ~]$ df`
		Sample output (abridged):
		`Filesystem 1K-blocks Used Available Use% Mounted on`
		`/dev/mapper/vgroot-plat_root 999320 294772 652120 32% /`
		`tmpfs 12303460 0 12303460 0% /dev/shm`
		`/dev/vda1 245679 41967 190605 19% /boot`
		`/dev/mapper/vgroot-plat_tmp 999320 1548 945344 1% /tmp`
		`/dev/mapper/vgroot-plat_usr 5029504 2962552 1804824 63% /usr`
		`/dev/mapper/vgroot-plat_var 999320 558260 388632 59% /var`
		`/dev/mapper/vgroot-plat_var_tklc 3997376 2917284 870380 78% /var/TKLC`
		3. Observe the line for the **/var** and **/usr** partition. If the Use% column is 70% or less, this procedure is complete. Continue with the back out per Table 22 (Emergency) or Table 23 (Normal).
		If the Use% of the /var and /usr partition is at 70% or greater, search the partition for files that can be safely deleted. **Use extreme caution in selecting files to be deleted. The deletion of critical system files could severely impair the DSR functionality.**
		4. Repeat this step for all servers to be backed out.

6.3 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures no changes are made to the database while the NOAMs and sites are backed out. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 36. Disable Global Provisioning

Step #	Procedure	Description
This procedure disables provisioning for the NOAM servers, prior to upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: Disable global provisioning and configuration updates on the entire network	1. Log into the active NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Disable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Enable Provisioning**. A yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] – Global provisioning has been manually disabled**. The active NOAM server has the following expected alarm: **Alarm ID = 10008 (Provisioning Manually Disabled)**

6.4 Perform Emergency Backout

EMERGENCY SITE BACKOUT

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

The procedures in this section perform a backout of all servers to restore the source release. An emergency backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact My Oracle Support (MOS) as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

6.4.1 Emergency Site Backout

The procedures in this section backout all servers at a specific site without regard to traffic impact.

!!WARNING!! Executing this procedure results in a total loss of all traffic being processed by this DSR. Traffic being processed by the mate DSR is not affected.

Procedure 37. Emergency Site Backout

Step #	Procedure	Description
This procedure backs out the DSR application software from multiple B- and C-level servers for a specific site. Any server requiring backout can be included: SOAMs, DA-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: Identify all servers that require backout (within a site)	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration >Software Management >Upgrade**. 3. Select the SOAM tab of the site being backed out. 4. Select each server group link, making note of the application version of the servers. 5. Identify the servers in the respective server groups with the target release **Application Version** value. These servers were previously upgraded but now require backout. 6. Make note of these servers. They have been identified for backout. 7. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. ☐	**Active SOAM VIP**: Disable site provisioning for the site to be backed out	1. Log into the SOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Disable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Enable Provisioning**. A yellow information box displays at the top of the view screen which states: **[Warning Code 004] – Site provisioning has been manually disabled**. The active SOAM server has the following expected alarm: **Alarm ID = 10008 (Provisioning Manually Disabled)**
!!WARNING!!		Step 3 results in a total loss of all traffic being processed by this DSR.
3. ☐	Back out all C-level servers, as applicable	**For all configurations**: Back out all C-level servers (IPFEs, SBRs, SBRs, and DA-MPs) identified in step 1: Execute Procedure 42.
4. ☐	Additional post back out steps	After all the servers in a particular server group are backed out, revert back the changes for the SBR server by executing Appendix M Additional Post-Backout Steps. Perform Appendix V to create a link of Comagent.

Step #	Procedure	Description
5. ☐	Back out the standby and spare SOAM servers, as applicable	Back out the standby and spare DSR SOAM servers: **If standby and spare SOAM servers are present:** Execute Procedure 42. **If only a spare SOAM server is present:** Execute Procedure 41.
6. ☐	Back out the active DSR SOAM server	Execute Procedure 41.
7. ☐	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s) by executing Appendix M Additional Post-Backout Steps.
8. ☐	**Active SOAM VIP**: Enable site provisioning	1. Log into the SOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Site Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Disable Site Provisioning**.

Note: If another site is to be backed out, follow all procedures in Table 22 in another maintenance window.

6.4.2 Emergency NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 38. Emergency NOAM Backout

Step #	Procedure	Description
This procedure is used to perform an emergency backout of the DSR application software from the NOAM servers. This procedure backs out the application software as quickly as possible, without regard to operational impact. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Back out the standby DR NOAM server (if equipped)	Execute Procedure 41.

Step #	Procedure	Description
2. ☐	Back out the active DR NOAM server (now the standby) (if equipped)	Execute Procedure 41.
3. ☐	Back out the standby DSR NOAM server (as applicable)	Execute Procedure 41.
4. ☐	Back out the active DSR NOAM server (now the standby)	Execute Procedure 41.
5. ☐	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the NOAM server(s) by executing Appendix M Additional Post-Backout Steps.
6. ☐	**Active NOAM VIP**: Enable global provisioning and configuration updates on the entire network	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Provisioning**. 4. Verify the button text changes to **Disable Provisioning**.

Step #	Procedure	Description
7. ☐	**Active NOAM VIP**: Remove **Ready** state for any backed out server	1. Navigate to **Status & Manage > Servers**. 2. If any backed-out server Application Status is **Disabled**, then navigate to the server row and click **Restart**. 3. Navigate to **Administration >Software Management >Upgrade**. 4. If any backed-out server shows an Upgrade State of **Ready** or **Success**, then select that server and click **Complete Upgrade**. Otherwise, skip this step. 5. Click **OK**. This removes the **Forced Standby** designation for the backed-out server. ***Note***: Due to backout being initiated from the command line instead of through the GUI, the following SOAP error may appear in the GUI banner. `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message. 6. Verify the Application Version value for servers has been downgraded to the original release version.

6.5 Perform Normal Backout

NORMAL SITE BACKOUT

Use this section to perform a normal backout of a DSR upgrade

The following procedures to perform a normal backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact My Oracle Support (MOS), as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

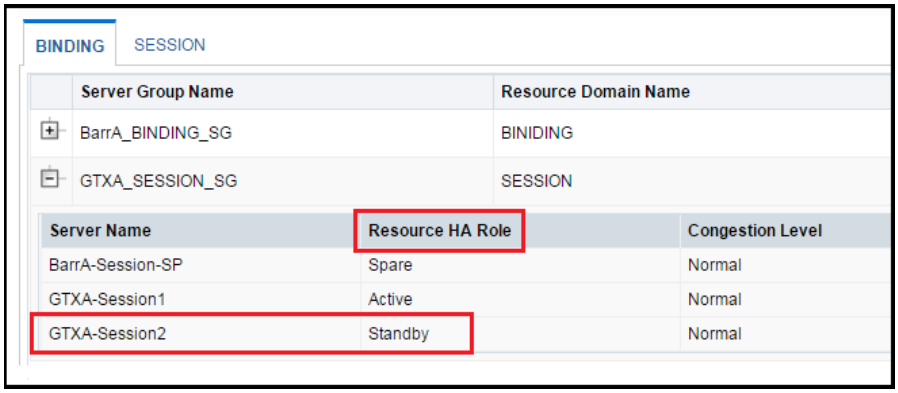
6.5.1 Normal Site Backout

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

Procedure 39. Normal Site Backout

Step #	Procedure	Description
This procedure backs out an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

Step #	Procedure	Description
1. ☐	**Active NOAM VIP**: Identify all servers that require backout (within a site)	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration >Software Management > Upgrade**. 3. Select the SOAM tab of the site being backed out. 4. Select each server group link, making note of the application version of each server. 5. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 6. Make note of these servers. They have been identified for backout. 7. Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2. ☐	**Active SOAM VIP**: Disable site provisioning for the site to be backed out	1. Log into the SOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Disable Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Enable Provisioning**. A yellow information box displays at the top of the view screen which states: **[Warning Code 004] – Site provisioning has been manually disabled**. The active SOAM server has the following expected alarm: **Alarm ID = 10008 (Provisioning Manually Disabled)**
3. ☐	Back out the first set of C-level servers, as applicable	***Note***: In a PCA System, the spare SBR server is located at the mated site of the site being backed out. These servers can be backed out in parallel (as applicable): • ½ of all DA-MPs for N+0 (multi-active) configuration • Standby SBR(s) • Spare SBR(s) • ½ of all IPFEs Execute Procedure 41 for each standby/spare C-level server identified.
	!!WARNING!!	Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact.

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Verify standby SBR server status	If the server being backed out is the standby SBR, execute this step. Otherwise, continue with step 6. 1. Navigate to **SBR > Maintenance > SBR Status.** Open the tab of the server group being upgraded. 2. Do not proceed to step 6 until the **Resource HA Role** for the standby server has a status of **Standby**.  BINDING SESSION Server Group Name: BarrA_BINDING_SG — Resource Domain Name: BINIDING Server Group Name: GTXA_SESSION_SG — Resource Domain Name: SESSION Server Name / Resource HA Role / Congestion Level BarrA-Session-SP / Spare / Normal GTXA-Session1 / Active / Normal GTXA-Session2 / Standby / Normal
5. ☐	**Active NOAM VIP**: Verify bulk download is complete between the active SBR in the server group to the standby and spare SBRs	1. Navigate to **Alarm & Event > View History**. 2. Export the Event log using the following filter: **Server Group**: Choose the SBR group that is in upgrade **Display Filter**: Event ID = 31127 – DB Replication Audit Complete **Collection Interval**: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time. 3. Wait for the following instances of Event 31127: • 1 for the Standby Binding SBR server • 1 for the Standby Session SBR server • 1 for the Spare Binding SBR server • 1 for the Spare Session SBR server • 1 for the 2nd Spare Binding SBR server, if equipped • 1 for the 2nd Spare Session SBR server, if equipped ***Note***: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.
6. ☐	Back out remaining C-level servers, as applicable	These servers can be backed out in parallel (as applicable) • ½ of all DA-MPs for N+0 (multi-active) configuration • Active SBR(s) • ½ of all IPFEs Execute Procedure 41 for each C-level server identified.

Step #	Procedure	Description
7. ☐	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SBR server(s) by executing Appendix M Additional Post-Backout Steps.
8. ☐	Back out the standby DSR SOAM server	Execute Procedure 41.
9. ☐	Back out spare DSR SOAM server, if applicable	***Note***: The spare server is located at the mated site of the site being backed out. Execute Procedure 41.
10. ☐	Back out active DSR SOAM server	Execute Procedure 41.
11. ☐	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s) by executing Appendix M Additional Post-Backout Steps. Perform Appendix V to create a link of Comagent.
12. ☐	**Active SOAM VIP**: Enable site provisioning	1. Log into the SOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Site Provisioning**. 4. Confirm the operation by clicking **OK** on the screen. 5. Verify the button text changes to **Disable Site Provisioning**.

Note: If another site is to be backed out, follow all procedures in Table 23 in another maintenance window.

6.5.2 Normal NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 40. Normal NOAM Backout

Step #	Procedure	Description
This procedure is used to perform a normal backout of the DSR application software from the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Back out the standby DR NOAM server (if equipped)	Execute Procedure 41.
2. ☐	Back out other DR NOAM server (if equipped)	Execute Procedure 41.
3. ☐	Back out standby DSR NOAM server (as applicable)	Execute Procedure 41.
4. ☐	Back out active DSR NOAM server	Execute Procedure 41.
5. ☐	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the NOAM server(s) by executing Appendix M Additional Post-Backout Steps.
6. ☐	**Active NOAM VIP**: Enable global provisioning and configuration updates on the entire network	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Database**. 3. Click **Enable Provisioning**. 4. Verify the button text changes to **Disable Provisioning**.

6.6 Back Out Single Server

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

CAUTION This procedure is executed as a component of the Emergency Backout Procedure (Section 6.4) or the Normal Backout Procedure (Section 6.5). This procedure should never be executed as a standalone procedure.

Procedure 41. Back Out Single Server

Step #	Procedure	Description
This procedure backs out the upgrade of application software. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: Prepare the server for backout	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being backed out. 3. Select the server group link containing the server to be backed out. 4. Verify the Upgrade State is **Accept or Reject**. Make the server **Backout Ready** as follows: 5. Navigate to **Status & Manage > HA**. 6. Click **Edit**. 7. Select the server to be backed out and choose a Max Allowed HA Role value of **Standby** (unless it is a Query server, in which case the value should remain set to **Observer**). ***Note***: When the active NOAM is the server being backed out, click **OK** to initiate an HA switchover and cause the GUI session to log out. 8. Click **OK**. ***Note***: If the server being backed out is the active NOAM and HA switchover does not happen, and the OAM HA Role of the NOAMP server to be backed out on the HA status screen is still **Active**, then you have encountered a known issue. Apply the workaround using Appendix R to have the NOAMP HA switchover. *** Critical *** Do NOT omit this step 9. Log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. 10. Verify the Max Allowed HA Role is set to the desired value for the server on the HA Status screen. 11. Navigate to **Status & Manage > Server**. 12. Select the server to back out and click **Stop**. 13. Click **OK** to confirm the operation and verify the Appl State changes to **Disabled**.

Step #	Procedure	Description
		14. Navigate to **Administration > Software Management > Upgrade**. 15. Select the SOAM tab of the site being backed out. 16. Select the link of the server group containing the server to be backed out. Verify the Upgrade State is now **Backout Ready**. ***Note***: It may take a couple of minutes for the status to update.

2.
☐
	Server CLI:
	SSH to server
		Use an SSH client to connect to the server (e.g., ssh, putty):
		`ssh admusr@<server address>`
		`password: <enter password>`
		Note: If direct access to the IMI is not available, or if TVOE is installed on a blade, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

3.
☐
	Server CLI:
	Execute the backout
		Execute this command to find the state of the server to be backed out:
		`$ ha.mystate`
		In this example, the HA state is **Stb** (highlighted).
		`[admusr@MauiNOAM1 ~]$ ha.mystate`
		`resourceId role node DC subResources lastUpdate`
		`DbReplication Act/Stb A2260.016 0 0727:005354.362`
		`VIP Act/Stb A2260.016 0 0727:005354.364`
		`CacdProcessRes Act/Stb A2260.016 0 0727:005803.864`
		`CAPM_HELP_Proc Act/OOS A2260.016 0 0727:005352.696`
		`DSROAM_Proc Act/Stb A2260.016 0 0727:005803.996`
		`CAPM_PSFS_Proc Act/Stb A2260.016 0 0727:005422.602`
		`$ sudo /var/TKLC/backout/reject`
		Note: If back out asks to continue, answer **y**.
		The reject command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.
		Sample output of the reject script:
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

4. ☐	Backout proceeds	Many informational messages display to the terminal screen as the backout proceeds. After backout is complete, the server automatically reboots.

5.
☐
	Server CLI:
	SSH to server
		Use an SSH client to connect to the server (e.g., ssh, putty):
		`ssh admusr@<server address>`
		`password: <enter password>`

Step #	Procedure	Description
		Perform Appendix V to create a link of Comagent.

6. ☐	**Server CLI**: Restore the full DB run environment	Execute the backout_restore utility to restore the full database run environment:
		`$ sudo /var/tmp/backout_restore`
		If asked to proceed, answer **y**.
		Note: In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory, resulting in the following error message:
		`/var/tmp/backout_restore: No such file or directory`
		If this message occurs, copy the file from **/usr/TKLC/appworks/sbin to /var/tmp** and repeat sub-step 1.
		The backout_restore command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.
		If the restore was successful, the following displays:
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		If an error is encountered and reported by the utility, it is recommended to consult with My Oracle Support (MOS) for further instructions.

7. ☐	**Server CLI**: Verify the backout	1. Examine the output of the following commands to determine if any errors were reported:
		`$ sudo verifyUpgrade`
		Note: The verifyUpgrade command detected errors that occurred in the initial upgrade and during the backout. Disregard the initial upgrade errors.
		Note: Disregard the **TKLCplat.sh** error:
		`[root@NO1 ~]# verifyUpgrade`
		`ERROR: TKLCplat.sh is required by upgrade.sh!`
		`ERROR: Could not load shell library!`
		`ERROR: LIB: /var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh`
		`ERROR:  RC: 1`
		Also, disregard this error:
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1513202476::zip error: Nothing to do!`
		`/usr/share/tomcat6/webapps/ohw.war`
		This command displays the current sw rev on the server:
		`$ appRev`
		`Install Time: Wed Apr  4 05:03:13 2018`
		`Product Name: DSR`
		`Product Release: 8.3.0.0.0_83.5.0`

Step #	Procedure	Description

		`Base Distro Product: TPD`
		`Base Distro Release: 7.5.0.0.0_88.46.0`
		`Base Distro ISO: TPD.install-7.5.0.0.0_88.46.0-OracleLinux6.9-x86_64.iso`
		`ISO name: DSR-8.3.0.0.0_83.5.0-x86_64.iso`
		`OS: OracleLinux 6.9`
		2. Enter this command
		`$ sudo verifyBackout`
		The verifyBackout command searches the upgrade log and report all errors found.
		3. If the backout was successful (no errors or failures reported), then proceed to step 8.
		4. If the backout failed with the following error, this error can be ignored and the backout may continue.
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1485165801::ERROR: <rpm name>-7.2.14-7.2.0.0.0_72.23.0: Failure running command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'`
		Also, disregard following error.
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1513202476::zip error: Nothing to do! /usr/share/tomcat6/webapps/ohw.war`
		5. If the backout failed with the following error:
		`ERROR: The upgrade log does not exist!`
		Examine the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for errors that occurred during the backout.
		If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) for further instructions.

8. ☐	**Server CLI**: Reboot the server	Enter this command to reboot the server: `$ sudo init 6` This step can take several minutes.

9.
☐
	Server CLI: Verify OAM services restart (NOAM/SOAM only)	**If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 10.**
		1. Wait several (approximately 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		`login as: admusr`
		`password: <enter password>`
		3. Execute the following command to verify the httpd service is running.
		`$ sudo service httpd status`

Step #	Procedure	Description

		The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		`httpd <process IDs will be listed here> is running...`
		If httpd is not running, repeat sub-steps 3 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further instructions.
		4. Verify if the file **id_dsa** has required ownership:
		1. Check the ownership of the file:
		`sudo ls -ltr /home/awadmin/.ssh/`
		The file permission should be defined as shown:
		`[admusr@HPC-NO1 ~]$ sudo ls -lrt /home/awadmin/.ssh/`
		`total 20`
		`-rw------- 1 awadmin awadm 1281 Sep 27 16:19 config`
		`-rw-r----- 1 awadmin awadm 605 Nov 18 13:20 id_dsa.pub`
		`-rw------- 1 awadmin awadm 668 Nov 18 13:20 id_dsa`
		`-rw------- 1 awadmin awadm 7275 Nov 18 18:09 authorized_keys`
		2. If the file ownership is not set for awadmin, then change the permission:
		`sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa`
		3. Verify file ownership is changed to **awadmin awadm**.

10. ☐	**Active NOAM VIP**: Verify server state is correct after back out	1. Navigate to **Administration > Software Management > Upgrade** to observe the server upgrade status. 2. Select the SOAM tab of the site being backed out. 3. Select the link of the server group containing the server being backed out. If the server status is **Not Ready**, proceed to the next step; otherwise, proceed to step 12.
11. ☐	**Active NOAM VIP**: Change/Correct the Upgrade State on backed out server to **Ready**	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 3. Select the backed out server and choose a Max Allowed HA Role value of **Active** (unless it is a Query server, in which case the value should remain set to **Observer**). 4. Click **OK**. 5. Verify the Max Allowed HA Role is set to the desired value for the server on the HA Status screen. 6. Navigate to **Status & Manage > Server**. 7. Select the server being backed out and click **Restart**. 8. Click **OK** to confirm the operation. 9. Verify the Appl State updates to **Enabled**. 10. Navigate to **Administration > Software Management > Upgrade**. 11. Select the tab of the server group containing the server to be backed out.

Step #	Procedure	Description
		12. Verify the Upgrade State is now **Ready**. It may take a couple minutes for the grid to update.
12. ☐	**Active NOAM VIP**: Verify application version is correct for the backed out server	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being backed out. 3. Select the link of the server group containing the server that was backed out. 4. Verify the **Application Version** value for this server has been downgraded to the original release version.
13. ☐	Additional backout steps	To support backout for major upgrade paths on the NOAM, SOAM, and SBR server(s), execute Appendix L (Additional Backout Steps).

6.7 Back Out Multiple Servers

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

CAUTION This procedure is executed as a component of the Emergency Backout Procedure (Section 6.4) or the Normal Backout Procedure (Section 6.5). This procedure should never be executed as a standalone procedure.

Procedure 42. Back Out Multiple Servers

Step #	Procedure	Description
This procedure backs out the upgrade of DSR 8.3 application software for multiple servers. Any server requiring a backout can be included: DA-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Prepare the server for backout	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the server group tab containing the server to be backed out. 3. Verify the Upgrade State is **Accept or Reject**. Make the server **Backout Ready** as follows: 4. Navigate to **Status & Manage > HA**. 5. Click **Edit**. 6. Select the server to back out and select a **Max Allowed HA Role** value of **Standby** (unless it is a Query server, in which case the value should remain set to **Observer**). ***Note***: When the active NOAM is the server being upgraded, click **OK** to initiate an HA switchover and cause the GUI session to log out. Before logging

Step #	Procedure	Description
		into the active OAM again, close and re-open the browser using the VIP address for the NOAM, and clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared. 7. Click **OK**. 8. Verify the **Max Allowed HA Role** is set to the desired value for the server on the HA Status screen. 9. Navigate to **Status & Manage > Server**. 10. Select the server to back out and click **Stop**. 11. Click **OK** to confirm the operation and verify the Appl State changed to **Disabled**. 12. Navigate to **Administration > Software Management > Upgrade**. 13. Select the SOAM tab of the site being backed out. 14. Select the tab of the server group containing the server to be backed out. Verify the **Upgrade State** is now **Backout Ready**. ***Note***: It may take a couple of minutes for the status to update.

2.
☐
	Server CLI: Log into the server(s)	Use an SSH client to connect to the server (for example, ssh, putty):
		`ssh admusr@<server address>`
		`password: <enter password>`
		Note: If direct access to the IMI is not available, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

Step #	Procedure	Description

3.
☐
	Server CLI: Execute the backout	Determine the state of the server to be backed out. The server role must be either **Standby** or **Spare**.
		Execute following command to find the server role :
		`$ ha.mystate`
		In this example output, the HA state is **Standby**.
		`[admusr@SO2 ~]$ ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		If the state of the server is **Active**, then return to step 1.
		Execute the **reject** command to initiate the backout:
		`$ sudo /var/TKLC/backout/reject`
		Note: If back out asks to continue, answer **y**.
		The reject command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.
		Sample output of the reject script:
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

4. ☐	**Server CLI**: Backout proceeds	Many informational messages display to the terminal screen as the backout proceeds. After backout is complete, the server automatically reboots.
5. ☐	Repeat for each server to be backed out	Repeat steps 1 through 4 for each server to be backed out.

Step #	Procedure	Description

6.
☐
	Server CLI: Log into the server	Use an SSH client to connect to the server (for example, ssh, putty):
		`ssh admusr@<server address>`
		`password:  <enter password>`

7.
☐
	Server CLI: Restore the full DB run environment	Execute the backout_restore utility to restore the full database run environment:
		`$ sudo /var/tmp/backout_restore`
		If asked to proceed, answer **y**.
		Note: In some incremental upgrade scenarios, the backout_restore file is not found in the **/var/tmp** directory, resulting in the following error message:
		`/var/tmp/backout_restore: No such file or directory`
		If this message occurs, copy the file from **/usr/TKLC/appworks/**sbin to **/var/tmp** and repeat sub-step 1.
		The backout_restore command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.
		If the restore was successful, the following displays:
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		If an error is encountered and reported by the utility, it is recommended to consult with My Oracle Support (MOS) by referring to Appendix V of this document for further instructions.

8.
☐
	Server CLI: Verify the backout	1. Examine the output of the following commands to determine if any errors were reported:
		`$ sudo verifyUpgrade`
		Note: The verifyUpgrade command detected errors that occurred in the initial upgrade and during the backout. Disregard the initial upgrade errors.
		Note: Disregard the **TKLCplat.sh** error:
		`[root@NO1 ~]# verifyUpgrade`
		`ERROR: TKLCplat.sh is required by upgrade.sh!`
		`ERROR: Could not load shell library!`
		`ERROR: LIB: /var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh`
		`ERROR:  RC: 1`
		
		Also, disregard following error.
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1513202476::zip error: Nothing to do!`
		`/usr/share/tomcat6/webapps/ohw.war`
		This command displays the current sw rev on the server:
		`$ appRev`
		`Install Time: Wed Apr  4 05:03:13 2018`
		`Product Name: DSR`

Step #	Procedure	Description

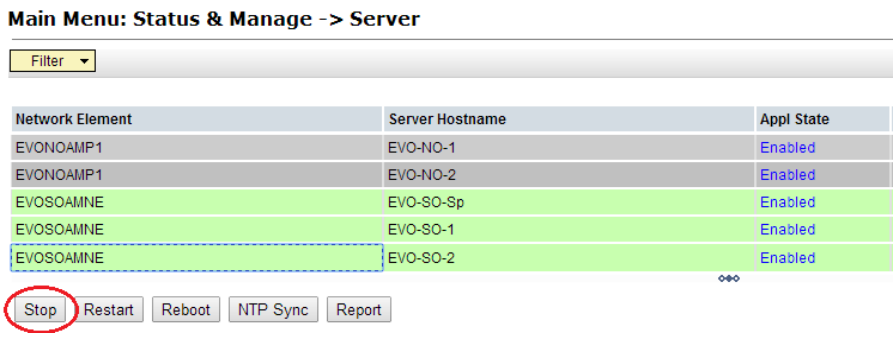
		`Product Release: 8.3.0.0.0_83.5.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.5.0.0.0_88.46.0`
		`Base Distro ISO: TPD.install-7.5.0.0.0_88.46.0-OracleLinux6.9-x86_64.iso`
		`ISO name: DSR-8.3.0.0.0_83.5.0-x86_64.iso`
		`OS: OracleLinux 6.9`
		2. Enter this command
		`$ sudo verifyBackout`
		The verifyBackout command searches the upgrade log and report all errors found.
		3. If the backout was successful (no errors or failures reported), then proceed to step 9.
		4. If the backout failed with the following error, this error can be ignored and the backout may continue.
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1485165801::ERROR: <rpm name>-7.2.14-7.2.0.0.0_72.23.0: Failure running`
		`command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'`
		
		Also, Disregard following error too
		`ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!`
		`ERROR: 1513202476::zip error: Nothing to do!`
		`/usr/share/tomcat6/webapps/ohw.war`
		5. If the backout failed with the following error:
		`ERROR: The upgrade log does not exist!`
		Examine the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for errors that occurred during the backout.
		6. If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) for further instructions.

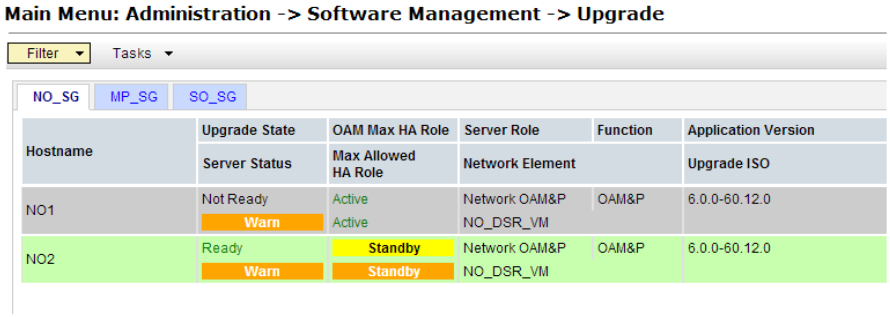
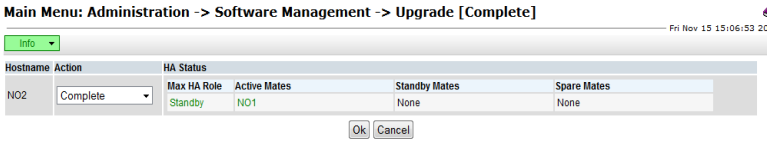
9. ☐	**Server CLI**: Reboot the server	Enter the following command to reboot the server: `$ sudo init 6` This step can take several minutes.

Step #	Procedure	Description

10.
☐
	Server CLI: Verify OAM services restart (NOAM/SOAM only)	**If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 11.**
		Perform Appendix V to create a link of Comagent.
		1. Wait several (approximately 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		`login as: admusr`
		`password: <enter password>`
		3. Execute the following command to verify the httpd service is running.
		`$ sudo service httpd status`
		The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		`httpd <process IDs will be listed here> is running...`
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further instructions.
		4. Verify if the file **id_dsa** has required ownership:
		1. Check the ownership of the file:
		`ls -ltr /home/awadmin/.ssh/`
		The file permission should be defined as shown:
		`[admusr@HPC-NO1 ~]$ sudo ls -lrt /home/awadmin/.ssh/`
		`total 20`
		`-rw------- 1 awadmin awadm 1281 Sep 27 16:19 config`
		`-rw-r----- 1 awadmin awadm 605 Nov 18 13:20 id_dsa.pub`
		`-rw------- 1 awadmin awadm 668 Nov 18 13:20 id_dsa`
		`-rw------- 1 awadmin awadm 7275 Nov 18 18:09 authorized_keys`
		2. If the file ownership is not set for awadmin, then change the permission:
		`sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa`
		3. Verify file ownership is changed to **awadmin awadm**.

11. ☐	Additional backout steps	To support backout for major upgrade paths, execute Appendix L (Additional Backout Steps).
12. ☐	Repeat for each server backed out	Repeat steps 6 through 11 for each server backed out.
13. ☐	**Active NOAM VIP**: Verify server state is correct after back out	1. Navigate to **Administration > Software Management > Upgrade** to observe the server upgrade status. 2. If the active NOAM is on release 7.3 or later, and the server status is **Not Ready**, proceed to the next step; otherwise, proceed to step 17.

Step #	Procedure	Description
14. ☐	**Active NOAM VIP**: Change/Correct the Upgrade State on backed out server to **Ready**	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 3. Select the backed out server and choose a Max Allowed HA Role value of **Active** (unless it is a Query server, in which case the value should remain set to **Observer**). 4. Click **OK**. 5. Verify the Max Allowed HA Role is set to the desired value for the server on the HA Status screen. 6. Navigate to **Status & Manage > Server**. 7. Select the server being backed out and click **Restart**. 8. Click **OK** to confirm the operation. 9. Verify the Appl State updates to **Enabled**. 10. Navigate to **Administration > Software Management > Upgrade**. 11. Select the tab of the server group containing the server to be backed out. 12. Verify the Upgrade State is now **Ready**. 13. Proceed to step 17. to complete the procedure.
15. ☐	**Active NOAM VIP**: Remove Upgrade Ready status	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Server**. 3. If the servers just backed-out show an Appl State of **Enabled**, then multi-select the server rows and click **Stop**. 4. Click **OK** to confirm the operation. 

Step #	Procedure	Description
16. ☐	**Active NOAM VIP**: Correct upgrade status on the backed out server	Correct the upgrade status on the backed out server. 1. Navigate to **Administration > Software Management > Upgrade**. 2. If the servers just backed out show an Upgrade State of **Ready** or **Success**, then select the backed-out server and click **Complete**. If the servers just backed out show Upgrade State of **Not Ready**, then proceed to the next step.  3. Leave the Action set to the default value of **Complete** on the Upgrade Complete screen. 4. Click **OK**. This updates the Max Allowed HA Role of the backed-out server to active, which causes the server's Upgrade State to change to **Not Ready**.  The following SOAP error may appear in the GUI banner: `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message.
17. ☐	**Active NOAM VIP**: Verify application version is correct for the backed out server	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site being backed out. 3. Select the link of the server group containing the server that was backed out. 4. Verify the **Application Version** value for this server has been downgraded to the original release version.

6.8 Post-Backout Health Check

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

Procedure 43. Post-Backout Health Check

Step #	Procedure	Description
This procedure performs a basic health check of the DSR to verify the health of the system following a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: Verify server status is normal	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Server**. 3. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 4. Do not proceed with the upgrade if any server status is not **Norm**. 5. Do not proceed with the upgrade if there are any Major or Critical alarms. Refer to Appendix K for details. ***Note***: It is recommended to troubleshoot if any server status is not Norm. A backout should return the servers to their pre-upgrade status.
2. ☐	**Active NOAM VIP**: Log all current alarms in the system	1. Navigate to **Alarms & Events > View Active**. 2. Click **Report** to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.

6.9 IDIH Backout

The procedures in this section back out the Oracle, Application, and Mediation servers to the previous release.

6.9.1 Oracle Server Backout

Backout of Oracle Server is not supported for release 7.1 or later.

The Oracle server is backed out using the disaster recovery procedure documented in [5].

6.9.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [5].

Appendix A. Post Upgrade Procedures

Execute the procedures in this section only **AFTER** the upgrade of **ALL** servers in the topology is completed.

Appendix A.1. Accept Upgrade

Detailed steps for accepting the upgrade are provided in the procedure. TPD requires that upgrades be accepted or rejected before any subsequent upgrades may be performed. **Alarm 32532 Server Upgrade Pending Accept/Reject** displays for each server until one of these two actions is performed.

An upgrade should be accepted only after it is 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 is not allowed to backout to a previous release.

Note: This procedure must be performed in a Maintenance Window.

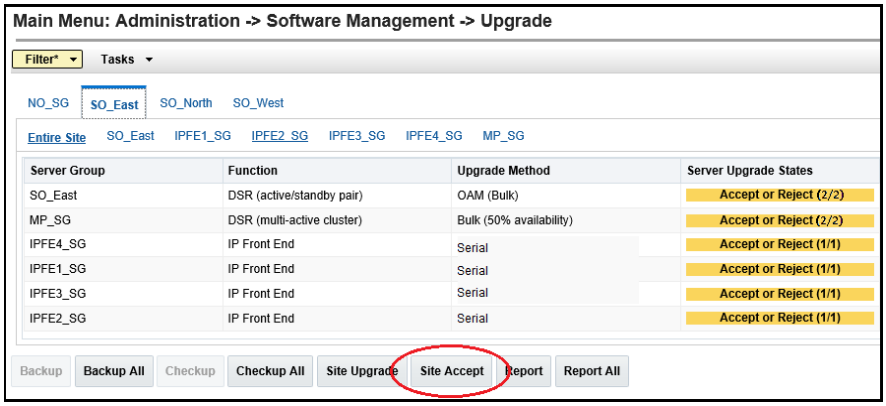
!!WARNING!!

Upgrade acceptance may only be executed with authorization from the customer.

Be advised that once an upgrade has been accepted, it is not possible to back out to the previous release.

Procedure 44. Accept Upgrade

Step #	Procedure	Description
This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	It is recommended that this procedure be performed two weeks after the upgrade	Verify the upgraded system has been stable for two weeks or more. ***Note***: It is not possible to back out after this is procedure is executed.
2. ☐	**Active NOAM VIP**: Execute this step if accepting a NOAM server. Log all current alarms present at the NOAM.	Log all alarms before accepting the NOAM upgrade. 1. Log into the NOAM GUI. 2. Navigate to **Alarms & Events > View Active**. 3. Click **Report** to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)**

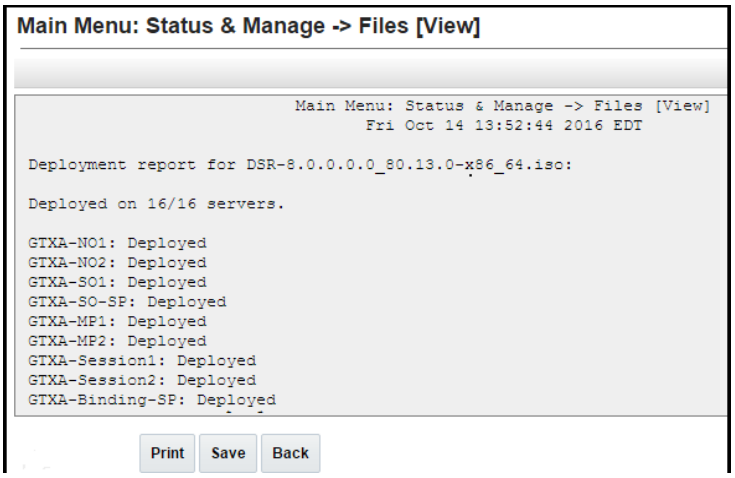
Step #	Procedure	Description
3. ☐	**Active SOAM VIP**: Execute this step if accepting a SOAM server. Log all current alarms present at the SOAM.	Log all alarms before accepting the SOAM upgrade. 1. Log into the SOAM GUI. 2. Navigate to **Alarms & Events > View Active**. 3. Click **Report** to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)**
4. ☐	**Active NOAM VIP**: Accept upgrade for multiple servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration >Software Management >Upgrade**. 3. Select the SOAM tab of the site being upgraded. ***Note***: The **Site Accept** button accepts the upgrade for every upgraded server at the selected site. This is the most efficient way to accept an upgrade. A manual alternative to this is to select the link of each server group in the site and use the **Accept** button to accept the upgrade of only the servers in the selected server group. 4. Click Site Accept.  A confirmation screen warns that once the server is accepted it is not able to revert back to the previous image state. 5. Click **OK**. **WARNING**: Accepting the upgrade may take several minutes depending on the servers in the network. Be patient and DO NOT TRY to accept the site again since this results in different accept states om the Server Upgrade States column on the Upgrade Administration screen. 6. Navigate to **Alarms & Events > View Active**. As upgrade is accepted on each server, the corresponding **Alarm ID – 32532 (Server Upgrade Pending Accept/Reject)** should automatically clear and server status transitions to **Backup Needed**.

Appendix A.2. Undeploy ISO

After the upgrade has been accepted, run this procedure to undeploy all deployed ISOs. When an ISO is undeployed, the ISO is deleted from all servers in the topology except for the active NOAM. On the active NOAM, the ISO remains in the File Management Area.

This procedure can be run at any time after the upgrade has been accepted.

Procedure 45. Undeploy ISO

Step #	Procedure	Description
This procedure undeploys an ISO from the DSR servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active NOAM VIP**: View the files in the file management area	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Files**.
2. ☐	**Active NOAM VIP**: Start ISO undeploy sequence	1. Select an ISO stored in the isos directory of the File Management Area. The ISO filename has the format: `isos/DSR-8.3.0.0.0_83.5.0-x86_64.iso` 2. Click Undeploy ISO. 3. Click **OK** on the confirmation screen to start the undeploy sequence.
3. ☐	**Active NOAM VIP**: Monitor the ISO undeploy progress	1. Select the ISO being deployed in step 2. 2. Click **View ISO Deployment Report**. 3. If some servers show the ISO as **Deployed**, click **Back** on the Files View screen. 4. Periodically repeat sub-steps 1 through 3 until all servers indicate **Not Deployed**. 

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Repeat as necessary	If there are additional ISOs in the File Management Area that need to be undeployed, repeat steps 2. and 3. as necessary.

Appendix A.3. Post Upgrade Accept Procedures

The following procedure is executed after the upgrade has been accepted

Procedure 46. Post Upgrade Accept Procedure.

Step #	Procedure	Description
This procedure performs miscellaneous actions that are required to be executed after the upgrade is accepted. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Active NOAM CLI**: Reset COMCOL compatibility flag	**This step is required only if the source release is pre-8.x.**
		1. Use an SSH client to connect to the active NOAM:
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter this command to reset the COMCOL backward compatibility flag. Backward compatibility is no longer required when all of the servers in the topology have been upgraded to release 8.0 or later.
		`$ iset -fvalue=0 LongParam where "name='cm.cm6compat'"`
		Sample output:
		`=== changed 1 records ===`
		3. Verify the changed value:
		`$ iqt -zp -fvalue LongParam where "name='cm.cm6compat'"`
		`value`
		`0`

Appendix B. Increase Maximum Number of Open Files

The following procedure increases the maximum number of files that can be opened for reading and writing. As the number of servers in the topology grows, so does the need for additional files to handle merging data to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files.

Note: Following procedure is for one NOAM server. Repeat this procedure for other NOAM servers.

Procedure 47. Increase Maximum Number of Open Files

Step #	Procedure	Description
This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

1.
☐
	Active NOAM CLI:
	Determine the number of files currently open
		1. Use an SSH client to connect to the active NOAM.
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter the following command to retrieve the pid of idbsvc. The pid is highlighted in this sample output:
		`$ ps -ef | grep -i idbsvc`
		`root 4369 idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2`
		3. The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 2 in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1278`
		4. Record the number of files currently open (the output of sub-step 3):
		_____
		5. Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in this sample output:
		`$ ps -ef | grep -i tpdProvd`
		`tpdProvd 347635 1 0 06:09 ? 00:00:11 /usr/TKLC/plat/bin/tpdProvd`
		6. The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 4 in place of XXXX in the lsof command.
		`$ sudo lsof -p XXXX | wc -l`
		`1280`
		7. Record the number of files currently open (the output of sub-step 5):
		_____

Step #	Procedure	Description

2.
☐
	Active NOAM CLI: Maximum number of open files	Display the maximum number of open files for idbsvc.
		8. Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  32768  32768  files`
		The output of the cat command displays the maximum number of files that can be open by the idbsvc process. Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____
		This system has over 1024 open files, but its current ulimit for idbsvc is high enough during normal operation that the amount of open files does not pose a problem. However, when an attempt to upgrade another process (tpdProvd) updates idbsvc max # of open files to 1024, it causes the upgrade to fail.
		Display the maximum number of open files for tpdProvd.
		9. Use the highlighted value from step 1, sub-step 4 for tpdProvd in place of XXXX in the cat command.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files  1024  4096  files`
		The output of the cat command displays the maximum number of files that can be open by the tpdProvd process. Record both values here:
		Soft Limit (1st value): _____ Hard Limit (2nd value): _____

3. ☐	Make sure the current number of open files used by idbsvc in in the safe limit	If the number of currently open files (step 1, sub-step 3) of idbsvc is less than the maximum allowed (step 2, sub-step 2 Soft Limit for tpdProvd), this procedure is complete, that is, number of currently open files (used by idbsvc) is less than 1024. Further steps are not required to be executed on this NOAM server. If the number of currently open files are more than the (step 2, sub-step 2 Soft Limit for tpdProvd), that is, 1024, go to step 5. Repeat this procedure (if required) for other NOAM server.
4. ☐	Make sure the current number of open files used by tpdProvd in in the safe limit	If the maximum number of open files value (step 2, sub-step 2 - Soft Limit) for tpdProvd is already set to 32768, this procedure is complete. Further steps are not required to be executed on this NOAM server. If maximum value is not already set, then go to step 5. Repeat this procedure (if required) for other NOAM server.

Step #	Procedure	Description

5.
☐
	Active NOAM CLI: Increase max number of open files	1. Using a text editor with sudo, edit the file **/etc/init/tpdProvd.conf** to add these two lines just before the comment line in the file **/etc/init/tpdProvd.conf** that reads **Start the daemon**:
		`# increase open file limit`
		`limit nofile 32768 32768`
		Insight of file as example:
		`#`
		`# restart tpdProvd up to 10 times within a 100 second period.`
		`# If tpdProvd fails to start 10 times within a 100 second period then`
		`# it most likely has a deeper problem that restarting will not overcome.`
		`respawn limit 10 100`
		`# increase open file limit`
		`limit nofile 32768 32768`
		`#`
		`# Start the daemon`
		`script`
		2. Save the file and close the editor.
		Caution: Do not edit any other line in this file. You can back up the file, if required.

6.
☐
	Active NOAM CLI: Restart tpdProvd service	1. Enter this command to stop tpdProvd:
		`$ sudo initctl stop tpdProvd`
		2. Enter this command to restart tpdProvd:
		`$ sudo initctl start tpdProvd`
		Sample output:
		`tpdProvd start/running, proceed 186743`

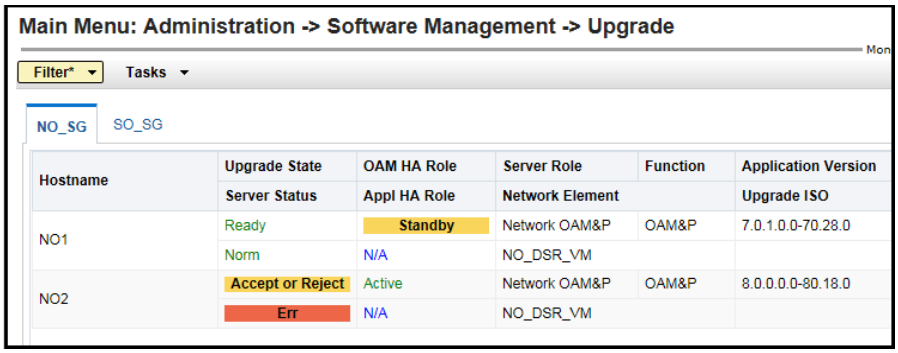
7.
☐
	Active NOAM CLI: Recheck open file maximum limit	3. Enter the following command to retrieve the pid of idbsvc. The pid is highlighted in this sample output:
		`$ ps -ef | grep -i idbsvc`
		`root 8670 idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2`
		4. Use the highlighted value from sub-step 1in place of XXXX in the cat command.
		`$ sudo cat /proc/XXXX/limits | grep -i open`
		`Max open files 32768 32768 files`
		5. Verify the output of sub-step 2 indicates that the max number of open files is 32768. If the value is NOT 32768, it is recommended to contact My Oracle Support (MOS).

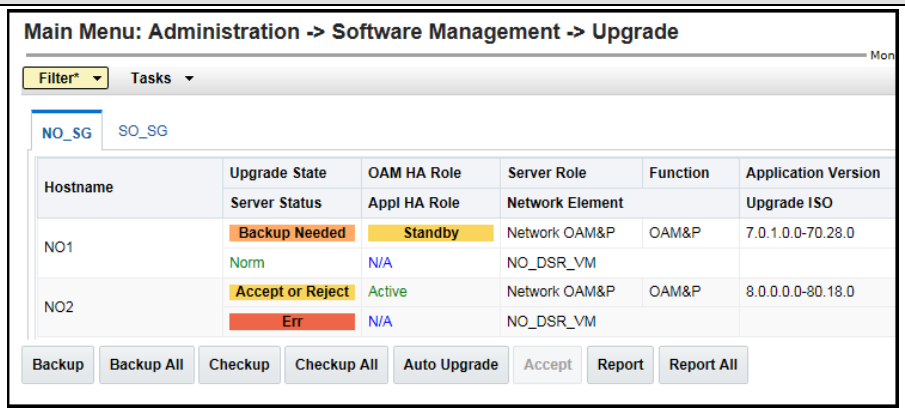
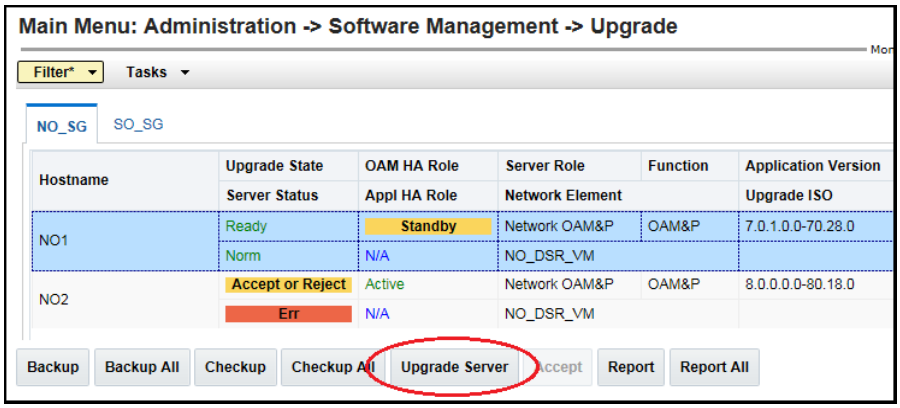
Appendix C. Upgrade Single Server – DSR 8.x

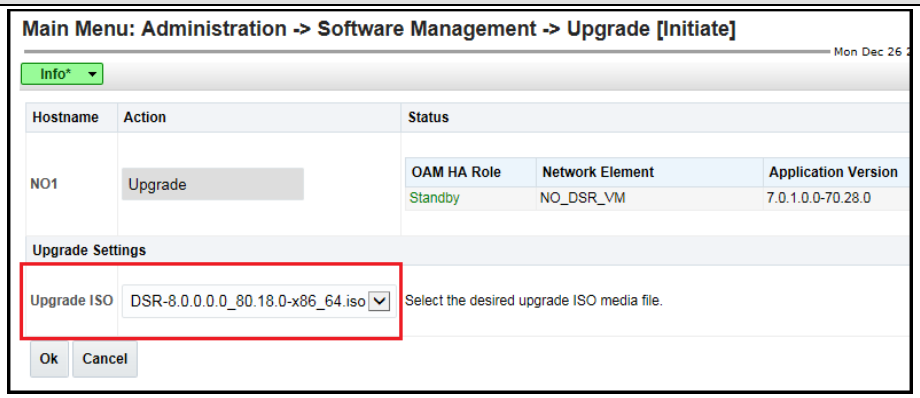
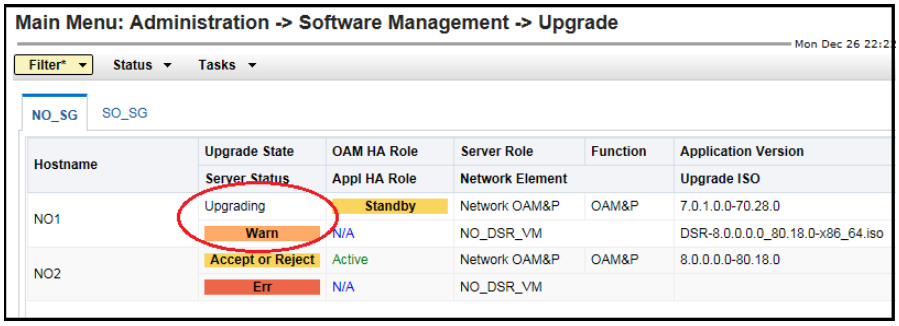
The following procedure upgrades a single DSR server of any type (NOAM, SOAM, MP, etc.) when the active NOAM is on DSR 8.x.

Note: This procedure may be executed multiple times during the overall upgrade, depending on the number of servers in the DSR and the chosen upgrade methodology. Make multiple copies of Appendix C to mark up, or keep another form of written record of the steps performed.

Procedure 48. Upgrade Single Server – Upgrade Administration – DSR 8.x

Step #	Procedure	Description
This procedure executes the Upgrade Single Server – Upgrade Administration steps for an active NOAM on release 8.x. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: View the pre-upgrade status of servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Select the Network Element of the server to be upgraded (NOAM or site).  The active NOAM server may have some or all of these expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)**
2. ☐	**Active NOAM VIP**: Verify status of server to be upgraded	1. Identify the server to be upgraded (NOAM, SOAM, MP, etc.) _____(record hostname) 2. Verify the Application Version value is the expected source software release version. 3. If the server is in the **Backup Needed** state, select the server and click **Backup**. 4. On the Upgrade Backup screen, click **OK**. The Upgrade State changes to **Backup in Progress**. 5. Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.

Step #	Procedure	Description
		 6. When the backup is complete, verify the server state changes to **Ready**.
3. ☐	**Active NOAM VIP**: Initiate the server upgrade	1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click **Upgrade Server**. The Initiate Upgrade form displays. 
4. ☐	**Active NOAM VIP**: Select upgrade ISO	Initiate the server upgrade. 1. From the **Upgrade Settings** – **Upgrade ISO** options, select the ISO to use in the server upgrade. ***Note***: When the active NOAM is the server being upgraded, click OK to initiate an HA switchover and cause the GUI session to log out. ***Note***: If the selected server is the active server in an active/standby pair, the OAM Max HA Role column displays **Active** with a red background. This is NOT an alarm condition. This indicator is to make the user aware the Make Ready action causes an HA switchover. 2. Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.

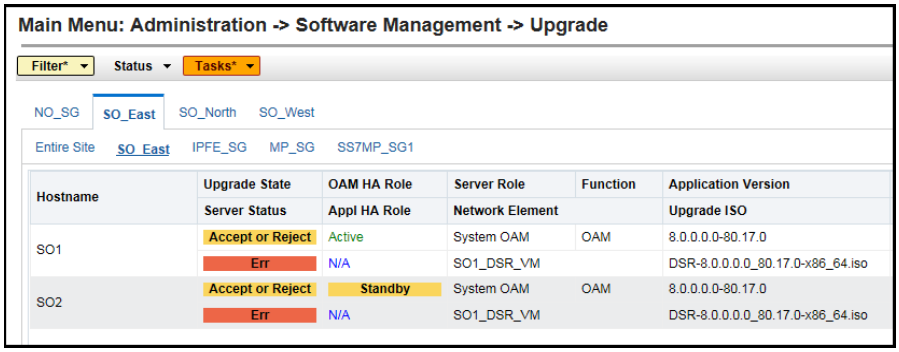
Step #	Procedure	Description
		 *** Critical *** Do NOT omit this step 3. Log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.
5. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	See step 6. for an optional method of monitoring upgrade progress. See step 7. for instructions if the upgrade fails. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Observe the upgrade status of the site on the Upgrade Administration screen by selecting the **Entire Site** link. An upgrade status summary of each server group in the site displays in the Server Upgrade States column.  Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)**

Step #	Procedure	Description
		Alarm ID = 31283 (Highly available server failed to receive mate heartbeats) **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31104 (DB Replication over SOAP has failed** **Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)** **Alarm ID = 31225 (HA Service Start Failure)** **Alarm ID = 31226 (HA Availability Status Degraded)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31149 (DB Late Write Nonactive)** 2. Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes. ***Note***: In the unlikely event that after the upgrade, if the **Upgrade State** of server is **Backout Ready** or **Failed** and the **Status Message** displays **Server could not restart the application to complete the upgrade**, then perform Appendix N Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade. Perform Appendix V to create a link of Comagent. If the upgrade fails, **do not proceed**. It is recommended to consult with Appendix V on the best course of action. Refer to Appendix J for failed server recovery procedures.

Step #	Procedure	Description

6.
☐
	Server CLI: (Optional) View in-progress status from command line of server	An optional method to view Upgrade progress from the command line:
		To view the detailed progress of the upgrade , access the server command line (via SSH or Console), and enter:
		`$ tail -f  /var/TKLC/log/upgrade/upgrade.log`
		This command displays the upgrade log entries as the events occur. Once the upgrade is complete, the server reboots. It takes a couple of minutes for the DSR application processes to start up.
		For example, this command displays the current rev on the server:
		`[admusr@NO2 ~]$ appRev`
		`Install Time: Thu Dec 15 00:05:46 2016`
		`Product Name: DSR`
		`Product Release: 8.1.0.0.0_80.17.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.3.0.0.0_88.30.0`
		`Base Distro ISO: TPD.install-7.3.0.0.0_88.30.0-OracleLinux6.8-x86_64.iso`
		`ISO name: DSR-8.1.0.0.0_80.17.0-x86_64.iso`
		`OS: OracleLinux 6.8`
		If the upgrade fails, **do not proceed**. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

7. ☐	**Server CLI**: If the upgrade fails	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/upgrade.log It is recommended to contact by referring to Appendix V of this document and provide these files. Refer to Appendix J for failed server recovery procedures.

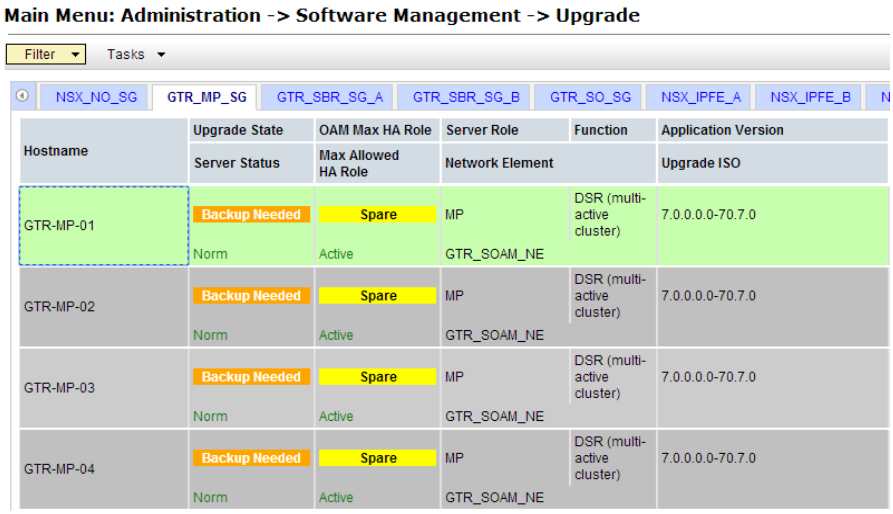
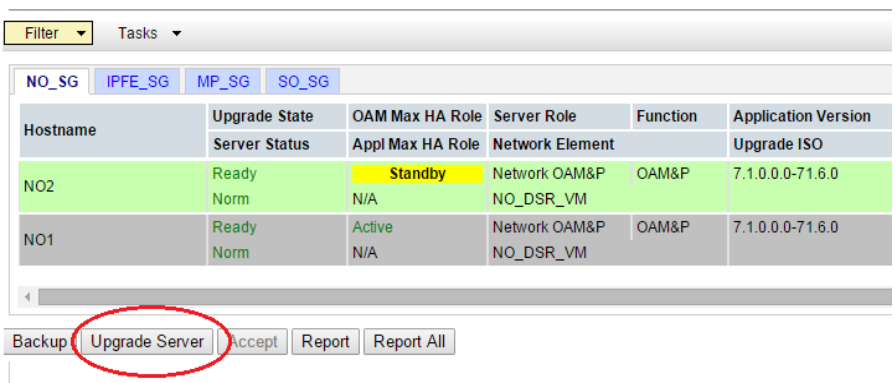
Step #	Procedure	Description
8. ☐	**Active NOAM VIP**: Verify post upgrade status	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the tab of the NOAM or site being upgraded. 3. Verify the Application Version value for this server has been updated to the target software release version. 4. Verify the Upgrade State of the upgraded server is **Accept or Reject**. 
9. ☐	**Active NOAM/SOAM VIP**: Verify the server was successfully upgraded	View the post-upgrade status of the server: Navigate to **Alarm & Events > View Active**. The active NOAM or SOAM server may have some or all the following expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10010 (Stateful database not yet synchronized with mate database)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31000 (Program impaired by S/W Fault)** **Alarm ID = 31201 (Process Not Running) for eclipseHelp process** **Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)** The active NOAM or SOAM has these expected alarms until both NOAMs/SOAMs are upgraded: **Alarm ID = 31233 – HA Secondary Path Down** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** ***Note***: Do not accept upgrade at this time. This alarm is OK.

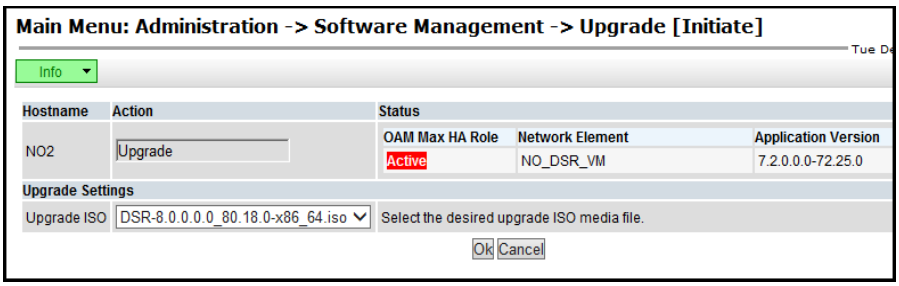
Appendix D. Upgrade Single Server – Pre-DSR 8.0

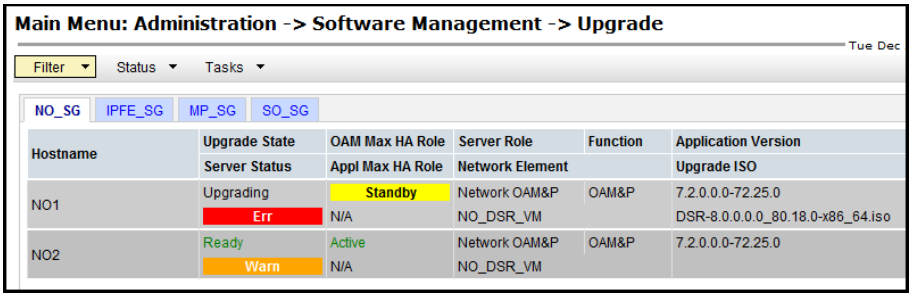
The following procedure upgrades a single DSR server when the active NOAM is on 7.x.y. This procedure upgrades the standby NOAM only. The remaining servers are upgraded using Procedure 50.

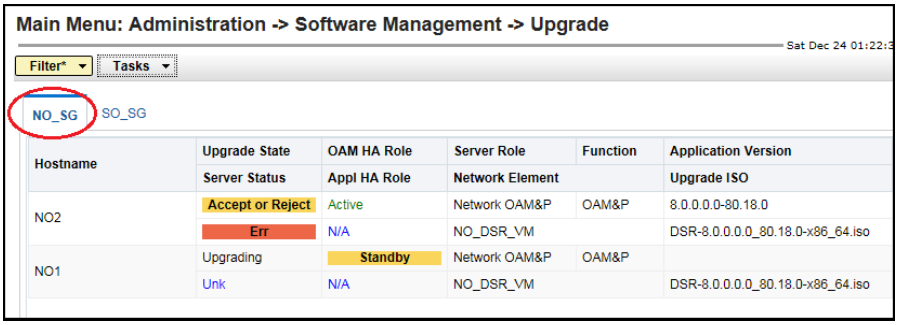
Procedure 49. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

Step #	Procedure	Description
This procedure executes the Upgrade Single Server when the active NOAM is on a release prior to DSR 8.x. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: View the pre-upgrade status of servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. The active NOAM server may have some or all of the following expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks NSX_NO_SG GTR_MP_SG GTR_SBR_SG_A GTR_SBR_SG_B GTR_SO_SG NSX_IPFE_A NSX_IPFE_B Hostname / Upgrade State / Server Status / OAM Max HA Role / Max Allowed HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO GTR-MP-01: Backup Needed, Norm, Spare, Active, MP, GTR_SOAM_NE, DSR (multi-active cluster), 7.0.0.0.0-70.7.0 GTR-MP-02: Backup Needed, Norm, Spare, Active, MP, GTR_SOAM_NE, DSR (multi-active cluster), 7.0.0.0.0-70.7.0 GTR-MP-03: Backup Needed, Norm, Spare, Active, MP, GTR_SOAM_NE, DSR (multi-active cluster), 7.0.0.0.0-70.7.0 GTR-MP-04: Backup Needed, Norm, Spare, Active, MP, GTR_SOAM_NE, DSR (multi-active cluster), 7.0.0.0.0-70.7.0

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Verify status of server to be upgraded	1. Identify the server (NOAM, SOAM, MP, etc.) _____ (record name) 2. Verify the Application Version value is the expected source software release version. 3. Navigate to **Administration > Software Management > Upgrade** and select the Server Group of the server to upgrade.  4. If the server is in the **Backup Needed** state, select the server and click **Backup**. 5. On the Upgrade Backup screen, click **OK**. The Upgrade State changes to **Backup in Progress**. 6. Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded. 7. When the backup is complete, verify the server state changes to **Ready**.
3. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 1)	1. From the Upgrade Administration screen, select the server to upgrade. 2. Click **Upgrade Server**.  The Initiate Upgrade form displays on the **Administration > Software Management > Upgrade Initiate** screen.

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 2) – Select ISO form	1. From the **Upgrade Settings** – **Upgrade ISO** options, select the ISO to use in the server upgrade, ***Note***: When the active NOAM is the server being upgraded, click **OK** to initiate an HA switchover and cause the GUI session to log out. ***Note***: If the selected server is the active server in an active/standby pair, the OAM Max HA Role column displays **Active** with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the action causes an HA switchover. 2. Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.  *** Critical *** Do NOT omit this step 3. If the server being upgraded is the active NOAM and clicking OK initiated a role change, log out of the GUI, clear the browser cache, and log back into the active NOAM via the VIP before continuing. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.

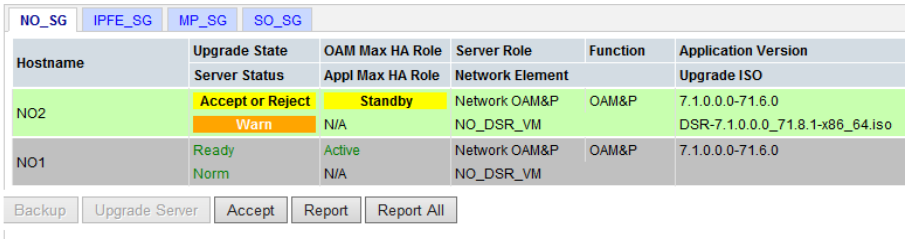
Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Observe the upgrade state of the server of interest. Upgrade status displays under the Status Message column.  Main Menu: Administration -> Software Management -> Upgrade Tue Dec Filter Status Tasks NO_SG IPFE_SG MP_SG SO_SG Hostname / Upgrade State / Server Status / OAM Max HA Role / Appl Max HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO NO1: Upgrading, Err; Standby, N/A; Network OAM&P, NO_DSR_VM; OAM&P; 7.2.0.0.0-72.25.0, DSR-8.0.0.0.0_80.18.0-x86_64.iso NO2: Ready, Warn; Active, N/A; Network OAM&P, NO_DSR_VM; OAM&P; 7.2.0.0.0-72.25.0 Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31104 (DB Replication over SOAP has failed** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)** 2. Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes. Perform Appendix V to create a link of Comagent. If the upgrade fails, **do not proceed**. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

Step #	Procedure	Description
6. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress **For active NOAM on DSR 8.1 only**	This step is for monitoring upgrade status of the formerly active NOAM after a role change. The NOAM that was active when the upgrade was initiated is now the standby NOAM. Monitoring from this point on is from the new active NOAM on DSR 8.2. See step 7. for an optional method of monitoring upgrade progress. See step 8. for instructions if the upgrade fails. ***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Observe the upgrade status of the standby NOAM on the Upgrade Administration screen by selecting the NOAM server group tab.  2. Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes. ***Note***: In the unlikely event that after the upgrade, if the **Upgrade State** of server is **Backout Ready** and the **Status Message** displays **Server could not restart the application to complete the upgrade**, then perform Appendix N Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade. If the upgrade fails, **do not proceed**. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

Step #	Procedure	Description

7.
☐
	Server CLI: (**Optional**) View in-progress status from command line of server	An optional method to view Upgrade progress from the command line:
		To view the detailed progress of the upgrade , access the server command line (via SSH or Console), and enter:
		`$ tail -f /var/TKLC/log/upgrade/upgrade.log`
		Once the server has upgraded, it reboots, and it takes a couple of minutes for the DSR application processes to start up.
		This command displays the current rev on the server:
		`$ appRev`
		`Install Time: Tue Jun 17 08:20:57 2014`
		`Product Name: DSR`
		`Product Release: 6.0.0_60.14.6`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.7.0.0.1_84.14.0`
		`Base Distro ISO: TPD.install-6.7.0.0.1_84.14.0-OracleLinux6.5-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

8.
☐
	Server CLI: If the upgrade fails	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		It is recommended to contact by referring to Appendix V of this document and provide these files. Refer to Appendix J for failed server recovery procedures.

9. ☐	**Active NOAM VIP**: Verify post upgrade status	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the Application Version value for this server has been updated to the target software release version. 3. Verify the Upgrade State of the upgraded server is **Accept or Reject**. 

Step #	Procedure	Description
10. ☐	**Active NOAM/SOAM VIP**: Verify the server was successfully upgraded	View the Post-Upgrade Status of the server: Navigate to **Alarm & Events > View Active**. The active NOAM or SOAM server may have some or all the following expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10010 (Stateful database not yet synchronized with mate database)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31000 (Program impaired by S/W Fault)** **Alarm ID = 31201 (Process Not Running) for eclipseHelp process** **Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** ***Note***: Do not accept upgrade at this time. This alarm is OK. The active NOAM or SOAM has the following expected alarm until both NOAMs/SOAMs are upgraded: **Alarm ID = 31233 – HA Secondary Path Down** The single server upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix D.

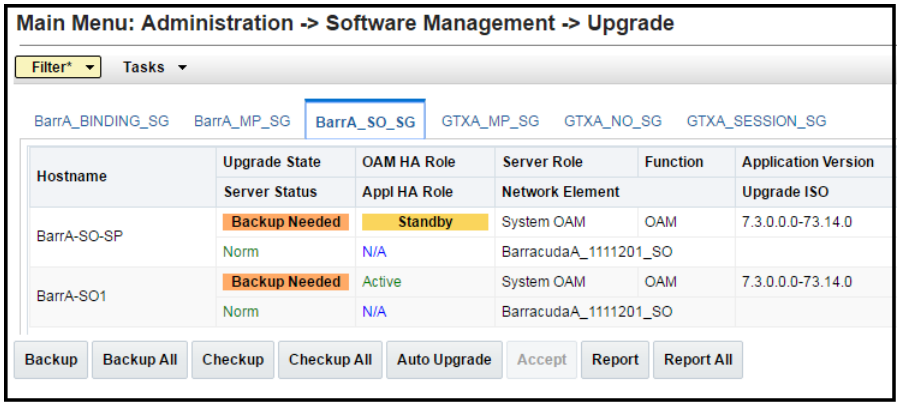
Appendix E. Upgrade Multiple Servers – Upgrade Administration

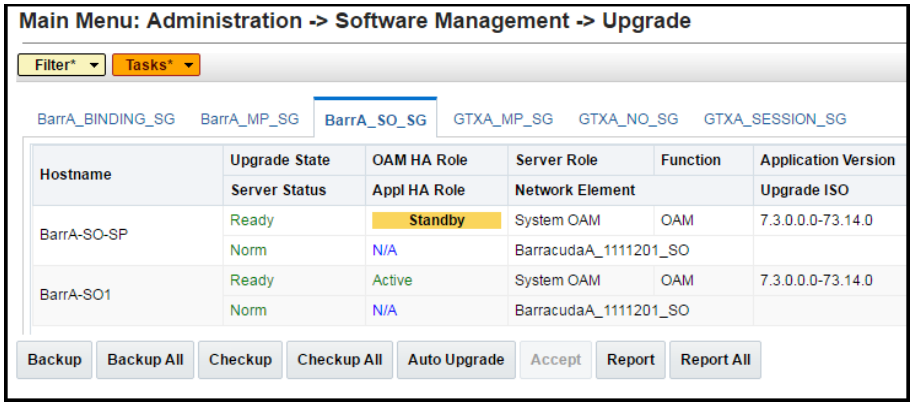
The following procedure upgrades multiple servers in parallel.

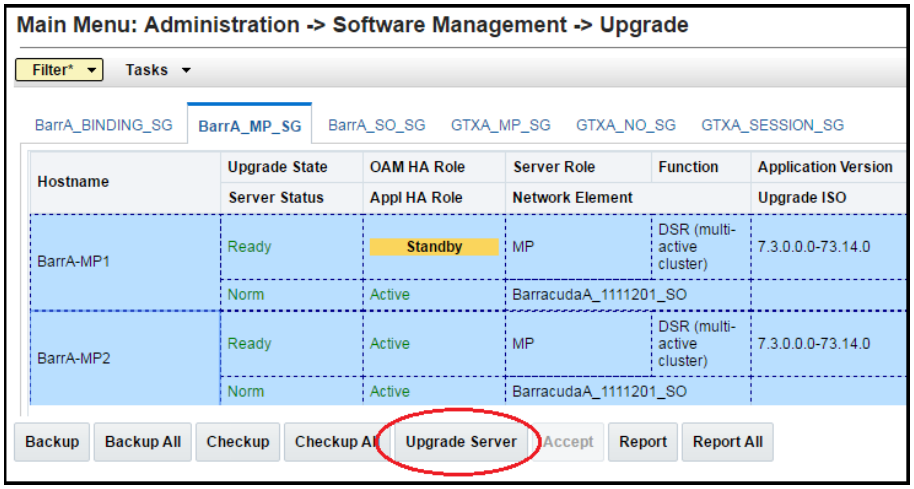
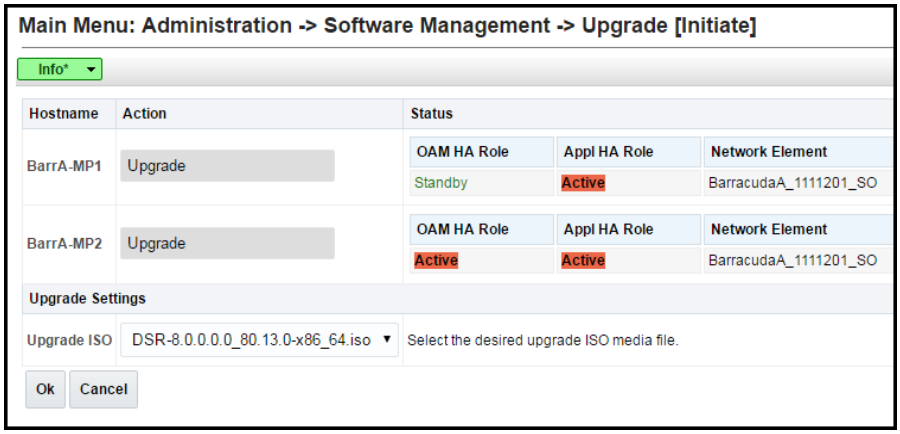
Note: This procedure is executed multiple times during the overall upgrade, depending on the number of servers in your DSR. Make multiple copies of Appendix E to mark up or keep another form of written record of the steps performed.

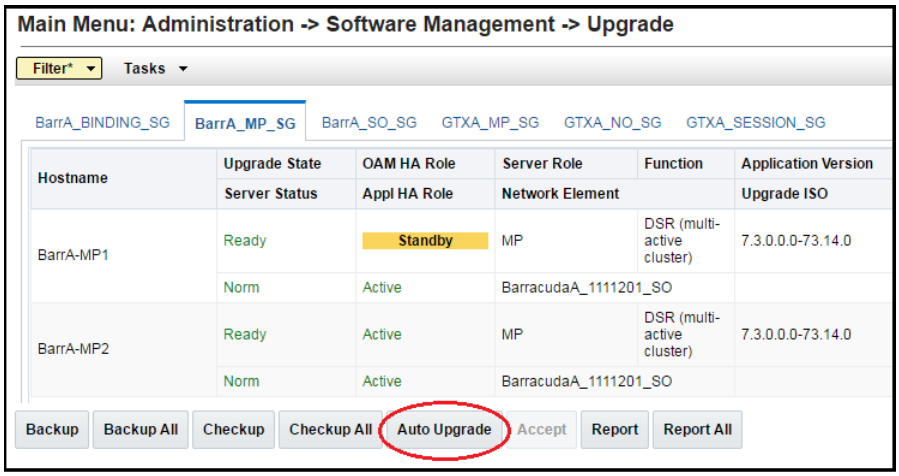
Procedure 50. Upgrade Multiple Servers – Upgrade Administration

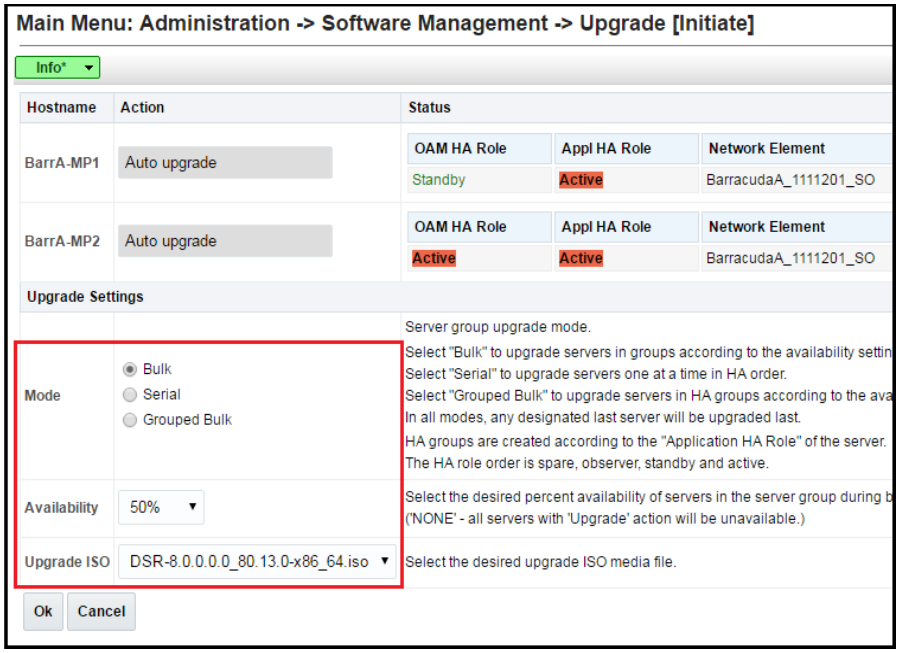
Step #	Procedure	Description
This procedure executes the Upgrade Multiple Servers – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: View pre-upgrade status of the servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. The active NOAM server may have some or all of the following expected alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks NSX_NO_SG GTR_MP_SG GTR_SBR_SG_A GTR_SBR_SG_B GTR_SO_SG NSX_IPFE_A NSX_IPFE_B Hostname / Upgrade State / OAM Max HA Role / Server Role / Function / Application Version Server Status / Max Allowed HA Role / Network Element / Upgrade ISO GTR-MP-01 Backup Needed Spare MP DSR (multi-active cluster) 7.0.0.0.0-70.7.0 Norm Active GTR_SOAM_NE GTR-MP-02 Backup Needed Spare MP DSR (multi-active cluster) 7.0.0.0.0-70.7.0 Norm Active GTR_SOAM_NE GTR-MP-03 Backup Needed Spare MP DSR (multi-active cluster) 7.0.0.0.0-70.7.0 Norm Active GTR_SOAM_NE GTR-MP-04 Backup Needed Spare MP DSR (multi-active cluster) 7.0.0.0.0-70.7.0 Norm Active GTR_SOAM_NE

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Verify status of servers to be upgraded	1. Identify the MP servers to be upgraded in parallel _____ (record names) 2. Verify the Application Version value is the expected source software release version for each MP server to be upgraded. 3. Navigate to **Administration > Software Management > Upgrade** and select the Server Group of the server to upgrade.  4. If the server is in **Backup Needed** state, select the servers and click **Backup**. The Upgrade State changes to **Backup in Progress**. When the backup is complete, the Upgrade State changes to **Ready**. 5. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded.

Step #	Procedure	Description
3. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready**	The Upgrade Administration form refreshes and the server to upgrade displays Upgrade Status = **Ready**. This may take a minute.  Depending on the server being upgraded, new alarms may occur. Servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 32515 (Server HA Failover Inhibited)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**
4. ☐	Determine upgrade method – manual or automatic	To upgrade multiple servers in parallel using the manual option, execute steps 5. and 6. To upgrade a server group using the Automated Server Group Upgrade option, proceed to step 7.

Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Initiate upgrade (part 1)	1. From the Upgrade Administration screen, select the servers to upgrade. 2. Click **Upgrade Server**.  The Initiate Upgrade form displays on the **Administration > Software Management > Upgrade Initiate** screen.
6. ☐	**Active NOAM VIP**: Initiate upgrade (part 2) – Select ISO form	1. From the **Upgrade Settings** – **Upgrade ISO** options, select the ISO to use in the server upgrade. 2. Click **OK**. The upgrade begins and control returns to the Upgrade Administration screen.  3. Proceed to step 8. to complete this procedure.

Step #	Procedure	Description
7. ☐	**Active NOAM VIP**: Initiate (part 1) – Automated Server Group Upgrade option	1. To utilize the Automated Server Group upgrade option, verify no servers in the server group are selected.  2. Click **Auto Upgrade**.

Step #	Procedure	Description
8. ☐	**Active NOAM VIP**: Initiate (part 2) – Automated Server Group Upgrade	***Note***: The settings to be used in this step are specified in the calling procedure. 1. The **Upgrade Settings** section of the Initiate screen controls the behavior of the automated upgrade. Select the settings that apply to the server type being upgraded. **Bulk**: Select this option for active/standby and multi-active server groups. For servers in an active/standby configuration, the standby server is upgraded first, followed by the active. Servers in a multi-active configuration are upgraded in parallel to the extent allowed by the Availability setting. **Serial**: Select this option to upgrade multiple servers one at a time. **Grouped Bulk**: Select this option for SBR server groups. Grouped bulk always upgrades the spare(s), followed by the standby, followed by the active. **Availability**: This setting determines how many servers remain in service while servers in the server group are upgraded. For example, a setting of 50% ensures at least half of the servers in the server group remain in service. ***Note***: The Serial upgrade mode is available as an alternative to Bulk and Grouped Bulk for a more conservative upgrade scenario. Serial mode upgrades each server in the server group one at a time, and can be used on any server group type. 2. Select the appropriate ISO from the **Upgrade ISO** options. 3. Click **OK** to start the upgrade. 
9. ☐	**Active NOAM VIP**: View the upgrade administration	See step 10. for an optional method of monitoring upgrade progress. See step 11. for instructions if the Upgrade fails, or if execution time exceeds 60 minutes.

Step #	Procedure	Description
	form to monitor upgrade progress	***Note***: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as **FAILED**. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Observe the upgrade status of the servers of interest. Upgrade status displays under the Status Message column. **Main Menu: Administration -> Software Management -> Upgrade** Filter* Status Tasks* BarrA_BINDING_SG BarrA_MP_SG BarrA_SO_SG GTXA_MP_SG GTXA_NO_SG GTXA_SESSION_SG GTXA_SO_SG Hostname: BarrA-MP1 Upgrade State: Pending Server Status: Err OAM HA Role: Active Appl HA Role: Active Server Role: MP Network Element: BarracudaA_1111201_SO Function: DSR (multi-active cluster) Application Version: 7.3.0.0.0-73.14.0 Upgrade ISO: DSR-8.0.0.0.0_80.13.0-x86_64.iso Hostname: BarrA-MP2 Upgrade State: Upgrading Server Status: Unk OAM HA Role: OOS Appl HA Role: N/A Server Role: MP Network Element: BarracudaA_1111201_SO Function: DSR (multi-active cluster) Application Version: Upgrade ISO: DSR-8.0.0.0.0_80.13.0-x86_64.iso During the upgrade, the servers may have a combination of the following expected alarms. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31101 (DB Replication To Slave Failure)** **Alarm ID = 31106 (DB Merge To Parent Failure)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31233 (HA Secondary Path Down)** **Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)** **Alarm ID = 32515 (Server HA Failover Inhibited)** 2. Wait for the upgrade to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes. When an upgraded SOAM becomes active on release 8.x, **Alarm 25607** displays to alert the operator to enable the new Signaling Firewall feature. This alarm is active until the firewall is enabled in Procedure 31. **Alarm ID = 25607 (DSR Signaling Firewall is administratively Disabled)** If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

Step #	Procedure	Description

10.
☐
	Server CLI: (Optional) View in-progress status from command line	Optional method to view upgrade progress from a command line:
		To view the detailed progress of the upgrade –
		Access the server command line (via ssh or Console), and:
		`$ tail -f  /var/TKLC/log/upgrade/upgrade.log`
		Once a server is upgraded, it reboots, and it takes a couple of minutes for the DSR application processes to start up.
		This command displays the current rev on the upgraded servers:
		`[admusr@NO1 ~]$ appRev`
		`Install Time: Wed Apr  4 05:03:13 2018`
		`Product Name: DSR`
		`Product Release: 8.3.0.0.0_83.5.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.5.0.0.0_88.46.0`
		`Base Distro ISO: TPD.install-7.5.0.0.0_88.46.0-OracleLinux6.9-x86_64.iso`
		`ISO name: DSR-8.3.0.0.0_83.5.0-x86_64.iso`
		`OS: OracleLinux 6.9`
		If the upgrade fails, **do not proceed**. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures.

11. ☐	**Server CLI**: If upgrade fails	If a server 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 /var/TKLC/log/platcfg/upgrade.log If the upgrade fails, **do not proceed**. It is recommended to consult with on the best course of action. Refer to Appendix J for failed server recovery procedures**.**
12. ☐	**Active NOAM VIP**: Verify post upgrade status	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the Application Version value for the servers has been updated to the target software release version. 3. Verify the Status Message indicates success. 4. Verify the Upgrade State of the upgraded servers is **Accept or Reject**.

Step #	Procedure	Description
13. ☐	Verify the servers were successfully upgraded	View Post-Upgrade Status of the server: The active SOAM server may have some or all the following expected alarm(s): **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10010 (Stateful database not yet synchronized with mate database)** **Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)** **Alarm ID = 31000 (Program impaired by S/W Fault)** **Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)** ***Note***: Do not accept upgrade at this time. This alarm is OK.

Appendix F. IDIH Upgrade at a Site

In IDIH release 7.1 and later, the mediation and application instance data is stored in the Oracle Database. This allows the Application and Mediation servers to be upgraded by performing a fresh installation. Upon completion of the upgrade, the mediation and application guests automatically restore the configuration data from the Oracle database.

Table 24 shows the elapsed time estimates for IDIH upgrade.

Table 24. IDIH Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 51	1:15-1:45	1:15-1:45	Procedure 51	None
Procedure 52	0:30-0:45	1:45-2:30	Procedure 52	None

Appendix F.1. Upgrade Oracle Guest

The Oracle Guest is upgraded first.

Procedure 51. Upgrade Oracle Guest

Step #	Procedure	Description
This procedure performs the IDIH Oracle Guest upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	IDIH CLI: Perform a system health check on the Oracle guest	1. Log into the Oracle guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Execute the analyze_server.sh script.
		`$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		Sample output:
		`[admusr@cat-ora ~]$ /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		`13:24:52: STARTING HEALTHCHECK PROCEDURE`
		`13:24:52: date: 03-17-15, hostname: cat-ora`
		`13:24:52: TPD VERSION: 7.0.0.0.0-86.14.0`
		`13:24:52: ----------`
		`13:24:52: Checking disk free space`
		`13:24:52: No disk space issues found`
		`:`
		`13:25:02: All tests passed!`
		`13:25:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 0`
		If the output indicates the following error, ignore the error and continue the upgrade. This error indicates the target release and the running release are the same.
		`00:47:29: Checking runlevel`
		`00:47:29: >>> Error: Runlevel value "3 4" is different from "N 4"`
		If the output indicates any other failure, do not proceed with the upgrade. It is recommended to contact for guidance.

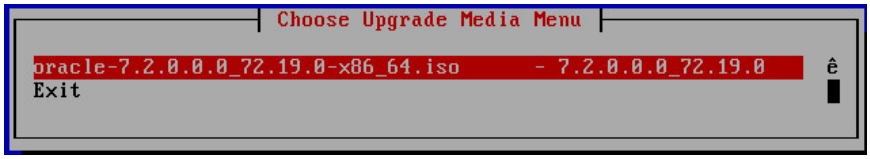
Step #	Procedure	Description

2.
☐
	IDIH CLI:
	Shut down the Mediation guest to prepare for the Oracle guest upgrade
		1. Log into the Mediation guest as admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Shut down the Mediation guest.
		`$ sudo init 0`
		The active SOAM server may have some or all of the following expected alarms:
		Alarm ID = 19800 Communication Agent Connection Down
		Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname
		The active NOAM server may have some or all of the following expected alarms:
		Alarm ID = 19800 Communication Agent Connection Down

3.
☐
	IDIH CLI:
	Shut down the Application guest to prepare for the Oracle guest upgrade
		1. Log into the Application guest as admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Shut down the Application guest.
		`$ sudo init 0`
		The active SOAM server may have some or all of the following expected alarms:
		Alarm ID = 19800 Communication Agent Connection Down
		Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname
		The active NOAM server may have some or all of the following expected alarms:
		Alarm ID = 19800 Communication Agent Connection Down

Step #	Procedure	Description

4.
☐
	IDIH Application Guest CLI:
	Increase Size of /var/TKLC
		1. It is seen that space available in /var/TKLC directory is less than the ISO size. So, there is need to increase the space of this directory.
		2. Log into the Application guest as admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		3. Check the space
		`df -kh /var/TKLC`
		4. Note down the current space. Available space should be more than 6 GB space for this. In case sufficient space is already there, skip next sub-steps.
		5. Increase the space
		`sudo lvresize -L +6G /dev/mapper/vgroot-plat_var_tklc`
		6. Resize the space
		`sudo resize2fs /dev/mapper/vgroot-plat_var_tklc`
		7. Check the space again
		`df -kh /var/TKLC`
		8. Available space should be more than 6 GB space for this.

5. ☐	Move Oracle ISO	Use a file transfer tool to copy the Oracle ISO to the Oracle guest as admusr. Example: `$ scp oracle-8.3.0.0.0_83.5.0-x86_64.iso admusr@<ora-guest-ip>:/var/TKLC/upgrade`
6. ☐	**IDIH CLI**: Start Oracle guest upgrade	The Oracle guest is upgraded using the Platform Configuration utility. 1. Launch the platform configuration utility. `$ sudo su - platcfg` 2. In the resulting menu, navigate to **Maintenance** > **Upgrade** > **Initiate Upgrade**. 3. At the ISO selection menu, select the target release Oracle ISO and press **Enter**. 
7. ☐	**IDIH CLI**: Monitor upgrade progress	The platform configuration menu exits and the guest reboots when the upgrade completes. To view the detailed progress of the upgrade, access the server command line (via SSH or Console), and enter: `$ tail -f /var/TKLC/log/upgrade/upgrade.log` Once the server has upgraded, it reboots. It takes a couple of minutes for the Oracle processes to start up.

Step #	Procedure	Description
8. ☐	**IDIH CLI**: Perform a system health check on the Oracle guest	Wait a few minute to allow the Oracle guest to stabilize after the reboot, and repeat step 1 to perform the post-upgrade system health check. ***Note***: The following warnings are expected due to the mediation and app servers being shut down. **Warning: mediation server is not reachable (or ping response exceeds 3 seconds)** **Warning: app server is not reachable (or ping response exceeds 3 seconds)**

Appendix F.2. Upgrade the Mediation and Application Guests

The Mediation and Application Guest upgrade is similar to the installation procedure.

Procedure 52. Upgrade the Mediation and Application Guests

Step #	Procedure	Description
This procedure performs the IDIH Mediation and Application server upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**CLOUD GUI**: Remove existing Application Server	Use the hypervisor-specific procedure to remove the current iDIH Application and iDIH Mediation guests.
2. ☐	**CLOUD GUI**: Deploy the latest application and mediation guest images	Use the hypervisor-specific procedure to deploy the latest Application and Mediation guests. Configure the iDIH mediation and application guests to reflect the guest profile in the installation document [1].
3. ☐	**IDIH CLI**: Configure the IDIH VM Networks	Configure the iDIH mediation and application guests according to Procedure 32 (Configure iDIH Virtual Machines) of installation document [1].
4. ☐	**IDIH CLI**: Run Post Installation scripts on iDIH VMs	Execute Post Installation iDIH mediation and application specific scripts on the respective iDIH guests according to Procedure 33 (Run Post Installation scripts on iDIH VMs) of installation document [1].
5.	**NOAM CLI**: Reset SOAP password	In case upgrading to release IDIH 8.2.1, reset the SOAP password to allow self-authentication of DSR with IDIH to send traces. Refer Appendix Y**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.**.

Appendix G. Alternate Server Upgrade Procedures

The following procedure provides alternative ways of upgrading various server types, using an array of differing methods. All of the procedures in this section are secondary to the upgrade methods provided in

Section 4 and Section 5. These procedures should be used only when directed by or by other procedures within this document.

Appendix G.1. Alternate Pre-Upgrade Backup

The following procedure is an alternative to the normal pre-upgrade backup provided in Procedure 17. It is recommended that this procedure be executed only under the direction of .

Procedure 53. Alternate Pre-Upgrade Backup

Step #	Procedure	Description
This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active SOAM CLI**: Log into the active SOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active SOAM: `ssh admusr@<SOAM_VIP>`
2. ☐	**Active SOAM CLI**: Start a screen session	Enter the command: `$ screen` The screen tool creates a no-hang-up shell session, so the command continues to execute if the user session is lost.

3.
☐
	Active SOAM CLI: Execute a backup of all servers managed from the SOAM to be upgraded	Execute the **backupAllHosts** utility on the active SOAM. This utility remotely accesses each specified server, and runs the backup command for that server.
		The **--site** parameter allows the user to backup all servers associated with a given SOAM site to be upgraded:
		WARNING: Failure to include the --site parameter with the backupAllHosts command results in overwriting the NOAM backup file created in Section 3.4.5. Backing out to the previous release is not possible if the file is overwritten.
		`$ /usr/TKLC/dpi/bin/backupAllHosts --site=<NEName>`
		where **<NEName>** is the Network Element Name (**NEName**) as seen using the following command:
		`$ iqt NetworkElement`
		This output displays when executing either of the options:
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.
		Do not proceed until the backup on each server is completed.
		Output similar to the following indicates successful completion:
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`

Step #	Procedure	Description

		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		Errors also report to the command line.
		Note: There is no progress indication for this command; only the final report when it completes.

4.
☐
	Active SOAM CLI: Exit the screen session	`# exit`
		`[screen is terminating]`
		Note: **screen -ls** is used to show active screen sessions on a server, and **screen -dr** is used to re-enter a disconnected screen session.

5.
☐
	ALTERNATIVE METHOD (Optional)
	Server CLI: If needed, the Alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script
		Alternative: A manual back up can be executed on each server individually, rather than using the script. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following indicates successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

6.
☐
	Active NOAM VIP: Verify backup files are present on each server.	1. Log into the active NOAM GUI using the VIP.
		2. Navigate to **Status & Manage > Files**.
		3. Click on each server tab, in turn.
		4. For each server, verify the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		5. Repeat sub-steps 1 through 4 for each site.

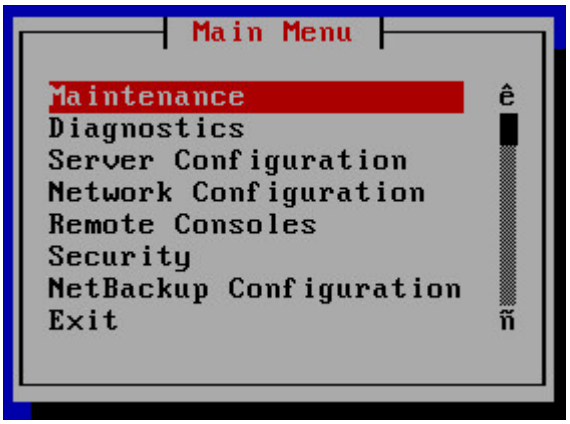
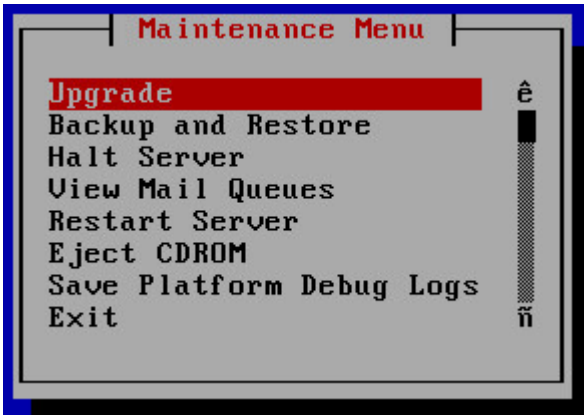
Appendix G.2. Server Upgrade Using platcfg

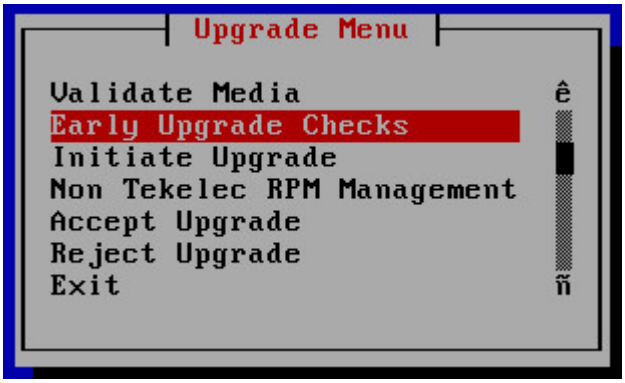
The following procedure enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of .

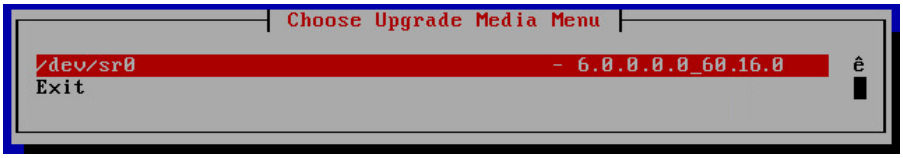
Procedure 54. Server Upgrade Using Platcfg

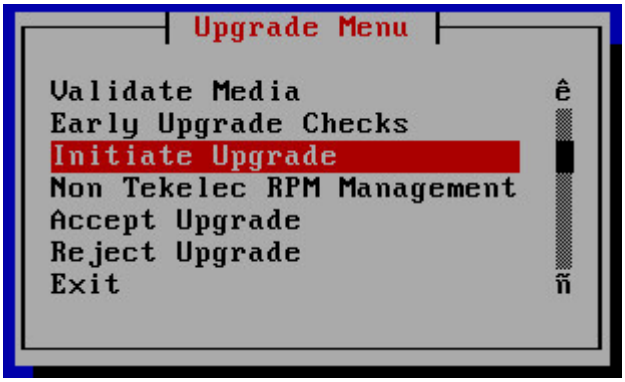
Step #	Procedure	Description
This procedure upgrades a server using the platcfg utility. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Server CLI: Log into the server console to be upgraded	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server to be upgraded:
		`ssh admusr@<server IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

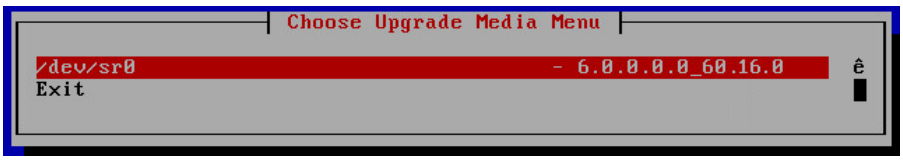
2. ☐	**Server CLI**: Enter the platcfg menu	Switch to the platcfg user to start the configuration menu. `$ sudo su - platcfg` From the Main Menu, select **Maintenance** 
3. ☐	**Server CLI**: Select upgrade	From the Maintenance Menu, select **Upgrade**. 

Step #	Procedure	Description
4. ☐	**Server CLI**: Select early upgrade checks	From the Upgrade Menu, select **Early Upgrade Checks**. 

5.
☐
	Server CLI:
	Select the upgrade media
		6. From the Choose Upgrade Media Menu, select the desired target media. This begins the early upgrade checks in the console window.
		 
		
		Informational messages display as the checks progress. At the end of a successful test, a message similar to this displays:
		`Running earlyUpgradeChecks () for Upgrade::EarlyPolicy::TPDEarlyChecks upgrade policy...`
		`Verified server is not pending accept of previous upgrade`
		`Hardware architectures match`
		`Install products match.`
		`Verified server is alarm free!`
		`Early Upgrade Checks Have Passed!`
		7. Verify early upgrade checks pass. In case of errors, it is recommended to contact .
		8. Press **q** to exit the screen session and return to the platcfg menu.
		9. From the Choose Upgrade Media Menu, select **Exit**.

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

Step #	Procedure	Description

7.
☐
	Server CLI:
	Select the upgrade media
		The screen displays a message that it is searching for upgrade media. Once the upgrade media is found, an Upgrade Media selection menu displayed similar to the example shown.
		From the Choose Upgrade Media Menu, select the desired target media. This begins the server upgrade.
		 
		
		Many informational messages display on the terminal screen as the upgrade proceeds.
		After upgrade is complete, the server reboots.
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

8.
☐
	Server CLI:
	Log into the server to be upgraded
		Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server to be upgraded:
		`ssh admusr@<server IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

9.
☐
	Server CLI:
	Check for upgrade errors
		1. Examine the upgrade logs in the **/var/TKLC/log/upgrade** directory and verify no errors were reported.
		`grep -i error /var/TKLC/log/upgrade/upgrade.log`
		2. Examine the output of the command to determine if any errors were reported.
		3. If the upgrade fails, collect the following files:
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		4. It is recommended to contact by referring to Appendix V of this document and provide these files.

10.
☐
	Server CLI:
	Verify the upgrade
		1. Check the upgrade log for the upgrade complete message
		`grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		2. Verify the **UPGRADE IS COMPLETE** message displays. If not, it is recommended to contact .
		`[admusr@NO2 ~]$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/ upgrade/upgrade.log`
		`1407786220:: UPGRADE IS COMPLETE`

Appendix G.3. Manual DA-MP (N+0) Upgrade Procedure

The following procedure is used to manually upgrade a multi-active DA-MP Server Group. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 55 must be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 55 must be executed four distinct times.

Procedure 55. Manual DA-MP (N+0) Upgrade Procedure

Step #	Procedure	Description
This procedure upgrades a multi-active DA-MP servers using the manual upgrade method. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Identify all the DA-MPs to be upgraded together	From the data captured in Table 5, identify the **DSR (multi-active cluster)** server group to be upgraded.
2. ☐	Upgrade DA-MP servers as identified in step 1	Upgrade up to (½) one half (no more than 50%) of the DA-MP servers in parallel using the Upgrade Multiple Servers procedure. ***Note***: When using the manual server upgrade method, it is recommended that the DA-MP leader be upgraded in the last group of servers to minimize DA-MP leader role changes. 1. Execute Appendix E Upgrade Multiple Servers – Upgrade Administration. 2. After successfully completing the procedure in Appendix E, return to this point and continue with the next step.
3. ☐	Repeat for all servers identified in step 1 of this procedure	Repeat step 2 of this procedure for the remaining DA-MP servers.

Appendix G.4. ASG SBR Upgrade Procedure

The following procedure is used to upgrade the SBR server group using Auto Server Group upgrade. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Procedure 56. ASG SBR Upgrade

Step #	Procedure	Description
This procedure upgrades the SBR Server Group using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Identify the SBR server group(s) to upgrade	From the data captured in Table 5, identify the SBR server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously.
2. ☐	Upgrade SBR server group(s) identified in step 1 of this procedure using the upgrade multiple servers procedure	***Note***: The spare SBRs of this server group are located at different sites. 1. Use the Automated Server Group Upgrade option. 2. Select the Serial upgrade mode. 3. Execute Appendix E Upgrade Multiple Servers – Upgrade Administration.
3. ☐	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2 (and an optional 2nd spare in Site 3)	Repeat step 2 for all remaining binding and session server groups to be upgraded.

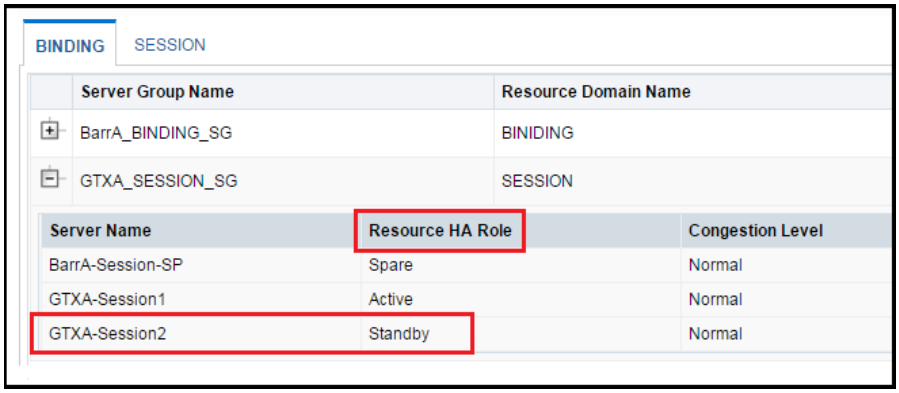
Appendix G.5. Manual SBR Upgrade Procedure

The following procedure is used to upgrade the SBR server group manually. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Note: Before upgrading the active SBR, it is imperative that the database audit of the spare and standby servers complete successfully. Failure to comply could result in a loss of session/binding data.

Procedure 57. Manual SBR Upgrade Procedure

Step #	Procedure	Description
This procedure upgrades an SBR server group using the manual upgrade option. ***Note***: This procedure upgrades all the servers in the server group; however, if it is recommended to upgrade one by one, such as spare, standby, and active in different upgrade iterations. Upgrade those servers manually and then return to this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

Step #	Procedure	Description
1. ☐	**Active NOAM VIP**: Identify the active, standby, and spare SBR server group(s) to upgrade	1. From the data captured in Table 5, identify the server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously. 2. Log into the NOAM GUI using the VIP. 3. Navigate to **SBR > Maintenance > SBR Status.** Open each server group chosen in sub-step 1. Note which server is active, standby, and spare (as designated by the Resource HA Role) for each server group chosen for upgrade. The following figure provides an example: • GTXA-Session1 – Active • GTXA-Session2 – Standby • BarrA-Session-SP – Spare  BINDING SESSION Server Group Name: BarrA_BINDING_SG — Resource Domain Name: BINIDING Server Group Name: GTXA_SESSION_SG — Resource Domain Name: SESSION Server Name / Resource HA Role / Congestion Level BarrA-Session-SP / Spare / Normal GTXA-Session1 / Active / Normal GTXA-Session2 / Standby / Normal ***Note***: SBR servers have two High Availability policies: one for controlling replication of session or binding data, and one for receipt of replicated configuration data from the NOAM and SOAM GUIs. During this upgrade procedure, ONLY the High Availability policy for replication of session or binding data is important. This means that the SBR Status screen MUST be used to determine the High Availability status (active, standby, or spare) of SBR servers. The HA Status screen and the OAM Max HA Role column on the Upgrade screen must NOT be used because they only show the status of the configuration replication policy. Because the two High Availability policies run independently, it is possible that a given server might be standby or spare for the session and binding replication policy, but active for the configuration replication policy. When this happens, it is necessary to ignore warnings on the Upgrade screen about selecting what it views as the active server (for the configuration replication policy).

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Upgrade spare SBR server identified in step 1 of this procedure **(If need to be upgraded in this upgrade iteration)**	***Note***: The spare SBRs of this server group are located at different sites. 1. Execute Appendix C Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix C, return to this point to monitor server status. 3. Navigate to **SBR > Maintenance > SBR Status**. Open the tab of the server group being upgraded. ***Note***: After executing Appendix C, the spare SBR temporarily disappears from the SBR Status screen. When the server comes back online, it reappears on the screen with a status of **Out of Service**. 4. Monitor the Resource HA Role status of the spare server. Wait for the status to transition from **Out of Service** to **Spare**. 5. If the system is equipped with a second spare SBR server, repeat sub-steps 1 thru 3 for the other spare. **Caution**: Do not proceed to step 3 until the Resource HA Role of the spare SBR server returns to **Spare**.
3. ☐	Upgrade standby SBR server identified in step 1 of this procedure **(If need to be upgraded in this upgrade iteration)**	1. Execute Appendix C Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.
!!WARNING!!		Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact.
4. ☐	**Active NOAM VIP**: Verify standby SBR server status **(If need to be upgraded in this upgrade iteration)**	1. Navigate to **SBR > Maintenance > SBR Status**. 2. Open the tab of the server group being upgraded. ***Note***: After executing Appendix C, the standby SBR temporarily disappears from the SBR Status screen, and the spare server assumes the standby role. When the upgraded server comes back online, it reappears on the screen with a status of **Out of Service**. 3. Monitor the Resource HA Role status of the upgraded server. Wait for the status to transition from **Out of Service** to **Standby**. **Caution**: Do not proceed to step 5 until the Resource HA Role of the upgraded server transitions to **Standby**.

Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Verify bulk download from the active SBR to the standby and spare SBRs completes **(If need to be upgraded in this upgrade iteration)**	1. Navigate to **Alarm & Event > View History**. 2. Export the Event log using the following filter: **Server Group**: Choose the SBR group that is in upgrade **Display Filter**: Event ID = 31127 – DB Replication Audit Complete **Collection Interval**: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time. 3. Wait for all instances of Event 31127: • 1 for the Standby binding SBR • 1 for the Standby session SBR • 1 for the Spare binding SBR • 1 for the Spare session SBR • 1 for the 3rd site Spare binding SBR (if equipped) • 1 for the 3rd site Spare session SBR (if equipped) ***Note***: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.

6.
☐
	Active SBR (CLI):
	Verify the replication status for DB Replication and pSbrBindingPolicy (Binding SBR)
	Or pSbrSessionPolicy (Session SBR)
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SBR of the first non-upgraded site:
		`ssh admusr@<SBR_XMI_IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Execute command
		`irepstat -w`
		Verify replication is showing as **Active** for ActStb [DbReplication] policy, pSbrSessionPolicy (for Session SBR), and pSbrBindingPolicy (for Binding SBR).
		Do not proceed if replication is not **Active** for all of the resource.
		Example:
		`[admusr@StThomas-sSBR-A ~]$ irepstat -w`
		`StThomas-sSBR-A  C2706.068  StThomas-sSBR-A  11:19:19  [R]`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`BC From D0 StThomas-SO2 Active 0 0.10 ^0.04%cpu 35.5/s`
		`CC To P0 StThomas-sSBR-B Active 0 0.10 1%S 0.08%cpu 48.3/s`
		`CC To P1 StThomas-sSBR-Sp Active 0 0.11 1%S 0.08%cpu 43.1/s`
		`-- Policy 20 pSbrSessionPolicy [pSbrSBaseRepl] ----------`
		`CC To P0 StThomas-sSBR-B Active 0 0.10 1%S 0.07%cpu 62.5/s`
		`CC To P1 StThomas-sSBR-Sp Active 0 0.10 1%S 0.08%cpu 56.2/s`

Step #	Procedure	Description
7. ☐	Upgrade active SBR server as identified in step 1 of this procedure **(If need to be upgraded in this upgrade iteration)**	1. Execute Appendix C Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.
8. ☐	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2	Repeat steps 1 through 6 for all remaining binding and session server groups to be upgraded.

Appendix H. Expired Password Workaround Procedure

This appendix provides the procedures to handle password expiration during upgrade. Procedure 58 is a temporary workaround to allow an expired password to be used on a non-upgrade site. This procedure is provided as a workaround when a password expires after the NOAM has been upgraded and before all sites have been upgraded.

The workaround must be removed using Procedure 59 after the site is upgraded. Failure to remove the workaround inhibits password aging on the server.

Appendix H.1. Inhibit Password Aging

The following procedure enacts a workaround that inhibits password aging on the SOAM. This procedure should be used only when the following conditions apply:

- An upgrade is in progress
- The NOAMs have been upgraded, but one or more sites have not been upgraded
- A login password has expired on a non-upgraded site

Once the workaround is enacted, no passwords expire at that site. Remove the workaround once the site is upgraded.

Procedure 58. Expired Password Workaround Procedure

Step #	Procedure	Description
This procedure disables password aging on a server, allowing “expired” credentials to be used for login. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active SOAM CLI: SSH to active SOAM server. Disable password aging	1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Create a text file with the following content (exactly as formatted):
		`[production]`
		`aw.policy.pwchange.isExpired =`
		`aw.policy.db.checkPw =`
		`[development : production]`
		`[test : development]`
		3. Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		4. Change the file permissions:
		`sudo chmod 644 pw.ini`
		5. Execute the following command:
		`clearCache`
		Note: For each server on which this workaround is enacted, the old **expired** password must be used for login. The new password used on the NOAM does not work on these servers.

2. ☐	Repeat for standby SOAM	Repeat step 1 for the standby SOAM
3. ☐	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.

Appendix H.2. Enable Password Aging

The following procedure removes the password expiration workaround that is enabled by Procedure 58.

Procedure 59. Expired Password Workaround Removal Procedure

Step #	Procedure	Description
This procedure removes the password aging workaround and re-enables password aging on a server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active SOAM CLI: SSH to active SOAM server. Re-enable password aging.	1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Delete the pw.ini file:
		`$ sudo rm /var/TKLC/appworks/ini/pw.ini`
		3. Execute this command:
		`$ sudo clearCache`
		4. Repeat sub-steps 1 through 3 for the standby SOAM

2. ☐	Repeat for all non-upgraded sites	Repeat this procedure for all non-upgraded sites.

Appendix H.3. Password Reset

The following procedure resets the GUI Admin (guiadmin) password on the NOAM. In a backout scenario where the password expired during the upgrade, it is possible for the customer to get locked out due to global provisioning being disabled. When this happens, this procedure can be used to reset the password to gain access to the GUI.

Procedure 60. Expired Password Reset Procedure

Step #	Procedure	Description
This procedure resets the guiadmin password on the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Active NOAM CLI: SSH to active NOAM server. Reset the password	1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active NOAM:
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Execute the reset command:
		`$ sudo /usr/TKLC/appworks/sbin/resetPassword guiadmin`
		3. At the **Enter new Password for guiadmin** prompt, enter a new password.
		4. Attempt to log into the NOAM GUI using the new password. If the login is not successful, it is recommended to contact for guidance.

Appendix I. Network IDIH Compatibility Procedures

The following procedure is used to provide IDIH compatibility when upgrading to Release 8.x. Procedure 61 is performed on a Release 8.x IDIH to make the trace data viewable on prior release IDIH systems, as described in Section 1.7.3. This procedure must be performed on every IDIH 8.x system from which trace data is expected.

When all IDIH systems have been upgraded to Release 8.x, Procedure 62 must be executed on every IDIH on which Procedure 61 was previously performed.

Procedure 61. Enable IDIH 8.x Compatibility

Step #	Procedure	Description
This procedure upgrades a server using the platcfg utility. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Appserver CLI: Log into the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the appserver:
		`ssh admusr@<server_ip>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Appserver CLI**: Change user	Change to the system user tekelec: `sudo su - tekelec`
3. ☐	**Appserver CLI**: Execute command	Execute the following command to enable backward compatibility `apps/ndih7-compat.sh enable`
4. ☐	Repeat as needed	Repeat this procedure on each IDIH 8.x appserver as needed.

Procedure 62. Disable IDIH 8.x Compatibility

Step #	Procedure	Description
This procedure upgrades a server using the platcfg utility. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

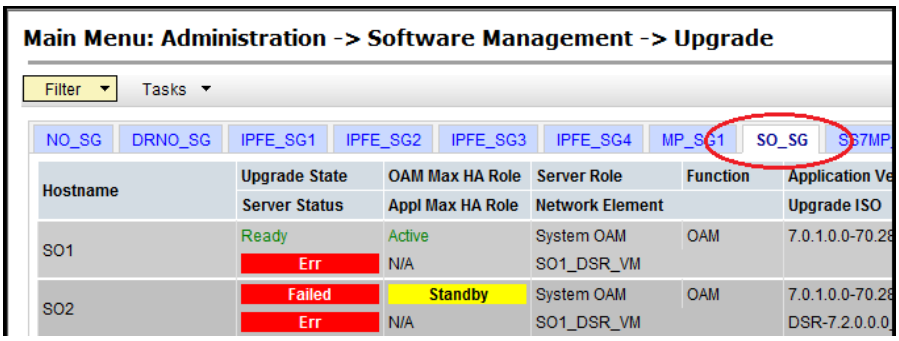
1.
☐
	Appserver CLI: Log into the appserver	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the appserver:
		`ssh admusr@<server_ip>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

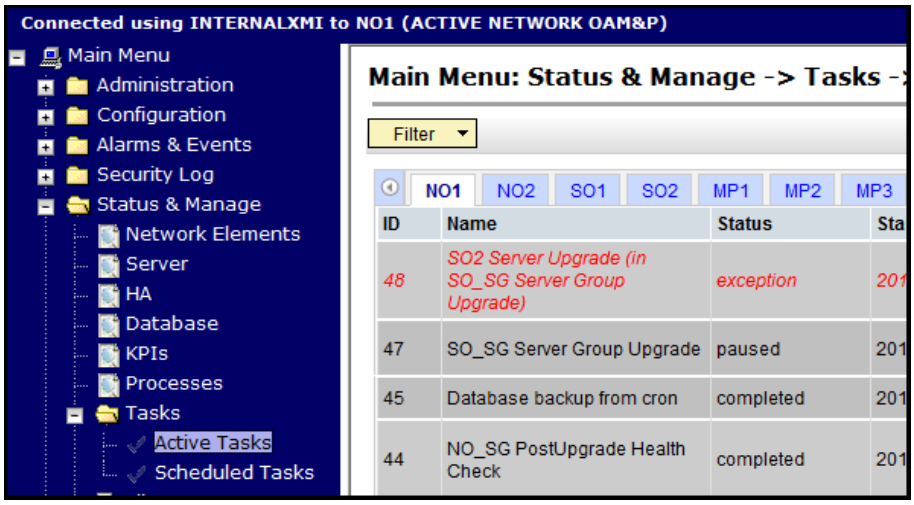
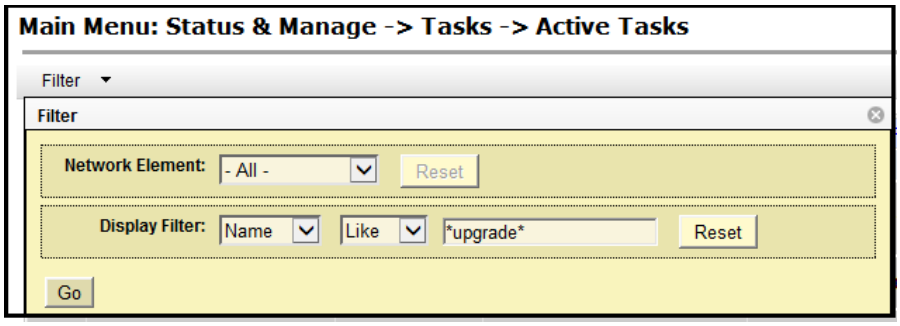
Step #	Procedure	Description
2. ☐	**Appserver CLI**: Change user	Change to the system user tekelec: `sudo su - tekelec`
3. ☐	**Appserver CLI**: Execute command	Execute this command to enable backward compatibility: `apps/ndih7-compat.sh disable`
4. ☐	Repeat as needed	Repeat this procedure on each IDIH 8.x appserver as needed.

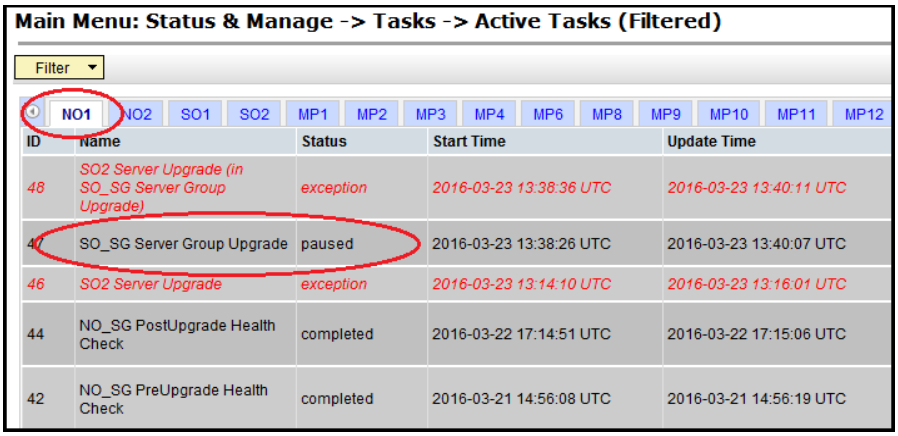
Appendix J. Recover From a Failed Upgrade

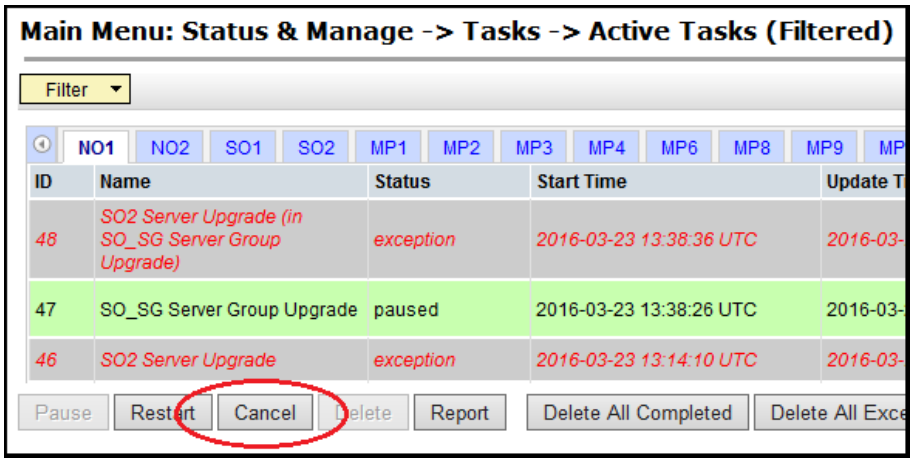
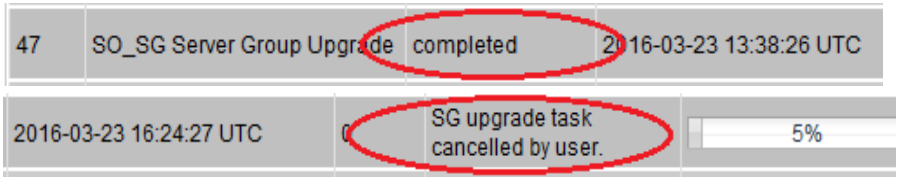
The following procedure provides the steps required to recover a server after a failed upgrade. Due to the complexity of the DSR system and the nature of troubleshooting, it is recommended to contact for guidance while executing this procedure.

Procedure 63. Recover from a Failed Upgrade

Step #	Procedure	Description
This procedure provides the basic steps for returning a server to a normal state after an upgrade failure. ***Note***: The server is returned to the source release by this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Select affected server group containing the failed server	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade**. 3. Select the server group tab for the server to be recovered.  • If the failed server was upgraded using the Upgrade Server option, then skip to step 7 of this procedure. • If the failed server was upgraded using the Auto Upgrade option, then continue with step 2 of this procedure.

Step #	Procedure	Description
2. ☐	**Active NOAM VIP**: Navigate to the Active Tasks screen to view active tasks	Navigate to **Status & Manage > Tasks > Active Tasks**. 
3. ☐	**Active NOAM VIP**: Use the filter to locate the server group upgrade task	1. From the **Filter** option, enter the following filter values: Network Element: **All** Display Filter: **Name Like *upgrade*** 2. Click **Go**. 

Step #	Procedure	Description
4. ☐	**Active NOAM VIP**: Identify the upgrade task	In the search results list, locate the **Server Group Upgrade** task. 1. If not already selected, select the tab displaying the hostname of the active NOAM server. 2. Locate the task for the **Server Group Upgrade**. It shows a status of **paused**.  ***Note***: Consider the case of an upgrade cycle where it is seen that the upgrade of one or more servers in the server group have status as exception (i.e., failed), while the other servers in that server group have upgraded successfully. However, the server group upgrade task still shows as running. In this case, please cancel the running (upgrade) task for that server group before reattempting ASU for the same. **Caution**: Before clicking **Cancel** for the server group upgrade task, ensure the upgrade status of the individual servers in that particular server group should have status as completed or exception (that is, failed for some reason). Make sure you are not cancelling a task with some servers still in running state.

Step #	Procedure	Description
5. ☐	**Active NOAM VIP**: Cancel the Server Group Upgrade task	3. Click the Server Group Upgrade task to select it. 4. Click **Cancel** to cancel the task. 5. Click **OK** on the confirmation screen to confirm the cancellation. 
6. ☐	**Active NOAM VIP**: Verify the Server Group Upgrade task is cancelled	On the Active Tasks screen, verify the task that was cancelled in step 5 shows a status of **completed**. 

7.
☐
	Failed Server CLI: Inspect upgrade log	Log into the failed server to inspect the upgrade log for the cause of the failure.
		1. Use an SSH client to connect to the failed server:
		`ssh <XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. View or edit the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for clues to the cause of the upgrade failure.
		3. If the upgrade log contains a message similar to the following, inspect the early upgrade log at **/var/TKLC/log/upgrade/earlyChecks.log** for additional clues.
		`1440613685::Early Checks failed for the next upgrade`
		`1440613691::Look at earlyChecks.log for more info`

Step #	Procedure	Description
		• Although outside of the scope of this document, the user is expected to use standard troubleshooting techniques to clear the alarm condition from the failed server. • If troubleshooting assistance is needed, it is recommended to contact . • DO NOT PROCEED TO STEP 8 OF THIS PROCEDURE UNTIL THE ALARM CONDITION HAS BEEN CLEARED!

8.
☐
	Failed Server CLI: Verify platform alarms are cleared from the failed server	Use the alarmMgr utility to verify all platform alarms have been cleared from the system.
		`$ sudo alarmMgr --alarmstatus`
		Example output:
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		`SEQ: 2 UPTIME: 827913 BIRTH: 1458738821 TYPE: SET ALARM: TKSPLATMI10|tpdNTPDaemonNotSynchronizedWarning|1.3.6.1.4.1.323.5.3.18.3.1.3.10|32509|Communications|Communications Subsystem Failure`
		user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		`[admusr@SO2 ~]$`

9. ☐	**Active NOAM VIP**: Re-execute the server upgrade	Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option. ***Note***: Once a server has failed while using the Automated Server Group Upgrade option, the Auto Upgrade option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the Upgrade Server option.

Appendix K. Critical and Major Alarms Analysis

The following procedure identifies critical and major alarms that should be resolved before proceeding with an upgrade and backout.

Note: During any time of upgrade if the **31149- DB Late Write Nonactive** alarm displays, ignore it. This alarm does not have any effect on functionality.

Procedure 64. Verify Critical and Major Alarms in the System Before the Upgrade

Step #	Procedure	Description
This procedure identifies the current alarms in the system before an upgrade can start. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**Active NOAM VIP**: Log/View all current alarms at the NOAM	1. Navigate to **Alarms & Events > View Active**. 2. Click **Report** to generate an Alarms report. 3. Save the report and/or print the report.
2. ☐	Analyze the active alarms data	Reference Table 25 and Table 26 for the alarms. If any alarms listed in the Table 25 and Table 26 display in the system, resolve the alarms before starting the upgrade. Refer to Reference [7] DSR Alarms and KPIs Reference for specific alarm in-depth details. Two categories from the alarm list. **High impact alarms** It's almost certain the presence of this alarm ID in the active alarm list should prevent upgrade from continuing. Alarms of this category should be resolved before upgrading. **Medium impact alarms** It's likely/possible the presence of this alarm ID should prevent upgrade from continuing; concurrence needed. Alarms of this category may/may not be resolved before upgrading. Some ideas of inclusion of alarms in the categories include. • Any alarm indicating an actual hardware error, or an impending/potential hardware error, is automatically mentioned in high impact alarm list. Included in this category are all Platform Group alarms (PLAT) of severity Minor, Major, and Critical. • If an alarm ID indicates some sort of (pending) resource exhaustion issue or other threshold crossed condition, it is almost always mentioned in Medium impact alarms. Resource exhaustion states have to be fixed before upgrading.

Table 25. High Impact Alarms

Alarm ID	Name
5010	Unknown Linux iptables command error
5011	System or platform error prohibiting operation
10000	Incompatible database version
10134	Server Upgrade Failed
10200	Remote database initialization in progress
19217	Node isolated - all links down
19805	Communication Agent Failed to Align Connection
19855	Communication Agent Resource Has Multiple Actives
19901	CFG-DB Validation Error
19902	CFG-DB Update Failure
19903	CFG-DB post-update Error
19904	CFG-DB post-update Failure
22223	MpMemCongested
22950	Connection Status Inconsistency Exists
22961	Insufficient Memory for Feature Set
22733	SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration
22734	Policy and Charging Unexpected Stack Event Version
25500	No DA-MP Leader Detected
25510	Multiple DA-MP Leader Detected
31101	Database replication to slave failure
31116	Excessive shared memory
31117	Low disk free
31125	Database durability degraded
31128	ADIC Found Error
31133	DB Replication Switchover Exceeds Threshold
31215	Process resources exceeded
31288	HA Site Configuration Error
32100	Breaker Panel Feed Unavailable
32101	Breaker Panel Breaker Failure
32102	Breaker Panel Monitoring Failure
32103	Power Feed Unavailable
32104	Power Supply 1 Failure
32105	Power Supply 2 Failure
32106	Power Supply 3 Failure

Alarm ID	Name
32107	Raid Feed Unavailable
32108	Raid Power 1 Failure
32109	Raid Power 2 Failure
32110	Raid Power 3 Failure
32111	Device Failure
32112	Device Interface Failure
32113	Uncorrectable ECC memory error
32114	SNMP get failure
32115	TPD NTP Daemon Not Synchronized Failure
32116	TPD Server's Time Has Gone Backwards
32117	TPD NTP Offset Check Failure
32300	Server fan failure
32301	Server internal disk error
32302	Server RAID disk error
32303	Server Platform error
32304	Server file system error
32305	Server Platform process error
32306	Server RAM shortage error
32307	Server swap space shortage failure
32308	Server provisioning network error
32309	Eagle Network A Error
32310	Eagle Network B Error
32311	Sync Network Error
32312	Server disk space shortage error
32313	Server default route network error
32314	Server temperature error
32315	Server mainboard voltage error
32316	Server power feed error
32317	Server disk health test error
32318	Server disk unavailable error
32319	Device error
32320	Device interface error
32321	Correctable ECC memory error
32322	Power Supply A error
32323	Power Supply B error

Alarm ID	Name
32324	Breaker panel feed error
32325	Breaker panel breaker error
32326	Breaker panel monitoring error
32327	Server HA Keep alive error
32328	DRBD is unavailable
32329	DRBD is not replicating
32330	DRBD peer problem
32331	HP disk problem
32332	HP Smart Array controller problem
32333	HP hpacucliStatus utility problem
32334	Multipath device access link problem
32335	Switch link down error
32336	Half Open Socket Limit
32337	Flash Program Failure
32338	Serial Mezzanine Unseated
32339	TPD Max Number Of Running Processes Error
32340	TPD NTP Daemon Not Synchronized Error
32341	TPD NTP Daemon Not Synchronized Error
32342	NTP Offset Check Error
32343	TPD RAID disk
32344	TPD RAID controller problem
32345	Server Upgrade snapshot(s) invalid
32346	OEM hardware management service reports an error
32347	The hwmgmtcliStatus daemon needs intervention
32348	FIPS subsystem problem
32349	File Tampering
32350	Security Process Terminated
32500	Server disk space shortage warning
32501	Server application process error
32502	Server hardware configuration error
32503	Server RAM shortage warning
32504	Software Configuration Error
32505	Server swap space shortage warning
32506	Server default router not defined
32507	Server temperature warning

Alarm ID	Name
32508	Server core file detected
32509	Server NTP Daemon not synchronized
32510	CMOS battery voltage low
32511	Server disk self-test warning
32512	Device warning
32513	Device interface warning
32514	Server reboot watchdog initiated
32515	Server HA failover inhibited
32516	Server HA Active to Standby transition
32517	Server HA Standby to Active transition
32518	Platform Health Check failure
32519	NTP Offset Check failure
32520	NTP Stratum Check failure
32521	SAS Presence Sensor Missing
32522	SAS Drive Missing
32523	DRBD failover busy
32524	HP disk resync
32525	Telco Fan Warning
32526	Telco Temperature Warning
32527	Telco Power Supply Warning
32528	Invalid BIOS value
32529	Server Kernel Dump File Detected
32530	TPD Upgrade Failed
32531	Half Open Socket Warning Limit
32532	Server Upgrade Pending Accept/Reject
32533	TPD Max Number Of Running Processes Warning
32534	TPD NTP Source Is Bad Warning
32535	TPD RAID disk resync
32536	TPD Server Upgrade snapshot(s) warning
32537	FIPS subsystem warning event
32538	Platform Data Collection Error
32539	Server Patch Pending Accept/Reject
32540	CPU Power limit mismatch

Table 26. Medium Impact Alarms

Alarm ID	Name
5002	IPFE Address configuration error
5003	IPFE state sync run error
5004	IPFE IP tables configuration error
5006	Error reading from Ethernet device
5012	Signaling interface heartbeat timeout
5013	Throttling traffic
5100	Traffic overload
5101	CPU Overload
5102	Disk Becoming Full
5103	Memory Overload
10003	Database backup failed
10006	Database restoration failed
10020	Backup failure
10117	Health Check Failed
10118	Health Check Not Run
10121	Server Group Upgrade Cancelled - Validation Failed
10123	Server Group Upgrade Failed
10131	Server Upgrade Cancelled (Validation Failed)
10133	Server Upgrade Failed
10141	Site Upgrade Cancelled (Validation Failed)
10143	Site Upgrade Failed
19200	RSP/Destination unavailable
19202	Linkset unavailable
19204	Preferred route unavailable
19246	Local SCCP subsystem prohibited
19251	Ingress message rate
19252	PDU buffer pool utilization
19253	SCCP stack event queue utilization
19254	M3RL stack event queue utilization
19255	M3RL network management event queue utilization
19256	M3UA stack event queue utilization
19258	SCTP Aggregate Egress queue utilization
19251	Ingress message rate
19252	PDU buffer pool utilization

Alarm ID	Name
19253	SCCP stack event queue utilization
19254	M3RL stack event queue utilization
19255	M3RL network management event queue utilization
19256	M3UA stack event queue utilization
19258	SCTP Aggregate Egress queue utilization
19272	TCAP active dialogue utilization
19273	TCAP active operation utilization
19274	TCAP stack event queue utilization
19276	SCCP Egress Message Rate
19408	Single Transport Egress-Queue Utilization
19800	Communication Agent Connection Down
19803	Communication Agent stack event queue utilization
19806	Communication Agent CommMessage mempool utilization
19807	Communication Agent User Data FIFO Queue Utilization
19808	Communication Agent Connection FIFO Queue utilization
19818	Communication Agent DataEvent Mempool utilization
19820	Communication Agent Routed Service Unavailable
19824	Communication Agent Pending Transaction Utilization
19825	Communication Agent Transaction Failure Rate
19827	SMS stack event queue utilization
19846	Communication Agent Resource Degraded
19847	Communication Agent Resource Unavailable
19848	Communication Agent Resource Error
19860	Communication Agent Configuration Daemon Table Monitoring Failure
19861	Communication Agent Configuration Daemon Script Failure
19862	Communication Agent Ingress Stack Event Rate
19900	Process CPU Utilization
19905	Measurement Initialization Failure
19910	Message Discarded at Test Connection
8000-001	MpEvFsmException_SocketFailure
8000-002	MpEvFsmException_BindFailure
8000-003	MpEvFsmException_OptionFailure
8000-101	MpEvFsmException_ListenFailure
8002-003	MpEvRxException_CpuCongested
8002-004	MpEvRxException_SigEvPoolCongested

Alarm ID	Name
8002-006	MpEvRxException_DstMpCongested
8002-007	MpEvRxException_DrlReqQueueCongested
8002-008	MpEvRxException_DrlAnsQueueCongested
8002-009	MpEvRxException_ComAgentCongested
8002-203	MpEvRxException_RadiusMsgPoolCongested
8006-101	EvFsmException_SocketFailure
8011	EcRate
8013	MpNgnPsStateMismatch
8200	MpRadiusMsgPoolCongested
8201	RclRxTaskQueueCongested
8202	RclItrPoolCongested
8203	RclTxTaskQueueCongested
8204	RclEtrPoolCongested
22016	Peer Node Alarm Aggregation Threshold
22017	Route List Alarm Aggregation Threshold
22056	Connection Admin State Inconsistency Exists
22200	MpCpuCongested
22201	MpRxAllRate
22202	MpDiamMsgPoolCongested
22203	PTR Buffer Pool Utilization
22204	Request Message Queue Utilization
22205	Answer Message Queue Utilization
22206	Reroute Queue Utilization
22207	DclTxTaskQueueCongested
22208	DclTxConnQueueCongested
22214	Message Copy Queue Utilization
22221	Routing MPS Rate
22222	Long Timeout PTR Buffer Pool Utilization
22349	IPFE Conneetion Alarm Aggregation Threshold
22350	Fixed Connection Alarm Aggregation Threshold
22407	Routing attempt failed duto internal database inconsistency failure
22500	DSR Application Unavailable
22501	DSR Application Degraded
22502	DSR Application Request Message Queue Utilization
22503	DSR Application Answer Message Queue Utilization

Alarm ID	Name
22504	DSR Application Ingress Message Rate
22607	Routing attempt failed due to DRL queue exhaustion
22608	Database query could not be sent due to DB congestion
22609	Database connection exhausted
22631	FABR DP Response Task Message Queue Utilization
22632	COM Agent Registration Failure
22703	Diameter Message Routing Failure Due to Full DRL Queue
22710	SBR Sessions Threshold Exceeded
22711	SBR Database Error
22712	SBR Communication Error
22717	SBR Alternate Key Creation Failure Rate
22720	Policy SBR To PCA Response Queue Utilization Threshold Exceeded
22721	Policy and Charging Server In Congestion
22722	Policy Binding Sub-resource Unavailable
22723	Policy and Charging Session Sub-resource Unavailable
22724	SBR Memory Utilization Threshold Exceeded
22725	SBR Server In Congestion
22726	SBR Queue Utilization Threshold Exceeded
22727	SBR Initialization Failure
22728	SBR Bindings Threshold Exceeded
22729	PCRF Not Configured
22730	Policy and Charging Configuration Error
22731	Policy and Charging Database Inconsistency
22732	SBR Process CPU Utilization Threshold Exceeded
22737	Configuration Database Not Synced
22740	SBR Reconfiguration Plan Completion Failure
31100	Database replication fault
31102	Database replication from master failure
31103	DB Replication update fault
31104	DB Replication latency over threshold
31106	Database merge to parent failure
31107	Database merge from child failure
31108	Database merge latency over threshold
31113	DB replication manually disabled
31114	DB replication over SOAP has failed

Alarm ID	Name
31118	Database disk store fault
31121	Low disk free early warning
31122	Excessive shared memory early warning
31124	ADIC error
31126	Audit blocked
31130	Network health warning
31131	DB Ousted Throttle Behind
31134	DB Site Replication To Slave Failure
31135	DB Site Replication to Master Failure
31137	DB Site Replication Latency Over Threshold
31146	DB mastership fault
31147	DB upsynclog overrun
31200	Process management fault
31201	Process not running
31202	Unkillable zombie process
31209	Hostname lookup failed
31217	Network Health Warning
31220	HA configuration monitor fault
31113	DB replication manually disabled
31114	DB replication over SOAP has failed
31118	Database disk store fault
31121	Low disk free early warning
31122	Excessive shared memory early warning
31124	ADIC error
31126	Audit blocked
31130	Network health warning
31131	DB Ousted Throttle Behind
31134	DB Site Replication To Slave Failure
31135	DB Site Replication to Master Failure
31137	DB Site Replication Latency Over Threshold
31146	DB mastership fault
31147	DB upsynclog overrun
31200	Process management fault
31201	Process not running
31202	Unkillable zombie process

Alarm ID	Name
31209	Hostname lookup failed
31217	Network Health Warning
31220	HA configuration monitor fault
31221	HA alarm monitor fault
31222	HA not configured
31233	HA Heartbeat transmit failure
31224	HA configuration error
31225	HA service start failure
31226	HA availability status degraded
31228	HA standby offline
31230	Recent alarm processing fault
31231	Platform alarm agent fault
31233	HA Path Down
31234	Untrusted Time Upon Initialization
31234	Untrusted time After Initialization
31236	HA Link Down
31282	HA Management Fault
31283	Lost Communication with server
31322	HA Configuration Error
33001	Diameter-to-MAP Service Registration Failure on DA-MP
33105	Routing Attempt failed due to queue exhaustion
33120	Policy SBR Binding Sub-Resource Unavailable
33301	Update Config Data Failure
33303	U-SBR Event Queue Utilization
33310	U-SBR Sub-resource Unavailable
33312	DCA Script Generation Error
33301	Update Config Data Failure

Appendix L. Additional Backout Steps

Procedure 65. Additional Backout Steps for NOAM, SOAM, and SBR Server(s)

Step #	Procedure	Description
This procedure provides the details about additional backout steps for NOAM, SOAM and SBR server(s) to support backout for major upgrade release paths. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		If server is NOAM or SOAM server, execute steps 2 to 5 and if server is SBR server, execute steps 6. to 7.
		Please note down the hostname of the server on which these steps are executed. Once all the servers in a server group will be backed out then the additional post-backout steps will be executed to revert back the changes done in this procedure.

2.
☐
	Server CLI: Set the resource as optional
	For OAM servers only
		Note: Make sure the resource being set is in system. Some of the resources shown are introduced in different releases.
		If the resource is not in the system, presence check will not result any output records. In this case, skip updating these fields for the resource not in the system.
		1. Check for the resource:
		`iqt -E HaResourceCfg where "name='<resource_name>'"`
		2. Execute this command:
		`iset -W -foptional='Yes' HaResourceCfg where "name='DSROAM_Proc'"`
		These commands change/update the results of some records.

3. ☐	**Server CLI**: Restart the HTTPD service For OAM servers only	Execute this command: `sudo service httpd restart`

4.
☐
	Active NOAM/SOAM Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NOAM/SOAM server in the same server group, in which server is under backout:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

Step #	Procedure	Description

5.
☐
	Server CLI:
	Verify that the replication is working fine.
	For OAM servers only
		1. Execute this command on an active NOAM/SOAM server in the same server group being backed out:
		`irepstat`
		2. Verify the `irepstat` command displays a replication row for the server which is being backed out.
		Note the replication status is **Active** before proceeding, if it is **Audit**, then wait until replication becomes Active.
		If this step is missed, data is lost and is unrecoverable.
		Example:
		Here Ford-B-NO is Active NOAM Server and Ford-A-NO is backed out.
		`Ford-B-NO  A3301.157  Ford-B-NO  09:32:17  [Rw]`
		`Policy 0 ActStb [DbReplication] ----------`
		`AA To  P0 Ford-A-NO  Active  0  0.00 1%R 0.12%cpu 1.88k/s`
		`AA To  P1 Chevy-DRNO-B Active  0  0.00 1%R 0.08%cpu 1.89k/s`
		`AB To  D0 Camaro-SO-B  Active  0  0.00 1%R 0.09%cpu 1.89k/s`
		`AB To  D0 Nova-SO-B  Active  0  0.00 1%R 0.08%cpu 1.90k/s`
		`AB To  D0 Pinto-SO-B  Active  0  0.00 1%R 0.10%cpu 1.89k/s`
		`AB To  D0 Mustang-SO-B Active  0  0.00 1%R 0.10%cpu 2.14k/s`
		3. Press **q** if you want to exit the irepstat command output.
		4. Execute `irepstat` again, if required.

6.
☐
	Server CLI:
	Setting the resource as optional
	For SBR servers only
		Note: Make sure the resource being set is in the system. Some of the resources listed below are introduced in different releases.
		If a resource is not in the system, presence check does not result in any output records. In this case, do not update the fields for the resource.
		Resource presence can be checked using:-
		`iqt -E HaResourceCfg where "name='<resource_name>'"`
		For example:-
		`iqt -E HaClusterResourceCfg where "resource='uSbrRes'"`
		Execute this command for Session SBR only:
		`iset -W -foptional='Yes' HaResourceCfg where "name='pSbrSBaseRepl'"`
		`iset -W -foptional='Yes' HaClusterResourceCfg where "resource='uSbrRes'"`
		`iset -W -foptional='Yes' HaClusterResourceCfg where "resource='pSbrSessionRes'"`
		Execute this command for Binding SBR only:
		`iset -W -foptional='Yes' HaResourceCfg where "name='pSbrBBaseRepl'"`
		`iset -W -foptional='Yes' HaClusterResourceCfg where "resource='uSbrRes'"`
		`iset -W -foptional='Yes' HaResourceCfg where "name='pSbrBindingRes'"`
		These commands change/update the results of some records.

Step #	Procedure	Description

7.
☐
	Server CLI:
	Verify that the replication is working fine
	For SBR servers only
		1. Execute this command on an active SBR server in the same server group as the server being backed out:
		`irepstat`
		2. Verify the `irepstat` command displays a replication row for the server which is being backed out.
		Note the replication status is **Active** before proceeding, if it is **Audit**, then wait until replication becomes Active.
		If this step is missed, data is lost and is unrecoverable.
		Example:
		Here Pinto-SBR-2 is Active SBR Server and Pinto-SBR-1 is backed out.
		Also, on Binding SBR, resource will be pSbrBindingPolicy
		And on Session SBR, resource will be pSbrSessionPolicy
		`Pinto-SBR-2  C3783.034  Pinto-SBR-2  13:39:38  [Rw]`
		`Policy 0 ActStb [DbReplication] ----------`
		`BC From  D0 Pinto-SO-B  Active  0  0.10 ^0.10%cpu 67.0/s`
		`CC To  P0 Pinto-SBR-1  Active  0  0.10 1%S 0.31%cpu 30.9/s`
		`CC To  P1 Mustang-SBR-3 Active  0  0.10 1%S 0.28%cpu 39.6/s`
		
		`Policy 21 pSbrBindingPolicy [pSbrBBaseRepl] ----------`
		`CC To  P0 Pinto-SBR-1  Active  0  0.10 1%S 0.63%cpu 186k/s`
		`CC To  P1 Mustang-SBR-3 Active  2  0.13 1%S 0.55%cpu 189k/s`
		3. Press **q** if you want to exit the irepstat command output.
		4. Execute `irepstat` again, if required.

Appendix M. Additional Post-Backout Steps

Procedure 66. Additional Post Backout Steps for NOAM, SOAM, and SBR Server(s)

Step #	Procedure	Description
This procedure provides the details about additional post backout steps for NOAM, SOAM and SBR server(s) to support backout for major upgrade release paths. This procedure is executed only after all servers in the same server group are backed out. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Server CLI:
	Log into the server (if not already done)
		Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		If the server is an NOAM or SOAM server, execute step 2.
		If the server is an SBR server, execute steps 3.
		Note the hostname of the server on which these steps are executed. Once all servers in a server group are backed out, additional post-backout steps are executed to revert the changes done in this procedure.
		Note:
		In case of backout from 8.x to 7.3, verify if all the services are Up.
		Execute the following commands on servers where the services are in pending state:
		`rm -rf /etc/ld.so.cache`
		`echo "/usr/TKLC/dsr/lib" | sudo tee -a /etc/ld.so.conf.d/dsr.conf`
		`sudo cat /etc/ld.so.conf.d/dsr.conf`
		`sudo ldconfig`
		Check for configured libraries, for example:
		`sudo ldconfig -p | grep -i pdra`
		Output must have the following information:
		`libPdraTraps.so (libc6,x86-64) => /usr/TKLC/dsr/lib/libPdraTraps.so`
		Check whether all the services are Up:
		`pl`

Step #	Procedure	Description

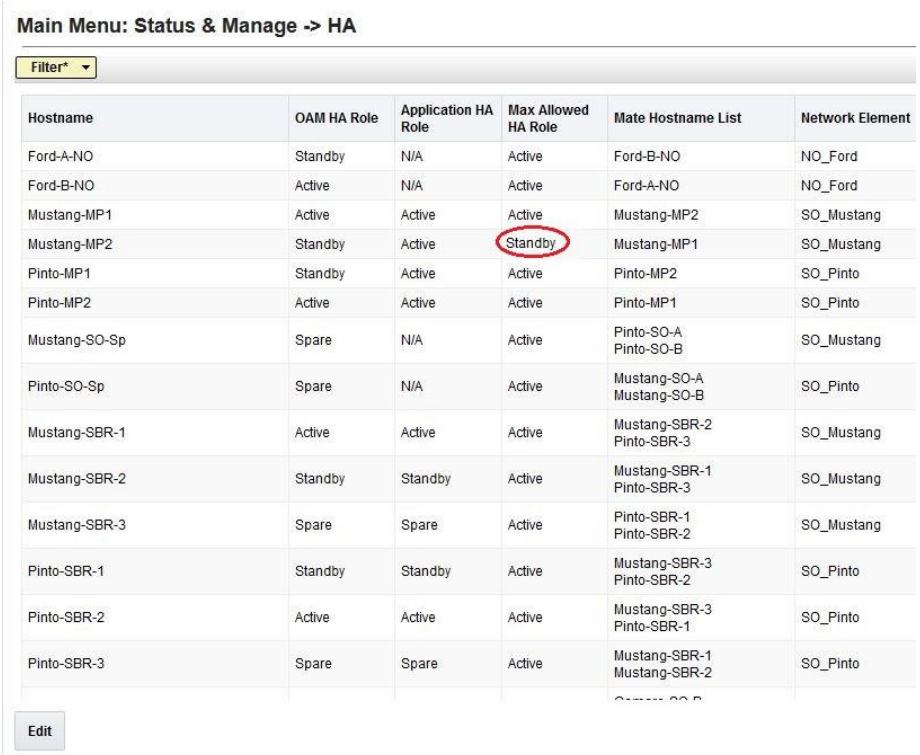
2.
☐
	Server CLI: Set the resource as optional
	For OAM servers only
		Note: Make sure the resource getting set is in system. Some of resources shown are introduced in different releases.
		If the resource is not in the system, presence check will not result any output records. In this case, skip updating these fields for the resource not in the system.
		1. Check for the resource:
		`iqt -E HaResourceCfg where "name='<resource_name>'"`
		2. Execute this command:
		`iset -W -foptional='Yes' HaResourceCfg where "name='DSROAM_Proc'"`
		These commands change/update the results of some records.

3.
☐
	Server CLI: Setting the resource as optional
	For SBR servers only
		Note: Make sure the resource being set is in the system. Some of the resources listed below are introduced in different releases.
		If a resource is not in the system, presence check does not result in any output records. In this case, do not update the fields for the resource.
		Resource presence can be checked using:-
		`iqt -E HaResourceCfg where "name='<resource_name>'"`
		For example:-
		`iqt -E HaClusterResourceCfg where "resource='uSbrRes'"`
		Execute this command for Session SBR only:
		`iset -W -foptional='No' HaResourceCfg where "name='pSbrSBaseRepl'"`
		`iset -W -foptional='No' HaClusterResourceCfg where "resource='uSbrRes'"`
		`iset -W -foptional='No' HaClusterResourceCfg where "resource='pSbrSessionRes'"`
		Execute this command for Binding SBR only:
		`iset -W -foptional='No' HaResourceCfg where "name='pSbrBBaseRepl'"`
		`iset -W -foptional='No' HaClusterResourceCfg where "resource='uSbrRes'"`
		`iset -W -foptional='No' HaResourceCfg where "name='pSbrBindingRes'"`
		These commands change/update the results of some records.
		Repeat this procedure for other servers in the server group being backed out.

Appendix N. Manual Completion of Server Upgrade

Procedure 67. Manual Completion of Server Upgrade

Step #	Procedure	Description
This procedure provides the details about manual completion of server upgrade. ***Note***: In the unlikely event that after the upgrade, if the **Upgrade State** of server is **Backout Ready** and the **Status Message** displays **Server could not restart the application to complete the upgrade**, then perform to restore the server to full operational status and return to this step to continue the upgrade. Perform Appendix V to create a link of Comagent Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**NOAMP VIP GUI**: Login: Log into the server (if not already done)	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Log into the NOAM GUI as the **guiadmin** user:

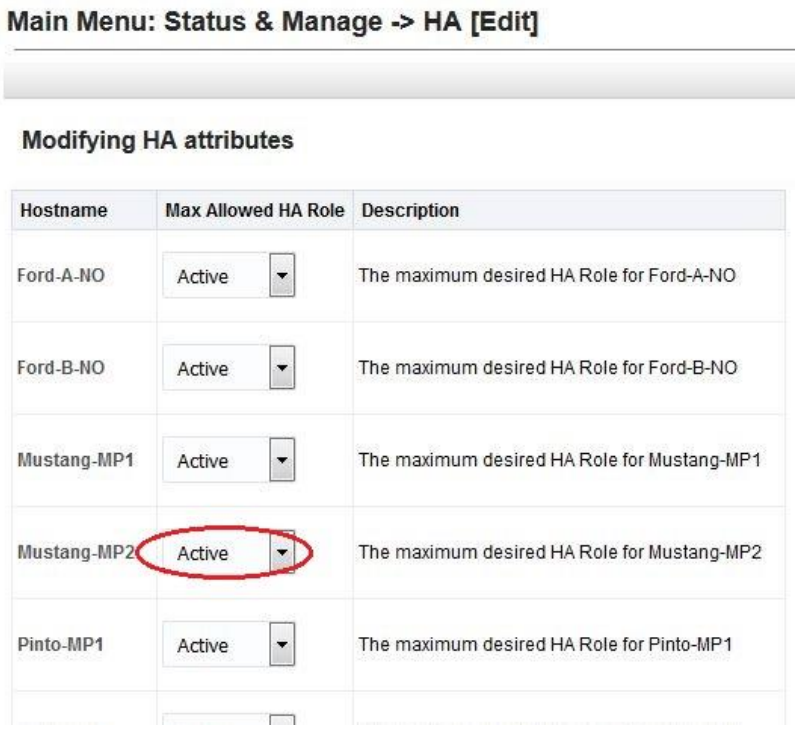
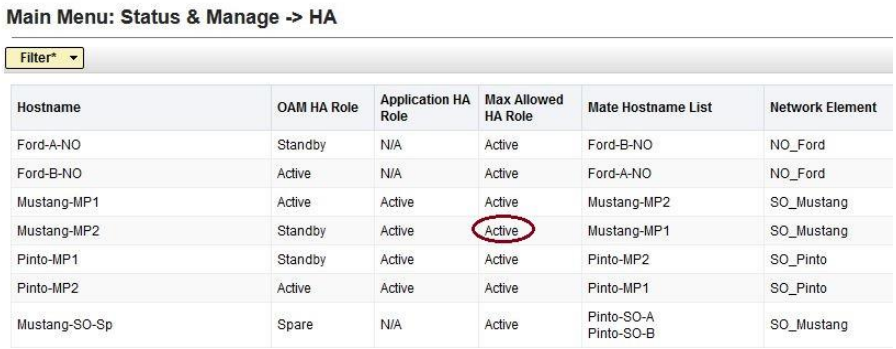
Step #	Procedure	Description
2. ☐	**NOAMP VIP GUI**: Verify server status	1. Navigate to **Status and Manage > HA**. 2. Locate the server you want to upgrade. 3. Verify the Max Allowed HA Role is Standby.  4. Click **Edit**.

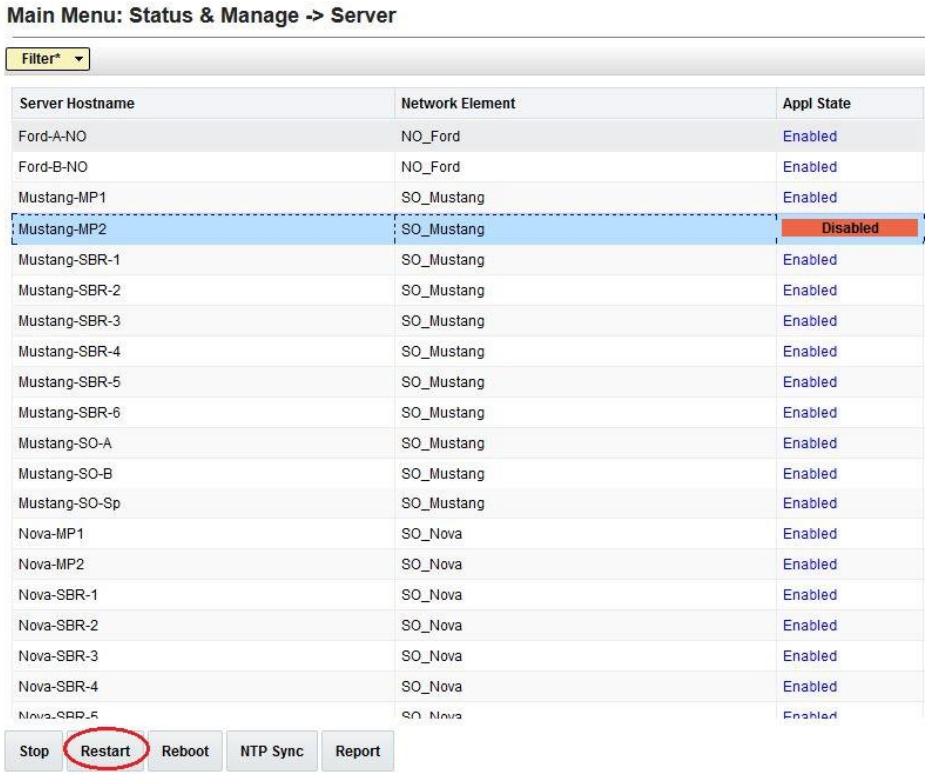
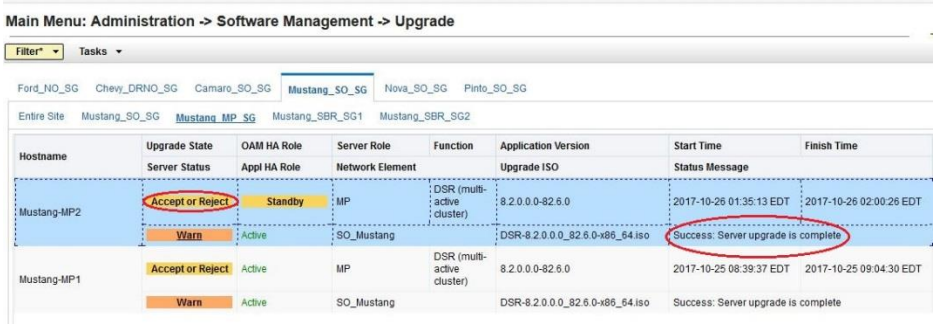
Main Menu: Status & Manage -> HA

Filter*

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element
Ford-A-NO	Standby	N/A	Active	Ford-B-NO	NO_Ford
Ford-B-NO	Active	N/A	Active	Ford-A-NO	NO_Ford
Mustang-MP1	Active	Active	Active	Mustang-MP2	SO_Mustang
Mustang-MP2	Standby	Active	Standby	Mustang-MP1	SO_Mustang
Pinto-MP1	Standby	Active	Active	Pinto-MP2	SO_Pinto
Pinto-MP2	Active	Active	Active	Pinto-MP1	SO_Pinto
Mustang-SO-Sp	Spare	N/A	Active	Pinto-SO-A Pinto-SO-B	SO_Mustang
Pinto-SO-Sp	Spare	N/A	Active	Mustang-SO-A Mustang-SO-B	SO_Pinto
Mustang-SBR-1	Active	Active	Active	Mustang-SBR-2 Pinto-SBR-3	SO_Mustang
Mustang-SBR-2	Standby	Standby	Active	Mustang-SBR-1 Pinto-SBR-3	SO_Mustang
Mustang-SBR-3	Spare	Spare	Active	Pinto-SBR-1 Pinto-SBR-2	SO_Mustang
Pinto-SBR-1	Standby	Standby	Active	Mustang-SBR-3 Pinto-SBR-2	SO_Pinto
Pinto-SBR-2	Active	Active	Active	Mustang-SBR-3 Pinto-SBR-1	SO_Pinto
Pinto-SBR-3	Spare	Spare	Active	Mustang-SBR-1 Mustang-SBR-2	SO_Pinto

Edit

Step #	Procedure	Description
3. ☐	**NOAMP VIP GUI**: Change role	1. Change the Max Allowed HA Role to Active. 2. Click **OK**. 
4. ☐	**NOAMP VIP GUI**: Verify change	Verify the **Max Allowed HA Role** changes to **Active**. 

Step #	Procedure	Description
5. ☐	**NOAMP VIP GUI**: Restart the server	1. Navigate to **Status & Manage > Server**. 2. Select the server to upgrade. 3. Click **Restart**.  After a few minutes, the Appl State change to **Enabled**.
6. ☐	**NOAMP VIP GUI**: Verify status	1. Navigate to **Administration > Software Management > Upgrade**. 2. Verify the Upgrade State changes to **Accept or Reject** and the Status Message changes to **Success: Server manually completed**. 

Appendix O. Identify the DC server

Procedure 68. Identification of the DC server

Step #	Procedure	Description
This procedure provides the details to identify the DC server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**NOAMP VIP GUI**: Login	Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Log into the NOAM GUI as the guiadmin user:
2. ☐	**NOAMP VIP GUI**: Select an MP server	1. Navigate to **Configuration > Server Groups**. 2. Select an MP server from the server group that needs to be upgraded.

3.
☐
	Log into MP Server using CLI
	SSH to MP server chosen above
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the MP server identified in Step 1.
		`ssh admusr@<MP_SERVER_XMI>`
		`password: <enter password>`
		2. Answer **yes** if you are asked to confirm the identity of the server

Step #	Procedure	Description

4.
☐
	MP Server CLI:
	Find DC server
		Identify the DC server in the server group with this command:
		`ha.info -d`
		If the server is the DC server, then output is similar to this:
		`[admusr@X6201-MP1 ~]$ ha.info -d`
		
		`Output from`
		`Node ID:  X6201-MP1`
		`Report Time: 12/14/2017 12:05:10.905`
		
		`***`
		`** Election Mgr: C2121 (27a64d)`
		`***`
		
		`DC: X6201-MP1  Generation: 2  State: DC`
		`  Elected: 12/12/2017 09:18:08.905`
		`  Other Non-DC Group Members:`
		`    X6201-MP5`
		`    X6201-MP3`
		`    X6201-MP4`
		`    X6201-MP2`
		`  DC Group Candidates: <none>`
		
		`***`
		`** End of Election Mgr: C2121`
		`***`
		If the server is not the DC server, then output is similar to this:
		`[admusr@X6201-MP3 ~]$ ha.info -d`
		
		`Output from`
		`Node ID:  X6201-MP3`
		`Report Time: 12/14/2017 12:05:38.314`
		
		`***`
		`** Election Mgr: C2121 (27a64d)`
		`***`
		
		`DC: X6201-MP1  Generation: 2  State: NON-DC`
		`ATTN: Reported from Non-DC node. Execute ha.info on DC for full status.`
		`  DC Group Candidates: <none>`
		
		`***`
		`** End of Election Mgr: C2121`
		`***`

Appendix P. Limitations of Automated Server Group and Automated Site Upgrade

For multi-active server groups, such as DA-MP/vSTP MPs, non-deterministic server selection **could possibly** result in a network outage during the upgrade. In certain scenarios, customer preferences or requirements can result in configurations in which it is imperative that DA-MP servers must be, or conversely, cannot be, upgraded together. These scenarios are described in this section with the recommendation that customers NOT use ASG if any of these exists in their network.

CAUTION

Oracle's recommendation for any customer whose network aligns with any of the following scenarios is that the Automated Server Group upgrade should NOT be used on multi-active DA-MP server groups. Use of ASG risks a potential network outage.

For Automated Site Upgrade, following limitations can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles then in that case manual upgrade section 5.3 method should be used.

Specialized Fixed Diameter Connections

In this scenario, each peer node is configured to connect to two specific DA-MPs for local redundancy (Figure 18). With ASG/ASU setup for 50% minimum availability, three of the DA-MPs in the server group are upgraded in parallel. However, it is not possible to determine in advance which three DA-MPs are selected. Although the DSR has redundant connections to the peer nodes, an unfortunate selection of servers for upgrade could result in an outage. Upgrade cycle 1 takes out both DA-MPs connected to the unhappy peer. This peer is isolated for the duration of the upgrade.

The happy peer is connected to DA-MPs that are selected by ASG/ASU for different upgrade cycles. This peer is never isolated during the upgrade.

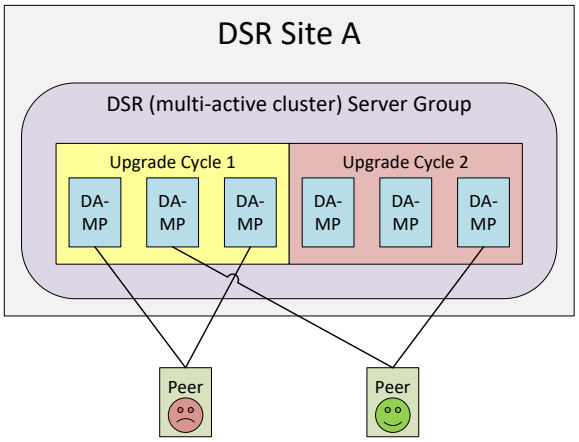


Figure 18. Specialized Fixed Diameter Connections

Specialized Floating Diameter Connections

In this scenario, each peer node is configured to connect to an IPFE TSA address hosted by a set of DA-MPs. When any particular TSA contains only a subset of the server group MPs, and the DSR upgrade logic happens to select that subset of MPs for simultaneous upgrade, then there is a signaling outage for that TSA. This scenario is depicted in Figure 19.

TSA1 is distributed across the first three DA-MPs, whereas TSA2 is distributed across all six DA-MPs. If ASG/ASU is initiated with 50% minimum availability, the DSR could select all three of the DA-MPs hosting TSA1 in the first upgrade cycle. The unhappy peer is isolated for the duration of upgrade cycle 1.

The happy peer is connected to TSA2, which is hosted by the DA-MP servers in such a way that the TSA is evenly hosted in both upgrade cycles. This peer is never isolated during the upgrade.

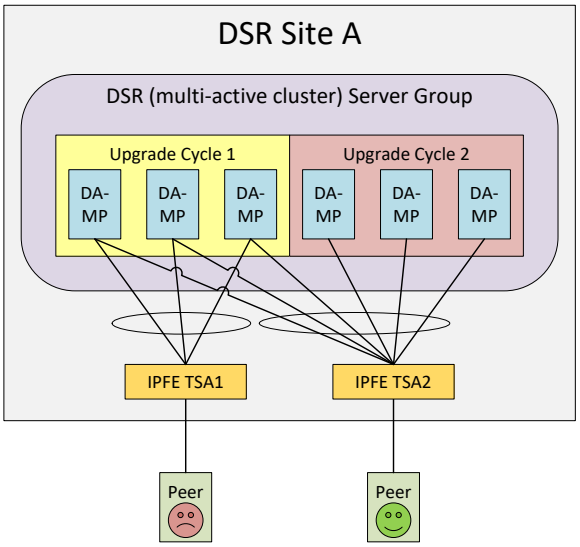


Figure 19. Specialized Floating Diameter Connections

Specialized Distribution of DSR Features

In this scenario, the customer has decided to enable P-DRA and RBAR on four DA-MP servers and DCA on two DA-MP servers, consistent with expected traffic load. With ASG setup for 50% minimum availability, the DA-MP server group is upgraded in two cycles. RBAR and P-DRA happen to be hosted by DA-MP servers selected by ASG/ASU to be in different upgrade cycles, albeit unbalanced. The RBAR peer is only marginally happy because during upgrade cycle 1, only 25% of RBAR and P-DRA capacity is available, even though the customer specified 50% availability.

DCA happens to be hosted by DA-MP servers selected by ASG/ASU to be in upgrade cycle 2. The DCA peer is unhappy because DCA is completely unavailable during upgrade cycle 2.

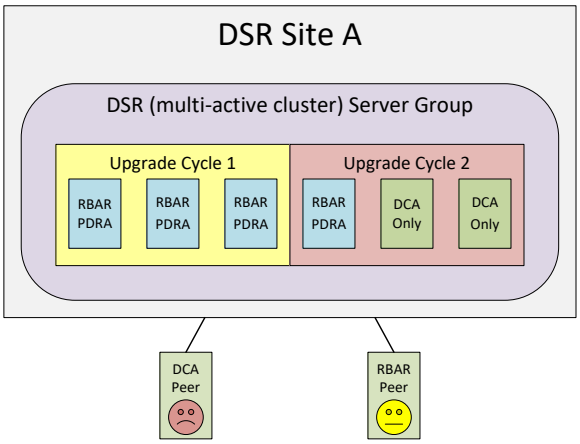


Figure 20. Specialized Distribution of DSR Features

Appendix Q. Advanced Health Check Procedure

Procedure 69. Firewall Check for DNS Port 53

Step #	Procedure	Description
This procedure verifies the UDP/TCP port 53 is open between NOAM and each DR-NOAM site, NOAM and each SOAM site, and between MPs and each name server of the file /etc/resolv.conf. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Verify if the UDP/TCP port 53 is open between NOAM and each DR-NOAM site	From the command prompt of the server with the alarm:
		1. Issue the sudo nmap -sTU -p 53 <DR-NOAM hostname> command.
		2. Verify that the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
		`[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-DRNOAM-A`
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:57 EST`
		`Nmap scan report for Icepick-DRNOAM-A (10.75.202.173)`
		`Host is up (0.00025s latency).`
		`rDNS record for 10.75.202.173: Icepick-DRNOAM-A.platform.cgbu.us.oracle.com`
		`PORT  STATE SERVICE`
		`53/tcp open  domain`
		`53/udp open  domain`
		`MAC Address: 02:05:39:E0:60:8A (Unknown)`
		`Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds`
		`[admusr@Icepick-NO-A ~]$`
		If port is reported as any state other than “Open”, then inform the Customer before accepting the upgrade.
		Note: If the ports are reported as “Closed” it may be because no services are running on the far end. Check with the Customer if the firewall has been configured to allow DNS traffic on port 53.
		If the port is reported as “Filtered” then the port is likely blocked by a Firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

Step #	Procedure	Description

2. ☐	Verify if the UDP/TCP port 53 is open between NOAM and each SOAM site	From the command prompt of the server with the alarm:
		1. Issue the sudo nmap -sTU -p 53 <SOAM hostname> command.
		2. Verify the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
		`[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-SO-A`
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:57 EST`
		`Nmap scan report for Icepick-SO-A (10.75.202.173)`
		`Host is up (0.00025s latency).`
		`rDNS record for 10.75.202.173: Icepick-SO-A.platform.cgbu.us.oracle.com`
		`PORT  STATE SERVICE`
		`53/tcp open  domain`
		`53/udp open  domain`
		`MAC Address: 02:05:39:E0:60:8A (Unknown)`
		`Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds`
		3. If port is reported as any state other than “Open” then inform the Customer before accepting the upgrade.
		Note: If the ports are reported as “Closed” it may be because no services are running on the far end. Verify with the Customer that the firewall has been configured to allow DNS traffic on port 53.
		4. If the port is reported as “Filtered” then the port is likely to be blocked by a firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

3. ☐	Verify if the UDP/TCP port 53 is open between MP and each name server of the **/etc/resolv.conf** file	1. List the contents of the file /etc/resolv.conf via the “sudo cat etc/resolv.conf” command.
		2. Verify that the Customer Firewall is configured to allow DNS traffic on UDP/TCP port 53 to the addressed from the file /etc/resolv.conf:
		`[admusr@Icepick-DAMP-1 ~]$ sudo cat /etc/resolv.conf  (lookups)`
		`domain platform.cgbu.us.oracle.com`
		`nameserver 10.240.50.134`
		`nameserver 10.240.50.133`
		`search platform.cgbu.us.oracle.com 500lab.com labs.tekelec.com labs.nc.tekelec.com`
		`[admusr@Icepick-DAMP-1 ~]$`

Step #	Procedure	Description

		`[admusr@Icepick-DAMP-1 ~]$  sudo nmap -sTU -p 53 10.240.50.134   10.240.50.133`
		
		`Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:46 EST`
		`Nmap scan report for Icepick-SO-B-imi.platform.cgbu.us.oracle.com (10.240.50.134)`
		`Host is up (0.00022s latency).`
		`PORT   STATE SERVICE`
		`53/tcp open  domain`
		`53/udp open  domain`
		`MAC Address: 02:17:B4:4F:DA:B6 (Unknown)`
		
		`Nmap scan report for Icepick-SO-A-imi.platform.cgbu.us.oracle.com (10.240.50.133)`
		`Host is up (0.00025s latency).`
		`PORT   STATE SERVICE`
		`53/tcp open  domain`
		`53/udp open  domain`
		`MAC Address: 02:EE:13:E2:2C:EF (Unknown)`
		`Nmap done: 2 IP addresses (2 hosts up) scanned in 5.66 seconds`
		`[admusr@Icepick-DAMP-1 ~]$`
		If port is reported as any state other than “Open” then inform the Customer before accepting the upgrade.
		Note: If the ports are reported as “Closed” it may be because no services are running on the far end. Verify with the Customer that the firewall has been configured to allow DNS traffic on port 53.
		If the port is reported as “Filtered” then the port is likely to be blocked by a Firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

Appendix R. Workaround to Resolve DB Site Replication Alarms

The following procedure resolves DB site replication alarms if encountered during the upgrade. Database (DB) replication failure alarms may display during an Auto Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved.

Procedure 70. Workaround to Resolve DB Site Replication Alarms

Step #	Procedure	Description
This procedure restarts the inetrep process on the server that has a DB replication failure alarm. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Server CLI: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Server CLI**: Check if the replication links are up	Execute this command: `irepstat` Some of the B-C and C-C replications links may be down.
3. ☐	**Server CLI**: Resolve replication issue(s)	Execute this command: `sudo pm.kill inetrep`
4. ☐	Repeat, if needed	Repeat procedure on each affected server

Appendix S. Workaround to Resolve the Server HA Switchover Issue

The following procedure resolves the HA switchover issue.

Procedure 71. Resolve the HA Switchover Issue on Affected Server(s)

Step #	Procedure	Description
This procedure restarts the cmha process on the server that has HA switchover issue. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Server CLI: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the NOAM server which is experiencing the HA switchover issue :
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Server CLI**: Resolve HA switchover issue(s)	Execute this command: `sudo pm.kill cmha`
3. ☐	Repeat, if needed	Repeat procedure on each affected server.

Appendix T. Workaround to Resolve Device Deployment Failed Alarm

Procedure 72. Resolve Device Deployment Failed Alarm

Step #	Procedure	Description
This procedure is to resolve the device deployment failed alarm i.e. 10054 Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	**NOAMP VIP GUI**: Login	Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Log into the NOAM GUI as the **guiadmin** user:
2. ☐	**NOAMP VIP GUI**: Identify server(s) and interface(s) with alarm	Navigate to current alarm details and identify the server and interface where the **10054 - Device Deployment Failed** alarm is displayed. 1. Navigate to **Alarms & Events > View Active**. 2. Look for the **10054** alarm make a list of the server(s) and interface(s).

Step #	Procedure	Description
3. ☐	**NOAMP VIP GUI**: Corrective action for alarm 10054	Interfaces like xmi and imi are in locked state and do not allow editing as a corrective action. For xmi and imi interfaces, first unlock the interface and for other interfaces skip steps (a) to (d) below. 1. Navigate to **Configuration > Networking > Networks**, select the respective “Network element” tab used for the server configuration 2. Click on the Network Name row. 3. Click **Unlock**. Click on the checkbox to confirm it and click **OK**. 4. To unlock the network for the particular device, navigate to **Configuration > Networking > Devices**. 5. Click on the Server tab from the list in Step 2. 6. Select each interface row one by one for which alarm is showing and click **Edit**. 7. Click **OK**. ***Note***: Give some time to system to auto correct the condition to clear the alarm. Once this step is done, lock the network back again which were unlocked above. **For xmi and imi interfaces, lock the interface back, for other interfaces skip (a) to (d) below.** 8. To lock the network for a specific device, navigate to **Configuration > Networking > Networks**, select the respective Network element tab used for the server configuration. 9. Click the Network Name row. 10. Click **Lock**. Click on the checkbox to confirm it and click **OK**.

Appendix U. Workaround to Resolve syscheck Error for CPU Failure

Procedure 73. Workaround to Resolve syscheck Error for CPU Failure

Step #	Procedure	Description
Workaround to resolve syscheck error for CPU failure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		

1.
☐
	Log into the server using CLI on which syscheck is failing	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.
		`ssh admusr@<SERVER_XMI>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server

2.
☐
	Server CLI: Execute workaround	1. Edit the cpu config file.
		`$ sudo vim /usr/TKLC/plat/lib/Syscheck/modules/system/cpu/config`
		2. Comment out the all texts that reads: **EXPECTED_CPUS=** by putting # at the beginning of the line, for example:
		`# EXPECTED_CPUS=2`
		3. Save the cpu config file.
		4. Reconfig the syscheck by running these commands:
		`sudo syscheck --unconfig`
		`sudo syscheck --reconfig`
		`sudo syscheck`
		CPU related errors do not display.

Appendix V. Create a Link for ComAgent

Procedure 74. Create a Link for ComAgent

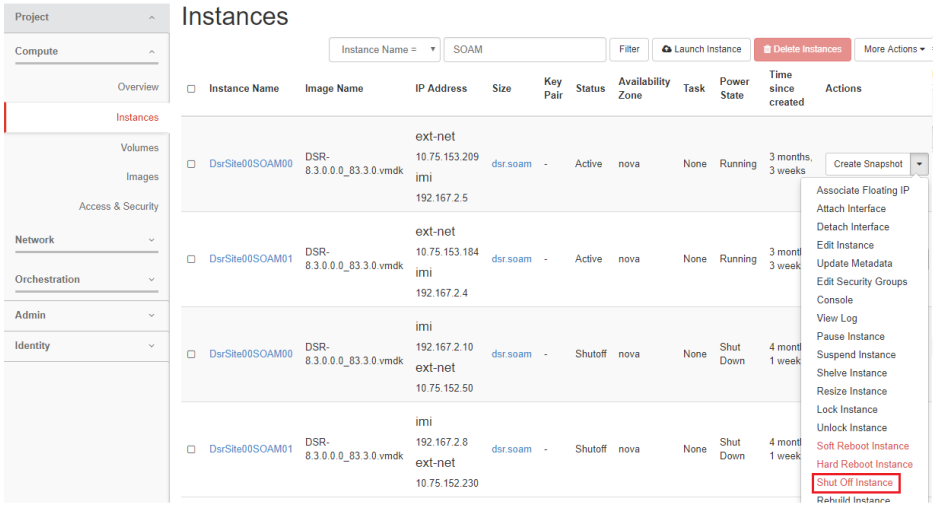
Step #	Procedure	Description
This procedure provides the details about creating a symbolic link of Comagent. ***Note***: This procedure is executed only after all servers in the same server group are backed out. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

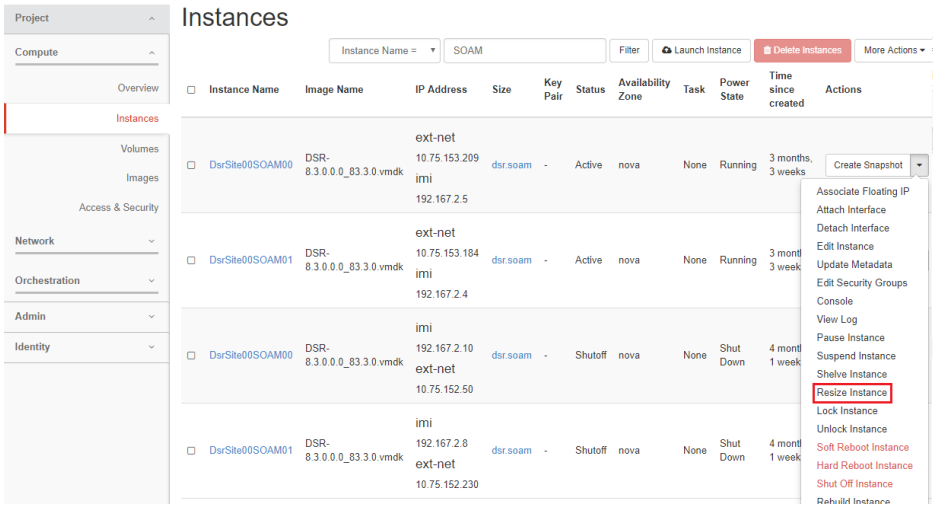
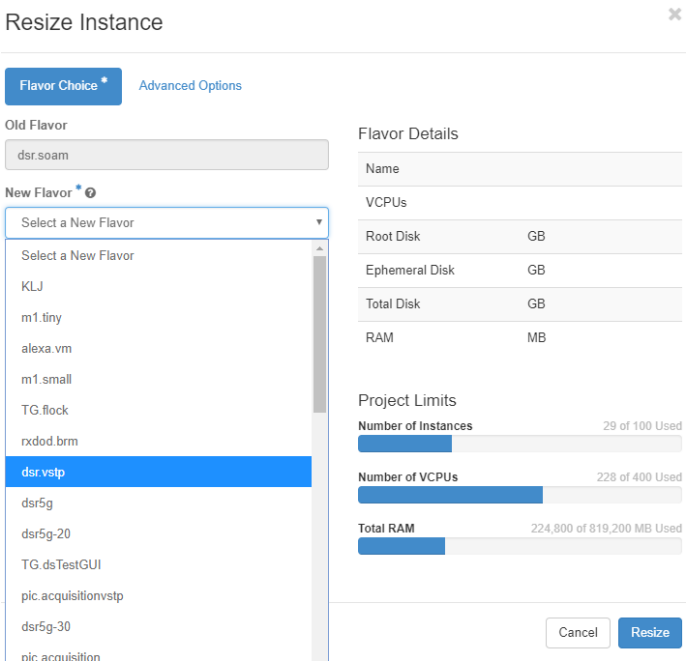
1.
☐
	Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2.
☐
	Server: Create a link for ComAgent	Execute the following commands to create a Comagent link:
		1. Navigate to **/var/TKLC/appworks/library**.
		`$ cd /var/TKLC/appworks/library`
		2. Create a link
		`$ sudo ln -s /usr/TKLC/comagent-gui/gui/ Comagent`
		Verify if the ComAgent link has been restored.
		`[admusr@HPC-NO1 library]$ ls -ltr`
		`total 56`
		`drwxr-xr-x 7 awadmin awadm 4096 Aug 25 2017 Diameter`
		`lrwxrwxrwx 1 root root 47 Dec 15 02:05 Zend -> /usr/TKLC/plat/www/zend-framework/library/Zend/`
		`lrwxrwxrwx 1 root root 21 Dec 15 02:07 Awpss7 -> /usr/TKLC/awpss7/gui/`
		`lrwxrwxrwx 1 root root 29 Dec 15 02:07 TransportMgr -> /usr/TKLC/awptransportmgr/gui`
		`lrwxrwxrwx 1 root root 38 Dec 15 02:07 Exgstack -> /usr/TKLC/awptransportmgr/gui/Exgstack`
		`drwxr-xr-x 3 awadmin awadm 4096 Dec 31 15:58 Rbar`
		`drwxr-xr-x 4 awadmin awadm 4096 May 22 10:42 AWCLI`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Radius`
		`drwxr-xr-x 4 awadmin awadm 4096 May 22 10:44 Dca`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Fabr`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Gla`
		`drwxr-xr-x 2 awadmin awadm 4096 May 22 10:44 Loadgen`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Mapiwf`
		`drwxr-xr-x 6 awadmin awadm 4096 May 22 10:44 Pdra`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Sbr`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Vstp`
		`lrwxrwxrwx 1 root root 18 May 22 10:44 Ipfe -> /usr/TKLC/ipfe/gui`
		`drwxr-xr-x 3 awadmin awadm 4096 May 22 10:45 Csbr`
		`drwxr-xr-x 17 awadmin awadm 4096 May 22 10:45 AppWorks`
		`lrwxrwxrwx 1 root root 27 May 22 11:47 Comagent -> /usr/TKLC/comagent-gui/gui/`
		If the output is received as highlighted in red, the softlink for Comagent directory has been restored.

Appendix W. Change SOAM VM Profile for Increased MP Capacity

Procedure 75. Change SOAM VM Profile for Increased MP Capacity

Step #	Procedure	Description
This procedure provides the details about changing SOAM VM profile for increased MP Capacity. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact and ask for assistance.		
1. ☐	Log into OpenStack	Log into Openstack GUI horizon dashboard).
2. ☐	Identify and shut down the instance	Go to the corresponding Instance and select the **Shut Off Instance** option from the list. 

Step #	Procedure	Description
3. ☐	Resize instance	Once the instance is in **Shutoff** state, select the **Resize Instance** option from the list: 
4. ☐	Select the new flavor that meets the standard VCPUs size and memory configuration	1. Select the **New Flavor** that meets the standard VCPUs size and memory configuration.  2. Click **Resize**. ***Note***: For information on the recommended vCPUs size and memory, refer to [8] DSR 8.3 Cloud Benchmarking document.

Appendix X. My Oracle Support (MOS)

My Oracle Support

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

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

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:

   For technical issues such as creating a new Service Request (SR), select **1**.

   For non-technical issues such as registration or assistance with MOS, select **2**.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, and 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at `1-800-223-1711` (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click Industries.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by

these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or "**Platforms**."

4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Appendix Y. Reset the SOAP Password

Procedure 76. Reset the SOAP Password

Step#	Procedure	Description
This procedure provides the details about resetting the SOAP password. When Oracle is upgraded, the following procedure resets the SOAP password, for the DSR to perform self-authenticate with IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		

1.
☐
	Login to NOAM: Login on the active NOAM server	1. Login as admusr on the active NOAM server.
		2. Retrieve the TPD web service password in plaintext by executing:
		`$ /usr/TKLC/appworks/bin/aw.wallet credential get cmsoapa password`
		
		The command will print the current plaintext configuration web service password.
		
		For example:
		`7w57q9U0OvOtKtgtLVTMajDcXfhCj2F4nyXw45qK6EXNHA9jACyQ`

2.
☐
	Login to the IDIH application server	1. Login as admusr on the IDIH application server.
		2. Change the user to tekelec by executing:
		`sudo su - tekelec`
		3. Reset/Create the Configuration web service password:
		a. Go to the directory `/usr/TKLC/xIH/apps/trace-refdata-adapter/`
		b. run `./resetSoapPassword.sh`
		c. When prompted for password:
		<enter the password obtained from Step1.2>
		Note: This script prints the encrypted password.
		The new encrypted SOAP password is stored into IDIH Oracle database.
		4. Verify if the password is stored in IDIH Oracle database by executing:
		a. `sqlplus /@NSP`
		b. Select * from `DSR_USER_CREDENTIALS`;
		Here you should see the same encrypted password as in Step 2.3.
		c. Type `exit` to exit from database.
		5. After verifying that password is stored in database in Step 2.4, the WebLogic application server must be restarted on IDIH application server.
		a. Become admusr by executing:
		`exit`
		b. Stop the WebLogic application server by executing:
		`sudo service xih-apps stop`
		c. Start the WebLogic application server by executing:
		`sudo service xih-apps start`
		The Weblogic server might take few minutes to resume its service.
		Note: Upon completion of the above steps, in IDIH `/var/TKLC/xIH/log/apps/weblogic/apps/application.log` file you should see NO Error.