Oracle® Communications

Diameter Signaling Router

Cloud Software Upgrade Guide

Release 8.0/8.1

E88905-01

March 2018

ORACLE

Oracle® Communications Diameter Signaling Router, Cloud Software Upgrade User's Guide, Release 8.0/8.1

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 10
1.1 Purpose and Scope 10
1.1.1 What is Not Covered by this Document 10
1.2 References 10
1.3 Acronyms 10
1.4 Terminology 12
1.5 How to Use this Document 13
1.5.1 Executing Procedures 14
1.6 Recommendations 14
1.6.1 Frequency of Health Checks 14
1.6.2 Large Installation Support 14
1.6.3 Logging of Upgrade Activities 14
1.7 Warnings, Cautions, and Notes 15
1.7.1 PCA/PDRA Application – PCRF Pooling Migration Precheck 15
1.7.2 PCA/PDRA Application – PCRF Pooling Enablement 15
1.7.3 Signaling Firewall 16
1.7.4 NetBackup 7.7 Support 17
1.7.5 Network IDIH Compatibility 17
1.7.6 Review Release Notes 17
2. General Description 17
2.1 Supported Upgrade Paths to 8.0 18
2.2 Supported Upgrade Paths to 8.1 19
2.3 Geo-Diverse Site (Active/Standby/Spare PCA Configuration) 20
2.4 Traffic Management During Upgrade 20
2.5 Automated Site Upgrade 21
2.5.1 Site Upgrade Execution 23
2.5.2 Minimum Server Availability 27
2.5.3 Site Upgrade Options 28
2.5.4 Cancel and Restart Auto Site Upgrade 30
2.6 Automated Server Group Upgrade 32
2.6.1 Cancel and Restart Automated Server Group Upgrade 32
2.6.2 Site Accept 33
3. Upgrade Planning and Pre-Upgrade Procedures 34
3.1 Required Materials and Information 35
3.1.1 Application ISO Image File/Media 35
3.1.2 Logins, Passwords and Server IP Addresses 35

3.2 Plan Upgrade Maintenance Windows 38
3.2.1 Calculating Maintenance Windows Required 38
3.3 Site Upgrade Methodology Selection 39
3.3.1 DA-MP Upgrade Planning 41
3.3.2 Maintenance Window 1 (NOAM Site Upgrades) 43
3.3.3 Maintenance Window 2 and Beyond (SOAM Site Upgrades) 43
3.4 Prerequisite Procedures 47
3.4.1 Required Materials Check 47
3.4.2 Data Collection — Verification of Global and Site Configuration Data 48
3.4.3 DSR ISO Administration 67
3.4.4 ISO Link Correction 72
3.4.5 Full Backup of DB Run Environment at Each Server 74
3.4.6 IDIH Pre-Upgrade 79
3.5 Software Upgrade Execution Overview 79
3.5.1 Accepting the Upgrade 80
4. NOAM Upgrade Execution 81
4.1 NOAM Pre-Upgrade Checks and Backup 82
4.1.1 NOAM Health Check for Source Release 7.0.1, 7.1.x 82
4.1.2 NOAM Health Check for Source Release 7.2, 7.3, 7.4 86
4.1.3 NOAM Health Check for Source Release 8.0 and Later 89
4.1.4 NOAM Pre-Upgrade Backup 92
4.2 Disable Global Provisioning 93
4.3 NOAM Upgrade 94
4.3.1 PCA (Formerly PDRA) Topology Hiding Configuration 96
4.4 Verify NOAM Post Upgrade Status 98
4.5 Allow Provisioning (Post NOAM Upgrade) 100
4.6 Workaround to Avoid Device Deployment Alarm for IPFE Server (s) (Post-NOAM Upgrade) .. 101
5. Site Upgrade Execution 102
5.1 Site Pre-Upgrade Activities 102
5.1.1 Site Pre-Upgrade Backups 103
5.1.2 Site Pre-Upgrade Health Checks 107
5.1.3 Site Upgrade Options Check 113
5.1.4 Disable Site Provisioning 114
5.2 Automated Site Upgrade 115
5.2.1 Site Upgrade Pre-Checks 115
5.2.2 Initiate Automated Site Upgrade 116
5.3 Automated Server Group/Manual Upgrade Overview 119

5.3.1 Site Upgrade Planning 121
5.3.2 SOAM Upgrade Overview 123
5.3.3 Upgrade SOAMs 123
5.3.4 Upgrade Iteration 3 125
5.3.5 Upgrade Iteration 4 141
5.3.6 Upgrade Iteration 5 147
5.4 Site Post-Upgrade Procedures 150
5.4.1 Allow Site Provisioning 150
5.4.2 Site Post-Upgrade Health Checks 151
5.4.3 Post-Upgrade Procedures 157
6. Backout Procedure Overview 158
6.1 Recovery Procedures 160
6.2 Backout Health Check 160
6.3 Disable Global Provisioning 164
6.4 Perform Emergency Backout 164
6.4.1 Emergency Site Backout 164
6.4.2 Emergency NOAM Backout 166
6.5 Perform Normal Backout 167
6.5.1 Normal Site Backout 168
6.5.2 Normal NOAM Backout 171
6.6 Back Out Single Server 172
6.7 Back Out Multiple Servers 179
6.8 Post-Backout Health Check 186
6.9 IDIH Backout 187
6.9.1 Oracle Server Backout 187
6.9.2 Mediation and Application Server Backout 187
Appendix A. Post Upgrade Procedures 187
Appendix A.1. Accept Upgrade 187
Appendix A.2. Undeploy ISO 190
Appendix A.3. Reset COMCOL Compatibility Flags 191
Appendix A.4. PCA Post Upgrade Procedure 192
Appendix B. Increase Maximum Number of Open Files 192
Appendix C. PCRF Pooling Migration Check 196
Appendix D. Upgrade Single Server – DSR 8.x 199
Appendix E. Upgrade Single Server – Pre-DSR 8.0 206
Appendix F. Upgrade Multiple Servers – Upgrade Administration 218
Appendix G. Alternate Server Upgrade Procedures 227

Appendix G.1. Alternate Pre-Upgrade Backup 227
Appendix G.2. Server Upgrade Using platcfg 229
Appendix G.3. Manual DA-MP (N+0) Upgrade Procedure 232
Appendix G.4. Manual DA-MP (1+1) Upgrade Procedure 233
Appendix G.5. ASG SBR Upgrade Procedure 234
Appendix G.6. Manual SBR Upgrade Procedure 234
Appendix H. Expired Password Workaround Procedure 238
Appendix H.1. Inhibit Password Aging 238
Appendix H.2. Enable Password Aging 239
Appendix H.3. Password Reset 240
Appendix I. Network IDIH Compatibility Procedures 241
Appendix J. IDIH Upgrade at a Site 242
Appendix J.1. Oracle Guest Upgrade 243
Appendix J.2. Upgrade the Mediation and Application Guests 245
Appendix K. Recover From a Failed Upgrade 246
Appendix L. Critical and Major Alarms Analysis 251
Appendix M. Advanced Health Check 263
Appendix N. Workaround to Resolve DB Site Replication Alarms 265
Appendix O. Workaround to Resolve Server HA Failover 266
Appendix P. My Oracle Support (MOS) 266

List of Tables

Table 1: Acronyms 10
Table 2: Terminology 12
Table 3. Server Selection vs. Server Group Function 26
Table 4. Site Upgrade Availability vs. Server Group Function 28
Table 5: Logins, Passwords, and Server IP Addresses 35
Table 6. Traffic Analysis Checklist 39
Table 7. DA-MP Upgrade Planning Sheet 42
Table 8. Prerequisite Procedures Overview 47
Table 9. Release Specific Data Collection Procedures 49
Table 10. IDIH Upgrade Preparation Overview 79
Table 11. NOAM Upgrade Execution Overview 81
Table 12. Site Upgrade Execution Overview 103
Table 13. Non-PCA/PDRA Site Upgrade Plan 120
Table 14. Two-Site Redundancy PCA Site Upgrade Plan 120
Table 15. Three-Site Redundancy PCA Site Upgrade Plan 121

Table 16. Site Upgrade Planning Sheet 121
Table 17. Site Upgrade Execution Overview 122
Table 18. SOAM Upgrade Execution Overview 123
Table 19. Iteration 3 Upgrade Execution Overview 125
Table 20. Iteration 4 Upgrade Execution Overview. 142
Table 21. Iteration 5 Upgrade Execution Overview 148
Table 22. Emergency Backout Procedure Overview 158
Table 23. Normal Backout Procedure Overview 159
Table 24. IDIH Upgrade Execution Overview 242
Table 25. High Impact Alarms 251
Table 26. Medium Impact Alarms 255

List of Figures

Figure 1. Example Procedure Steps Used in This Document 14
Figure 2. DSR 8.0 Supported Upgrade Paths 19
Figure 3. DSR 8.1 Supported Upgrade Paths 20
Figure 4. Upgrade Perspective of DSR "Site" Topology 22
Figure 5. Site Upgrade – NOAM View 23
Figure 6. Site Upgrade - Entire Site View 24
Figure 7. Site Upgrade - Site Initiate Screen 25
Figure 8. Site Upgrade Monitoring 27
Figure 9. Server Group Upgrade Monitoring 27
Figure 10. Auto Site Upgrade General Options 28
Figure 11. Site Upgrade Active Tasks 30
Figure 12. Canceled Site Upgrade Tasks 30
Figure 13. Partially Upgraded Site 31
Figure 14. Restarting Site Upgrade 31
Figure 15. Active Tasks Screen 32
Figure 16. Site Accept Button 33
Figure 17. Site Accept Screen 34
Figure 18. Upgrade Maintenance Windows for 3-Tier Upgrade 38

List of Procedures

Procedure 1. Required Materials Check 47
Procedure 2. Verification of Configuration Data 48
Procedure 3. Data Collection for Source Release 7.0.1 50

Procedure 4. Data Collection for Source Release 7.1.x 54
Procedure 5. Data Collection for Source Release 7.2, 7.3, 7.4 59
Procedure 6. Data Collection for Source Release 8.0 and Later 63
Procedure 7. DSR ISO Administration 67
Procedure 8. ISO Link Correction 72
Procedure 9. Full Backup of DB Run Environment for Release 7.0.1 75
Procedure 10. Full Backup of DB Run Environment for Release 7.1.x and Later 77
Procedure 11. IDIH Upgrade Preparation 79
Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x 82
Procedure 13. NOAM Health Check for Source Release 7.2, 7.3, 7.4 86
Procedure 14. NOAM Health Check for Source Release 8.0 or Later 89
Procedure 15. NOAM Pre-Upgrade Backup 92
Procedure 16. Disable Global Provisioning 93
Procedure 17. NOAM Upgrade 94
Procedure 18. PCA (Formerly PDRA) Topology Hiding Configuration 96
Procedure 19. Verify NOAM Post Upgrade Status 98
Procedure 20. Allow Provisioning (Post NOAM Upgrade) 100
Procedure 21. Avoid the Device Deployment Failed Alarm On Affected Server(s) 101
Procedure 22. Site Pre-Upgrade Backups 104
Procedure 23. Site Pre-Upgrade Health Check for Release 8.0 and Later 107
Procedure 24. Site Pre-Upgrade Health Check for Release 7.x/8.x 110
Procedure 25. Site Upgrade Options Check 113
Procedure 26. Disable Site Provisioning 114
Procedure 27. Site Upgrade Pre-Checks 115
Procedure 28. Automated Site Upgrade 116
Procedure 29. SOAM Upgrade Pre-Checks 124
Procedure 30. Automated SOAM Upgrade (Active/Standby) 124
Procedure 31. Manual SOAM Upgrade (Active/Standby/Spare) 125
Procedure 32. Upgrade Iteration 3 126
Procedure 33. Upgrade Iteration 4 142
Procedure 34. Upgrade Iteration 5 148
Procedure 35. Allow Site Provisioning 151
Procedure 36. Site Post-Upgrade Health Check 152
Procedure 37. Alternate SOAM Post-Upgrade Health Check 155
Procedure 38. Post-Upgrade Procedures 157
Procedure 39. Backout Health Check 160
Procedure 40. Disable Global Provisioning 164

Procedure 41. Emergency Site Backout 165
Procedure 42. Emergency NOAM Backout 166
Procedure 43. Normal Site Backout 168
Procedure 44. Normal NOAM Backout 171
Procedure 45. Back Out Single Server 172
Procedure 46. Back Out Multiple Servers 179
Procedure 47. Post-Backout Health Check 186
Procedure 48. Oracle Server Backout 187
Procedure 49. Accept Upgrade 188
Procedure 50. Undeploy ISO 190
Procedure 51. Reset COMCOL Compatibility Flags 191
Procedure 52. PCA Post Upgrade Procedure 192
Procedure 53. Increase Maximum Number of Open Files 193
Procedure 54. PCRF Pooling Migration Check 196
Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x 199
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x 206
Procedure 57. Upgrade Multiple Servers – Upgrade Administration 218
Procedure 58. Alternate Pre-Upgrade Backup 227
Procedure 59. Server Upgrade Using Platcfg 229
Procedure 60. Manual DA-MP (N+0) Upgrade Procedure 232
Procedure 61. Manual DA-MP (1+1) Upgrade Procedure 233
Procedure 62. ASG SBR Upgrade 234
Procedure 63. Manual SBR Upgrade Procedure 234
Procedure 64. Expired Password Workaround Procedure 238
Procedure 65. Enable Password Aging 239
Procedure 66. Expired Password Reset Procedure 240
Procedure 67. Enable IDIH 8.x Compatibility 241
Procedure 68. Disable IDIH 8.x Compatibility 241
Procedure 69. Oracle Guest Upgrade 243
Procedure 70. Upgrade the Mediation and Application Guests 245
Procedure 71. Recover from a Failed Upgrade 246
Procedure 72. Verify Critical and Major Alarms in the System Before the Upgrade 251
Procedure 73. Advanced Health Check 263
Procedure 74. Restart the inetrep Process on the Affected Server(s) 265
Procedure 75. Resolve the HA Switchover Issue on Affected Server(s) 266

1. Introduction

1.1 Purpose and Scope

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

- Major upgrade from DSR 7.0.1, 7.1.x, 7.2, 7.3, 7.4, 8.0, to 8.1
- Incremental upgrade from an earlier DSR 8.1 build to a later 8.1 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.

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/8.0/8.1 software loads. It is recommended to contact MOS for the software loads as described in Appendix P.
- Initial installation of DSR software. Refer to [1].
- SDS installation. Refer to [2].

1.2 References

[1] DSR 8.0/8.1 Cloud Installation Guide

[2] SDS Cloud Installation document

[3] Maintenance Window Analysis Tool CGBU_010314

[4] DSR 6.0 to 7.0 Migration – IPFE Aspects, CGBU_770

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

[6] Cloud DSR 8.0/8.1 Disaster Recovery Guide

[7] Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) In DSR 7.1 By Enabling SCTP AUTH Extensions By Default, OSD 2019141.1

[8] DSR Alarms and KPIs Reference

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1: Acronyms

Acronym	Meaning
ASG	Automated Server Group upgrade
ASU	Automated Site Upgrade
CD-ROM	Compact Disc Read-only Media

Acronym	Meaning
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
SOAM	System OAM
TPD	Tekelec Platform Distribution

Acronym	Meaning
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, for example, DSR 7.0.1 to DSR 7.x or 8.0; or, for example, DSR 7.0.1 to 8.1 or DSR 8.0 to 8.1.
Incremental Upgrade	An upgrade within a given DSR release, for example, 8.0.x to 8.0.y and 8.1.x to 8.1.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 8.0/8.1 server from its current release to a newer release.
Backout	The process of converting a single DSR 8.0/8.1 server to a prior version. This could be performed due to failure in Single Server Upgrade or the upgrade cannot be accepted for some other reason. Backout is a user initiated process.
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 PMAC 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.
1+1	Set up with one active and one standby DA-MP.
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 My Oracle Support (MOS) for assistance, as described in Appendix P, before attempting to continue.

1.5.1 Executing Procedures

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

- Each step has a checkbox that the user should check-off to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- The title box describes the operations to be performed during that step.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Each command that the user enters, as well as any response output, is formatted in `10-point 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 My Oracle Support (MOS) as directed in Appendix P before starting the upgrade.

1.7.1 PCA/PDRA Application – PCRF Pooling Migration Precheck

If the source release is less than 7.1 and the PCA/PDRA application has been activated in the source release, PCRF Pooling MUST be enabled, and the PCRF Pooling Migration MUST be completed prior to the start of a major upgrade to DSR 8.0/8.1.

WARNING!

THE UPGRADE TO RELEASE 8.0/8.1 FAILS IF PCRF POOLING MIGRATION IS NOT COMPLETED WHEN THE PCA/PDRA APPLICATION IS ENABLED.

The PCRF Pooling Migration Tool is provided to determine the status of the PCRF Pooling Migration. The tool has options to determine if the migration is complete, to indicate if upgrade is allowed or not allowed, and to estimate the time required to complete the Pooling migration.

The upgrade to DSR 8.0/8.1 CANNOT be scheduled until the PCRF Pooling Migration Tool is run to determine the status of the migration. Pooling migration can take days or weeks to complete, depending on the PCA/PDRA configuration and when PCRF Pooling was enabled.

When the tool determines that pooling migration is completed, a flag is set internally, which allows the upgrade to proceed.

Refer to Appendix C: PCRF Pooling Migration Check for instructions on how to execute the PCRF Pooling Migration check.

The PCRF Pooling Migration Check is not required in the following scenarios:

1. The PCA/PDRA application has not been activated.
2. When upgrading from release 7.1, 7.2, 7.3, or 7.4 to 8.0 or 7.1,7.2, 7.3, 7.4, or 8.0 to 8.1 (in this case, pooling migration has already completed).
3. DSR 8.0 incremental upgrade.
4. DSR 8.1 incremental upgrade

1.7.2 PCA/PDRA Application – PCRF Pooling Enablement

For PCA/PDRA customers on Release 5.1, 6.0, or 7.0, PCRF Pooling must be enabled prior to upgrading to DSR 8.0. For upgrade to DSR 8.1, if customers are on Release 7.0.1, PCRF Pooling must be enabled prior to upgrading. In addition, a workaround is required to correlate binding-dependent session creation messages on IMSI or MSISDN without an APN. There are two possible workarounds, described in the following sections. It is recommended to ontact My Oracle Support (MOS) as directed in Appendix P on which option is best for the customer.

1.7.2.1 Option A – Using Mediation Rules

This section provides an outline of the steps required to implement the mediation workaround. Note that this is not a step-by-step procedure for creating and using the mediation rules, but rather an overview of the process.

1. Verify all APNs are mapped to the Default PCRF Pool.

- This ensures only one binding exists for a given subscriber even after enabling PCRF Pooling.

2. Configure ingress mediation rule to add a Called-Station-Id AVP (code=30, RFC 4005) to binding dependent session creation Diameter messages (for example, Rx AAR).
   - The AVP value must match one of the APNs that created the binding(s) for the subscriber.
   - Using this APN value, existing PDRA/SBR logic finds a bound PCRF and routes the Diameter message to it.
   - Since ALL APNs are bound to the same PCRF, it is not important what APN was used to find the binding as long as a binding is found.
3. Configure egress mediation rule to remove the Called-Station-Id AVP if it was added by mediation at ingress.
4. Enable PCRF Pooling and wait for the migration to complete.
   - All PCRF Pooling configuration requirements for binding capable interfaces must still be met.
5. Upgrade to DSR 8.0/8.1.

1.7.2.2 Option B – Patch

This section provides an outline of the steps required to implement the patch workaround. Note that this is not a step-by-step procedure for creating and using the patch.

1. Build patches on a customer-to-customer basis.
2. The patch:
   - Relaxes the mandate to have APNs in the binding dependent session creation request.
   - Finds the first final binding for the subscriber and return the PCRF identifier.
   - Routes the binding dependent session creation request to the bound PCRF.
3. Verify all APNs are mapped to the **Default** PCRF Pool.
   - This ensures only one binding exists for a given subscriber even after enabling PCRF pooling.
   - Enable PCRF Pooling and wait for the migration to complete.
   - All PCRF Pooling configuration requirements for binding capable interfaces must still be met.
2. Upgrade to DSR 8.0/8.1.

1.7.3 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 8.0/8.1, 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 8.0/8.1, SCTP multi-homed connection cannot be enabled if signaling firewall is already enabled.

1.7.4 NetBackup 7.7 Support

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

WARNING!

Upgrade DSR to release 8.0 or later before upgrading to NetBackup 7.7.

1.7.5 Network IDIH Compatibility

Upgrading an IDIH site to release 8.0/8.1 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 8.0/8.1.

To view network traces for a network of IDIH systems where there is a mix of systems running release 8.0/8.1 and systems running a prior release, Procedure 67 in Appendix I must be executed to prepare the systems running IDIH release 8.0/8.1 to support IDIH systems running the prior release. After executing Procedure 67, network traces should be viewed only from an IDIH system running the prior IDIH release. Viewing a network trace from an IDIH 8.0/8.1 results in a visualization that is incomplete because the IDIH 8.0/8.1 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 8.0/8.1, Procedure 68 should be executed on each IDIH system where Procedure 67 was previously executed to ensure that no errors occur when viewing network traces.

1.7.6 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.

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 8.0/8.1. An incremental upgrade advances the DSR from an earlier DSR 8.0/8.1 source release to a more recent 8.0/8.1 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 8.0.0.0.0-80.1.0 to 8.0.0.0.0-80.2.0 is an incremental upgrade. But, advancing a DSR running a 7.2 release to an 8.0 target release constitutes a major upgrade.

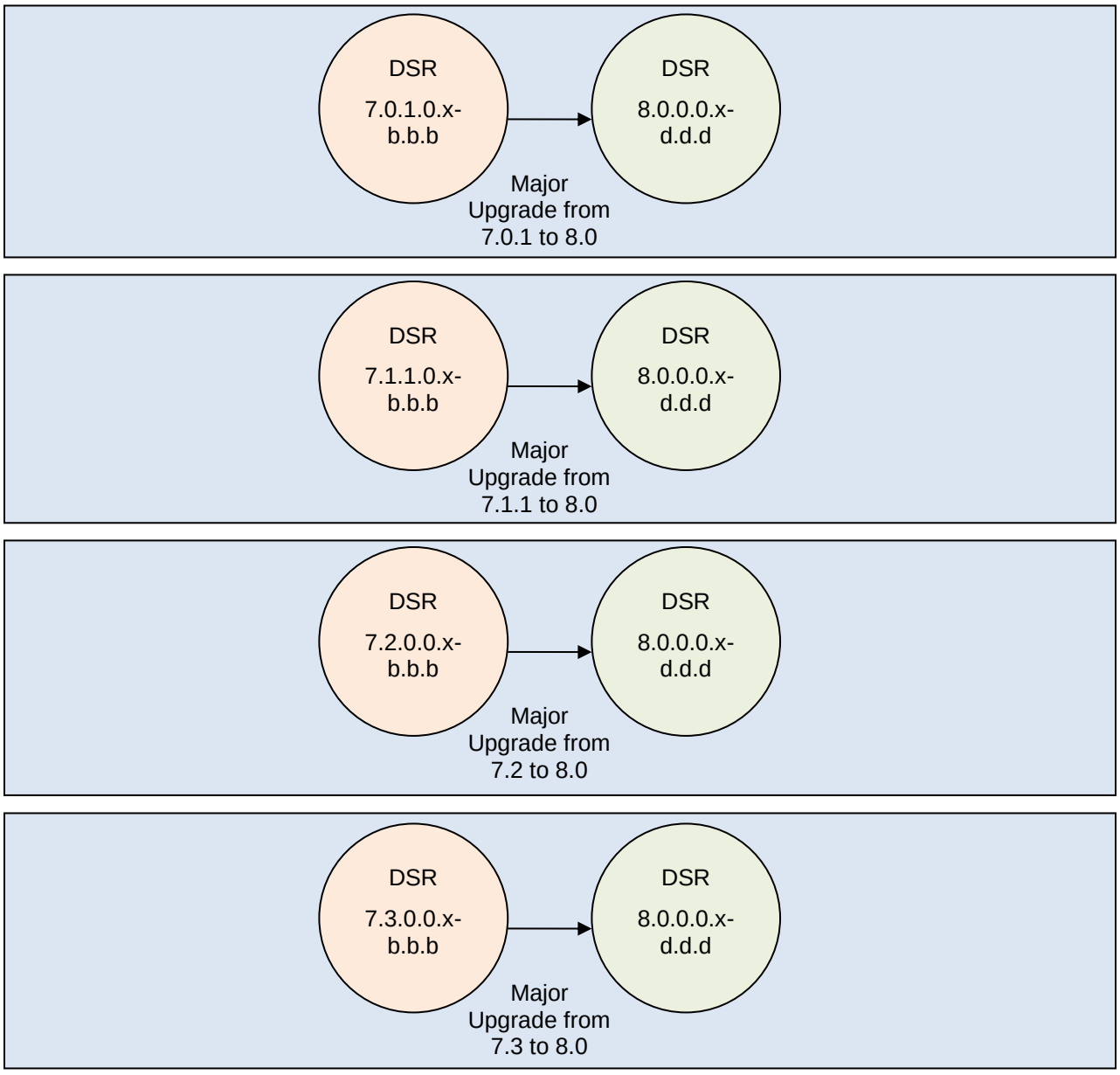
Similarly, for 8.1, for example advancing a DSR from 8.1.0.0.0_81.x.y to 8.1.0.0.0_81.z.k is an incremental upgrade. But advancing a DSR running a 7.1 release to an 8.1 target release constitutes a major upgrade.

From release 8.1, Virtual Signaling Transfer Point (vSTP) MP support is available. While upgrading from pre 8.1 releases, vSTP MP server is not in the system. So, after major upgrade is completed. In case vSTP server is required, it is freshly installed on the 8.1 release using reference [1]. For release 8.1, an incremental upgrade is supported for the vSTP MP server.

2.1 Supported Upgrade Paths to 8.0

The supported paths to upgrade to a DSR 8.0 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.



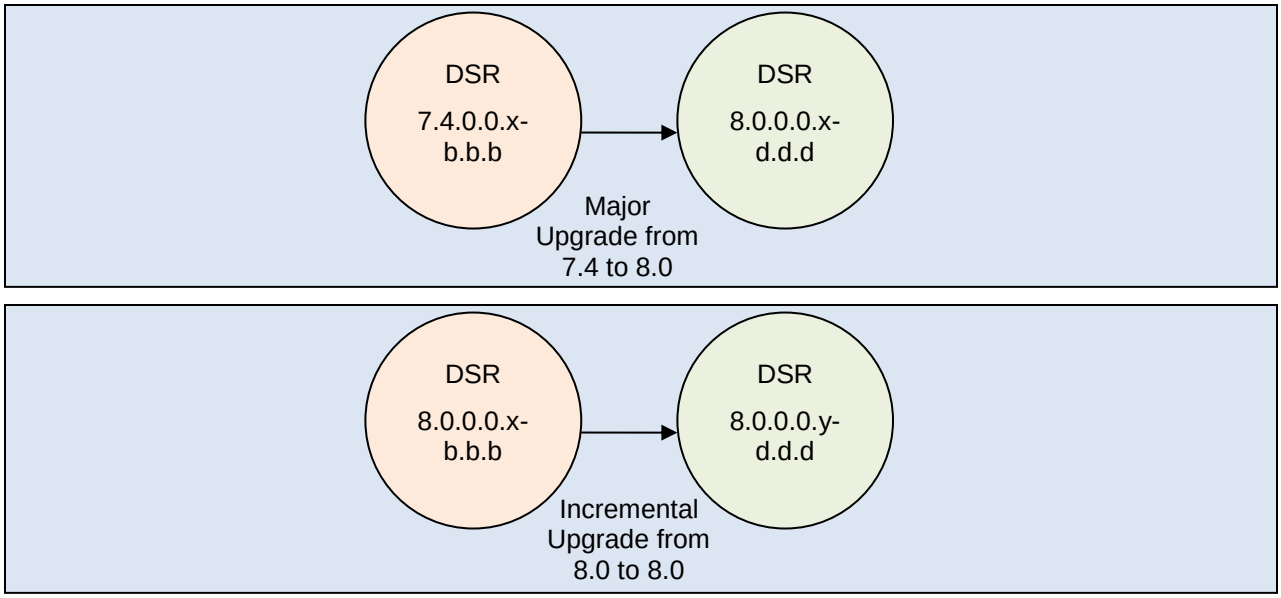
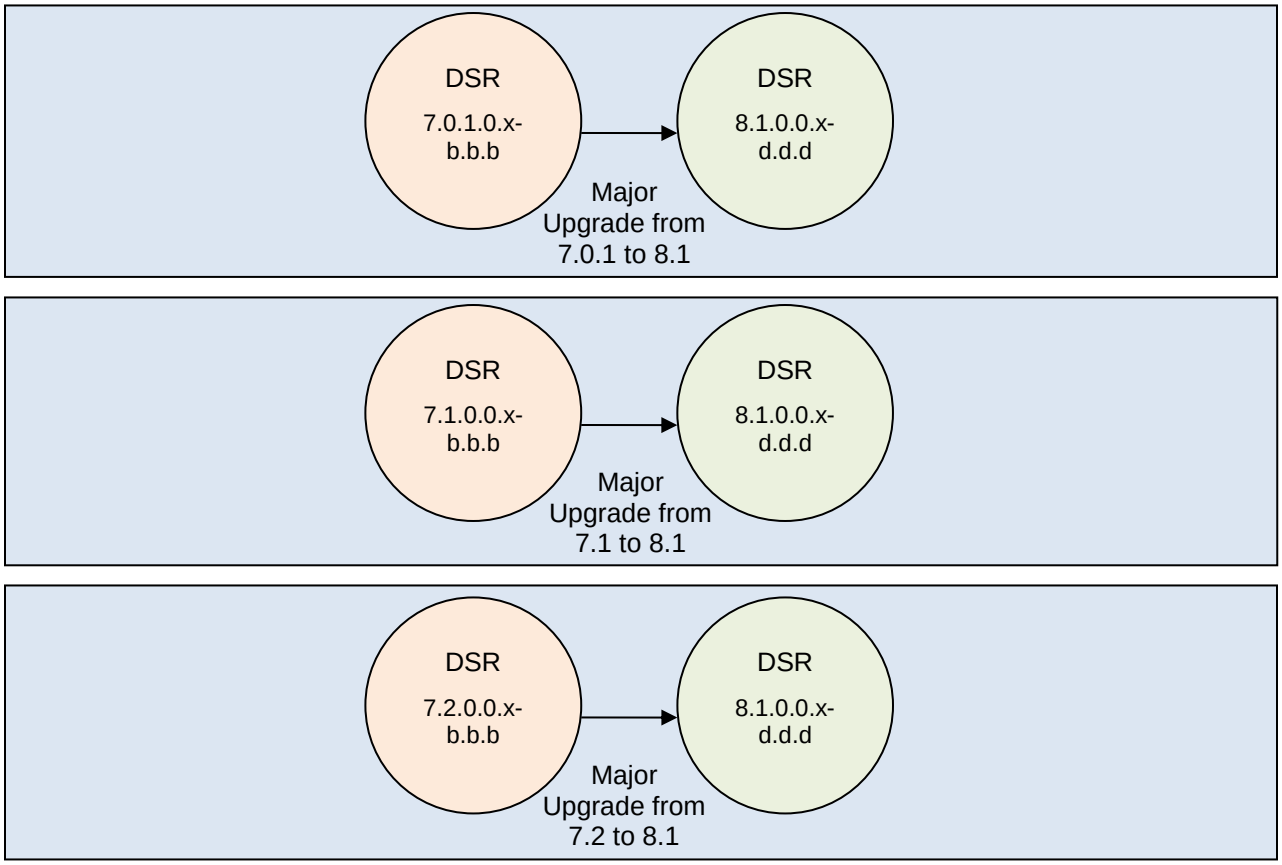


Figure 2. DSR 8.0 Supported Upgrade Paths

2.2 Supported Upgrade Paths to 8.1

The supported upgrade paths to a DSR 8.1 target release are shown in Figure 3.

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



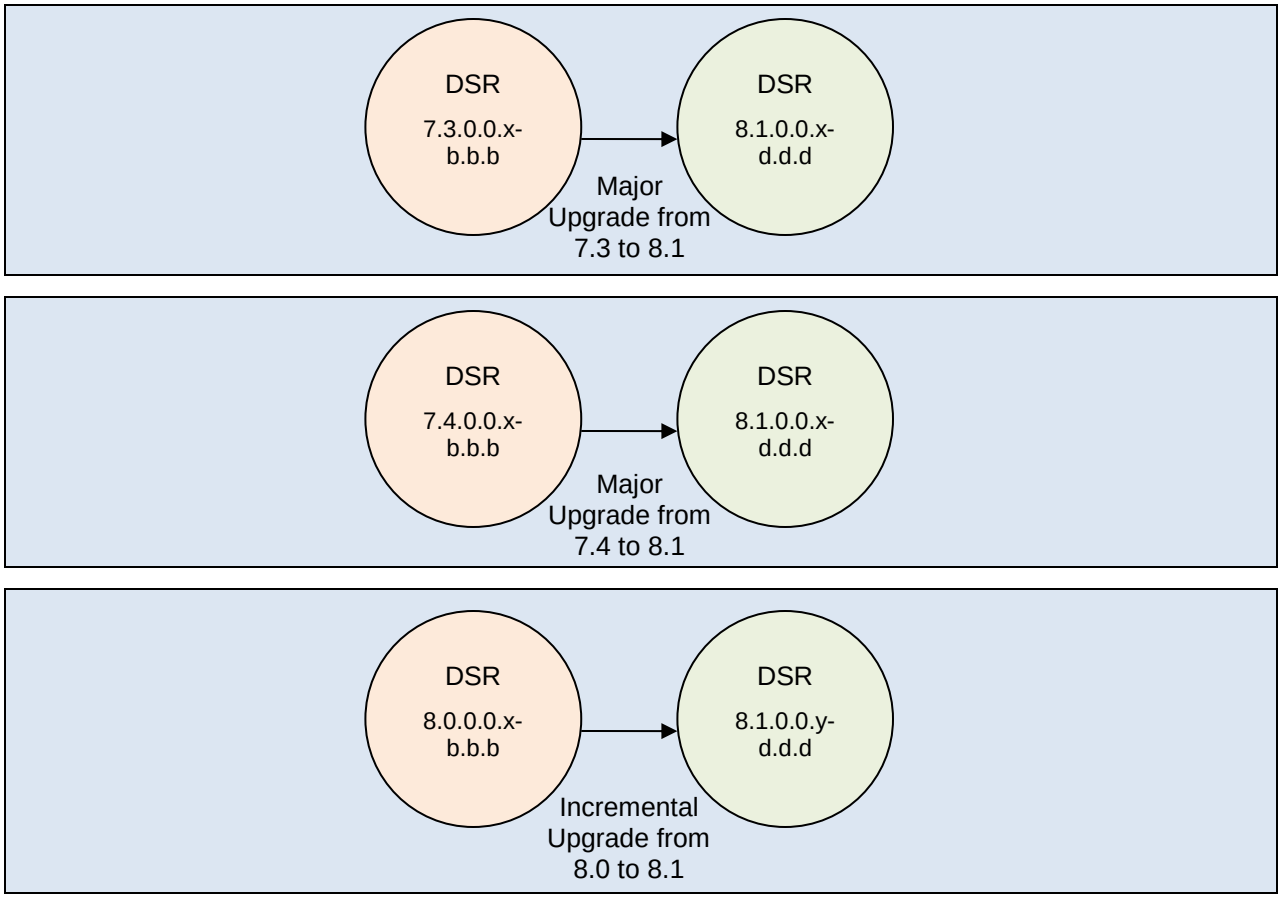


Figure 3. DSR 8.1 Supported Upgrade Paths

2.3 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.

2.4 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 7.1 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 [7]. It is highly recommended that customers upgrading to Release 8.0/8.1 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 8.0/8.1. In the event that the SCTP connections do not re-establish after the upgrade, follow the Disable/Enable DTLS procedure in [1].

2.5 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.

The Virtual Signaling Transfer Point (vSTP) MP server is introduced in release 8.1 but it does not support Automated Site Upgrade yet.

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 4 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 (for example, 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**.

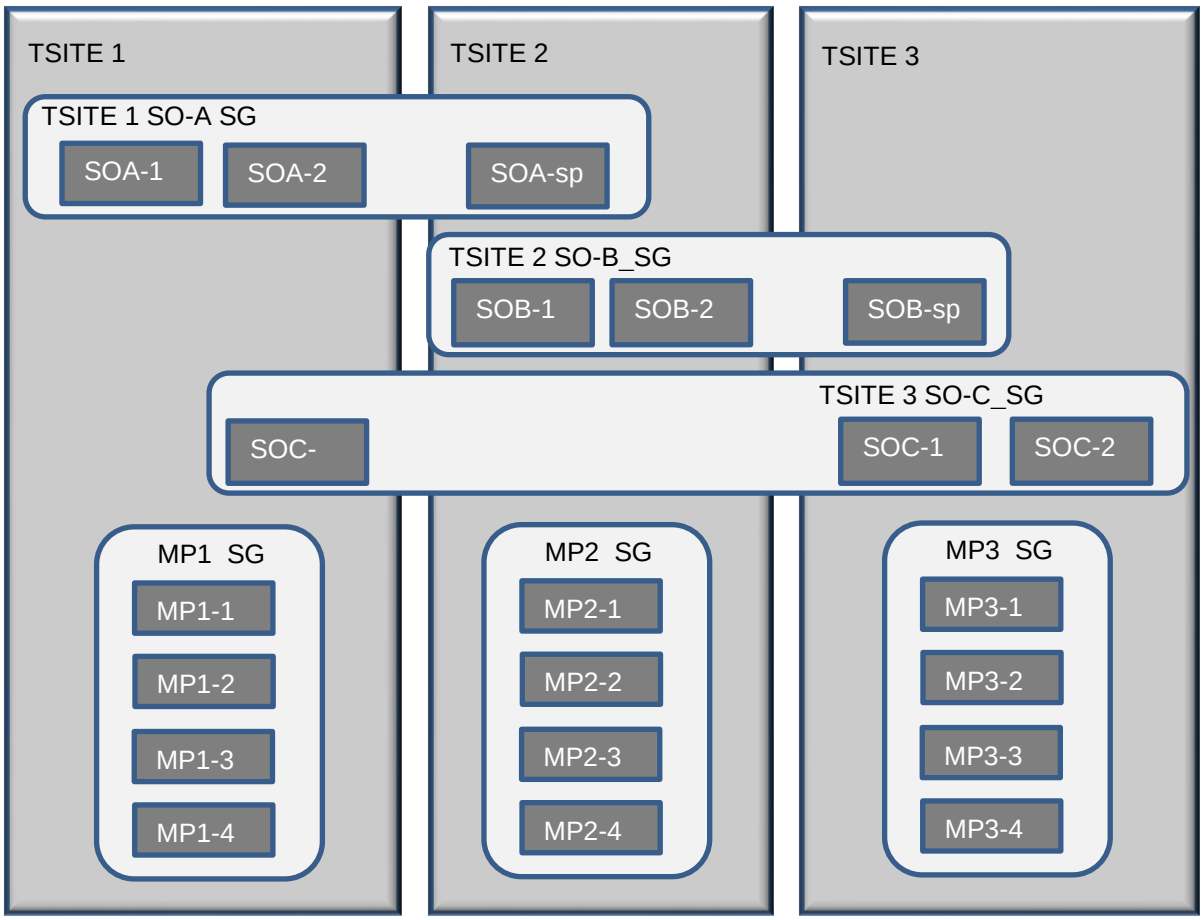


Figure 4. Upgrade Perspective of DSR "Site" Topology

2.5.1 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 5). When the NOAM server group tab is selected (as shown in Figure 5), 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).

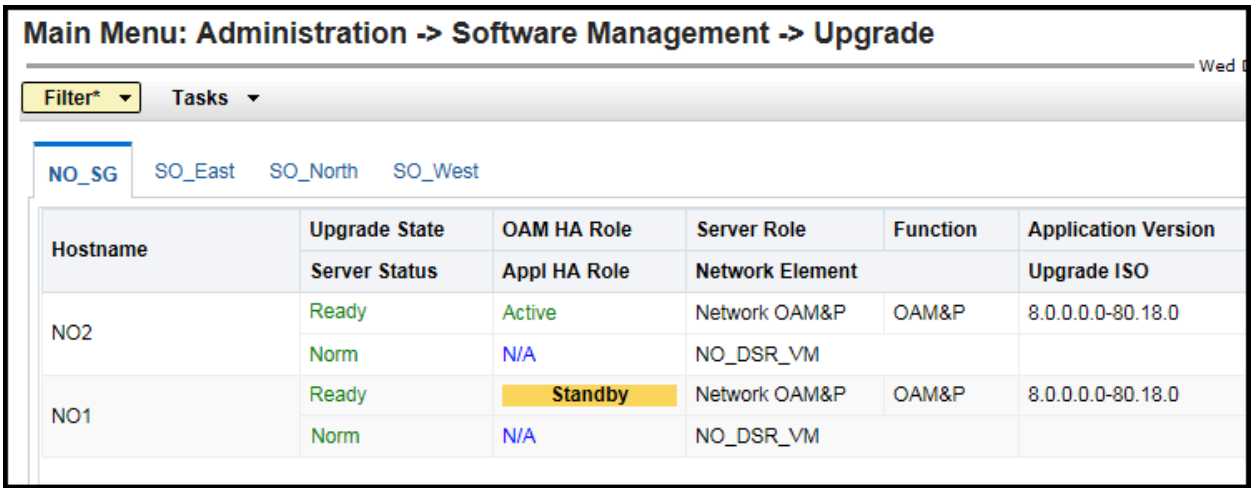


Figure 5. Site Upgrade – NOAM View

After selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen is displayed (Figure 6). 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 0 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.

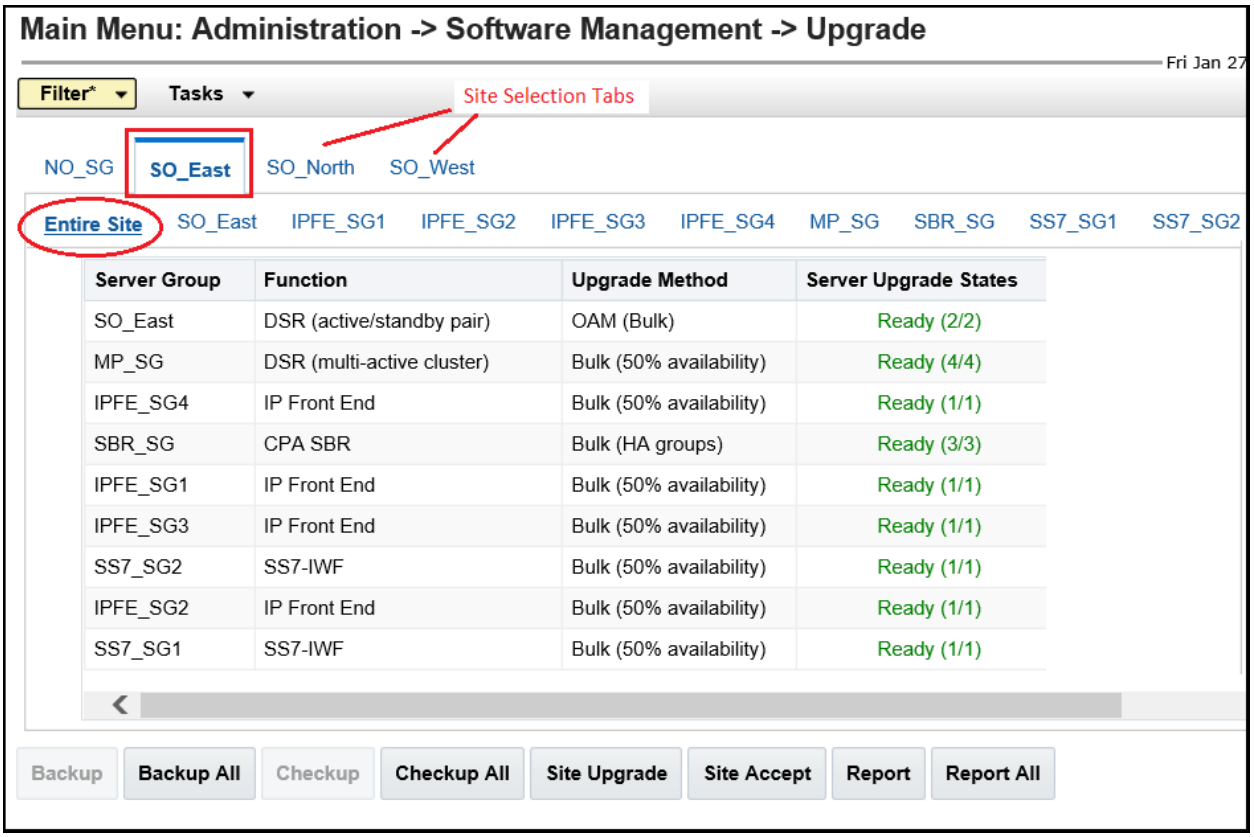


Figure 6. Site Upgrade - Entire Site View

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 7). The **Site Initiate** screen presents the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 7, 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 2.5.3.) 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.

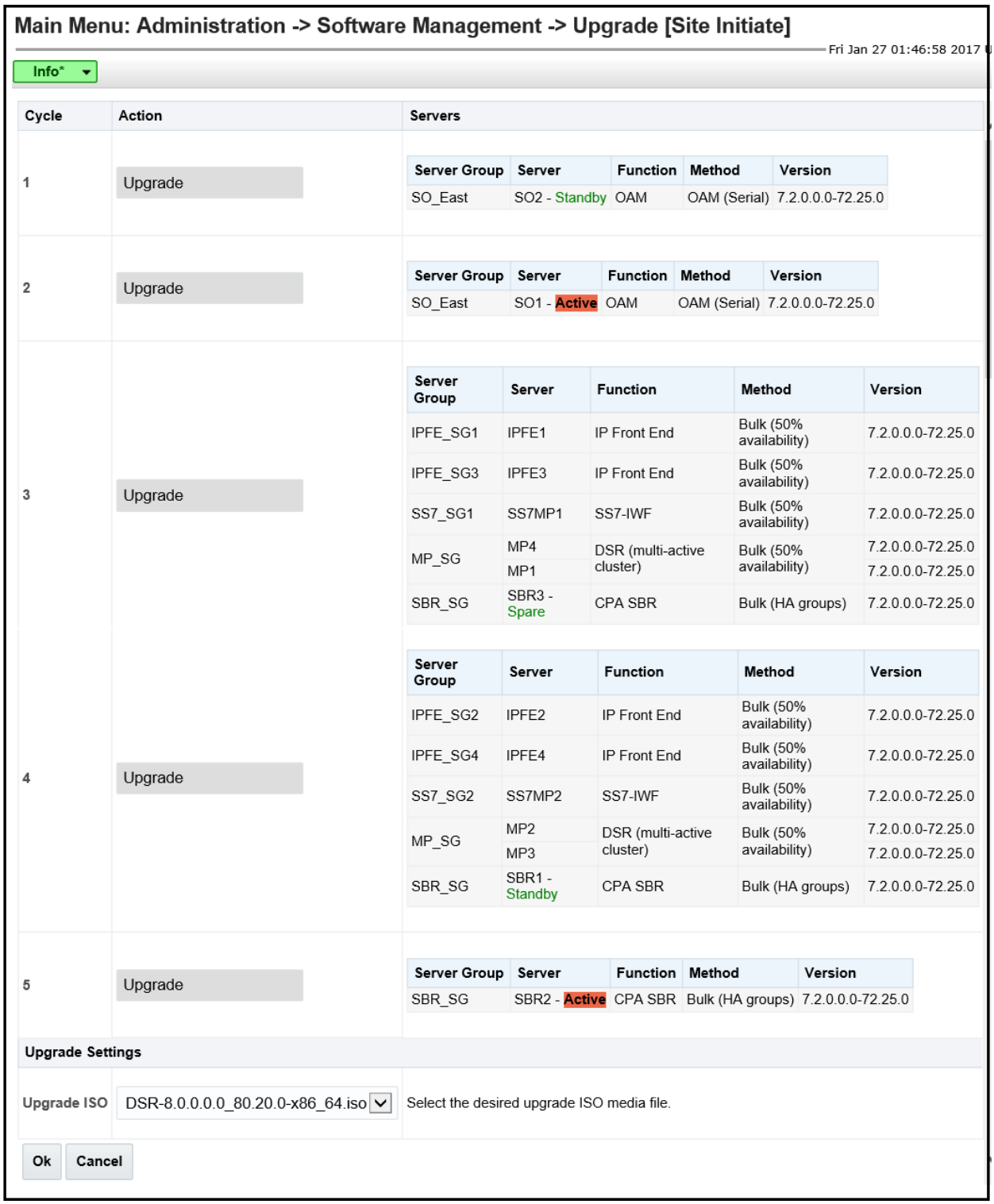


Figure 7. Site Upgrade - Site Initiate Screen

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

In Figure 7, 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 2.5.2.

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, DA-MP)	The DA-MP active/standby pair configuration is supported for Automated Site Upgrade starting with release 8.1.
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 0.
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.
SS7-IWF	SS7-MPs are treated as a multi-active cluster of servers, similar to DA-MPs, even though each server is in a separate server group. The selection of SS7-MPs 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.
STP	The Virtual Signaling Transfer Point (vSTP) MP server is introduced in release 8.1, but it does not support Automated Site Upgrade yet.

[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 7). Once the **OK** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 8). 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.

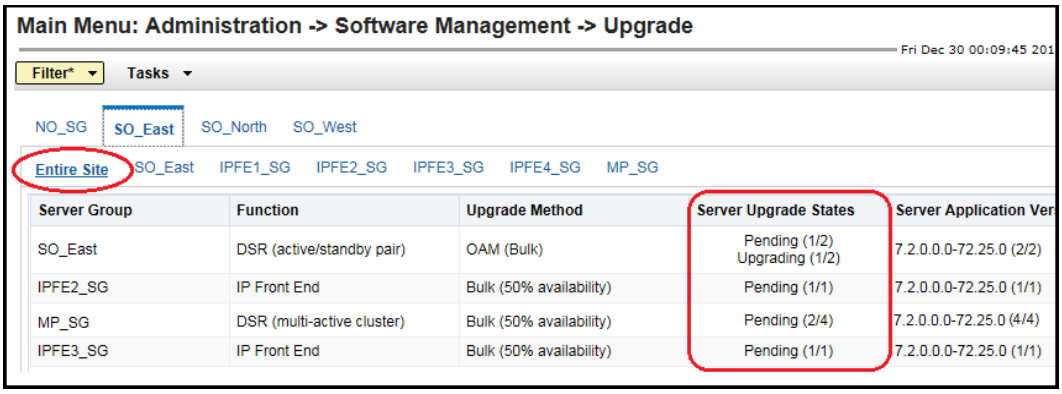


Figure 8. Site Upgrade Monitoring

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 9).

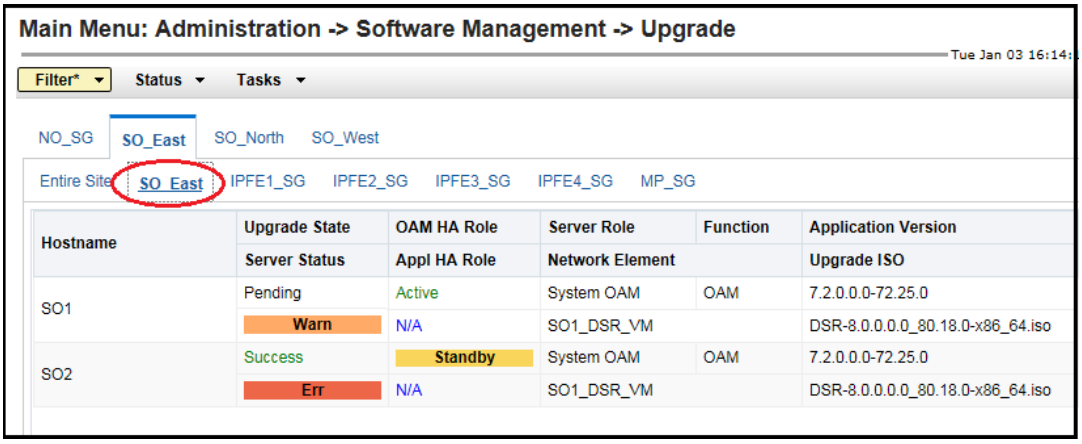


Figure 9. Server Group Upgrade Monitoring

Upon completion of a successful upgrade, every server in the site is in the **Accept** or **Reject** state. See Section 2.5.4 for a description of canceling and restarting the Automated Site Upgrade.

2.5.2 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 0.

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	Availability percentage applies to all IPFEs provisioned in the site. For this function type, the IPFE server groups are treated as a multi-active cluster of servers. To avoid a traffic outage, IPFE-A1 and IPFE-A2 are not upgraded together, and IPFE-B1 and IPFE-B2 are not upgraded together. IPFE-A1 and IPFE-B1 (as well as IPFE-A1 and IPFE-B2) may be upgraded together, if permitted by the availability percentage.
SS7-IWF	Availability percentage applies to all SS7-MPs provisioned in the site. For this function, the SS7-IWF server groups are treated as a multi-active cluster of servers. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.

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.

2.5.3 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 10). The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

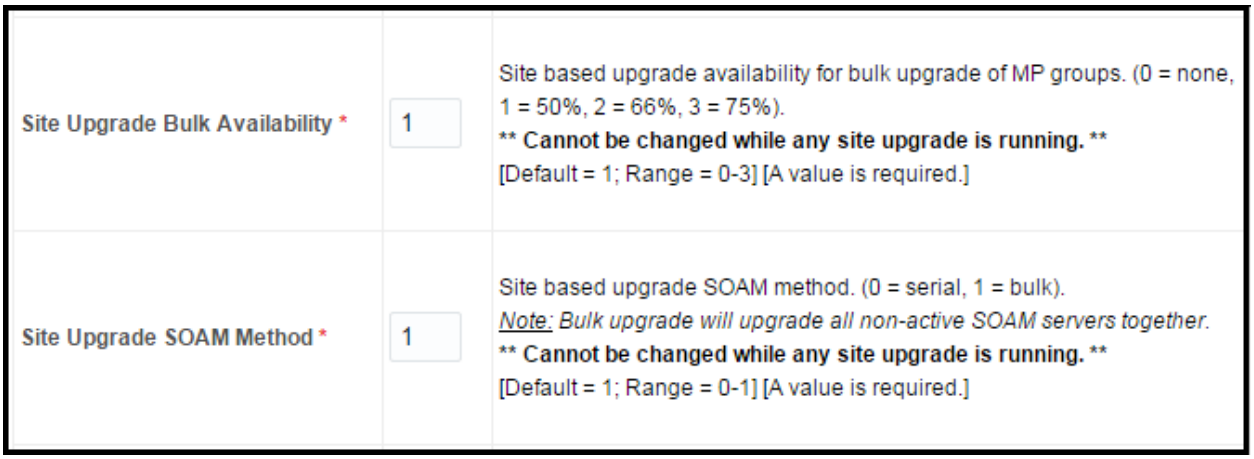


Figure 10. Auto Site Upgrade General Options

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. But for other server types, such as SS7-MP, there is only one server per server group. For this server type, the SS7-MP server groups are treated as a multi-active cluster of servers. The availability percentage applies across all of the SS7-MP server groups. 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
```

2.5.4 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 11, 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).

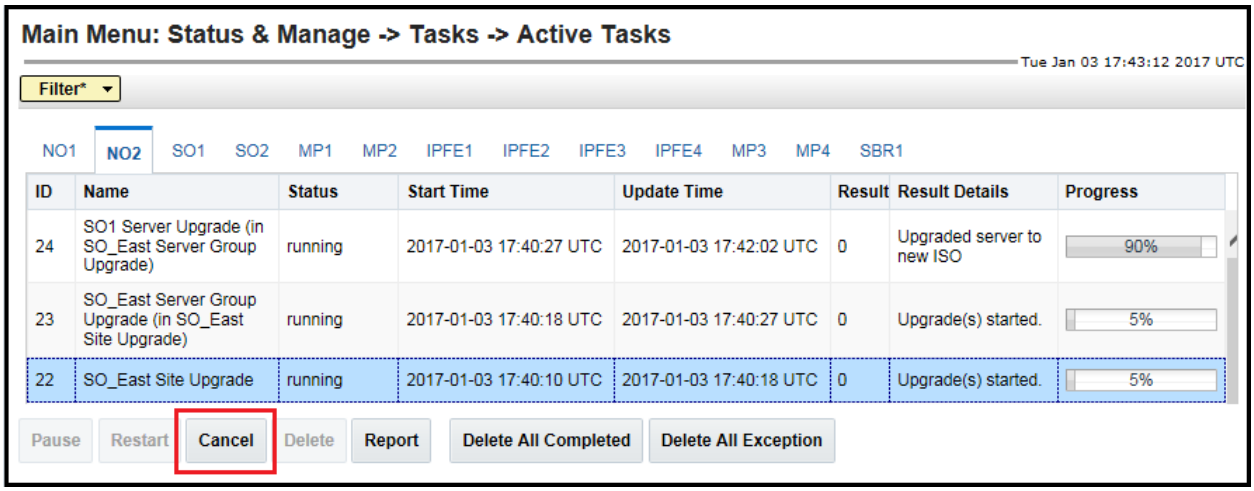


Figure 11. Site Upgrade Active Tasks

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 12 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.

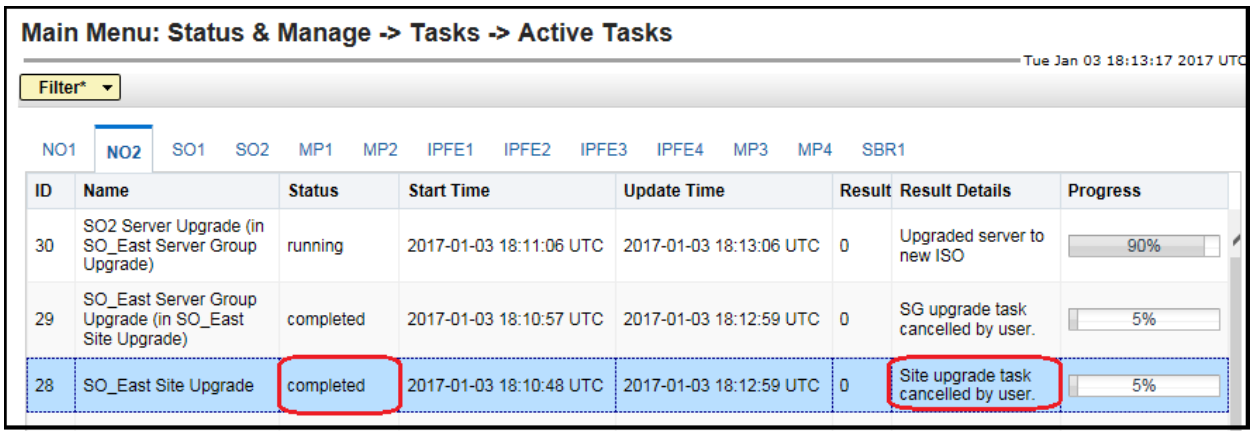


Figure 12. Canceled Site Upgrade Tasks

Figure 13 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.

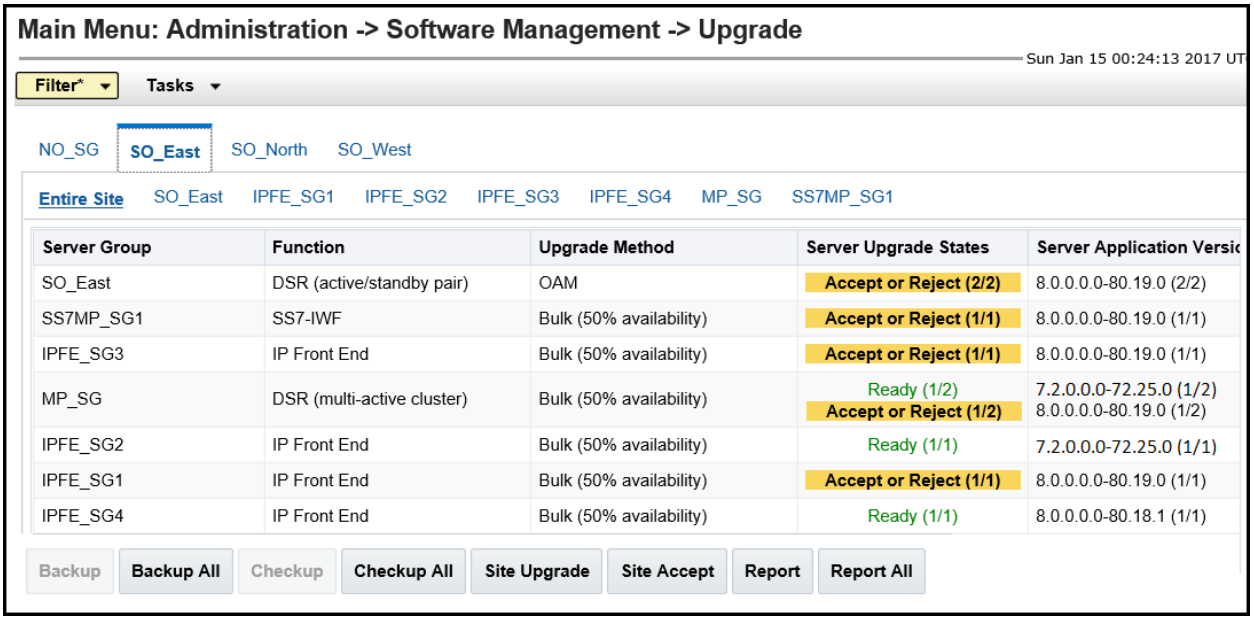


Figure 13. Partially Upgraded Site

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 12, 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.

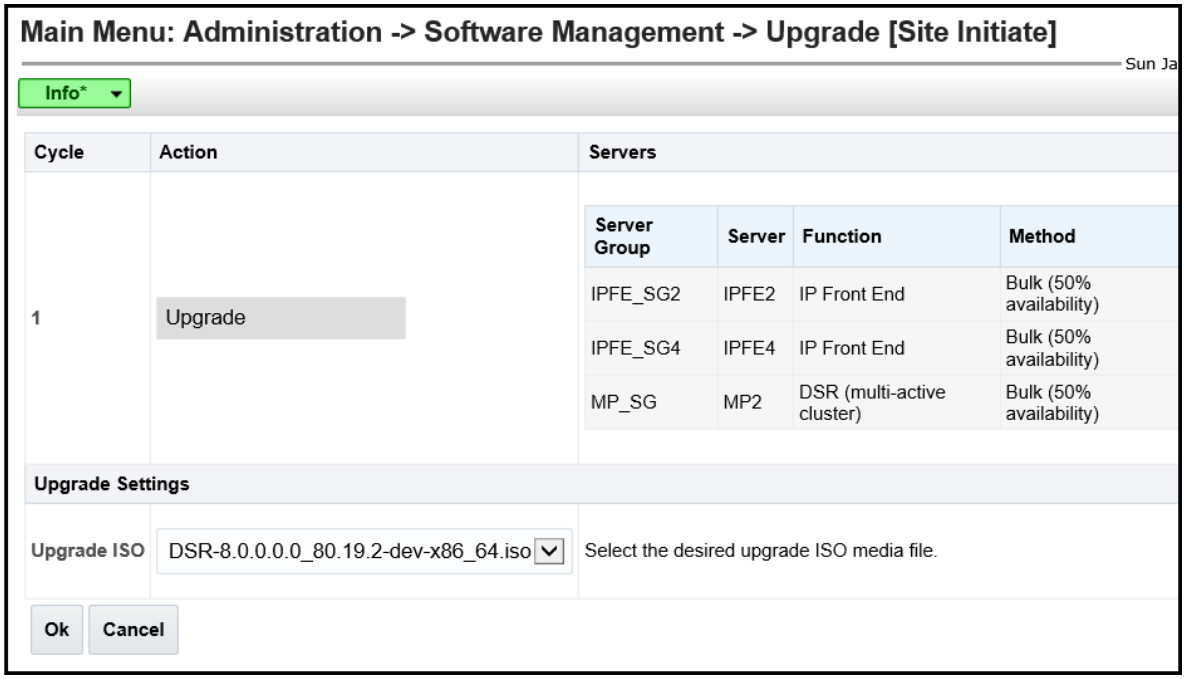


Figure 14. Restarting Site Upgrade

2.6 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.

2.6.1 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 15) 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 15, 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 15). Because the ASG task is canceled, no new server upgrades are initiated by the task.

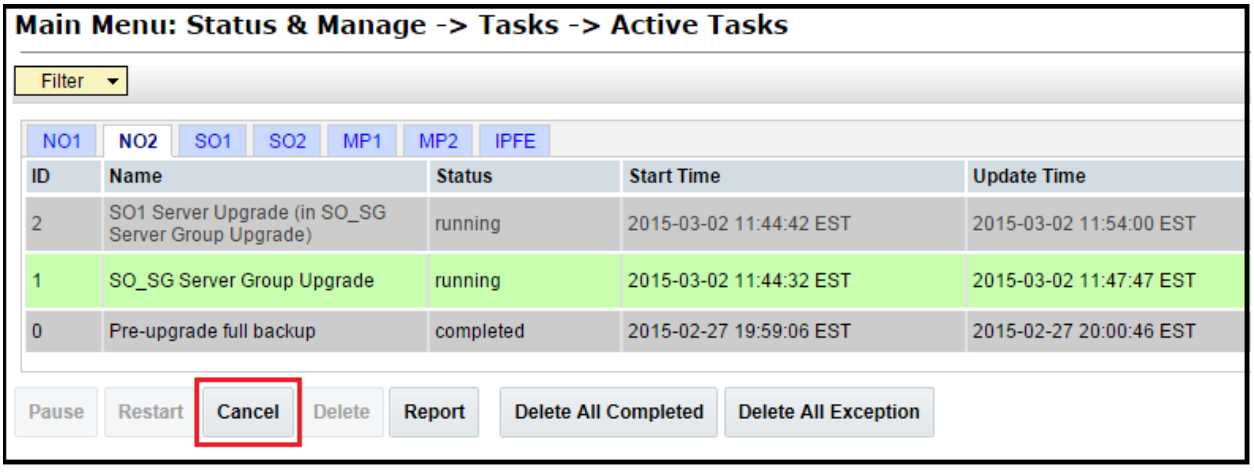


Figure 15. Active Tasks Screen

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.

2.6.2 Site Accept

Before DSR 8.0, the customer was required to **Accept** the upgrade of individual servers in each server group of a site. While the Accept is a relatively quick operation, it could nonetheless be a tedious task for larger sites with numerous servers. Starting with DSR 8.0, a new feature has been added to make the upgrade Accept much easier for all customers, large and small.

The **Site Accept** button on the upgrade GUI (Figure 16) 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 17) displays the servers that are ready for the Accept action.

Figure 16. 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**.

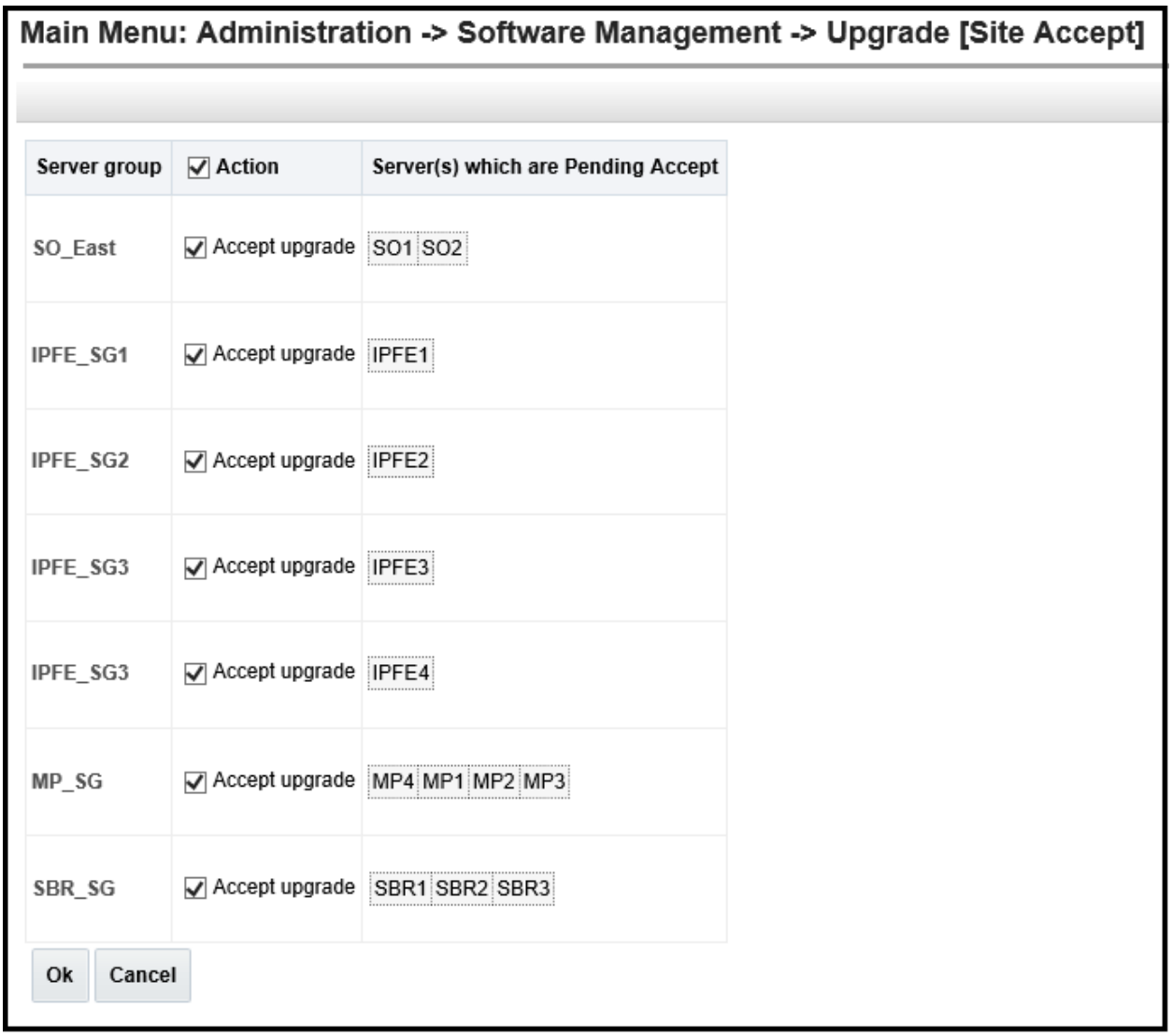


Figure 17. Site Accept Screen

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 Required Materials Check.

From release 8.1, vSTP MP support is available. While upgrading from pre-8.1 releases, the 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.

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-8.0.0.0.0_80.xx.0-x86_64.iso
```

AND

The DSR 8.1 ISO image file name is in the following format:

```
DSR-8.1.0.0.0_80.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]	

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

Item	Description	Recorded Value
	GUI Admin Password	
	DSR admusr Password[2]	
	DSR Root Password[2]	
VPN Access Details	Customer VPN information (if needed)	
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)	

[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.

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

Item	Description	Recorded Value
	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)	
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)	
SS7-IWF Server Groups	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
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.

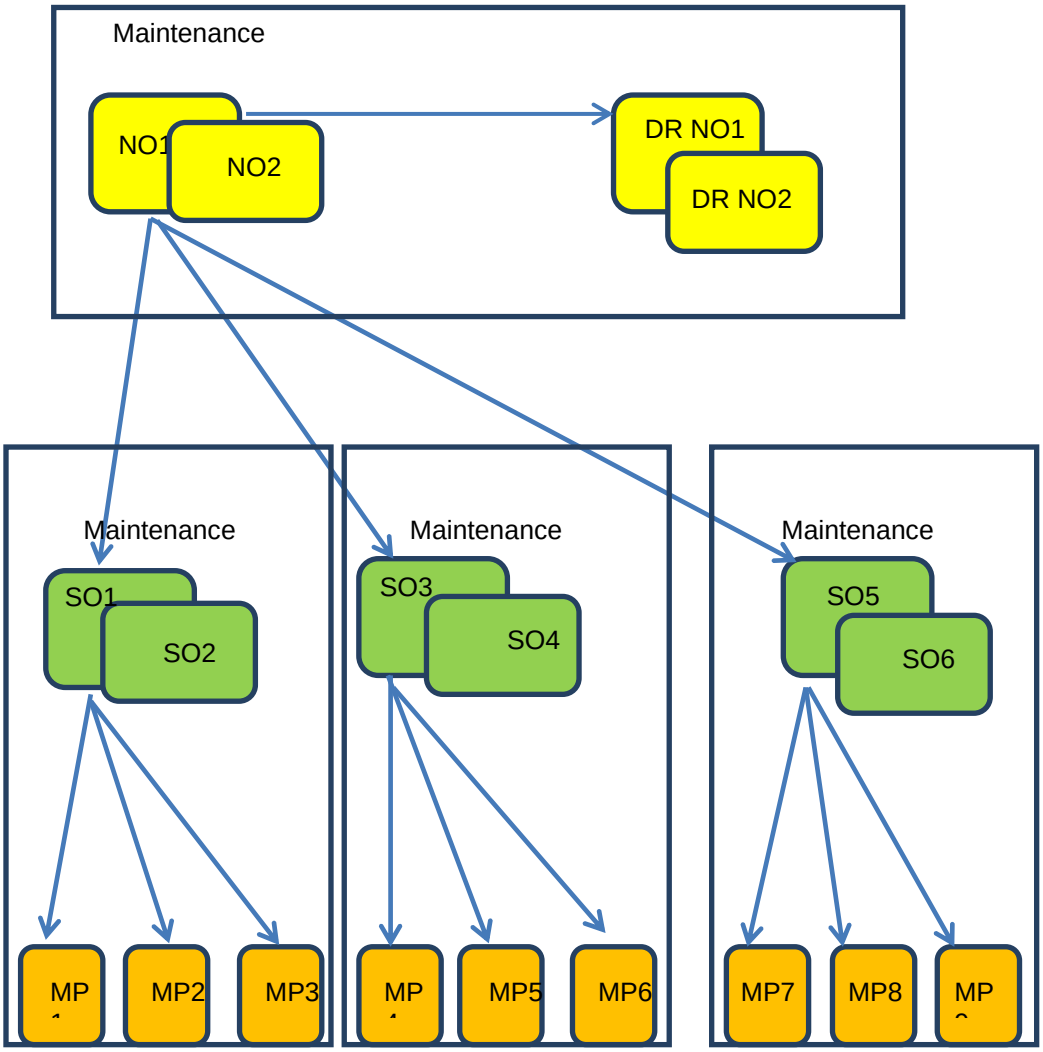


Figure 18. Upgrade Maintenance Windows for 3-Tier Upgrade

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

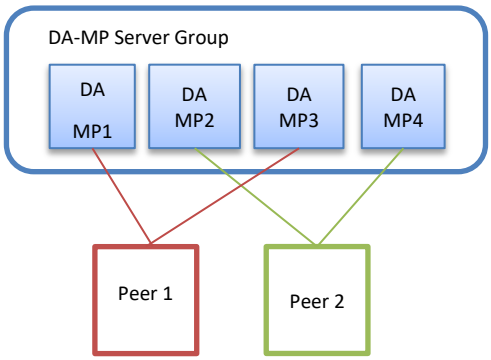
need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in Reference [3]. Please see the instructions tab of the spreadsheet for more information and details.

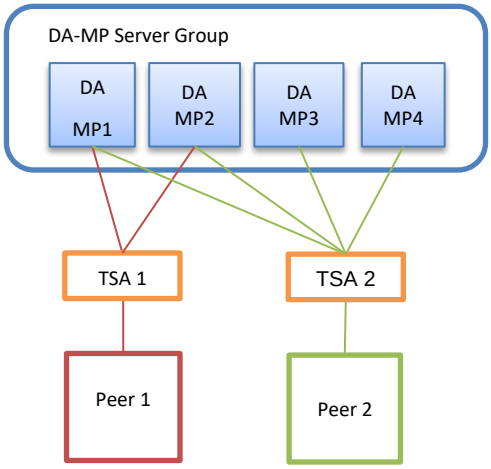
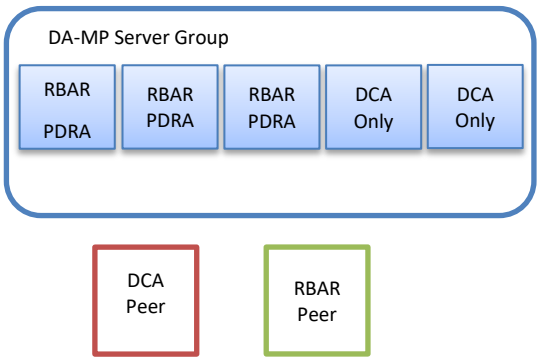
3.3 Site Upgrade Methodology Selection

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 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) are upgraded simultaneously, thereby isolating the peer. Automated Site Upgrade and Auto Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. 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 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) are upgraded simultaneously, thereby isolating the peer. Automated Site Upgrade and Auto Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. 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 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) are upgraded simultaneously, thereby eliminating service functionality. Automated Site Upgrade and Auto Server Group Upgrade should not be used for this configuration. If yes, proceed to step 8. If no, continue with step 4.
4.	Is the DA-MP server group in the active/standby pair (1+1) configuration?	☐	☐	Starting with release 8.1, the DA-MP active/standby pair is supported for Automated Site Upgrade. The site is a candidate for Auto Server Group upgrade. If yes, proceed to step 7. If no, continue with step 5.

	Criteria	Yes	No	Notes
5.	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.
6.	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.
7.	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.
8.	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**.

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 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): _____

3.3.3 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 (for example, 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**: _____ ***Note***: For 1+1 configuration, only 2 DA-MP(s) are present, one is Active while the other is Standby.	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: _____
	☐ SS7-MP1: _____ ☐ SS7-MP2: _____ ☐ SS7-MP3: _____ ☐ SS7-MP4: _____ ☐ SS7-MP5: _____ ☐ SS7-MP6: _____ ☐ SS7-MP7: _____ ☐ SS7-MP8: _____
	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	Required Materials Check
Procedure 2	0:20-0:30	0:30-1:00	Verification of Configuration Data
Procedure 3 or Procedure 4 or Procedure 5 or Procedure 6	0:45-2:00 0:45-1:00 0:15-0:20 0:15-0:20	1:15-3:00 1:15-2:00 0:45-1:20 0:45-1:20	Data Collection for Source Release 7.0.1 Data Collection for Source Release 7.1.x Data Collection for Source Release 7.2, 7.3, 7.4 Data Collection for Source Release 8.0 and Later
Procedure 7[1]	0:15-3:001	1:00-6:00	DSR ISO Administration
Procedure 8	0:05	1:05-6:05	ISO Link Correction
Procedure 9 or Procedure 10	0:10-2:00	1:15-8:05	Full Backup of DB Run Environment for Release 7.0.1 or Full Backup of DB Run Environment for Release 7.1.x and Later

[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

S T E P #	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 My Oracle Support (MOS) 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.

Procedure 1. Required Materials Check

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 P for these instructions. ***Note***: Obtaining a new online support account can take up to 48 hours.

3.4.2 Data Collection — Verification of Global and Site Configuration Data

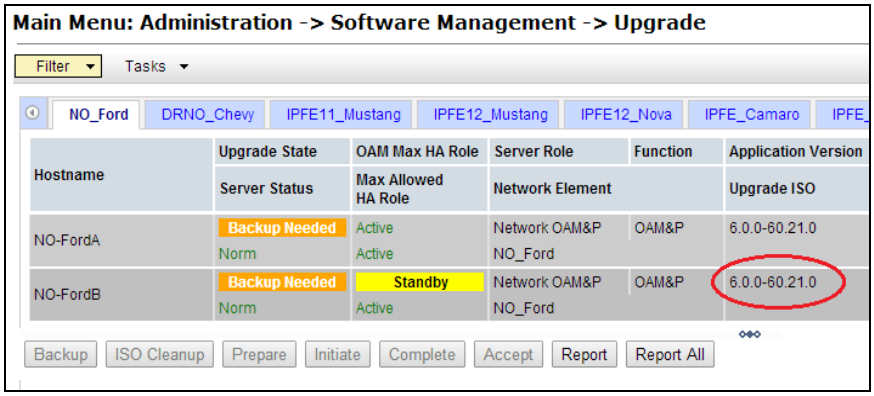
The procedures in this section are part of software upgrade preparation and are used to collect data required for network analysis, disaster recovery, and upgrade verification. Data is collected from both the active NOAM and various other servers at each site.

3.4.2.1 Verification of Configuration Data

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

Procedure 2. Verification of Configuration Data

S T E P #		
	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 My Oracle Support (MOS) 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.



Procedure 2. Verification of Configuration Data

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
7.0.x	Data Collection for Source Release 7.0.1
7.1.x	Data Collection for Source Release 7.1.x
7.2, 7.3, or 7.4	Data Collection for Source Release 7.2, 7.3, 7.4
8.0 and later	Data Collection for Source Release 8.0 and Later

3.4.2.2 Data Collection for Source Release 7.0.1

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.0.1.

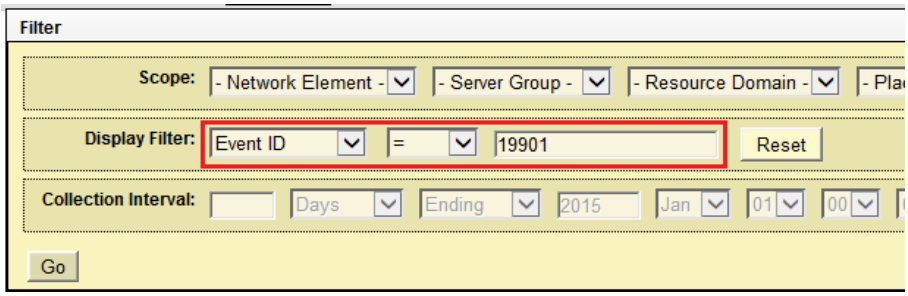
Procedure 3. Data Collection for Source Release 7.0.1

S T E P #		
	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 My Oracle Support (MOS) and ask for assistance.	

1. ☐	**Active SOAM CLI**: Database consistency check	Check the transport connections tables.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Enter these commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		`iqt -zhp ConnectionAdmin | wc -l`
		`iqt -zhp TransportConnection | wc -l`
		Sample output:
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		3. If the entry counts match, proceed to step 2.
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, do not proceed with the upgrade. It is recommended to consult with My Oracle Support (MOS) before continuing.

Procedure 3. Data Collection for Source Release 7.0.1

2. ☐	**Server CLI**: Verify uptime for each server in the topology	Starting with the active NOAM, execute this procedure.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server using the server XMI IP Address.
		`ssh admusr@<target_server_XMI_IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Execute the **uptime** command:
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		`02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		3. Record the hostname of any server with an uptime value > 200 days.
		4. Inform the customer that a cold reboot is required for all servers with an uptime value > 200 days before beginning any upgrade activity.
		Note: This is required response due to **Red Hat Bug 765720**. It is recommended to contact My Oracle Support (MOS) if instruction is needed on how to gracefully perform a cold reboot.
		5. Repeat steps 1 through 4 for each server in the topology.

3. ☐	Repeat checks	Repeat steps 1 through 4 for each SOAM site in the topology.
4. ☐	**Active NOAM VIP**: Alarm check	Check for the presence of **Alarm 19901 – CFG-DB Validation Error**. 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  If the filter returns no results, the database is consistent; proceed to the next step. Otherwise, do not proceed with the upgrade until the alarm is cleared. It is recommended to consult with My Oracle Support (MOS) for guidance if the alarm does not clear within 60 minutes.

Procedure 3. Data Collection for Source Release 7.0.1

5. ☐	**Active NOAM VIP**: Verify IPFE Server Groups	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE Server Group. Verify that each IPFE Server Group is configured with one, **and only one**, IPFE server. 4. If any IPFE Server Group contains more than one IPFE server, refer to the Server Group Configuration procedure of [1] to correct the configuration.
6. ☐	**Active NOAM VIP**: Verify and collect Network Element Configuration data	1. Navigate to **Configuration > Network Elements** to view Network Elements Configuration screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
7. ☐	**Active NOAM VIP**: Verify and collect Server Group Configuration data	1. Navigate to **Configuration > Server Groups** to view the Server Group screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
8. ☐	**Active NOAM VIP**: Verify and collect Server Configuration data	1. Navigate to **Configuration > Servers** to view the Server screen 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
9. ☐	**Active NOAM VIP**: Verify and collect Services Configuration data	1. Navigate to **Configuration > Services** to view Services screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.

Procedure 3. Data Collection for Source Release 7.0.1

10. ☐	**Active NOAM VIP**: Verify and collect Signaling Network Configuration data for DSR	1. Navigate to **Configuration > Network** to view the Signaling Networks. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference. 5. Navigate to **Configuration > Network > Devices**. 6. Click **Report All** at the bottom of the table to generate a report for all entries. 7. Save the report and/or print the report. Keep these copies for future reference. 8. Navigate to **Configuration > Network > Routes**. 9. Click **Report All** at the bottom of the table to generate a report for all entries. 10. Save the report and/or print the report. Keep these copies for future reference.
11. ☐	**Active NOAM VIP**: Verify Server Status is Normal – NOAM	1. Navigate to **Status & Manage > Server**. 2. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). Do not proceed with the upgrade if any server status displayed is not **Norm**. Do not proceed if there are any Major or Critical alarms. Refer Appendix L for details.
12. ☐	**Active NOAM VIP**: Log all current alarms at 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. Keep these copies for future reference. ***Note***: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
13. ☐	**Active NOAM VIP**: View Communication Agent status for all connections	1. Navigate to **Communication Agent > Maintenance > Connection Status**. 2. Verify the Connection Status of each connection is InService.

Procedure 3. Data Collection for Source Release 7.0.1

14. ☐	**Active NOAM VIP**: View SBR status (if equipped) if PDRA/PCA is enabled	**If the active NOAM is on release 7.0.x, 7.1.x:** 1. Navigate to **Policy and Charging > Maintenance > SBR Status**. 2. Select the Binding tab. 3. Expand each Server Group. 4. Verify Congestion Level is **Normal** for all servers. 5. Repeat sub-steps 3 and 4 for the PDRA Mated Triplet tab. **If the active NOAM is on release 7.2 and later:** 6. Navigate to **SBR > Maintenance > SBR Status**. 7. Select the Binding tab. 8. Expand each Server Group. 9. Verify Congestion Level is **Normal** for all servers. 10. Repeat sub-steps 3 and 4 for the PCA Mated Triplet tab.
15. ☐	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 3.4.2.1 and steps 1 through 16 of this procedure. 2. It is recommended to plan for MP upgrades by consulting Section My Oracle Support (MOS) to assess the impact of out-of-service MP servers 3. Determine the exact sequence in which MP servers are upgraded for each site.

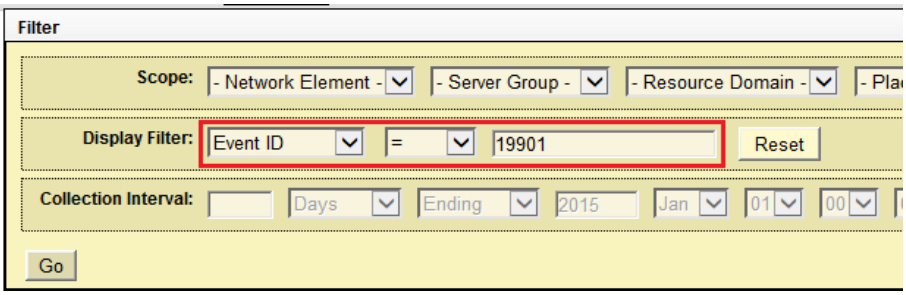
3.4.2.3 Data Collection for Source Release 7.1.x

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.1.x.

Procedure 4. Data Collection for Source Release 7.1.x

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM VIP**: Verify IPFE server groups are properly configured	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE server group. Verify each IPFE server group is configured with one, **and only one**, IPFE server. If any IPFE server group contains more than one IPFE server, DO NOT PROCEED WITH THE UPGRADE. It is recommended to consult with My Oracle Support (MOS) before continuing.

Procedure 4. Data Collection for Source Release 7.1.x

2. ☐	**Active NOAM VIP**: Alarm check	Check for the presence of **Alarm 19901 – CFG-DB Validation Error**. 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  4. If the filter returns no results, the database is consistent; proceed to the next step. Otherwise, do not proceed with the upgrade until the alarm is cleared. It is recommended to consult with My Oracle Support (MOS) for guidance if the alarm does not clear within 60 minutes.

Procedure 4. Data Collection for Source Release 7.1.x

3. ☐	**Active NOAM CLI**: Verify NOAM pre-upgrade status	Execute this step on the active DSR NOAM and active DR NOAM servers.
		1. Use an SSH client to connect to the active NOAM:
		`ssh admusr@<NOAM 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 preUpgradeHealthCheck`
		This command creates three files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<NOserver_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.

Procedure 4. Data Collection for Source Release 7.1.x

4. ☐	**Server CLI**: Verify uptime for each server in the topology	Starting with the active NOAM, execute this procedure.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server using the server XMI IP address.
		`ssh admusr@<target_server_XMI_IP>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.
		2. Execute the **uptime** command:
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		`02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		3. Record the hostname of any server with an uptime value > 200 days.
		4. Inform the customer that a cold reboot is required for all servers with an uptime value > 200 days before beginning any upgrade activity.
		Note: This is a required response due to **Red Hat Bug 765720**. It is recommended to contact My Oracle Support (MOS) if instruction is needed on how to gracefully perform a cold reboot.
		5. Repeat steps 1 through 4 for each server in the topology.

5. ☐	**Active SOAM CLI**: Database consistency check	Check the transport connections tables.
		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. Enter these commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		`iqt –zhp ConnectionAdmin | wc –l`
		`iqt –zhp TransportConnection | wc –l`
		Sample output:
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		3. If the entry counts match, proceed to step 6.
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, do not proceed with the upgrade. It is recommended to consult with My Oracle Support (MOS) before continuing.

Procedure 4. Data Collection for Source Release 7.1.x

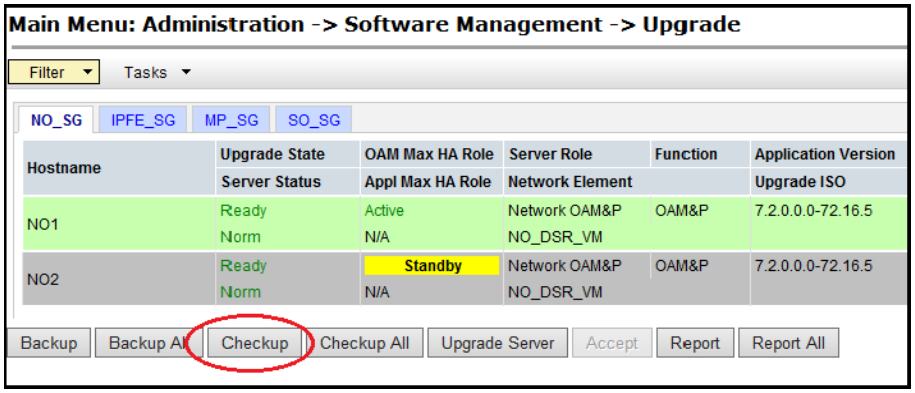
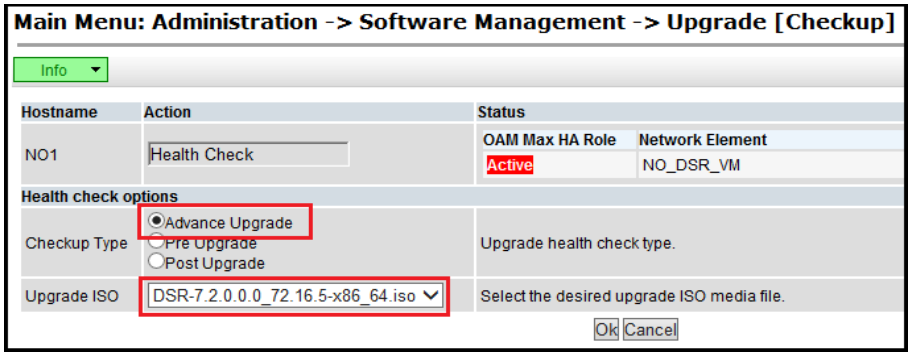
6. ☐	**Active SOAM CLI**: Log SOAM alarm status	1. Use an SSH client to connect to the active SOAM:
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		Note: The static XMI IP address for each server should be available in Table 5.
		2. Enter the command:
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		This command creates two files in **/var/TKLC/db/filemgmt/ UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		Note: The message **FIPS integrity verification test failed** may display when the upgradeHealthCheck command runs. This message can be ignored. 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.
		3. Verify all peer MPs are available.
		4. Note the number of Total Connections Established _____
		5. Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.

7. ☐	**Active SOAM CLI**: Verify PCA status (if equipped)	1. Enter the command: `$ upgradeHealthCheck pcaStatus` 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 Operational Status is **Available** for all applications.
8. ☐	Repeat for each network element	Repeat steps 5 – 7 for each SOAM site in the topology.
9. ☐	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 3.4.2.1 and steps 1 through 8 of this procedure. 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 exact sequence in which MP servers are upgraded for each site.

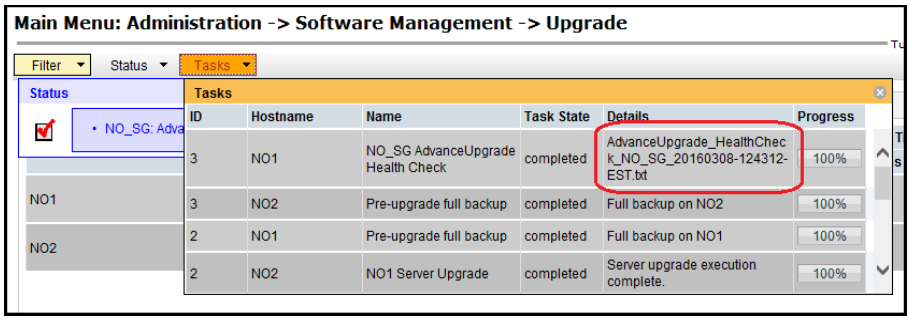
3.4.2.4 Data Collection for Source Release 7.2, 7.3, 7.4

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.2, 7.3, or 7.4.

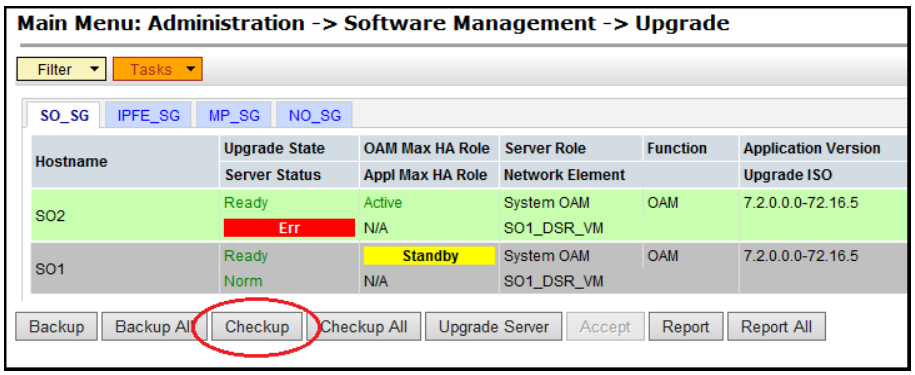
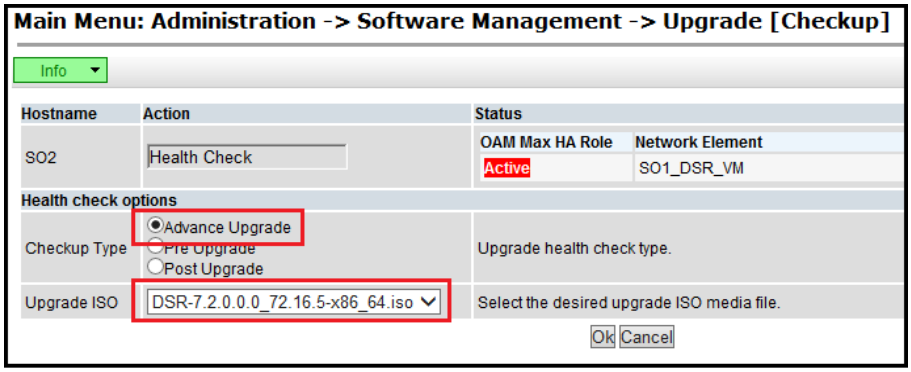
Procedure 5. Data Collection for Source Release 7.2, 7.3, 7.4

S T E P #	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 My Oracle Support (MOS) 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.  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. 

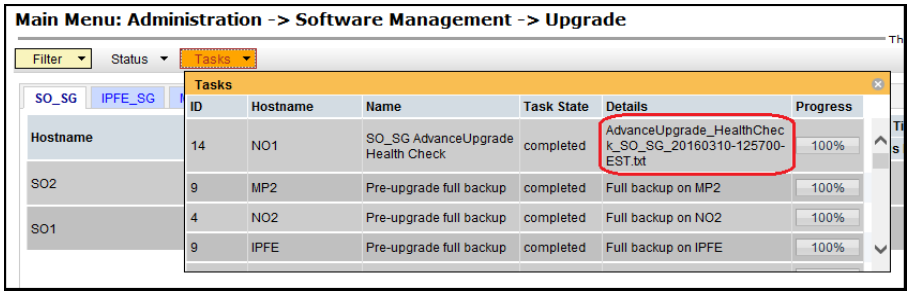
Procedure 5. Data Collection for Source Release 7.2, 7.3, 7.4

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 My Oracle Support (MOS) for guidance as described in Appendix P.

Procedure 5. Data Collection for Source Release 7.2, 7.3, 7.4

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. 

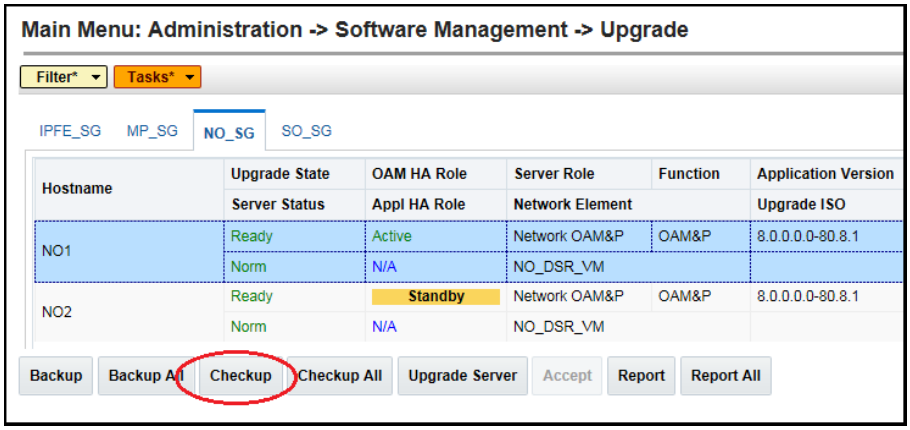
Procedure 5. Data Collection for Source Release 7.2, 7.3, 7.4

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 My Oracle Support (MOS) for guidance as described in Appendix P. 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 3.4.2.1 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.

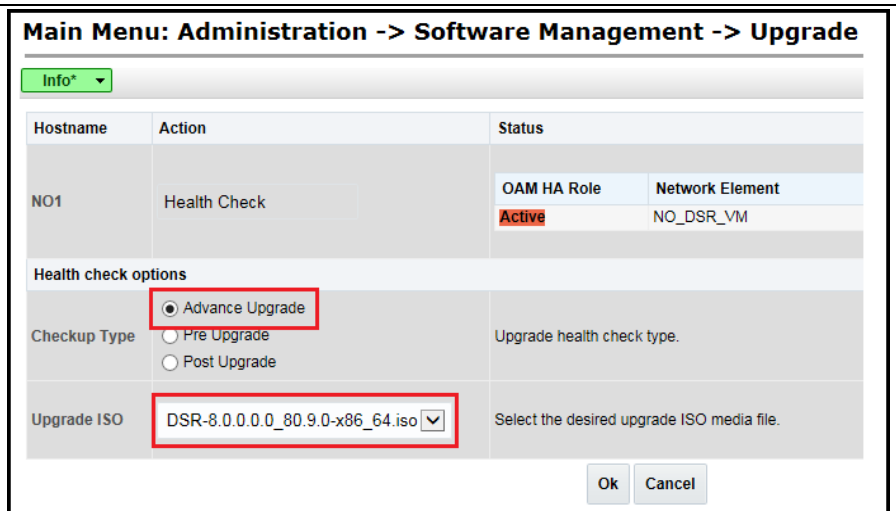
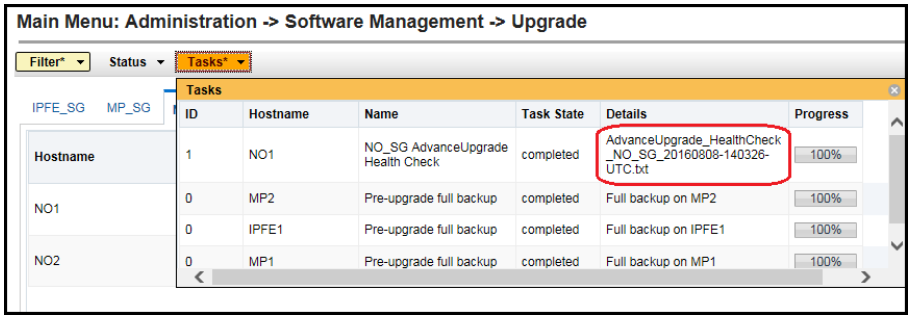
3.4.2.5 Data Collection for Source Release 8.0 and Later

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

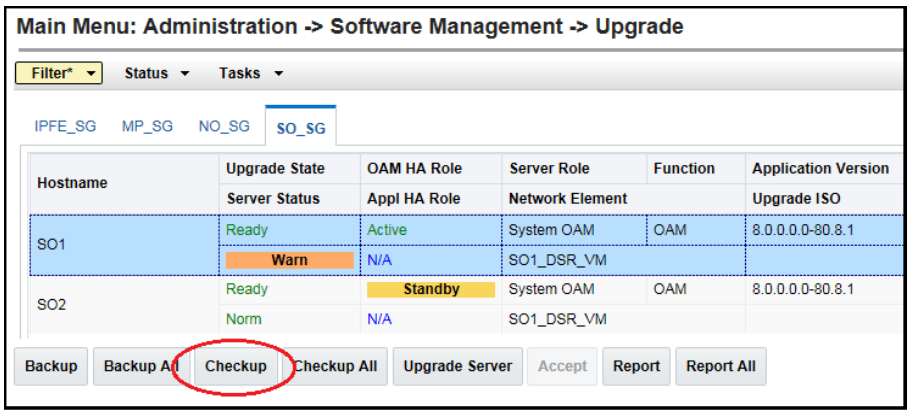
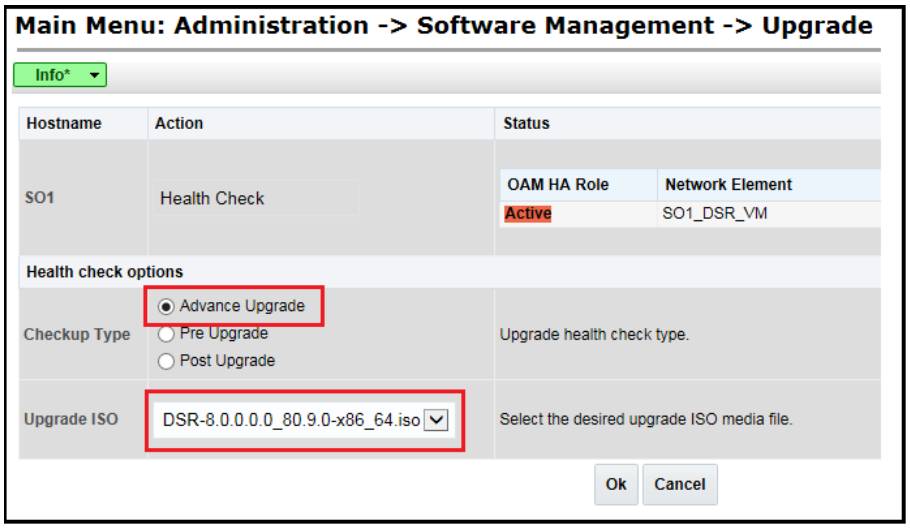
Procedure 6. Data Collection for Source Release 8.0 and Later

S T E P #	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 My Oracle Support (MOS) 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.  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.

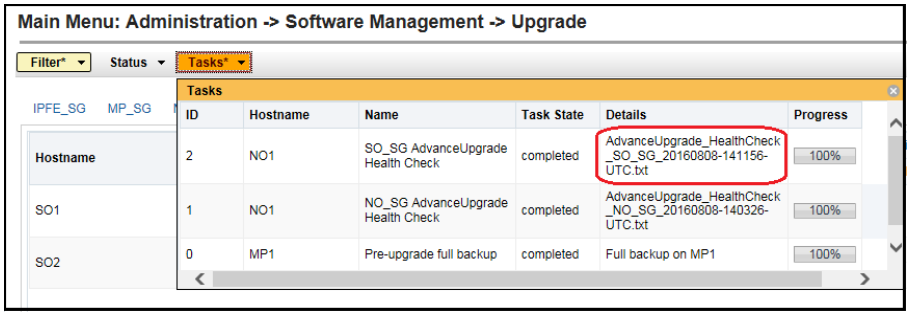
Procedure 6. Data Collection for Source Release 8.0 and Later

		
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 My Oracle Support (MOS) for guidance as described in Appendix P.

Procedure 6. Data Collection for Source Release 8.0 and Later

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. 

Procedure 6. Data Collection for Source Release 8.0 and Later

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 My Oracle Support (MOS) for guidance as described in Appendix P. 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 3.4.2.1 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.

3.4.3 DSR ISO Administration

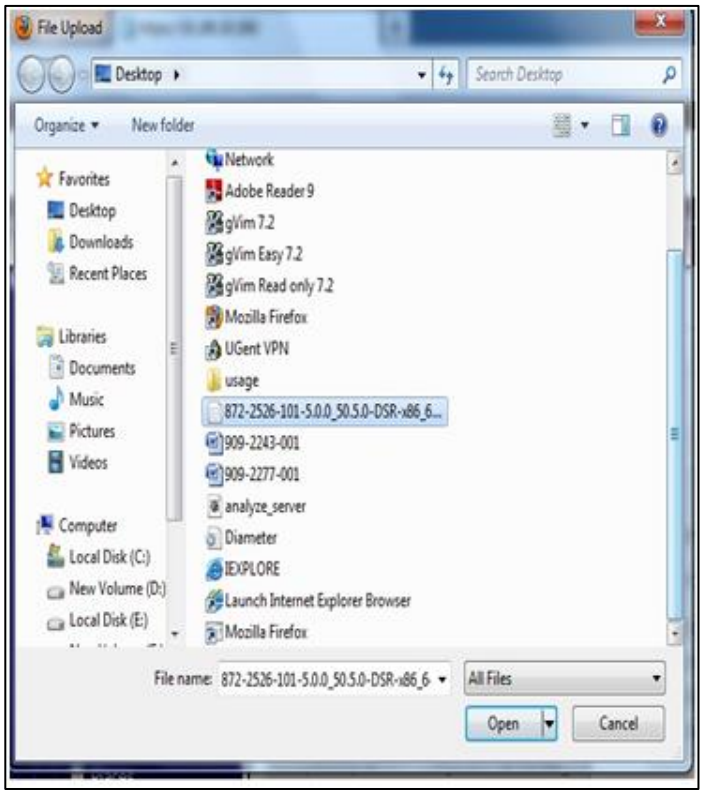
This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

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 7. DSR ISO Administration

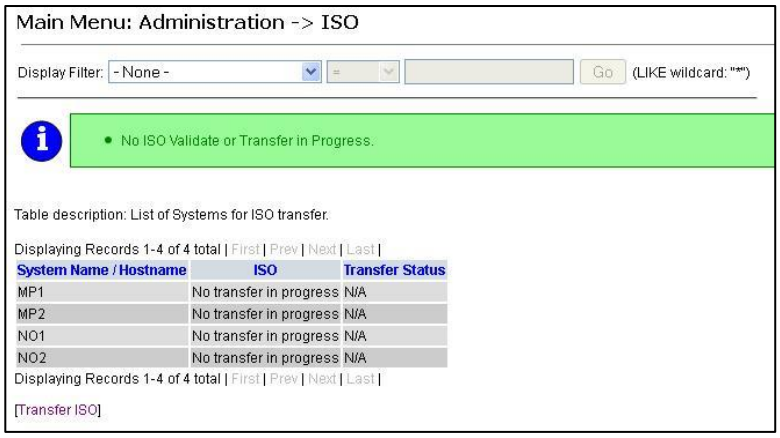
S T E P #	This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**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.

Procedure 7. DSR ISO Administration

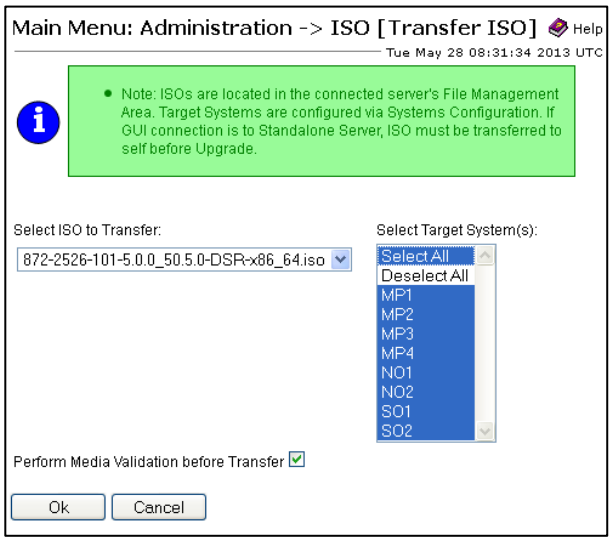
2. ☐	**Active NOAM VIP**	1. Click **Browse** to select the file to upload. 2. Select the target release ISO image file and click **Open**.  3. Click **Upload**. The ISO file begins uploading to the file management storage area. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This usually takes between 2 to 10 minutes, but more if the network upload speed is slow.

Procedure 7. DSR ISO Administration

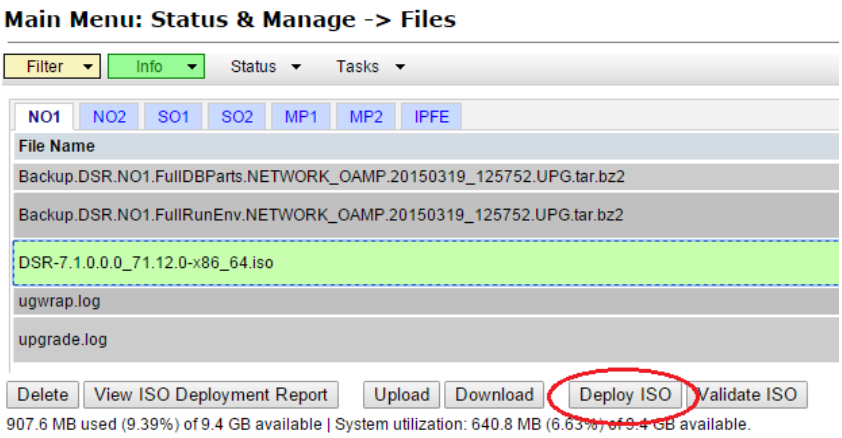
3. ☐	**Active NOAM VIP**: Copy ISO to the standby NOAM
	For an active NOAM on release 7.0.1
		If the active NOAM is on release 7.0.1, perform this step; otherwise, proceed to step 6.
		1. Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM:
		`ssh admusr@<NOAM_VIP>`
		`login as: admusr`
		`password: <enter password>`
		2. Copy the ISO file to the standby NOAM.
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename> admusr@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`

4. ☐	**Active NOAM VIP**: Using NOAM GUI, transfer the target release ISO image file from the active NOAM to all DSR servers to be upgraded. **For active NOAM on release 7.0.x**	1. Navigate to **Administration >Software Management > ISO Deployment**. 2. Click **Transfer ISO**. 

Procedure 7. DSR ISO Administration

5. ☐	**Active NOAM VIP**: ISO transfer continued For active NOAM on release 7.0.1	1. Under the **Select ISO to Transfer** option, select the DSR 8.1 ISO. 2. Under the **Select Target System(s)** option, click **Select All**. 3. Mark the **Perform Media Validation before Transfer** checkbox.  4. Click **OK**. Control returns to the ISO screen. 5. Monitor the progress until all file transfers have completed. Click **Refresh** to update the status of the transfer. If a file transfer fails, it must be retried. ***Note***: In the unlikely event that an ISO file transfer fails, repeat the transfer selecting only the specific system to which the transfer failed. If file transfers fail repeatedly, it is recommended to contact My Oracle Support (MOS) for assistance.

Procedure 7. DSR ISO Administration

6. ☐	**Active NOAM VIP**: Using NOAM GUI, deploy ISO to all servers to be upgraded. For active NOAM on release 7.1.1 or later	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 My Oracle Support (MOS). 8. If the ISO is valid, select the ISO, and click **Deploy ISO**. Click **OK** on the confirmation screen. 

Procedure 7. DSR ISO Administration

7. ☐	**Active NOAM VIP**: Monitor ISO deployment For active NOAM on release 7.1.1 or later	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] Fri Mar 20 11:35:43 2015 EDT Deployment report for DSR-7.1.0.0.0_71.11.0-x86_64.iso: Deployed on 7/7 servers. NO1: Deployed NO2: Deployed SO1: Deployed SO2: Deployed MP1: Deployed MP2: Deployed IPFE: Deployed

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 8.0 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 7.0 or 8.x.

Procedure 8. ISO Link Correction

S T E P #	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 My Oracle Support (MOS) 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 8.0/8.1 ISO been deployed? If **Yes**, then proceed to next step. If **No**, this procedure is complete.

Procedure 8. ISO Link Correction

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 8.0/8.1 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-8.0.0.0.0_80.x.y-x86_64.iso /mnt/upgrade`
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 8.0/8.1 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.

Procedure 8. ISO Link Correction

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-8.1.0.0.0_80.16.0-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-8.1.0.0.0_80.16.0-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-8.1.0.0.0_80.16.0-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 My Oracle Support (MOS) for guidance.

3.4.5 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.

3.4.5.1 Full Backup of DB Run Environment for Release 7.0.1

This procedure backs up the DB run environment when the active NOAM is on release 7.0.1.

Procedure 9. Full Backup of DB Run Environment for Release 7.0.1

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**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>`
2. ☐	**Active NOAM 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 NOAM CLI**: Execute Full Backup for all servers (managed from this NOAM)	Execute the **backupAllHosts** utility on the active NOAM. This utility remotely accesses each server managed by the NOAM, and runs the backup command for that server.
		`$ /usr/TKLC/dpi/bin/backupAllHosts`
		`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`
		`----------`
		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		Errors also report back to the command line.
		Note: There is no progress indication for this command; only the final report when it completes.

4. ☐	**Active NOAM 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.

Procedure 9. Full Backup of DB Run Environment for Release 7.0.1

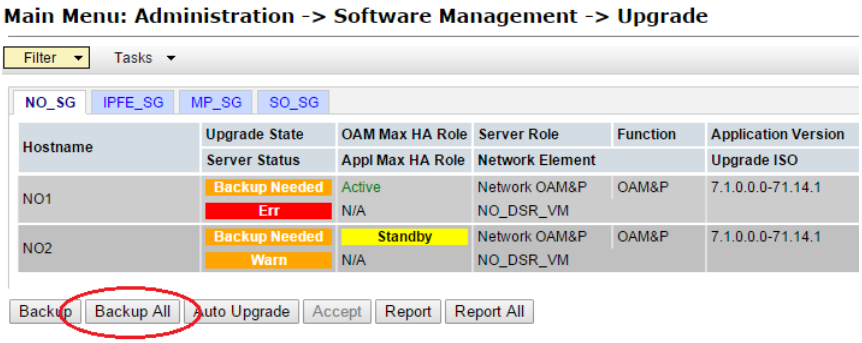
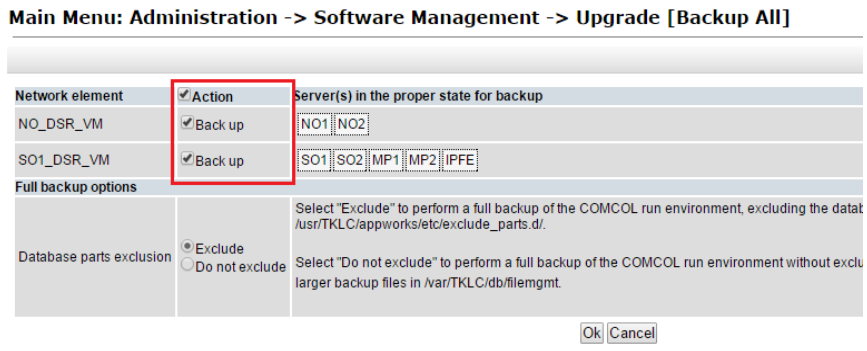
5. ☐	**ALTERNATIVE METHOD** (Optional)
	Server CLI: If needed, the alternative backup method can be executed on each individual server instead of using the **backupAllHosts** script
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the GUI method. To do this, 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.
		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`

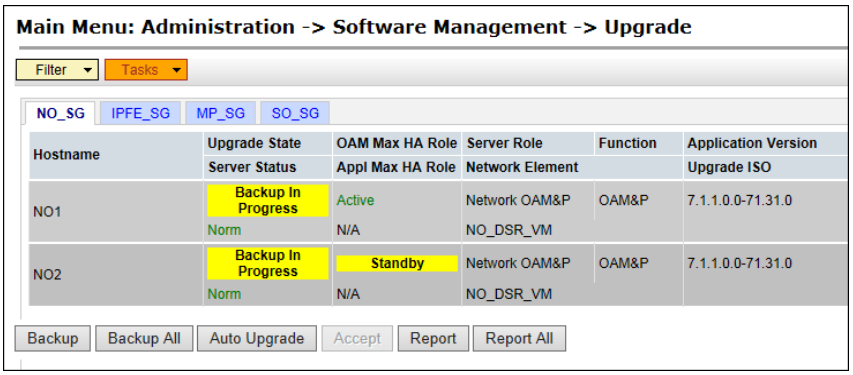
3.4.5.2 Full Backup of DB Run Environment for Release 7.1.x and Later

This procedure backs up the DB run environment when the active NOAM is on release 7.1.x and later.

Procedure 10. Full Backup of DB Run Environment for Release 7.1.x and Later

S T E P #		
	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 My Oracle Support (MOS) 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**. 
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. 

Procedure 10. Full Backup of DB Run Environment for Release 7.1.x and Later

3. ☐	**Active NOAM VIP**: Monitor backup progress	Select each server group tab and verify each server transitions from **Backup in Progress** to **Ready**. 

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`

3.4.6 IDIH Pre-Upgrade

If IDIH is a component of a Network Element, it may be upgraded either before or after the DSR. The order of upgrade does not impact the functionality of either component. However, it should be noted that certain compatibility limitations may exist while the two components are not on the same release.

The IDIH upgrade procedures are provided in Appendix J and may be performed at any time after Section 3.4.6.1 has been completed.

Table 10. IDIH Upgrade Preparation Overview

Procedure	Elapsed Time (hr:min)		Procedure Title
	This Step	Cum.	
Procedure 11	0:15-0:30	0:15-0:30	IDIH Upgrade Preparation

3.4.6.1 IDIH Upgrade Preparation

Procedure 11. IDIH Upgrade Preparation

S T E P #	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 My Oracle Support (MOS) 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 My Oracle Support (MOS) as described in Appendix P 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 My Oracle Support (MOS) 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 My Oracle Support (MOS) 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 49 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 12 or Procedure 13 or Procedure 14	0:30-0:45 0:20-0:30 0:20-0:30	0:30-0:45 0:20-0:30 0:20-0:30	NOAM Health Check for Source Release 7.0.1, 7.1.x NOAM Health Check for Source Release 7.2, 7.3, 7.4 NOAM Health Check for Source Release 8.0 or Later	None None None
Procedure 15	0:05-0:10	0:25-0:55	NOAM Pre-Upgrade Backup	None
Procedure 16	0:01-0:05	0:26-1:00	Disable Global Provisioning	Global Provisioning Disabled
Procedure 17	0:40-1:20	1:06-2:20	NOAM Upgrade	No Traffic Impact
Procedure 18	0:01-0:05	1:07-2:25	PCA (Formerly PDRA) Topology Hiding Configuration	No Traffic Impact
Procedure 19	0:05-0:15	1:12-2:40	Verify NOAM Post Upgrade Status	None
Procedure 20	0:05-0:10	1:17-2:50	Allow Provisioning (Post NOAM Upgrade)	Global Provisioning Enabled
Procedure 21	0:05-0:10	1:22-2:60	Avoid the Device Deployment Failed Alarm On Affected Server(s)	None

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 17.

WARNING!

Increase 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.

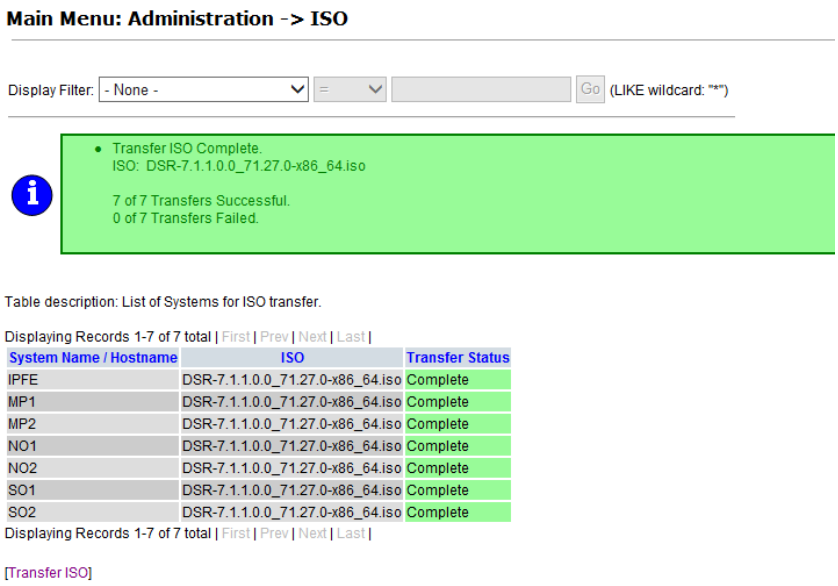
4.1.1 NOAM Health Check for Source Release 7.0.1, 7.1.x

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 7.0.1 or 7.1.x. This procedure must be executed on the active NOAM.

Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM VIP**: Verify upgrade DSR ISO has been transferred to all servers **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x. If the active NOAM is on release 7.1.x, proceed to step 2**. 1. Navigate to **Administration > Software Management > ISO Deployment**. 2. Verify the Transfer Status is **Complete** for each server in the topology. If any server shows **Not Complete**, perform 3.4.3 DSR ISO Administration.

Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x

		 Proceed to step 3 to complete this procedure.

2. ☐	**Active NOAM VIP**: Verify DSR ISO for upgrade has been transferred to all servers
	For active NOAM on release 7.1.x only
		1. Navigate to **Status & Manage > Files**.
		2. Select the target release DSR ISO and click **View ISO Deployment Report**.
		3. Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.1.0.0.0_80.27.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x

3. ☐	**Active NOAM CLI**: Verify NOAM pre-upgrade status	Execute these commands on the active DSR NOAM and active DR NOAM servers.
		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 command:
		`$ upgradeHealthCheck preUpgradeHealthCheck`
		This command creates two files in **/var/TKLC/db/filemgmt/UpgradeHealthCheck/** with the filename format:
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		If any alarms are present in the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		If the system is PDRA, one additional file is generated:
		`<NOserver_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.

4. ☐	**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. 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.

Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x

5. ☐	**Active SOAM CLI**: Pre-upgrade health checks	Execute SOAM pre-upgrade alarm status health checks.
		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 alarmStatusOnSoam`
		If any alarms are present in the system, this command creates a file in **/var/TKLC/db/filemgmt/ UpgradeHealthCheck/** with the filename format:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		Note: The **FIPS integrity verification test failed** message may display when the upgradeHealthCheck command runs. This message can be ignored.
		3. Keep this report for future reference. This report is compared to alarm and status reports after the upgrade is complete.

6. ☐	**Active SOAM CLI**: Pre-upgrade health checks	Execute SOAM pre-upgrade DA-MP status health checks. 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 _____
7. ☐	**Active SOAM CLI**: Verify PCA status (if equipped)	Execute SOAM pre-upgrade PCA status health checks, if equipped. 1. Enter the command: `$ upgradeHealthCheck pcaStatus` 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 Operational Status is **Available** for all applications.
8. ☐	Repeat for each network element	Repeat steps 5. – 7. for each SOAM site in the topology.

Procedure 12. NOAM Health Check for Source Release 7.0.1, 7.1.x

9. ☐	**Active NOAM VIP**: Verify recent COMCOL Environment backup for all servers	1. Navigate to **Status & Manage > Files**.
		2. Select each server tab, in turn.
		3. Verify the following two files have been created and have a current timestamp:
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		4. Repeat this procedure for each site.
		See section 3.4.4 to perform (or repeat) a full backup, if needed.

4.1.2 NOAM Health Check for Source Release 7.2, 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 7.2, 7.3, or 7.4. This procedure must be executed on the active NOAM.

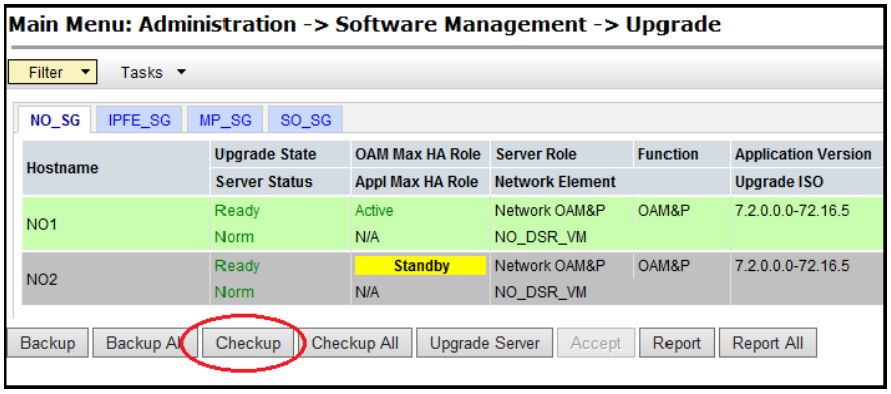
Note: This procedure may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 17.

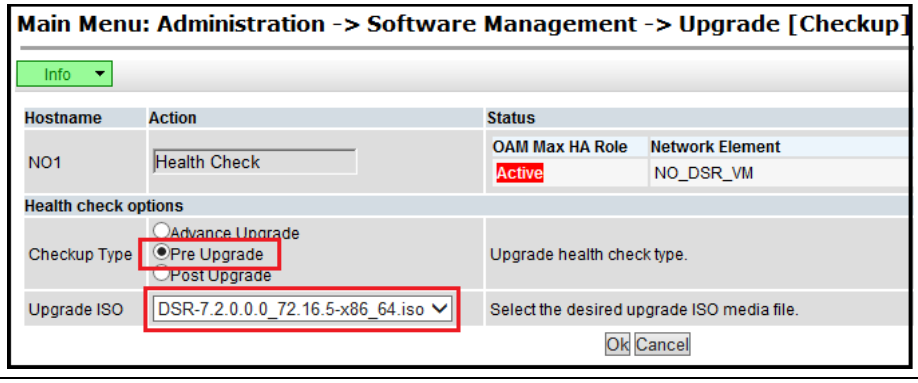
Procedure 13. NOAM Health Check for Source Release 7.2, 7.3, 7.4

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	

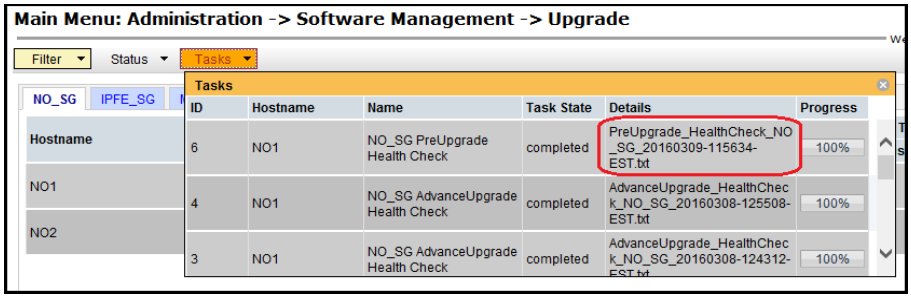
1. ☐	**Active NOAM VIP**: Verify upgrade DSR ISO has been transferred to all servers	1. Navigate to **Status & Manage > Files**.
		2. Select the target release DSR ISO and click **View ISO Deployment Report**.
		3. Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.0.0.0.0_80.27.0-x86_64.iso:`
		`Deployed on 7/7 servers.`
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

Procedure 13. NOAM Health Check for Source Release 7.2, 7.3, 7.4

<table>
<tr>
<td>2. ☐</td>
<td>Active NOAM VIP: Export and archive the Diameter configuration data</td>
<td>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.</td>
</tr>
<tr>
<td>3. ☐</td>
<td>Active NOAM VIP: Initiate NOAM health checks</td>
<td>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.
 
</td>
</tr>
</table>

Procedure 13. NOAM Health Check for Source Release 7.2, 7.3, 7.4

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 **UpgradeHealthCheck.log** 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 My Oracle Support (MOS) for guidance as described in Appendix P. If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform health checks in accordance with Procedure 13.

4.1.3 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.

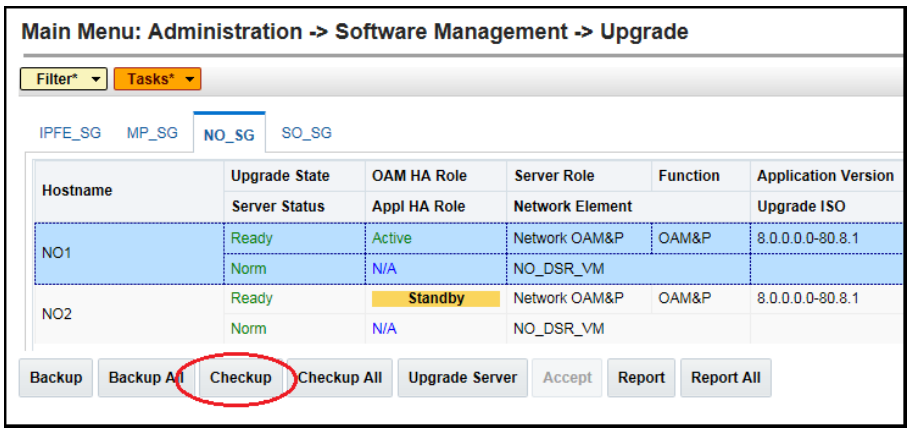
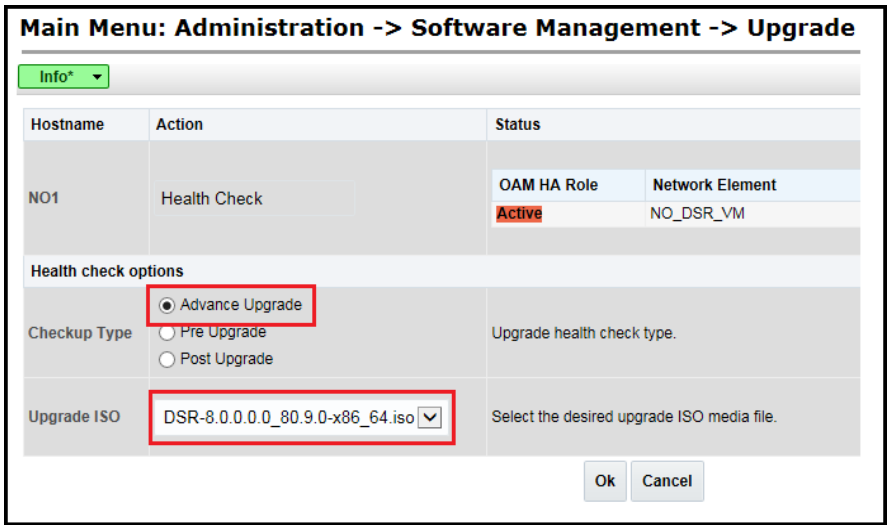
Procedure 14. NOAM Health Check for Source Release 8.0 or Later

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	

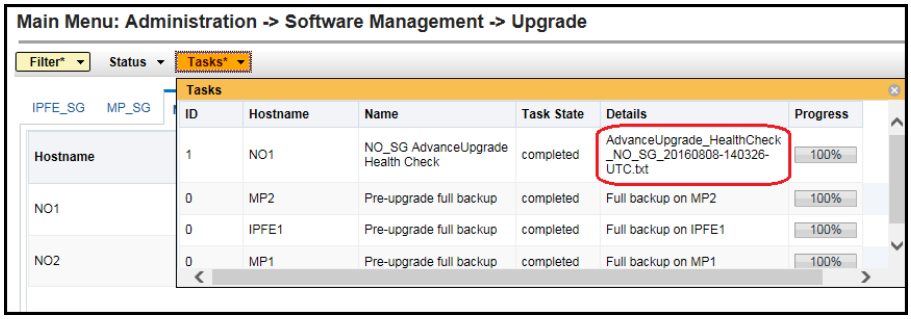
1. ☐	**Active NOAM VIP**: Verify upgrade DSR ISO has been transferred to all servers	1. Navigate to **Status & Manage > Files**.
		2. Select the target release DSR ISO and click **View ISO Deployment Report**.
		3. Review the report to ensure the ISO is deployed to all servers in the topology.
		Sample report:
		`Deployment report for DSR-8.0.0.0.0_80.27.0-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.

Procedure 14. NOAM Health Check for Source Release 8.0 or Later

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. 

Procedure 14. NOAM Health Check for Source Release 8.0 or Later

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 **UpgradeHealthCheck.log** 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 My Oracle Support (MOS) for guidance as described in Appendix P. If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform health checks in accordance with Procedure 13 or Procedure 14.

4.1.4 NOAM Pre-Upgrade Backup

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

Procedure 15. NOAM Pre-Upgrade Backup

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM VIP**: Backup all global configuration databases for NOAM ***Important***: Required for disaster recovery	1. Navigate to **Status & Manage > Database** to return to the Database Status screen. 2. Click to highlight the active NOAM server and click **Backup**. ***Note***: **Backup** is only enabled when the active server is selected. 3. Mark the **Configuration** checkbox. 4. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 5. Enter **Comments** (optional). 6. 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 16. Disable Global Provisioning

S T E P #	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 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 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 17. NOAM Upgrade

S T E P #	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 My Oracle Support (MOS) 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 D -- Upgrade Single Server – DSR 8.x. **Otherwise**: Execute Appendix E - Upgrade Single Server – Pre-DSR 8.0. 2. After successfully completing the procedure in Appendix D or Appendix E, 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 My Oracle Support (MOS) on the best course of action. If the active NOAM is on release 7.1.1 or later, proceed to step 3.

Procedure 17. NOAM Upgrade

2. ☐	**Active NOAM VIP**: Prepare the active NOAM for upgrade For NOAM on release 7.0.1 only	This step is for an active NOAM on release 7.0.1 only. 1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the NOAM server group. 3. Select the active NOAM. 4. On the upgrade form, make the active NOAM **Upgrade Ready**, by clicking **Prepare**. 5. On the Upgrade Prepare form, select **Prepare** in the Action options. Click **OK**. This starts the Prepare action on the active NOAM and forces an HA failover. *** Critical *** Do NOT omit this step. 6. 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. 7. Clear the **Prepared** state for the now-standby NOAM. This is required due to the transition from the source release-to-release 8.0/8.1. 8. Navigate to **Status & Manage > HA**. 9. Click **Edit**. 10. For the NOAM to be upgraded (now the standby), set the Max Allowed HA Role to **Active**, and click **OK**. 11. Navigate to **Status & Manage > Server**. 12. Select the standby NOAM and click **Restart**. 13. Click **OK** and verify the Appl State changes to **Enabled**.
3. ☐	Upgrade second DSR NOAM	Upgrade the second DSR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
4. ☐	Upgrade standby DR NOAM	Upgrade the standby DR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
5. ☐	Upgrade active DR NOAM	Upgrade the active DR NOAM server using the Upgrade Single Server procedure: Execute Appendix D -- Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, return to this point and continue with the next procedure per Table 11.

4.3.1 PCA (Formerly PDRA) Topology Hiding Configuration

In DSR 7.0, the Policy and Charging Topology Hiding configuration moved from being site-specific at the SOAM, to being network-wide specific at the NOAM. Because each site could be independently configured, manual intervention is required to determine the appropriate setting for the network-wide configuration. The network-wide settings apply to ALL sites once the site is upgraded.

This procedure is applicable only to systems with the Policy and Charging feature enabled.

This procedure is applicable only to major upgrades from 7.0.1 to DSR 8.0/8.1.

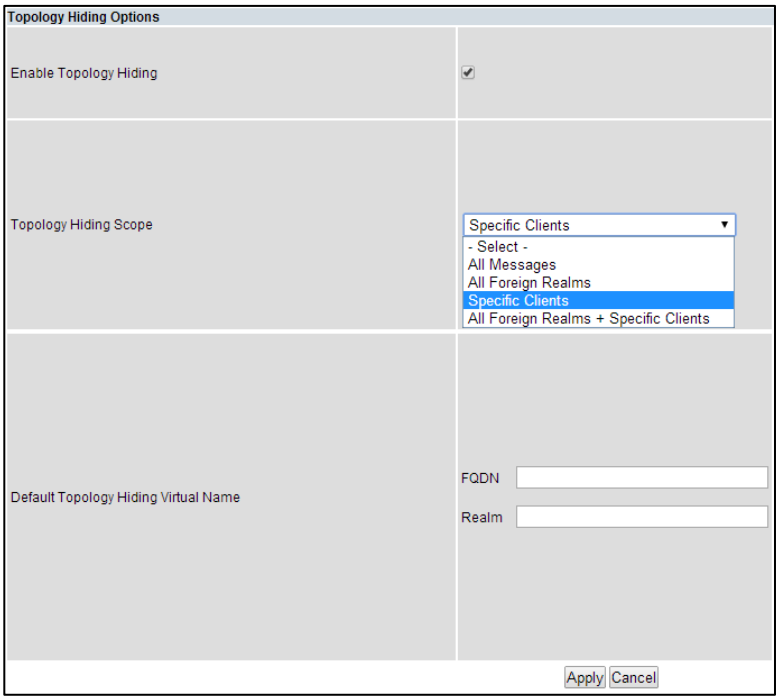
Note: The network-wide Topology Hiding settings at the NOAM apply to each site as it is upgraded. This may result in a behavior change if the pre-upgrade site settings differ from the network-wide settings.

Note: This procedure can be skipped if Topology Hiding is not in use for this system.

Procedure 18. PCA (Formerly PDRA) Topology Hiding Configuration

S T E P #	This procedure sets the network-wide Topology Hiding configuration. This procedure applies only to systems with the Policy and Charging feature enabled. 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**: Enable global provisioning	Before the Topology Hiding configuration can be modified, Global Provisioning must be enabled temporarily. 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**.

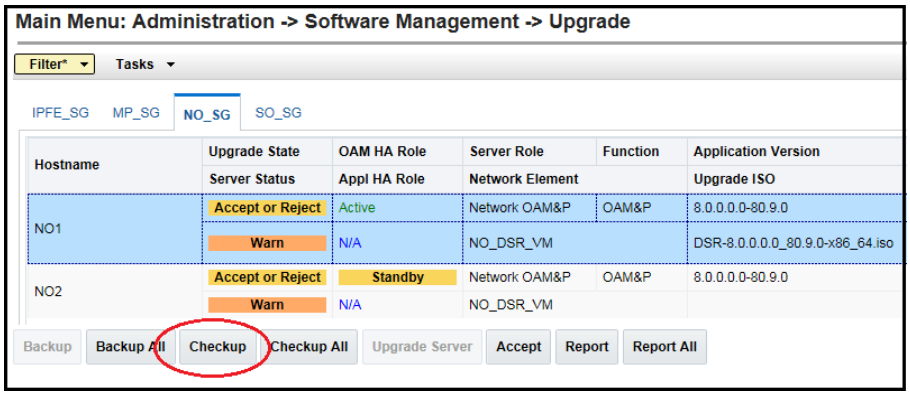
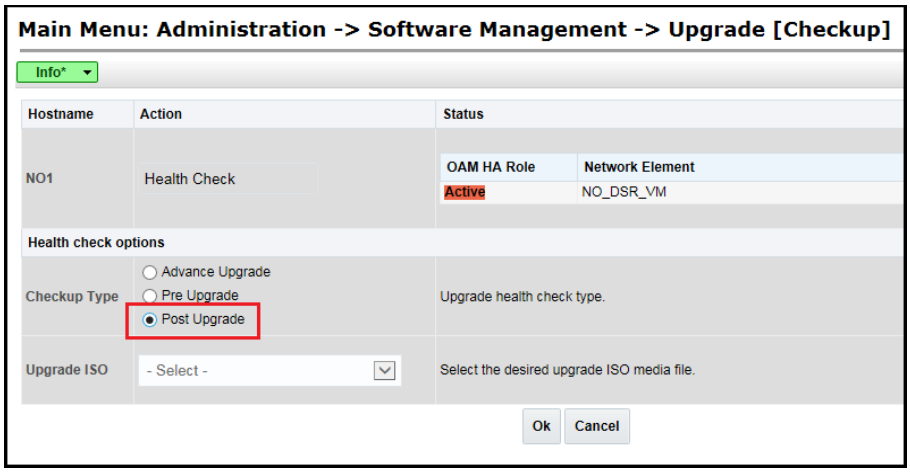
Procedure 18. PCA (Formerly PDRA) Topology Hiding Configuration

2. ☐	**Active NOAM VIP**: Configure topology hiding settings	1. Navigate to **Policy and Charging > Configuration > Policy DRA > Network-Wide Options**. 2. In the Topology Hiding Options section, mark the **Enable Topology Hiding** checkbox. 3. Select the appropriate Topology Hiding Scope setting. 4. Enter a Default Topology Hiding Virtual Name – FQDN and Realm. These default values are used if specific values have not been set at a site. 5. Click **Apply**. 
3. ☐	**Active NOAM VIP**: Disable global provisioning	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 displays 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)**

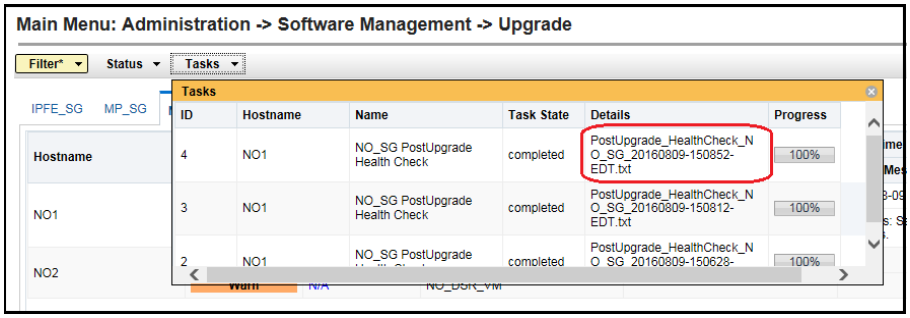
4.4 Verify NOAM Post Upgrade Status

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

Procedure 19. Verify NOAM Post Upgrade Status

S T E P #	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 My Oracle Support (MOS) 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. 

Procedure 19. Verify NOAM Post Upgrade Status

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 My Oracle Support (MOS) for guidance as described in Appendix P.

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 20. Allow Provisioning (Post NOAM Upgrade)

S T E P #	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 My Oracle Support (MOS) 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).

4.6 Workaround to Avoid Device Deployment Alarm for IPFE Server (s) (Post-NOAM Upgrade)

This procedure applies the device deployment alarm workaround for IPFE server(s).

Procedure 21. Avoid the Device Deployment Failed Alarm On Affected Server(s)

S T E P #	This procedure avoids the device deployment failed alarm on IPFE server(s). Do not do this procedure if there are no IPFE server(s) in the system. 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 active NOAM server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM server:
		`ssh admusr@<server address>`
		`password: <enter password>`
		Answer **yes** if you are asked to confirm the identity of the server.

2. ☐	**Server CLI**: Verify the current ethtool settings for all IPFE devices	`iqt -pE NetworkDeviceOption where "Value like '*combinedChannels*'"` This command results some records that mean there is an issue in the system. ***Note***: If there are no records in the results, then this workaround is not required. Return to the procedure step that directed the execution of this procedure. ***Note***: If the command does not work properly, copy the command to the notepad to get rid of special formatting and execute the command again.
3. ☐	**Server CLI**: Remove ethtool settings for all IPFE devices	`iset -fValue='' NetworkDeviceOption where "Keyword like 'ethtoolOpts'"` ***Note***: If the command does not work properly, copy the command to the notepad to get rid of special formatting and execute the command again.
4. ☐	**Server CLI**: Add only the ring buffer configuration to IPFE device	`iset -fValue='rx=4078' NetworkDeviceOption where "Keyword like 'ethtoolOpts'"` ***Note***: If the command does not work properly, copy the command to the notepad to get rid of special formatting and execute the command again.

Procedure 21. Avoid the Device Deployment Failed Alarm On Affected Server(s)

5. ☐	**Server CLI**: Verify ethtool settings have been updated	`iqt -pE NetworkDeviceOption where "Value like '*combinedChannels*'"`
		This command should not return any records. But the following command does result in records.
		`iqt -pE NetworkDeviceOption where "Value like '*rx=4078*'"`
		If this is the case, the workaround is applied. Return to the procedure step that directed the execution of this procedure.
		Note: If the command does not work properly, copy the command to the notepad to get rid of special formatting and execute the command again.

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 5.2Automated 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.

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 22	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 23 or Procedure 24	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:35	Site Pre-Upgrade Health Check for Release 8.0 and Later Site Pre-Upgrade Health Check for Release 7.x/8.x	None None
Procedure 25	0:03	0:18-0:38	Site Upgrade Options Check	None
Procedure 26	0:01-0:05	0:19-0:48	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 27	0:05-0:10	0:24-0:58	Site Upgrade Pre-Checks	None
Procedure 28	2:40-4:00	3:04-4:58	Automated Site Upgrade	Traffic is not serviced by servers that are actively upgrading.
Procedure 29	0:02	3:06-5:00	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 30	0:10-0:15	3:26-5:15	Site Post-Upgrade Health Check	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.

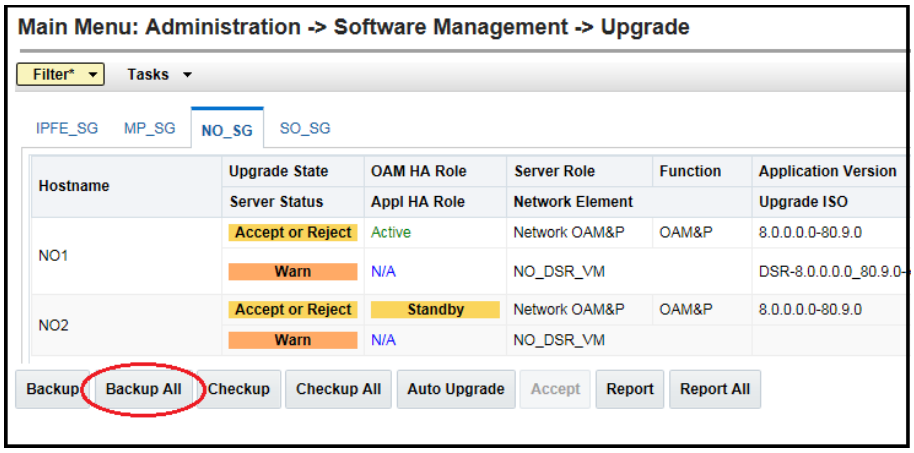
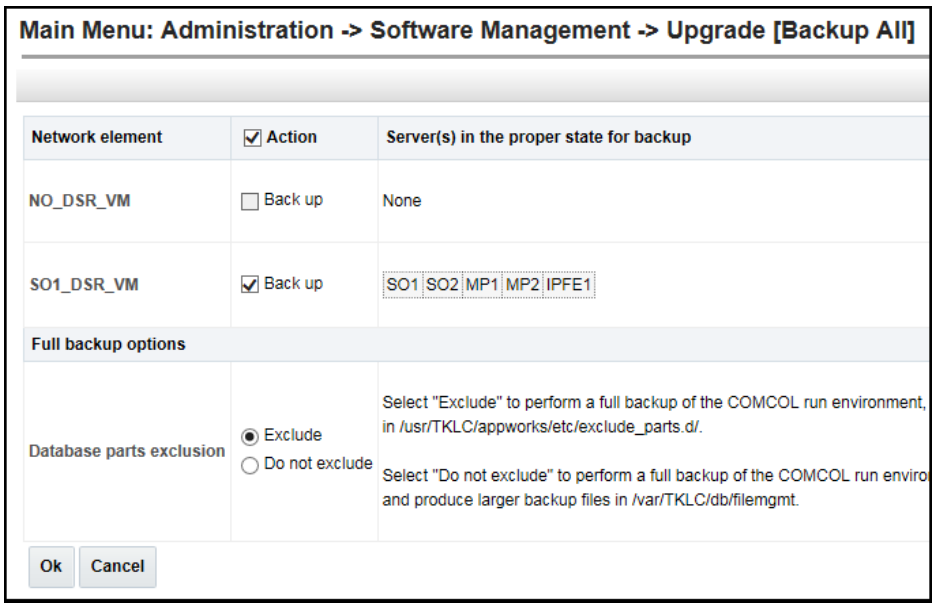
Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 22 is an alternate procedure that can be used to backup a site using the command line. Procedure 22 should only be used by direction of My Oracle Support (MOS).

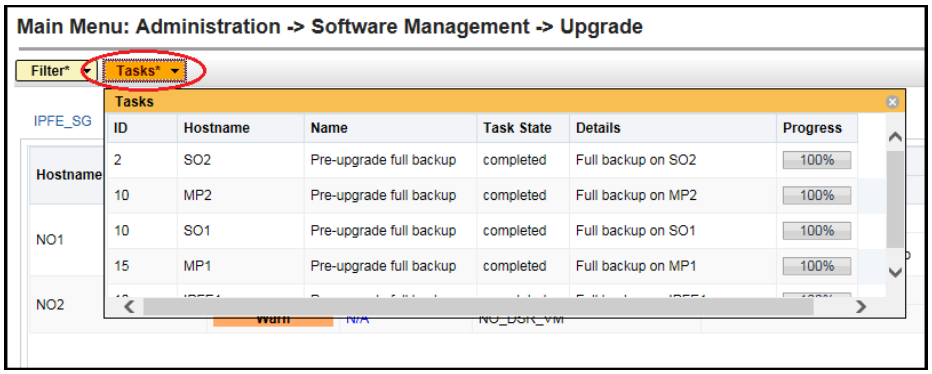
Procedure 22. Site Pre-Upgrade Backups

S T E P #	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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**.
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**.

Procedure 22. Site Pre-Upgrade Backups

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**. 
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. 

Procedure 22. Site Pre-Upgrade Backups

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. 

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

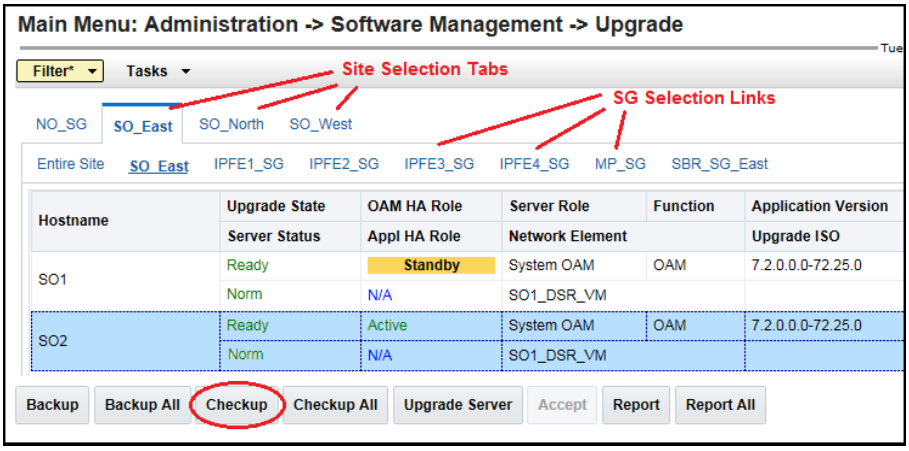
This section provides procedures to verify the health of the SOAM site prior to upgrade. Procedure 23 is the primary procedure to be executed when the active NOAM is on release 8.0 and later. Alternate release-specific procedures are also provided, to be used as directed.

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

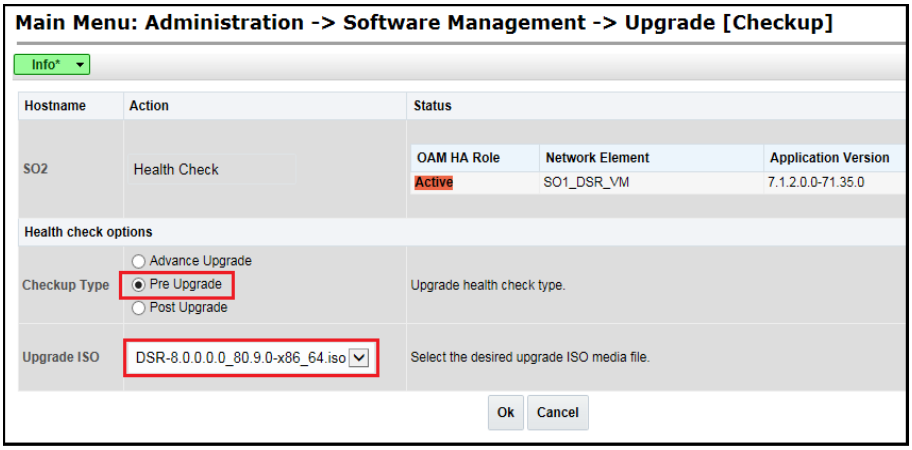
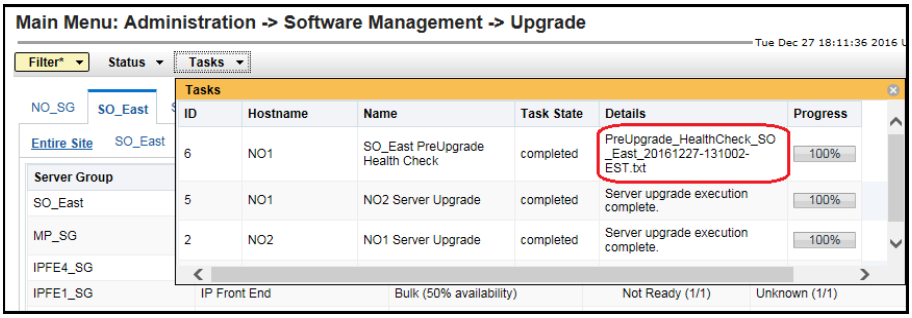
This procedure is used when the NOAMs are on release 8.0 and later. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

Procedure 23. Site Pre-Upgrade Health Check for Release 8.0 and Later

S T E P #		
	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 My Oracle Support (MOS) 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**.



Procedure 23. Site Pre-Upgrade Health Check for Release 8.0 and Later

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. 

Procedure 23. Site Pre-Upgrade Health Check for Release 8.0 and Later

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 My Oracle Support (MOS) for guidance as described in Appendix P. 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 24 Site Pre-Upgrade Health Check for Release 7.x/8.x.
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/8.x

This procedure is an alternate health check that is used when upgrading to release 8.0/8.1 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 23, step 4.

Procedure 24. Site Pre-Upgrade Health Check for Release 7.x/8.x

S T E P #	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 My Oracle Support (MOS) 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 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.

Procedure 24. Site Pre-Upgrade Health Check for Release 7.x/8.x

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.

Procedure 24. Site Pre-Upgrade Health Check for Release 7.x/8.x

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 2.5.3. 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 25. Site Upgrade Options Check

S T E P #	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 26. Disable Site Provisioning

S T E P #	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 My Oracle Support (MOS) 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 22; [Procedure 23 or Procedure 24]; Procedure 25; Procedure 26; and Procedure 27.

Read 2.5 **Error! Reference source not found.** for details.

Upgrade cycles are created when using the Automated Site Upgrade. Limitations in **Error! Reference source not found.** 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.

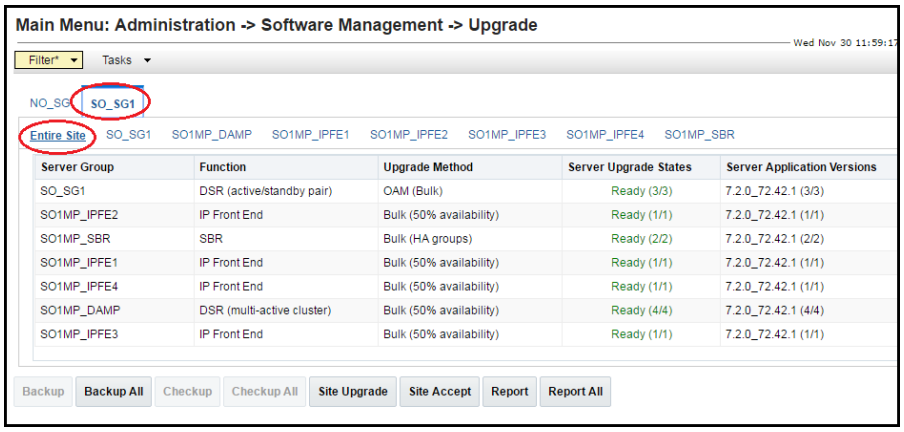
Procedure 27. Site Upgrade Pre-Checks

S T E P #	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 My Oracle Support (MOS) 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 26. 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 26 Disable Site Provisioning.

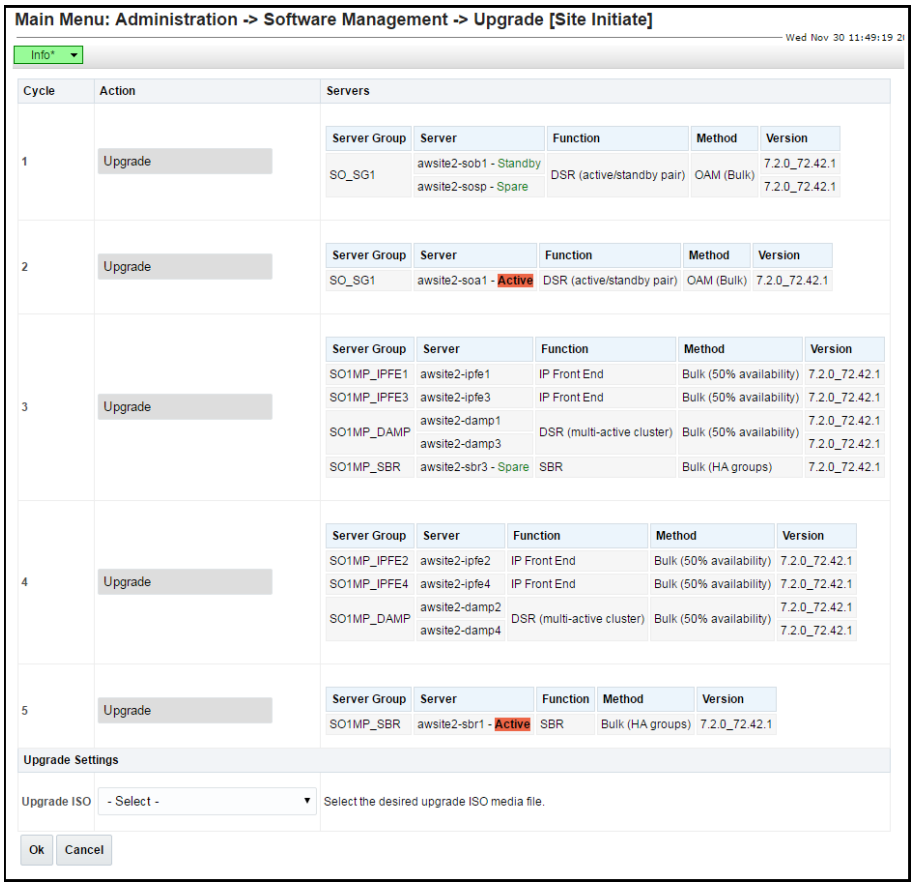
5.2.2 Initiate Automated Site Upgrade

This procedure initiates the Automated Site Upgrade sequence.

Procedure 28. Automated Site Upgrade

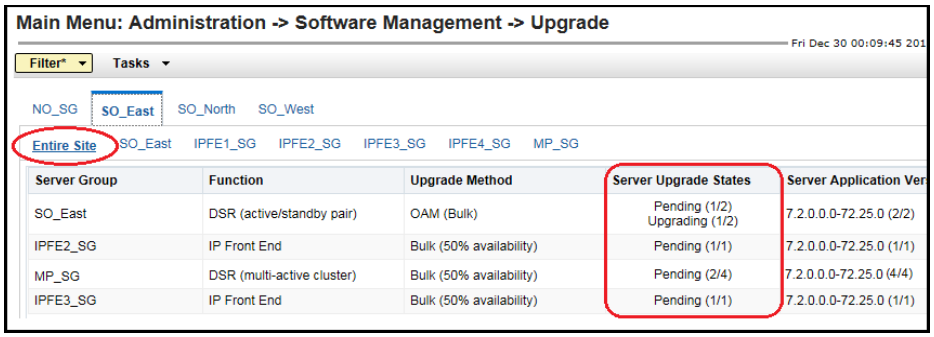
S T E P #		
	This procedure upgrades an entire site using the Automated Site Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
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.  ***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.

Procedure 28. Automated Site Upgrade

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. Due to the dynamic nature of the upgrade, some servers (typically only C-level) may be upgraded in a different cycle than displayed here.  4. In the Upgrade Settings section of the form, use the **Upgrade ISO** options to select the target ISO. 5. 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. 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

Procedure 28. Automated Site Upgrade

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)

Alarm ID = 31114 (DB Replication over SOAP has failed)

Alarm ID = 31225 (HA Service Start Failure)

Note: Do not accept any upgrades at this time.

If the upgrade fails, do not proceed. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 28. Automated Site Upgrade

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 My Oracle Support (MOS) by referring to Appendix P of this document and provide these files. Refer to Appendix K 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. ☐	**Server CLI**: Update the tuned profile	After a successful upgrade has been verified, access the server on command line (using ssh or console) and update the tuned profile on each server.
		`$ sudo /usr/TKLC/dsr/bin/tuned.sh`
		Verify whether the tuned profile has been successfully set to **comcol_app**.
		`$ sudo tuned-adm active`
		Sample output:
		`admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`
		`[admusr@SOAM1 ~]$`

6. ☐	Post upgrade verification	Proceed to section 5.4 Site Post-Upgrade Procedures for post upgrade verification procedures.

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, SS7-MPs, vSTP MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions in-service to process traffic. In case of incremental upgrades, starting with release 8.1, one-half of the vSTP MPs can be upgraded. In release 8.1, there can be only one vSTP MP server in one vSTP server group and eventually one in a site.

The fourth cycle upgrades the second half of the DA-MPs, SS7-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 SS7-MPs	½ SS7-MPs
		½ IPFEs	½ IPFEs
		1 vSTP MP	

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, SS7-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, SS7-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 SS7-MPs	½ SS7-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. 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, SS7-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, SS7-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 SS7-MPs	½ SS7-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 SS7-MP, 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.

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
SS7-MP 1 Hostname		Manual upgrade
SS7-MP 3 Hostname		Manual upgrade
SS7-MP 5 Hostname		Manual upgrade
SS7-MP 7 Hostname		Manual 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
SS7-MP 2 Hostname		Manual upgrade
SS7-MP 4 Hostname		Manual upgrade
SS7-MP 6 Hostname		Manual upgrade
SS7-MP 8 Hostname		Manual 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 22	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 23 or Procedure 24	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:25	Site Pre-Upgrade Health Check for Release 8.0 and Later Site Pre-Upgrade Health Check for Release 7.x/8.x	None None
Procedure 25	0:01-0:05	0:16-0:35	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 29	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 SS7-MPs, ½ IPFEs, Spare SBR(s), 1 vSTP MP	Refer to Section 5.3.4 for details
Iteration 4	0:40-1:00	2:57-4:40	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s)	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	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 35	0:02	2:59-5:42	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 36	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 31 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 31 Manual SOAM Upgrade (Active/Standby/Spare) is the recommended procedure. The manual upgrade procedure upgrades the standby and spare SOAMs in parallel, followed by the active SOAM.

Table 18. SOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Iteration 1 & 2 Procedure 30 or Procedure 31	1:20-2:40	1:20-2:40	Automated SOAM Upgrade (Active/Standby) Manual SOAM Upgrade (Active/Standby/Spare)	No traffic impact

5.3.3 Upgrade SOAMs

WARNING!

The following procedures must be completed before the start of SOAM upgrade: Procedure 22; [Procedure 23 or Procedure 24]; Procedure 26.

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 29 is required to ensure site provisioning is disabled.

If the site does **not** include a spare SOAM, use the automated SOAM upgrade in Procedure 30.

If the site does include a spare SOAM, use the manual SOAM upgrade in Procedure 31.

Procedure 29. SOAM Upgrade Pre-Checks

S T E P #	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 My Oracle Support (MOS) 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 26. 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 26 Disable Site Provisioning.

5.3.3.1 Automated SOAM Upgrade (Active/Standby)

Procedure 30 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 31. Upon completion of this procedure, proceed to Section 5.3.4 Upgrade Iteration 3.

Procedure 30. Automated SOAM Upgrade (Active/Standby)

S T E P #	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 My Oracle Support (MOS) 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 F Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix F, 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 31 upgrades the SOAM server group if the site includes a spare SOAM. If the SOAM server group was upgraded using Procedure 30, then do not execute this procedure; proceed to section 5.3.4 Upgrade Iteration 3.

Procedure 31. Manual SOAM Upgrade (Active/Standby/Spare)

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	Upgrade standby and spare SOAMs in parallel using the Upgrade Multiple Servers procedure	Execute Appendix F Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix F, return to this point and continue with the next step.
2. ☐	Upgrade active SOAM using Upgrade Single Server procedure	Execute Appendix D Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix D, 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, SS7-MPs, IPFEs, spare SBR(s), and vSTP MP server, if equipped. The vSTP server group can have only one server in release 8.1 and eventually one vSTP MP server in a site. 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

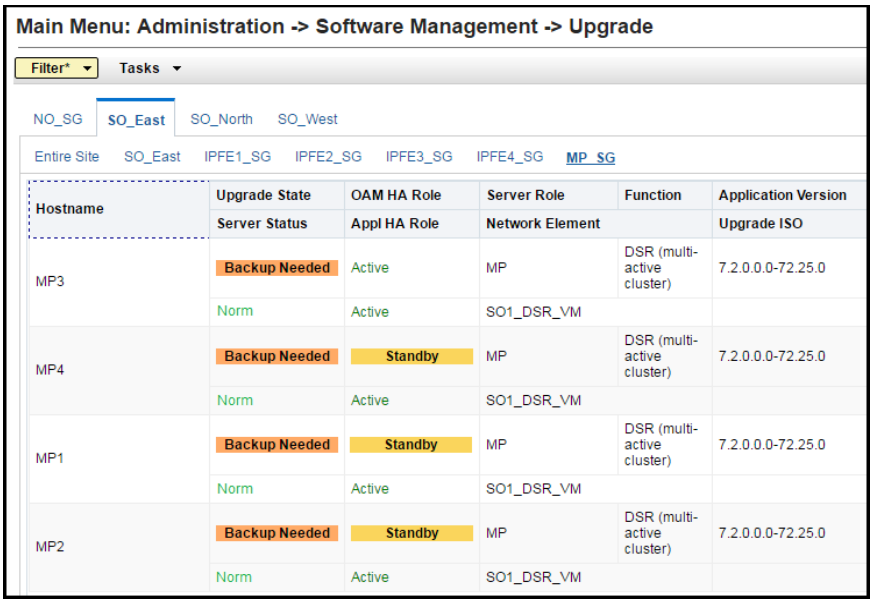
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 32	0:40-1:00	0:40-1:00	Upgrade Iteration 3	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, spare SBR(s), 1 of the vSTP MP servers will be offline

CAUTION

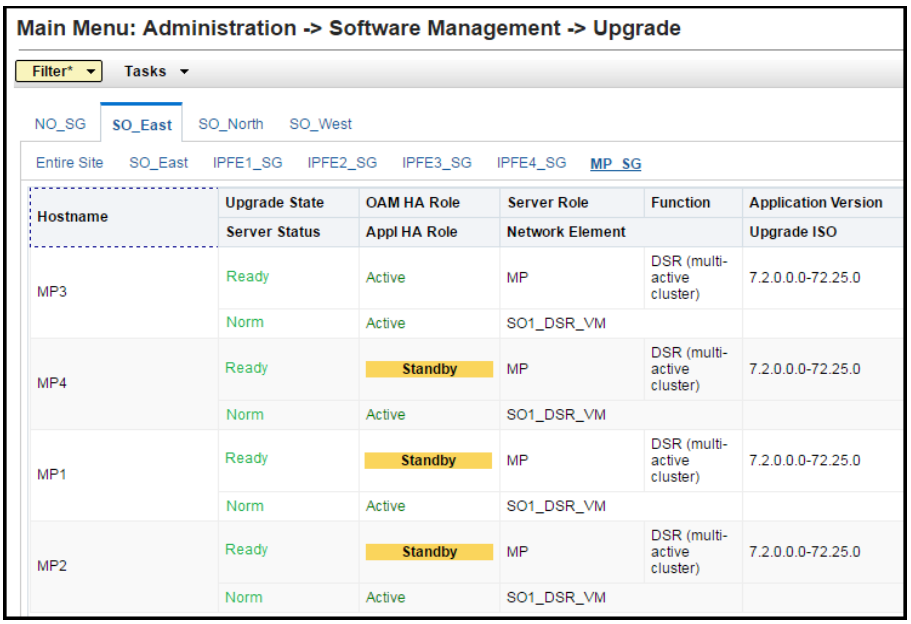
ASG does not allow the operator to specify the upgrade order of the DA-MP servers. If a manual upgrade was recommended in section 3.3, do not use ASG to upgrade the DA-MPS in this iteration. Alternate upgrade procedures are provided Appendix G.3

Procedure 32 upgrades ½ of the DA-MPs, ½ of the SS7-MPs, ½ of the IPFEs, and the spare SBR(s). For release 8.1, ½ of the vSTP MP servers for incremental upgrade. The vSTP server group can have only one server in 8.1. Refer to Table 16 for the hostnames of the servers to be upgraded in this iteration.

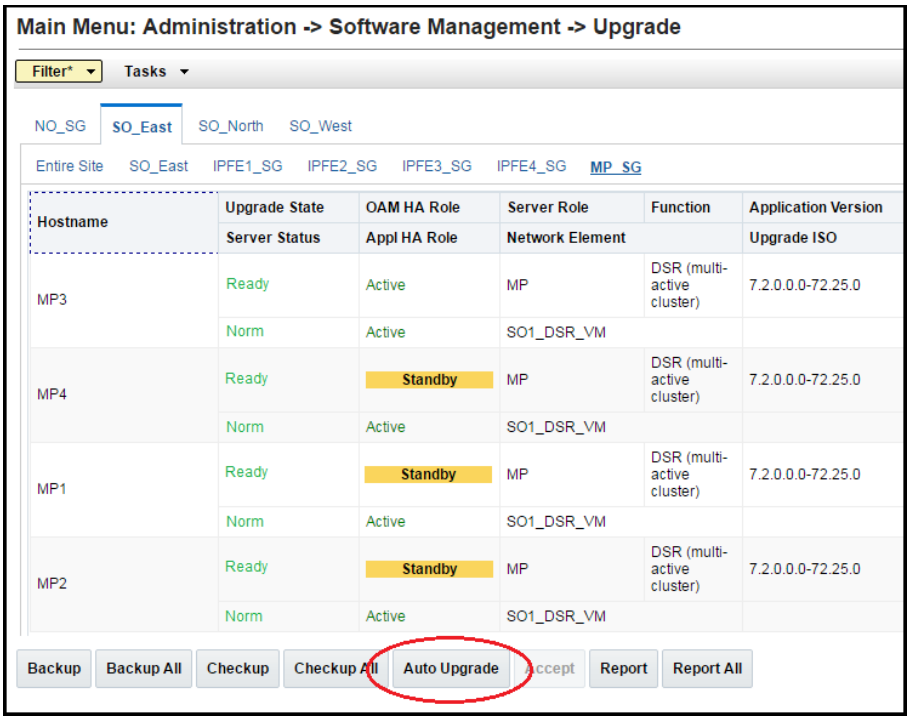
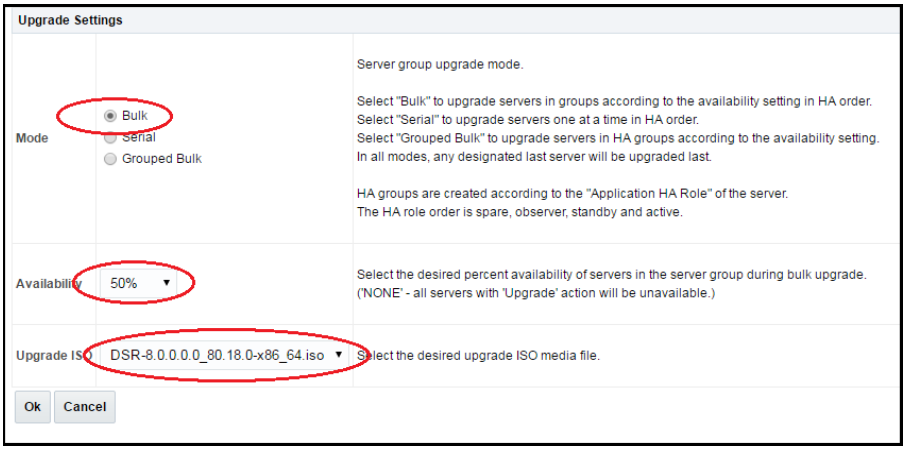
Procedure 32. Upgrade Iteration 3

S T E P #		
	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 My Oracle Support (MOS) 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. 

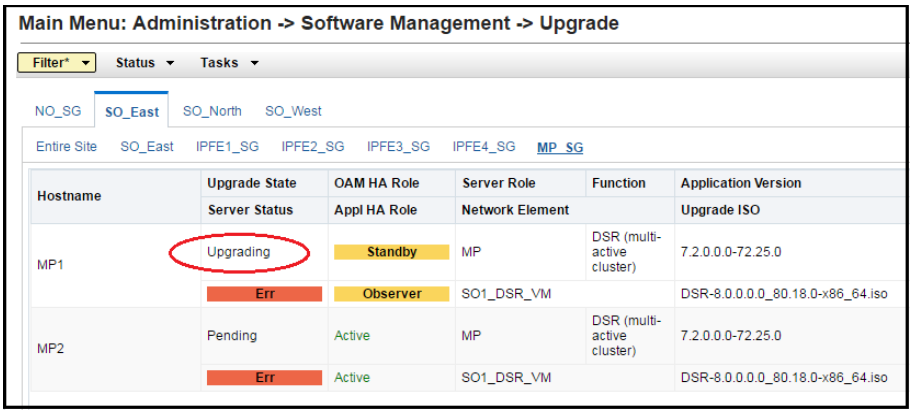
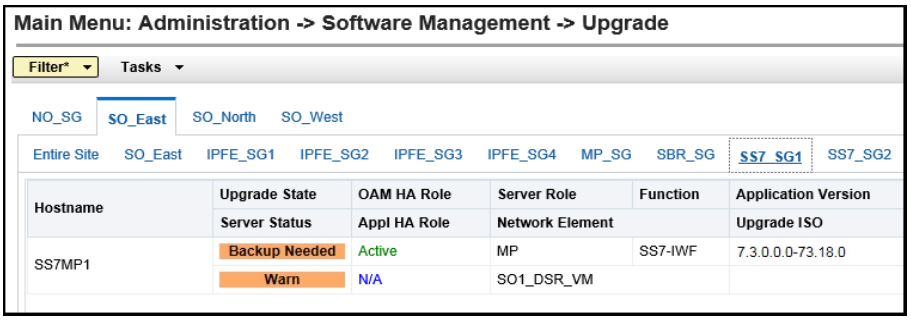
Procedure 32. Upgrade Iteration 3

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.  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)**

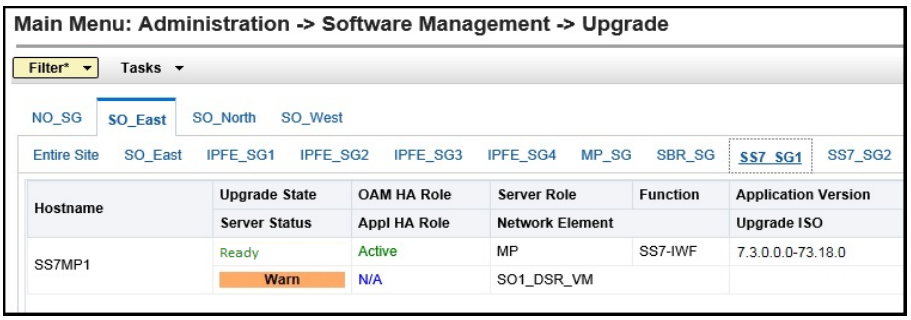
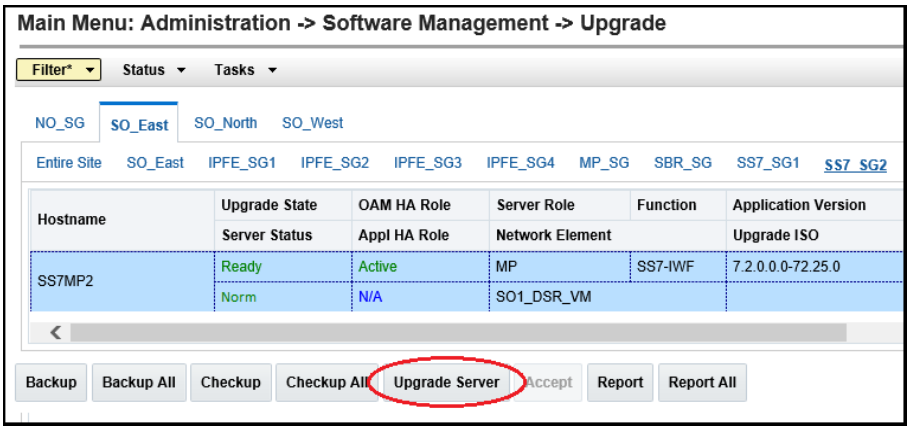
Procedure 32. Upgrade Iteration 3

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. 

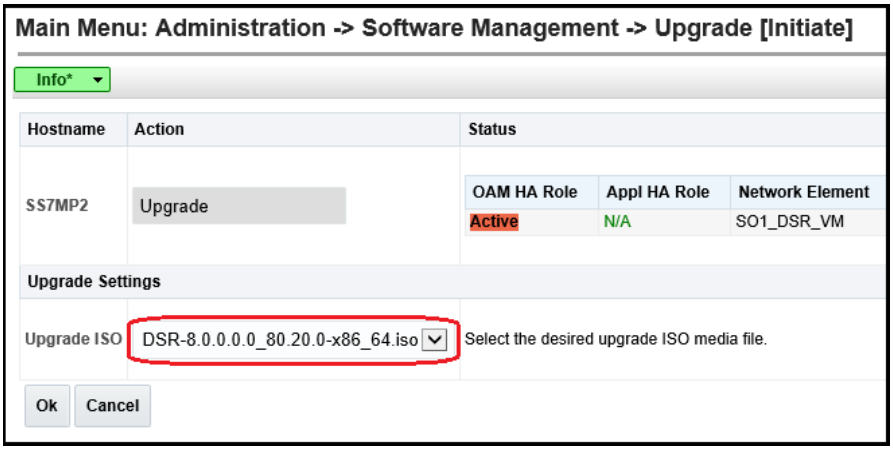
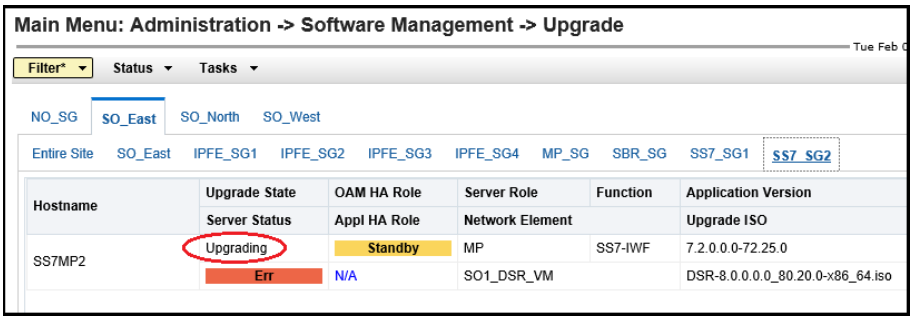
Procedure 32. Upgrade Iteration 3

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.  Main Menu: Administration -> Software Management -> Upgrade Filter* Status 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 MP1 — Upgrading — Standby — MP — DSR (multi-active cluster) — 7.2.0.0.0-72.25.0 Err — Observer — SO1_DSR_VM — DSR-8.0.0.0.0_80.18.0-x86_64.iso MP2 — Pending — Active — MP — DSR (multi-active cluster) — 7.2.0.0.0-72.25.0 Err — Active — SO1_DSR_VM — DSR-8.0.0.0.0_80.18.0-x86_64.iso While the DA-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
7. ☐	Identify the SS7-MP server group(s) to upgrade	From the data captured in Table 16, identify the SS7-MP server group(s) to upgrade in iteration 3.
8. ☐	**Active NOAM VIP**: View pre-upgrade status of SS7-MPs 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 SS7-MP Server Group to upgrade. 4. For the SS7-MP 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 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 SS7MP1 — Backup Needed — Active — MP — SS7-IWF — 7.3.0.0.0-73.18.0 Warn — N/A — SO1_DSR_VM

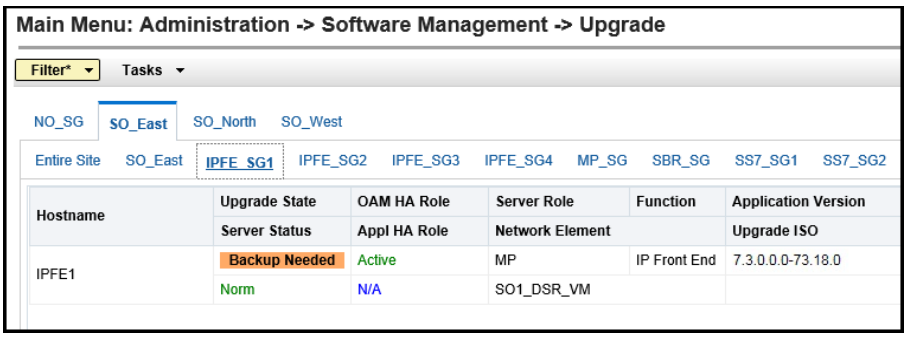
Procedure 32. Upgrade Iteration 3

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 SS7-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)**
10. ☐	**Active NOAM VIP**: Initiate SS7-MP upgrade (part 1)	Select the Upgrade Server method. 1. From the Upgrade Administration screen, select the server to upgrade. 2. Click **Upgrade Server**. 

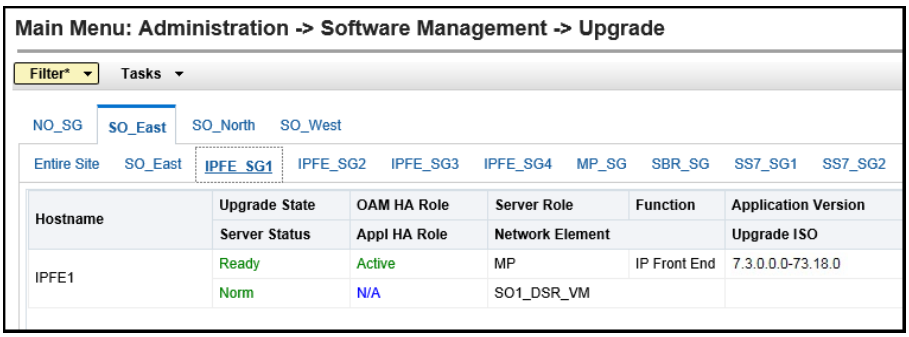
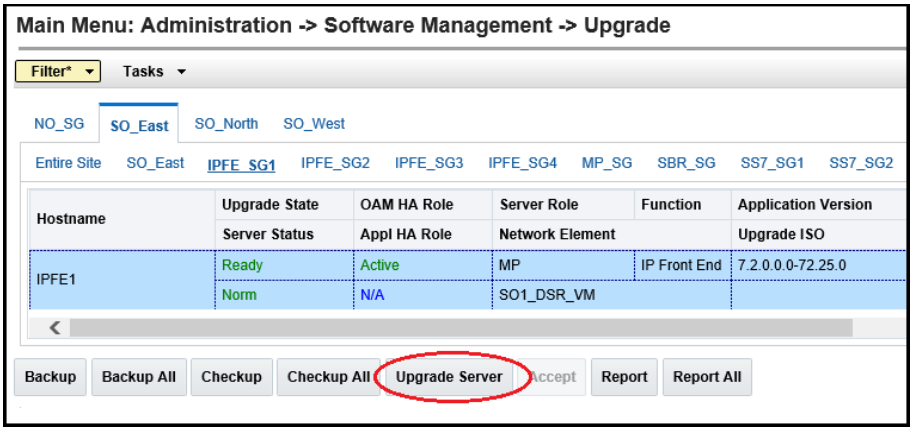
Procedure 32. Upgrade Iteration 3

11. ☐	**Active NOAM VIP**: Initiate SS7-MP 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. 
12. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	Observe the upgrade state of the SS7-MP server. Upgrade status is displayed under the Status Message column. 
13. ☐	Repeat for each SS7-MP	Repeat steps 6. through 12. for the next SS7-MP to upgrade per Table 16.
14. ☐	Continue upgrade iteration 3	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
15. ☐	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.

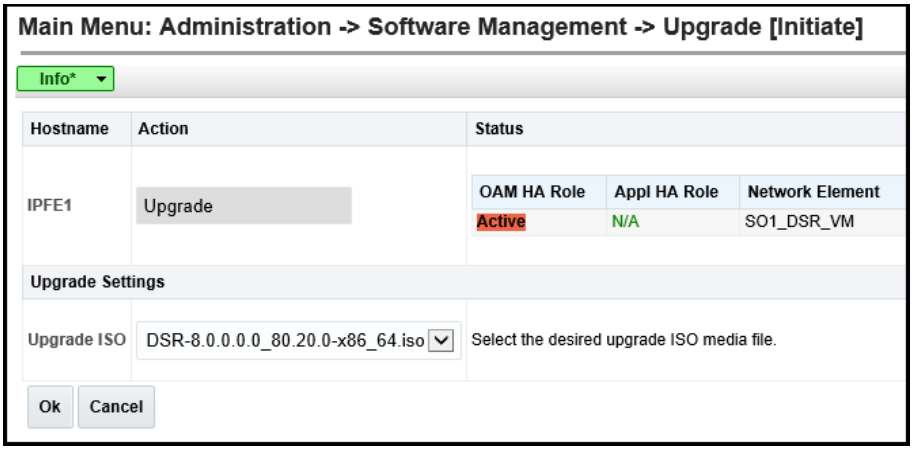
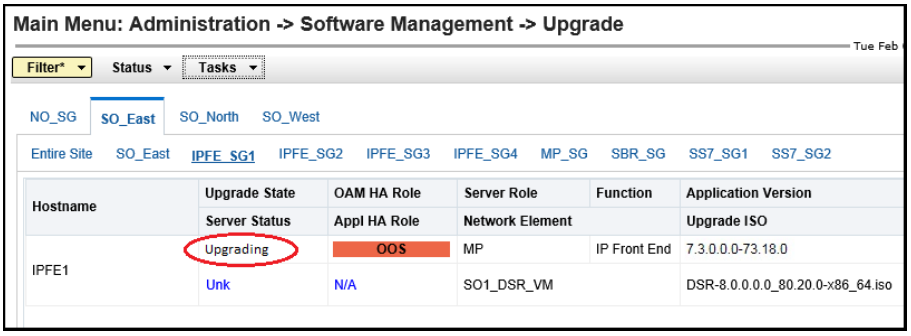
Procedure 32. Upgrade Iteration 3

16. ☐	**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. 

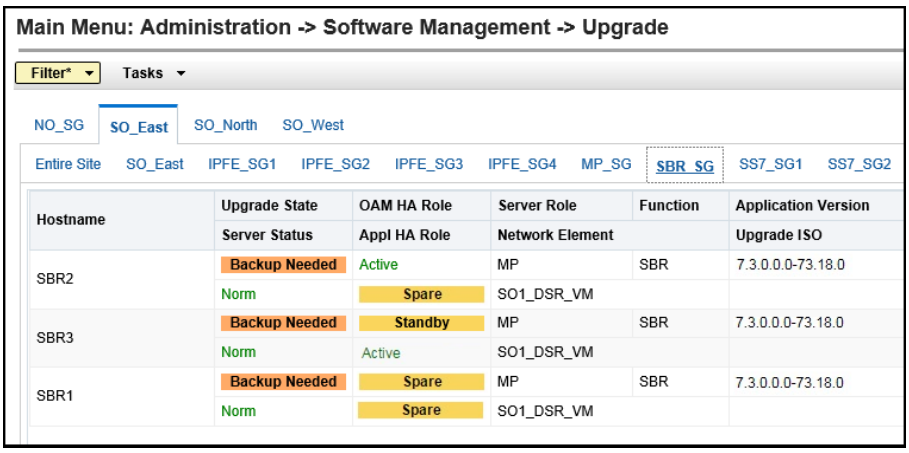
Procedure 32. Upgrade Iteration 3

17. ☐	**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)**
18. ☐	**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**. 

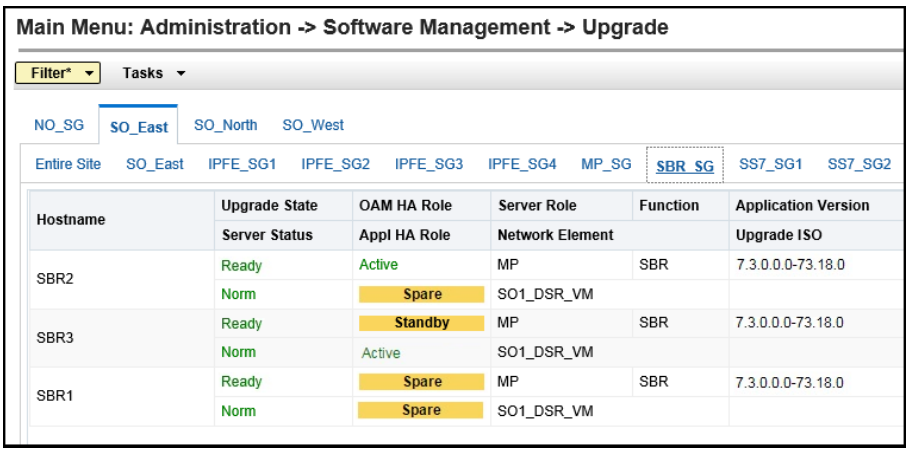
Procedure 32. Upgrade Iteration 3

19. ☐	**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. 
20. ☐	**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. 
21. ☐	Repeat for each IPFE	Repeat steps 15. through 20. for the next IPFE to be upgraded in this iteration per Table 16.
22. ☐	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.

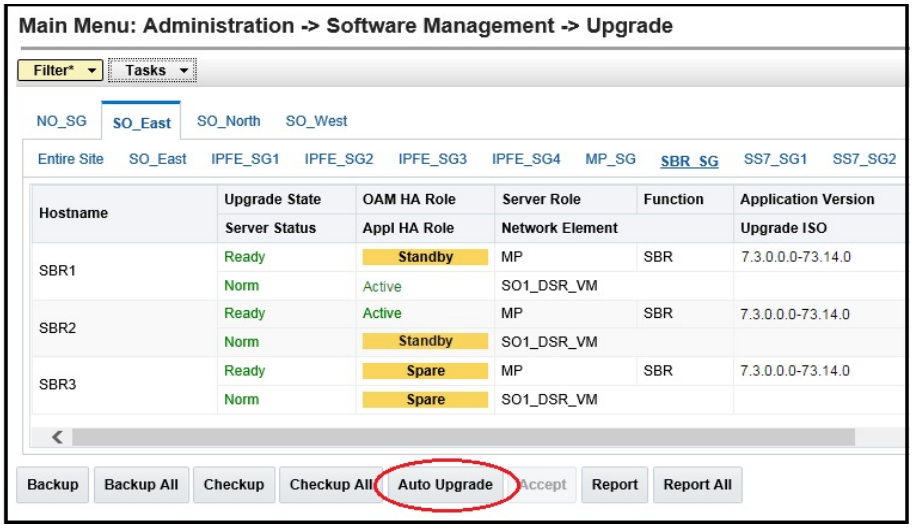
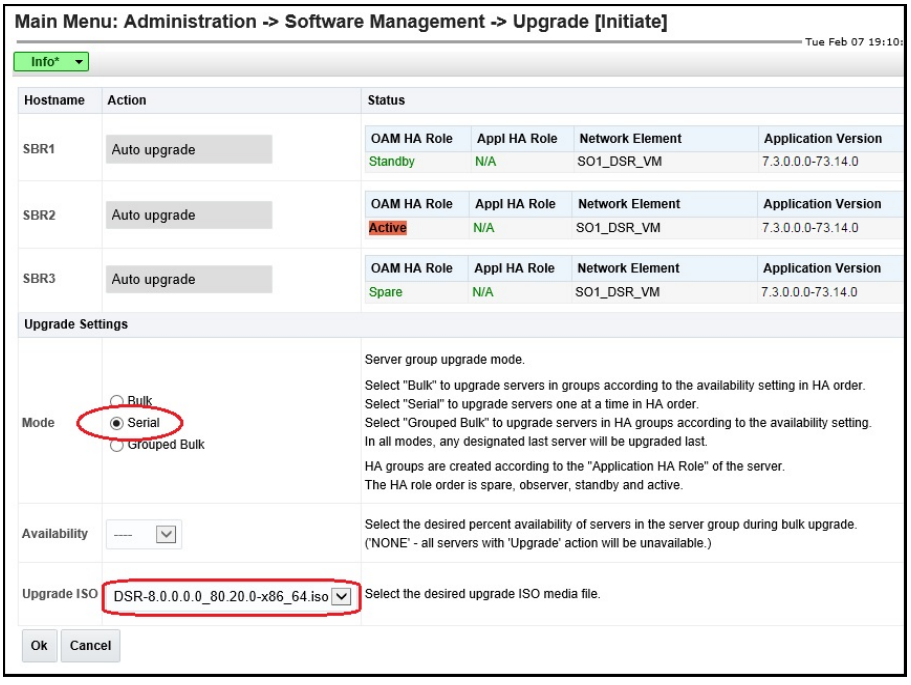
Procedure 32. Upgrade Iteration 3

23. ☐	**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. 

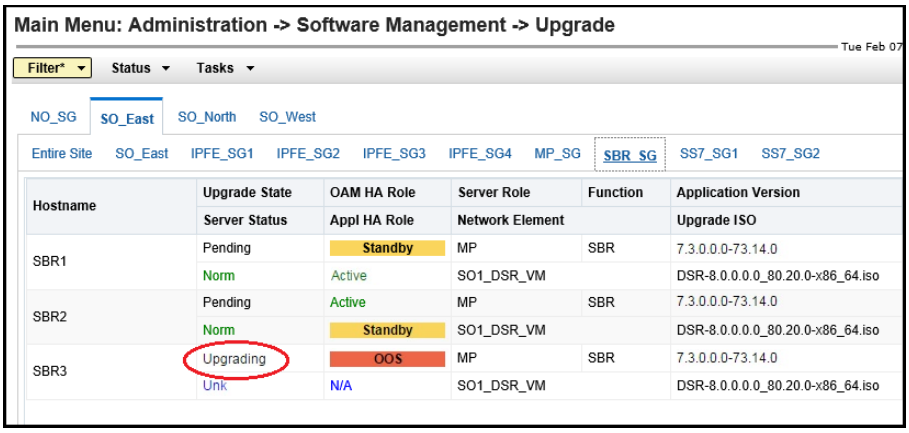
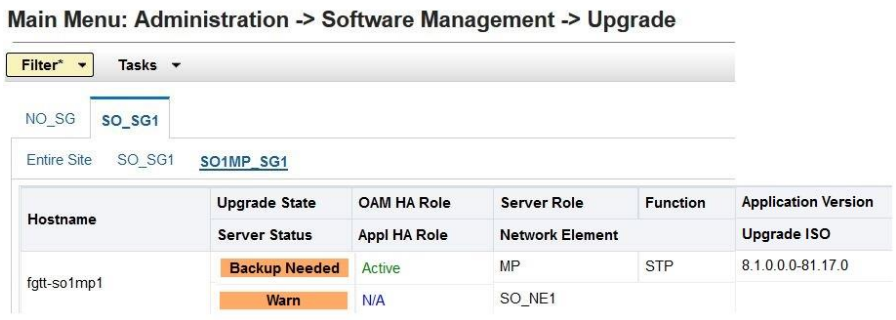
Procedure 32. Upgrade Iteration 3

24. ☐	**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.  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)**

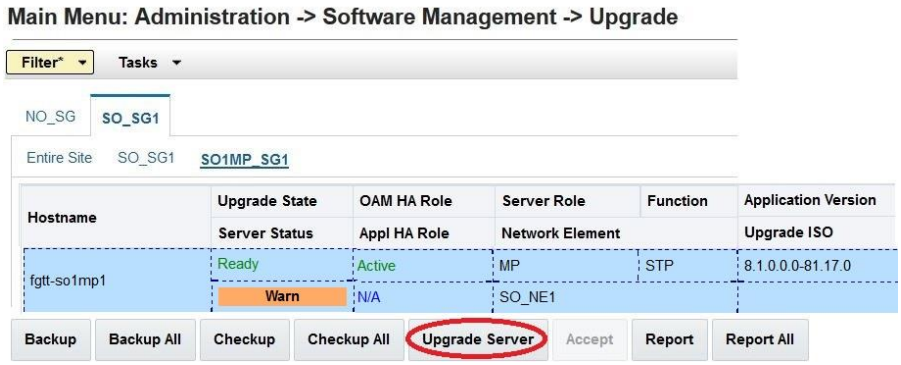
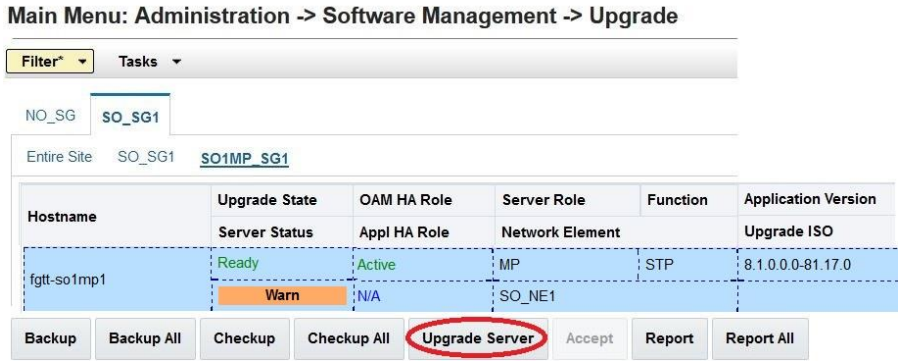
Procedure 32. Upgrade Iteration 3

25. ☐	**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**. 
26. ☐	**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. 

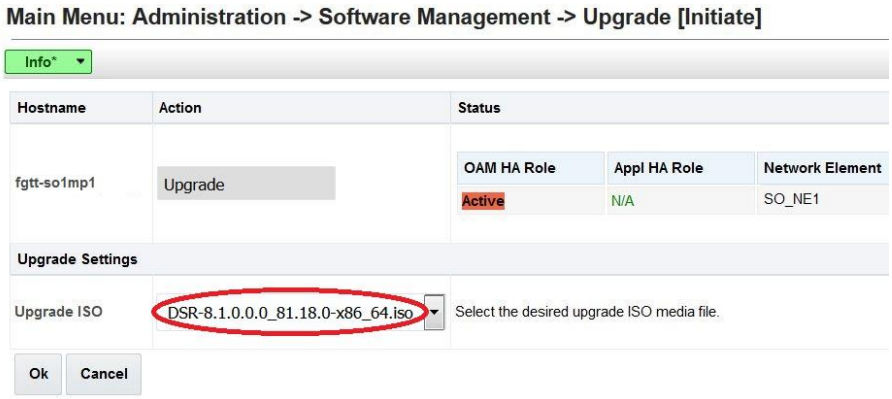
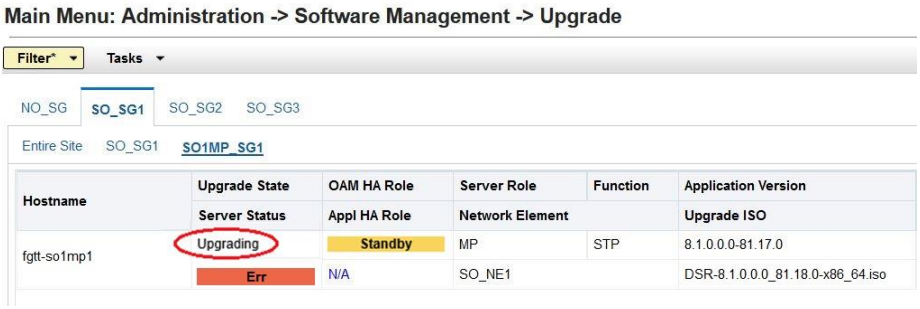
Procedure 32. Upgrade Iteration 3

27. ☐	**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). 
28. ☐	Repeat for each SBR server group	Repeat steps 22. through 27. for the next SBR server group to be upgraded per Table 16.
29. ☐	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.
30. ☐	**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. 

Procedure 32. Upgrade Iteration 3

31. ☐	**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)**
32. ☐	**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**. 

Procedure 32. Upgrade Iteration 3

33. ☐	**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. 
34. ☐	**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. 
35. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	See step 36. 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. ***Note***: Not all servers have all alarms: **Alarm ID = 10008 (Provisioning Manually Disabled)** **Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)**

Procedure 32. Upgrade Iteration 3

		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 L to 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 SS7-MP and 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 SS7-MP and 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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.**

36. ☐	**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 My Oracle Support (MOS) by referring to Appendix P of this document and provide these files. Refer to Appendix K 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, SS7-MPs, vSTPs, and IPFEs, as well as the standby SBR(s), if equipped.

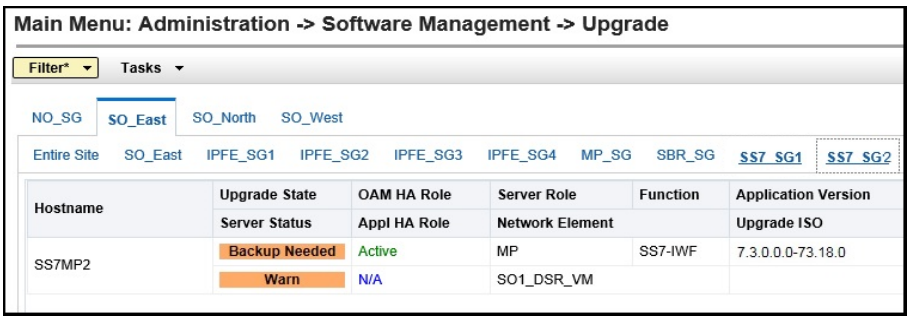
Table 20 shows the estimated time required to upgrade the C-level servers for iteration 4.

Table 20. Iteration 4 Upgrade Execution Overview.

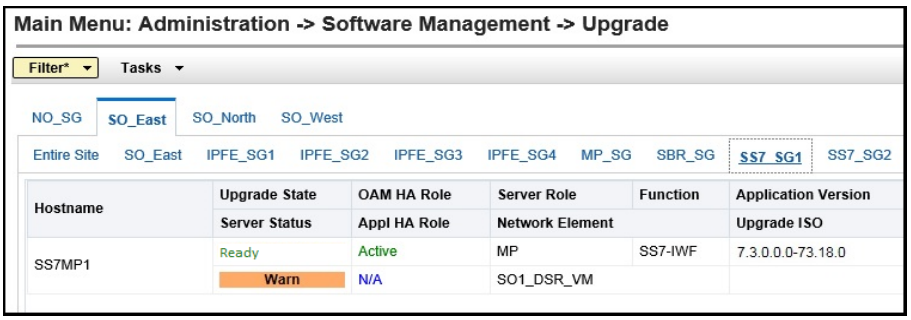
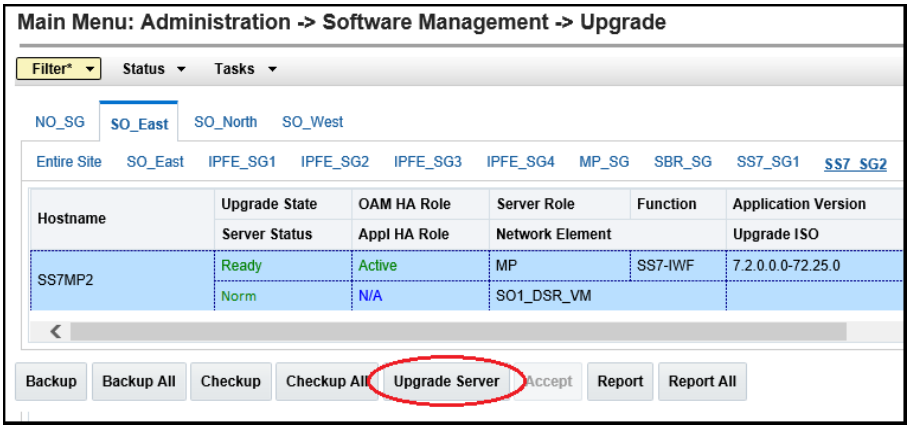
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 33	0:40-1:00	0:40-1:00	Upgrade Iteration 4	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, standby SBR(s), and vSTP servers will be offline

Procedure 33 provides the steps to upgrade ½ of the SS7-MPs, and ½ of the IPFEs. ASG automatically upgrades the DA-MPs and SBRs.

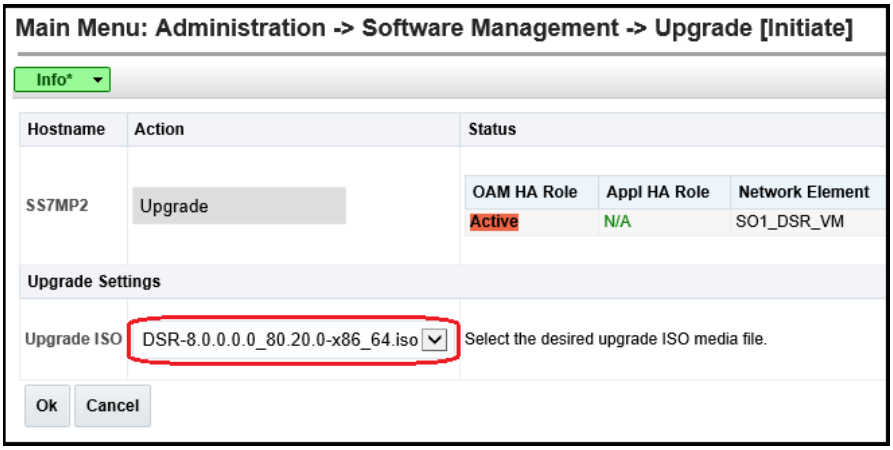
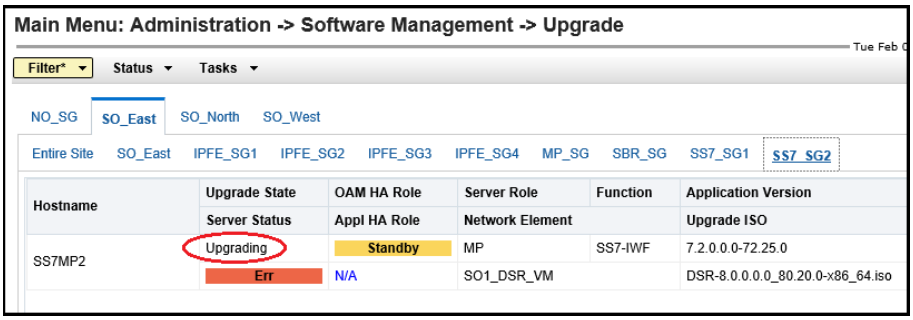
Procedure 33. Upgrade Iteration 4

S T E P #		
	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	Identify the SS7-MP server group(s) to upgrade	From the data captured in Table 16, identify the SS7-MP server group(s) to upgrade in iteration 4.
2. ☐	**Active NOAM VIP**: View pre-upgrade status of SS7-MPs	1. Navigate to **Administration > Software Management > Upgrade**. 2. Select the SOAM tab of the site to upgrade. 3. Select the link for each SS7-MP server group to be upgraded. 4. For the SS7-MP 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. 

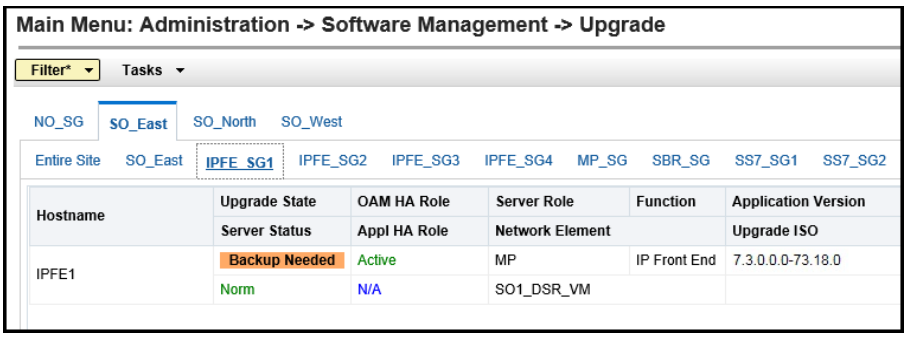
Procedure 33. Upgrade Iteration 4

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 SS7-MP server group to upgrade.  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 SS7-MP upgrade (part 1)	Select the Upgrade Server method. 1. From the Upgrade Administration screen, select the server to upgrade. 2. Click **Upgrade Server**. 

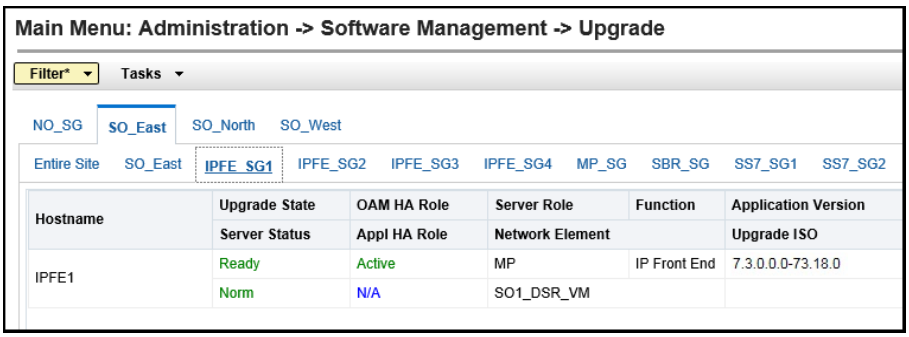
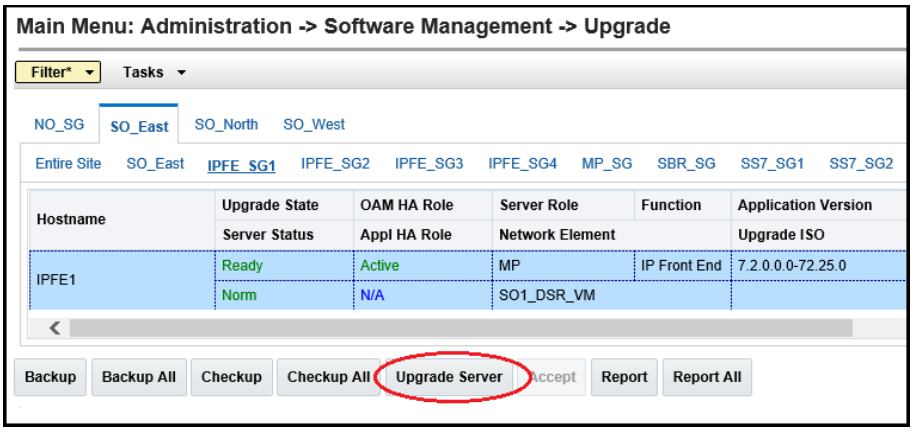
Procedure 33. Upgrade Iteration 4

5. ☐	**Active NOAM VIP**: Initiate SS7-MP 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 SS7-MP server. Upgrade status displays under the Status Message column. 
7. ☐	Repeat for each SS7-MP	Repeat steps 1. through 6. for the next SS7-MP to be upgraded in this iteration per Table 16.
8. ☐	Continue upgrade iteration 4	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
9. ☐	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.

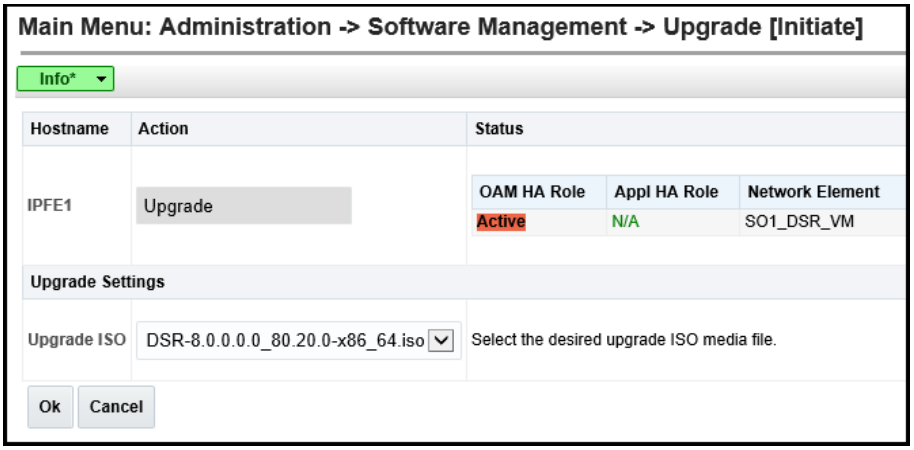
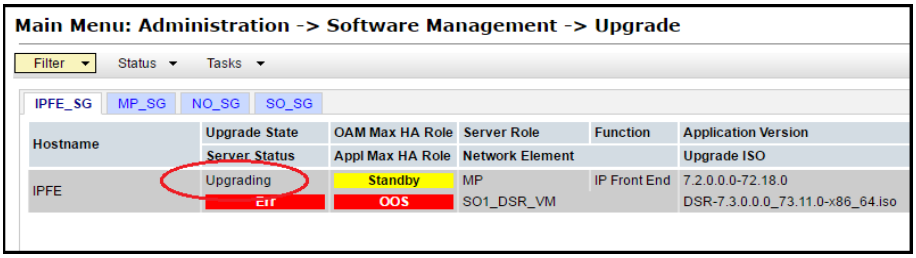
Procedure 33. Upgrade Iteration 4

10. ☐	**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. 

Procedure 33. Upgrade Iteration 4

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 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)**
12. ☐	**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**. 

Procedure 33. Upgrade Iteration 4

13. ☐	**Active NOAM VIP**: Initiate SS7-MP 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 IPFE server. Upgrade status displays under the Status Message column. 
15. ☐	Repeat for each IPFE	Repeat steps 9. through 14. for the next IPFE to be upgraded per Table 16.

16. ☐	**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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

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).

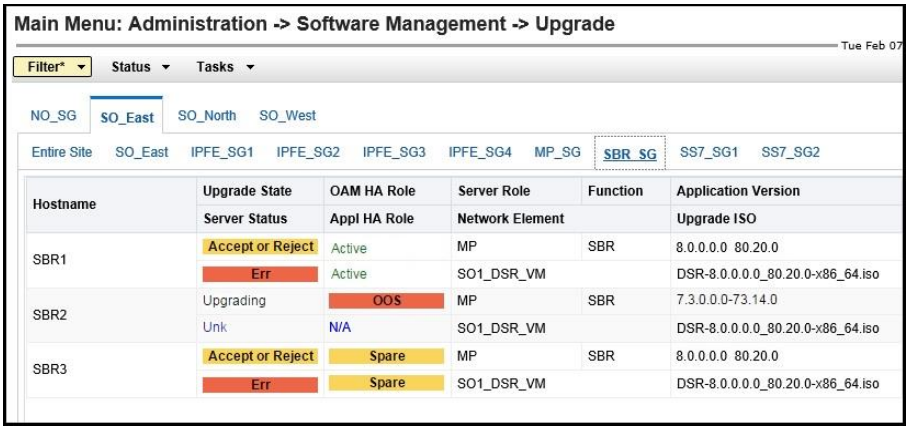
Table 21 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

Table 21. Iteration 5 Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 34	0:40-1:00	0:40-1:00	Upgrade Iteration 5	Standby SBR becomes active; previously active SBR is offline for upgrade

The SBRs are automatically upgraded by ASG so the task for iteration 5 is to monitor the upgrade progress. Refer to Table 16 for the hostnames of the servers upgraded in this iteration.

Procedure 34. Upgrade Iteration 5

S T E P #		
	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM VIP**: Iteration 5	At iteration 5, the active SBR is upgraded, causing the standby to become active. 

Procedure 34. Upgrade Iteration 5

2. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress	See step 3 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. ***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 L 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.

Procedure 34. Upgrade Iteration 5

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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K 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:

- Allow Site Provisioning
- Site Post-Upgrade Health Check

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

- 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 35. Allow Site Provisioning

S T E P #	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 My Oracle Support (MOS) 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**.

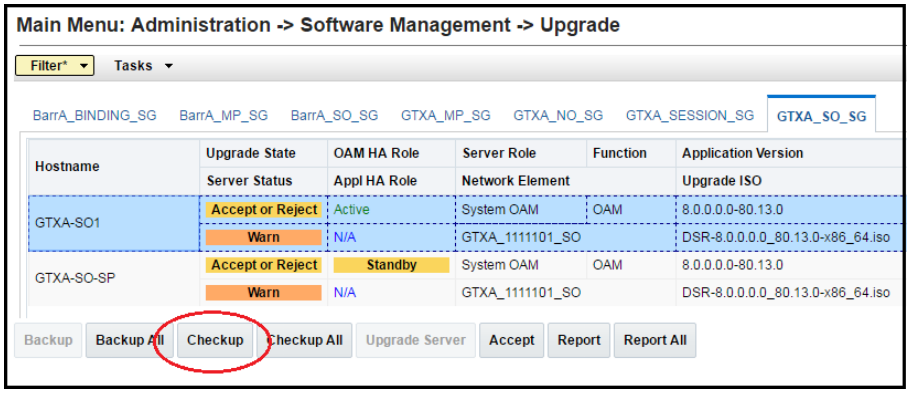
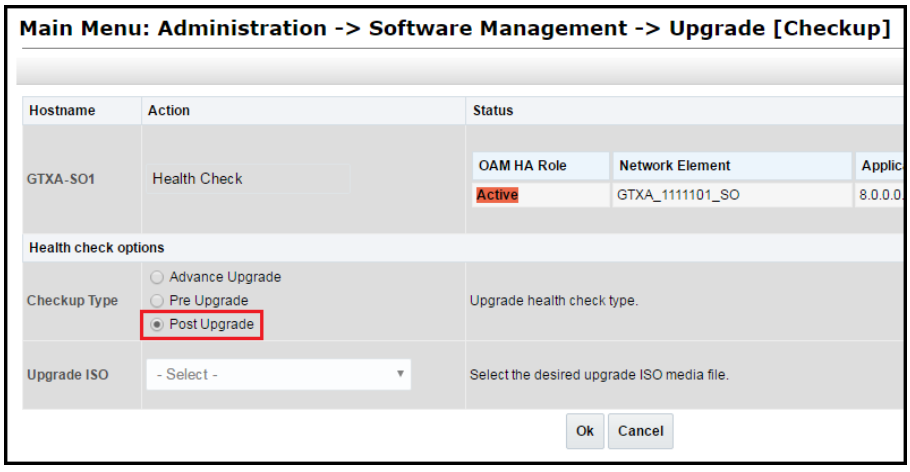
5.4.2 Site Post-Upgrade Health Checks

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

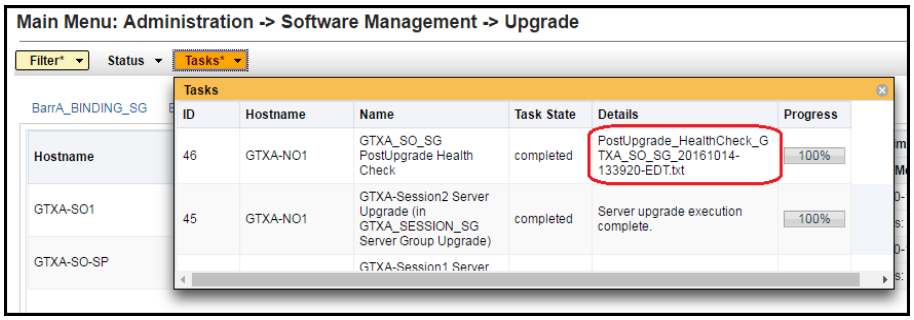
5.4.2.1 Site Post-Upgrade Health Check

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

Procedure 36. Site Post-Upgrade Health Check

S T E P #	This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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.** 

Procedure 36. Site Post-Upgrade Health Check

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. 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 My Oracle Support (MOS) for guidance as described in Appendix P. If the health check log contains the **Unable to execute Health Check on <Active NOAM hostname>** message, perform the health checks in Procedure 37 Alternate SOAM Post-Upgrade Health Check.
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.

Procedure 36. Site Post-Upgrade Health Check

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 2 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 My Oracle Support (MOS).

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 36.

Procedure 37. Alternate SOAM Post-Upgrade Health Check

S T E P #	This procedure verifies post-upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. 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.

Procedure 37. Alternate SOAM Post-Upgrade Health Check

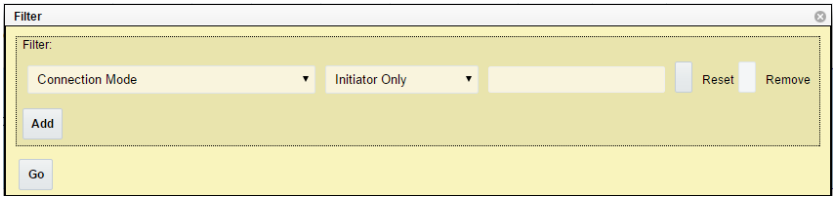
2. ☐	**Active SOAM CLI**: Capture Diameter maintenance status	Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command displays a series of messages providing Diameter Maintenance status. Capture this output and save for later use. ***Note***: The output is also captured in **/var/TKLC/db/filemgmt/UpgradeHealthCheck.log**. ***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 38. Post-Upgrade Procedures

S T E P #	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 8.0/8.1 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.
2. ☐	**Active SOAM VIP**: Toggle initiator connections **For source release 7.0 only**	**This step is required only if the source release is DSR 7.0**. 1. Navigate to **Diameter > Maintenance > Connections**. 2. Use the filter settings to search for **Initiator Only** connections.  3. If the resulting list is empty, this step is complete. Otherwise, for the connections in the search results: 4. Select one or more connections ***Note***: The following steps momentarily disrupt traffic flow for the selected connections. 5. Click **Disable**. 6. Click **Enable**. 7. Verify the Admin State changes to **Enabled**.

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 39	0:10-0:30	0:10-0:30	Backout Health Check 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 40	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 41	See Note	See Note	Emergency Site Backout ***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 46	See Note	See Note	Back Out Multiple Servers ***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 42	See Note	See Note	Emergency NOAM Backout ***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 47	0:01-0:05	Varies	Post-Backout Health Check	None

Table 23. Normal Backout Procedure Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum		
Procedure 39	0:10-0:30	0:10-0:30	Backout Health Check 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 40	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning
Procedure 43	See Note	See Note	Normal Site Backout ***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 46	See Note	See Note	Back Out Multiple Servers ***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 44	See Note	See Note	Normal NOAM Backout ***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 47	0:01-0:05	Varies	Post-Backout Health Check	None

6.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to My Oracle Support (MOS) by referring to Appendix P of this document. Before executing any of these procedures, it is recommended to contact My Oracle Support (MOS).

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 P.

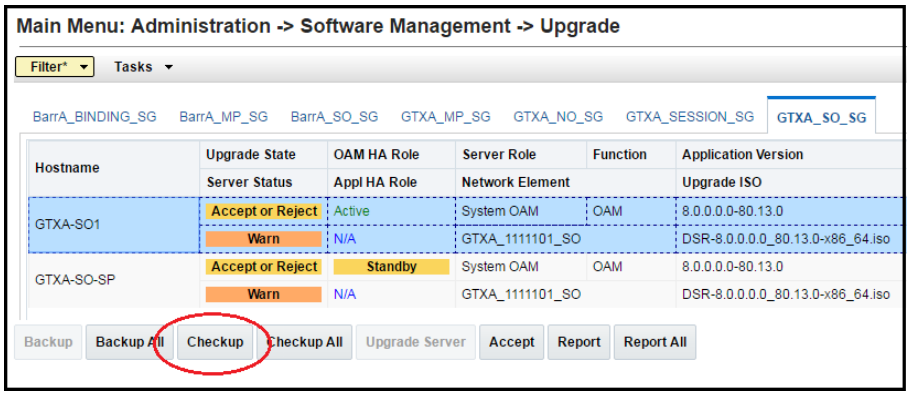
Backout procedures cause traffic loss.

Note: These recovery procedures are provided for the backout of an upgrade ONLY (that is, from a failed 8.0/8.1 release to the previously installed 7.0.w release). Backout of an initial installation is not supported.

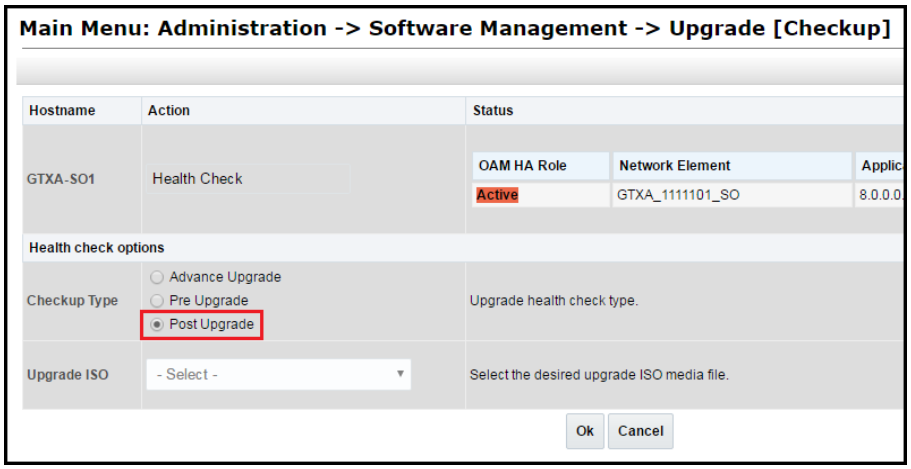
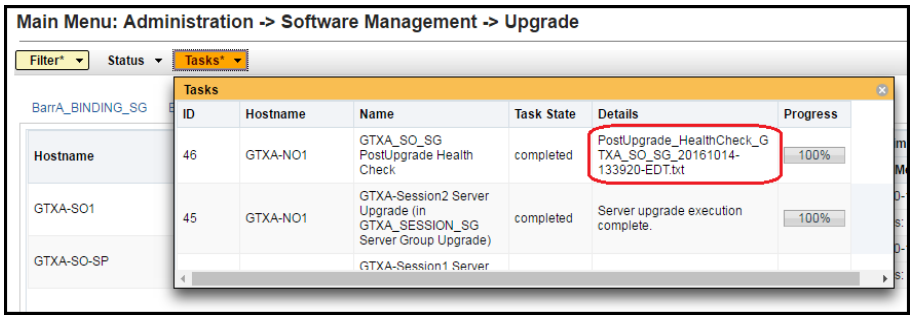
6.2 Backout Health Check

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 39. Backout Health Check

S T E P #	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 My Oracle Support (MOS) and ask for assistance.	
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**.

Procedure 39. Backout Health Check

		7. Click **OK**. Control returns to the Upgrade screen. 
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. 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 My Oracle Support (MOS) for guidance as described in Appendix P.

Procedure 39. Backout Health Check

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.

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`

Procedure 39. Backout Health Check

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 74% 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 75% 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 40. Disable Global Provisioning

S T E P #	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 41. Emergency Site Backout

S T E P #		
	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, SS7-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, DA-MPs, and SS7-MPs) identified in step 1: Execute Procedure 46 Back Out Multiple Servers.

Procedure 41. Emergency Site Backout

4. ☐	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 46 Back Out Multiple Servers. **If only a spare SOAM server is present:** Execute Procedure 45 Back Out Single Server.
5. ☐	Back out the active DSR SOAM server	Execute Procedure 45 Back Out Single Server.
6. ☐	**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 42. Emergency NOAM Backout

STEP #	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 45 Back Out Single Server.
2. ☐	Back out the active DR NOAM server (now the standby) (if equipped)	Execute Procedure 45 Back Out Single Server.
3. ☐	Back out the standby DSR NOAM server (as applicable)	Execute Procedure 45 Back Out Single Server.
4. ☐	Back out the active DSR NOAM server (now the standby)	Execute Procedure 45 Back Out Single Server.

Procedure 42. Emergency NOAM Backout

5. ☐	**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. ☐	**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 43. Normal Site Backout

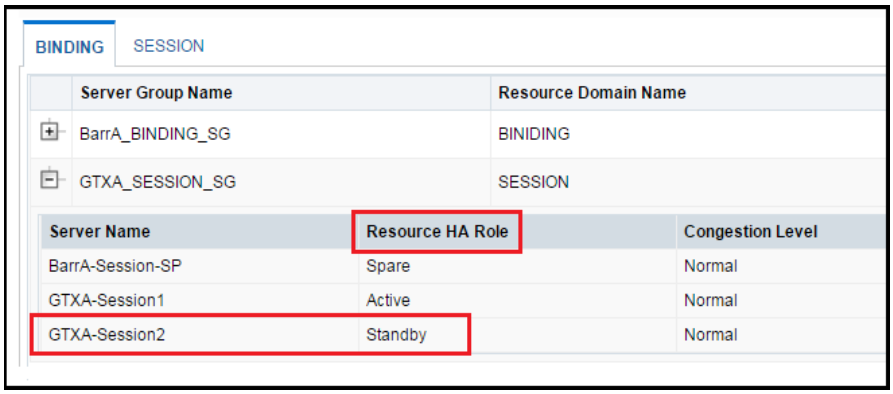
S T E P #	This procedure backs out an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step 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 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)**

Procedure 43. Normal Site Backout

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): • Standby DA-MP for 1+1 (active/standby) configuration, or • ½ of all DA-MPs for N+0 (multi-active) configuration • Standby SBR(s) • Spare SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs Execute Procedure 45 Back Out Single Server 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.

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	Resource Domain Name
BarrA_BINDING_SG	BINIDING
GTXA_SESSION_SG	SESSION

Server Name	Resource HA Role	Congestion Level
BarrA-Session-SP	Spare	Normal
GTXA-Session1	Active	Normal
GTXA-Session2	Standby	Normal

Procedure 43. Normal Site Backout

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) • Active DA-MP for 1+1 (active/standby) configuration • ½ of all DA-MPs for N+0 (multi-active) configuration • Active SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs Execute Procedure 45 Back Out Single Server for each C-level server identified.
7. ☐	Back out the standby DSR SOAM server	Execute Procedure 45 Back Out Single Server.
8. ☐	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 45 Back Out Single Server.
9. ☐	Back out active DSR SOAM server	Execute Procedure 45 Back Out Single Server.

Procedure 43. Normal Site Backout

10. ☐	**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 44. Normal NOAM Backout

S T E P #	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 45 Back Out Single Server.
2. ☐	Back out other DR NOAM server (if equipped)	Execute Procedure 45 Back Out Single Server.
3. ☐	Back out standby DSR NOAM server (as applicable)	Execute Procedure 45 Back Out Single Server.
4. ☐	Back out active DSR NOAM server	Execute Procedure 45 Back Out Single Server.
5. ☐	**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 backout 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 45. Back Out Single Server

S T E P #	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. **For active NOAM on release 7.1 or later only**	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 O to have the NOAMP HA switch over. *** 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

Procedure 45. Back Out Single Server

		Disabled. 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 (for example, 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.

Procedure 45. Back Out Single Server

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

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) by referring to Appendix P of this document 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:

Procedure 45. Back Out Single Server

		`$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the server is on release 7.0.x or later:
		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.
		6. If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) by referring to Appendix P of this document for further instructions.

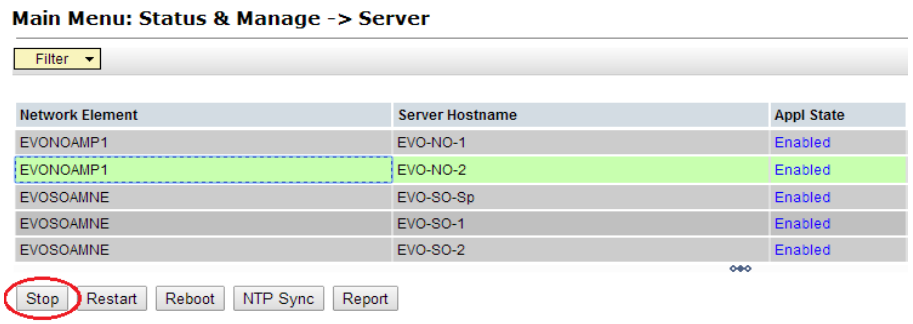
8. ☐	**Server CLI**: Reboot the server	Enter this command to reboot the server: `$ sudo init 6` This step can take several minutes.

Procedure 45. Back Out Single Server

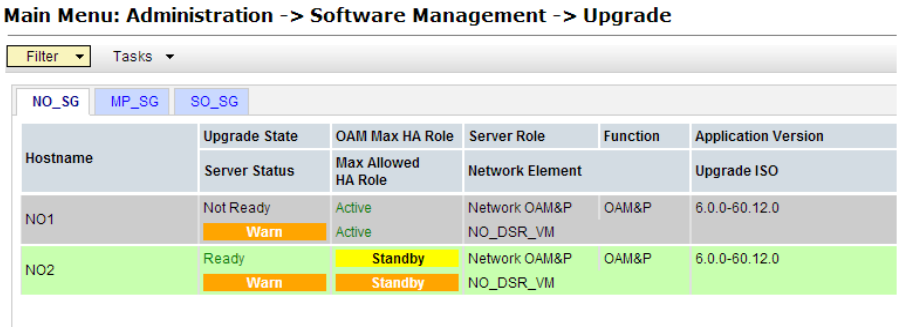
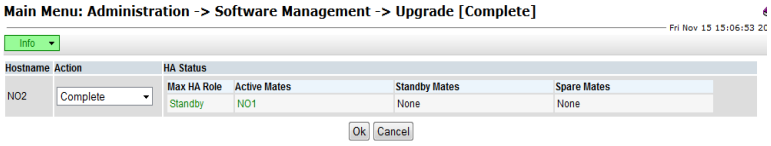
9. ☐	**Server CLI**: Verify OAM services restart (NOAM/SOAM only)	**If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 10.**
		1. Wait several (approximately 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH 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`
		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) by referring to Appendix P of this document 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**.

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 active NOAM is on release 7.1.x and later**: If the server status is **Not Ready**, proceed to the next step; otherwise, proceed to step 14. **If the active NOAM is on release 6.0 or 7.0.x**: If the server status is **Ready**, proceed to step 12. ; otherwise, proceed to step 14.

Procedure 45. Back Out Single Server

11. ☐	**Active NOAM VIP**: Change/Correct the Upgrade State on backed out server to **Ready** **For active NOAM on release 7.1.x and later**	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**. It may take a couple minutes for the grid to update. 13. Proceed to step 14 to complete this procedure.
12. ☐	**Active NOAM VIP**: Remove Upgrade Ready status and stop the Application **For active NOAM on release 7.0.x only**	To transition to the **Not Ready** state, stop the Application. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Status & Manage > Server**. 3. If the server just backed-out shows an Appl State of **Enabled**, then select the server row and click **Stop**. 

Procedure 45. Back Out Single Server

13. ☐	**Active NOAM VIP**: Change/Correct the Upgrade State on backed out server **For active NOAM on release 7.0.x only**	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 being backed out. 4. If the server just backed-out shows an Upgrade State of **Ready** or **Success**, then select the backed-out server and click **Complete**. **Otherwise, skip to step 14.**  5. Leave the Action set to the default value of **Complete** on the Upgrade Complete screen. 6. 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 display 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.
14. ☐	**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. The single server backout is now complete. Return to the overall DSR backout procedure step that directed the execution of this procedure.

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.

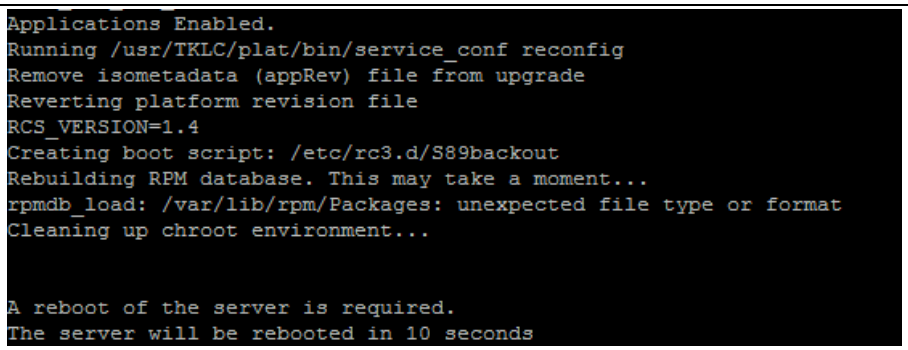
Procedure 46. Back Out Multiple Servers

S T E P #		
	This procedure backs out the upgrade of DSR 8.0/8.1 application software for multiple servers. Any server requiring a backout can be included: DA-MPs, SS7-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**: Prepare the server for backout For active NOAM on release 7.1.1 and later	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 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 upgraded, click **OK** to initiate an HA switchover and cause the GUI session to log out. Before logging into the active OAM again, close and re-open the browser using the VIP address for the NOAM, and 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 changes 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.

Procedure 46. Back Out Multiple Servers

<table>
<tr><td></td><td></td><td>Verify the Upgrade State is now Backout Ready.
Note: It may take a couple of minutes for the status to update.</td></tr>
<tr><td>2.
☐</td><td>Server CLI: Log into the server(s)</td><td>Use an SSH client to connect to the server (for example, ssh, putty):
<code>ssh admusr@<server address></code>
<code>password: <enter password></code>
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.</td></tr>
<tr><td>3.
☐</td><td>Server CLI:
Execute the backout</td><td>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 :
<code>$ ha.mystate</code>
In this example output, the HA state is Standby.
<pre>[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</pre>
If the state of the server is Active, then return to step 1.
Execute the reject command to imitate the backout:
<code>$ sudo /var/TKLC/backout/reject</code>
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:</td></tr>
</table>

Procedure 46. Back Out Multiple Servers

		
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.

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 P 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

Procedure 46. Back Out Multiple Servers

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 Feb 25 02:52:47 2015
        Product Name: DSR
     Product Release: 7.1.0.0.0_71.10.0
 Base Distro Product: TPD
 Base Distro Release: 7.0.0.0.0_86.14.0
     Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-
OracleLinux6.5-x86_64.iso
            ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso
                  OS: OracleLinux 6.5
```

If the server is on release 7.0.x or later:

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'
   ```

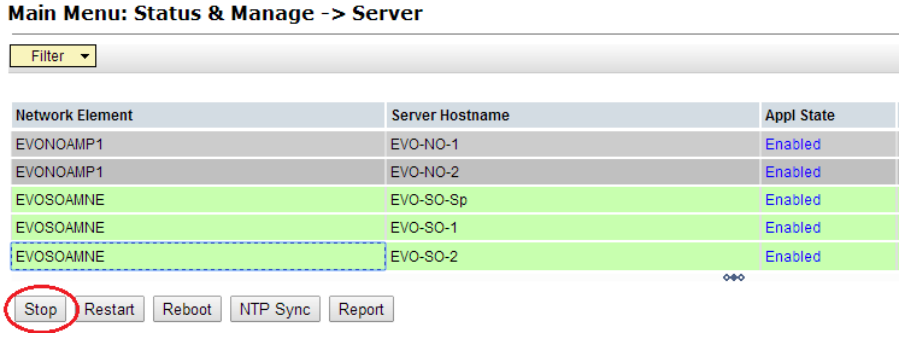
   Also, Disregard following error too

   ```
   ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log)
   reports errors!
   ```

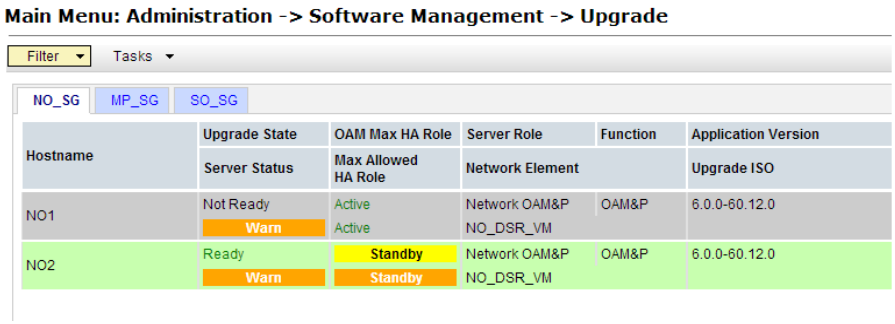
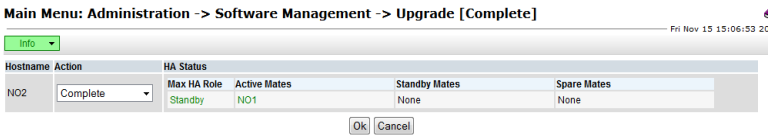
Procedure 46. Back Out Multiple Servers

		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) by referring to Appendix P of this document 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.
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.** 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) by referring to Appendix P of this document 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**.

Procedure 46. Back Out Multiple Servers

11. ☐	Repeat for each server backed out	Repeat steps 6 through 10 for each server backed out.
12. ☐	**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 7.1.1 or later, and the server status is **Not Ready**, proceed the next step; otherwise, proceed to step 16. 3. If the active NOAM is on release 7.0.1 and the server status is **Ready**, proceed to step 14. ; otherwise, proceed to step 16.
13. ☐	**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 16. to complete the procedure.
14. ☐	**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. 

Procedure 46. Back Out Multiple Servers

15. ☐	**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 an Upgrade State of **Not Ready**, then proceed to step 16.  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.
16. ☐	**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 47. Post-Backout Health Check

S T E P #	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 L 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

This procedure backs out the Oracle server.

This procedure is required only if backing out to IDIH release 7.0 or earlier. Do not back out the Oracle server if backing out to release 7.1 or later.

Procedure 48. Oracle Server Backout

S T E P #	This procedure performs a backout of the Oracle 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 My Oracle Support (MOS) and ask for assistance.	

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

2. ☐	**Oracle Server CLI**: Back out the server	Execute the following commands to back out the server.
		`sudo /opt/xIH/plat/bin/db_rollback.sh MED`
		`sudo /opt/xiH/plat/bin/db_rollback.sh APP`

6.9.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [6].

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!

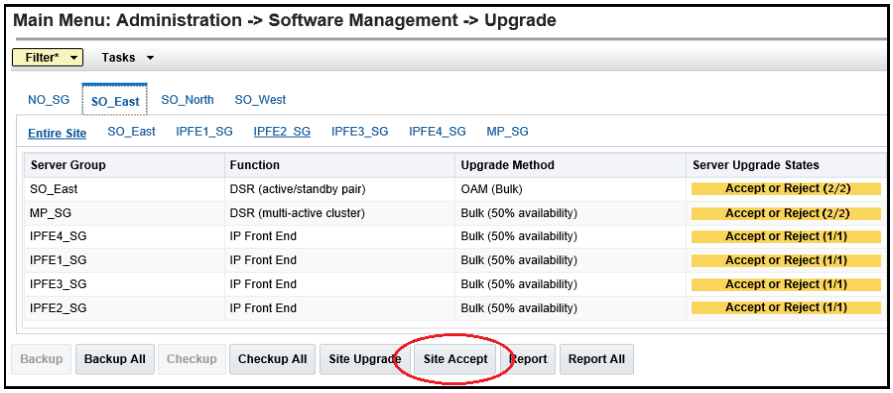
UPGRADE ACCEPTANCE MAY ONLY BE EXECUTED WITH AUTHORIZATION FROM THE CUSTOMER.

BE ADVISED THAT ONCE UPGRADE HAS BEEN ACCEPTED, IT IS NOT POSSIBLE TO BACK OUT TO THE PREVIOUS RELEASE

Procedure 49. Accept Upgrade

S T E P #	This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. 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)**
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)**

Procedure 49. Accept Upgrade

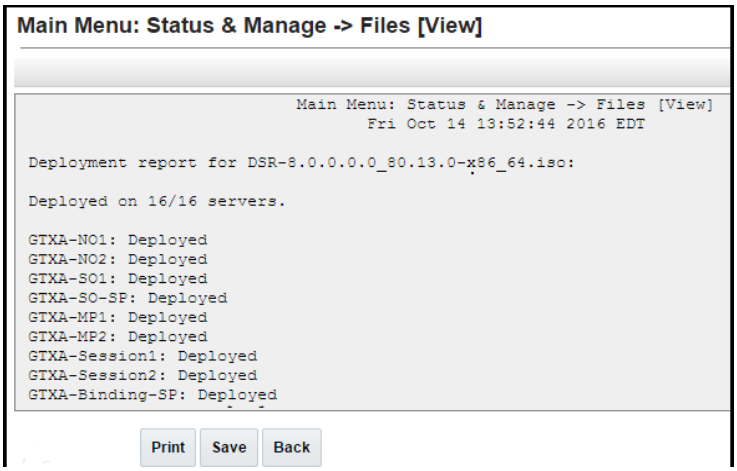
4. ☐	**Active NOAM VIP**: Accept upgrade for multiple servers	1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration >Software Management >Upgrade**. 3. Select the SOAM tab of the site being upgraded. ***Note***: The **Site Accept** button accepts the upgrade for every upgraded server 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**. **WARNING**: If you are upgrading from a release prior to SDS 7.1 and upgrade to release 7.1 or later, DNS port needs to be enabled. Refer to Appendix M for more information.  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 on 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 50. Undeploy ISO

S T E P #	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-8.0.0.0.0_80.12.0-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**. 
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. Reset COMCOL Compatibility Flags

Procedure 51. Reset COMCOL Compatibility Flags

S T E P #		
	This required procedure is 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	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 A.4. PCA Post Upgrade Procedure

CAUTION

This procedure is for PCA systems only!

Procedure 52 must be executed on PCA systems after the upgrade to DSR 8.0/8.1 is accepted. Do not run this procedure until **after** Procedure 49 has been completed. This procedure executes the PCA top-level activation script to remedy a potential PCA activation issue from earlier releases.

Procedure 52. PCA Post Upgrade Procedure

S T E P #	This procedure executes the PCA top level activation script. 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**: 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@<server address>`
		`password: <enter password>`

2. ☐	**Active NOAM CLI**: Run PCA activation script	Execute the top level PCA script:
		`/usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivationTopLevel`
		At the completion of the activation script, the following message is output:
		`Execution of PCA Activation Script complete.`

3. ☐	**Active NOAM CLI**: Clear cache	Execute the following command to reset the initialization caches: `clearCache`

Appendix B. Increase Maximum Number of Open Files

This 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 53. Increase Maximum Number of Open Files

S T E P #	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): _____

Procedure 53. Increase Maximum Number of Open Files

2. ☐	**Active NOAM CLI**: Maximum number of open files	Display the maximum number of open files for idbsvc.
		1. 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.
		2. 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.

Procedure 53. Increase Maximum Number of Open Files

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	1. 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`
		2. 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`
		3. 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) per Appendix P.

Appendix C. PCRF Pooling Migration Check

If the PCA application or the PDRA application has been activated in the source release, a check of the PCRF pooling migration is **REQUIRED** before the start of a major upgrade to DSR 8.0/8.1.

The PCRF Pooling Migration check is NOT required for a DSR 8.0 and DSR 8.1 incremental upgrade.

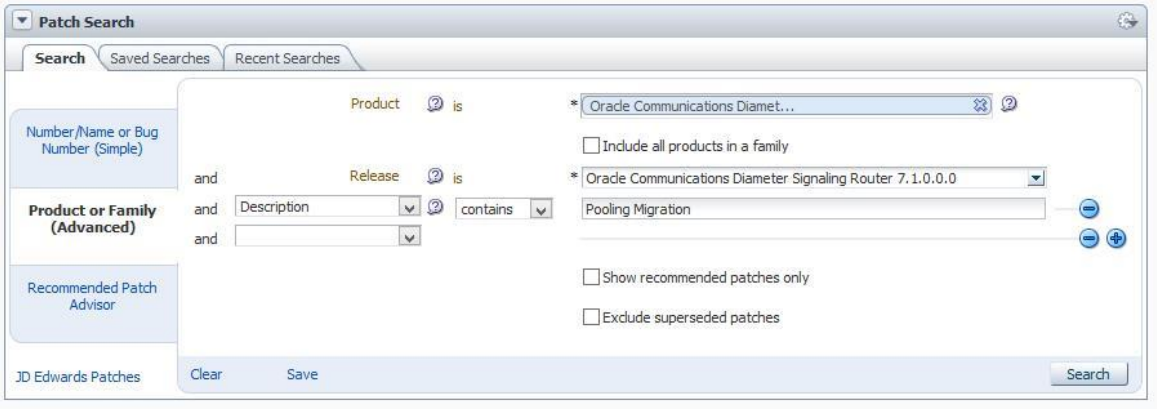
The PCRF Pooling Migration check is NOT required for a DSR 7.1, 7.2, 7.3, or 7.4 to 8.0 upgrade.

The PCRF Pooling Migration check is NOT required for a DSR 7.1, 7.2, 7.3, 7.4, or 8.0 to 8.1 upgrade.

Follow the steps in Procedure 54 to execute the PCRF Pooling Migration Check.

Note: If the PCRF pooling migration is NOT complete, this check must be repeated until PCRF pooling migration is complete and the tool indicates that upgrade is allowed.

Procedure 54. PCRF Pooling Migration Check

S T E P #		
	This procedure checks the PCRF Pooling Migration status to determine if the migration is complete. 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. ☐	Download PCRF Pooling Migration Tool from My Oracle Support (MOS)	The tool is used to determine the status of the PCRF pooling migration. 1. Navigate to the MOS site at **https://support.oracle.com/** and sign in. 2. Select the Patches & Updates tab. 3. In the Patch Search window, select the **Product or Family (Advanced)** tab on left. 4. Use the following search criteria to locate and download the migration tool (as shown in the figure): Product is: Oracle Communications Diameter Signaling Router (DSR) Release is: Oracle Communications Diameter Signaling Router (DSR) 7.1.0.0.0 ***Note***: The 7.1 Migration Tool is also valid for DSR 8.0/8.1. **Description contains**: Pooling Migration
		

Procedure 54. PCRF Pooling Migration Check

2. ☐	Copy the PCRF Pooling Migration Tool to the active NOAM	`scp –p <patchfilename> admusr@<Active_NOAM>`

3. ☐	**Active NOAM CLI**: SSH to the active NOAM	Using a SSH tool, log into the active NOAM server.
		`ssh admusr@<NOAM_VIP>`
		`password: <enter password>`

4. ☐	**Active NOAM CLI**: Move the patch file to the working directory	`sudo mv <patchfilename> /usr/TKLC/dsr/tools`
5. ☐	**Active NOAM CLI**: Change directory to the PCA tool directory	`cd /usr/TKLC/dsr/tools/`
6. ☐	**Active NOAM CLI**: Unzip the patch	Unzip the PCRF Pooling Migration Tool using the **unzip** command. Example: `sudo unzip <patchfilename>`

7. ☐	**Active NOAM CLI**: Check the PCRF pooling migration status	Check the PCRF Pooling Migration Status using the following command:
		`./verifyPCRFPoolingMigration.sh --checkPCRFPoolingMigrationStatus`
		Sample output:
		`Preparing log directory ...`
		`Creating log directory...`
		`Logging is started in /var/TKLC/log/migrationStatusToolLogs/migrationStatusTool.log`
		`Preparation of log directory done.`
		`============= Execution of PCRF Pooling Migration Verification Tool Started ===============`
		`Checking host server status whether it is active NOAMP server or not.`
		`This server is Active NOAMP server.`
		`Application Release is 7.0.1.0.0`
		`PDRA/PCA application is activated on this system.`
		`'PCRFPooling' feature is enabled on this system.`
		`PCRF Pooling Migration is not required. No need to check PCRF pool migration status. Exiting ...`
		`PCRF Pooling Migration is completed or not required on all servers.`
		`Execute tool again with option --verifyUpgradeAllowed to check if upgrade is allowed or not.`
		`============= Execution of PCRF Pooling Migration Verification Tool Completed =============`

Procedure 54. PCRF Pooling Migration Check

8. ☐	**Active NOAM CLI**: Verify PCRF pooling migration is complete	After executing the PCRF Pooling Migration tool, determine if the PCRF pooling migration has completed using the following command:
		`./verifyPCRFPoolingMigration.sh --verifyUpgradeAllowed`
		Note: This command informs the user when the PCRF pooling migration has completed.
		If PCRF pooling migration is complete, the command prints:
		`Upgrade is allowed.`
		If PCRF pooling migration is **NOT** complete, the command prints:
		`Upgrade is not allowed.`

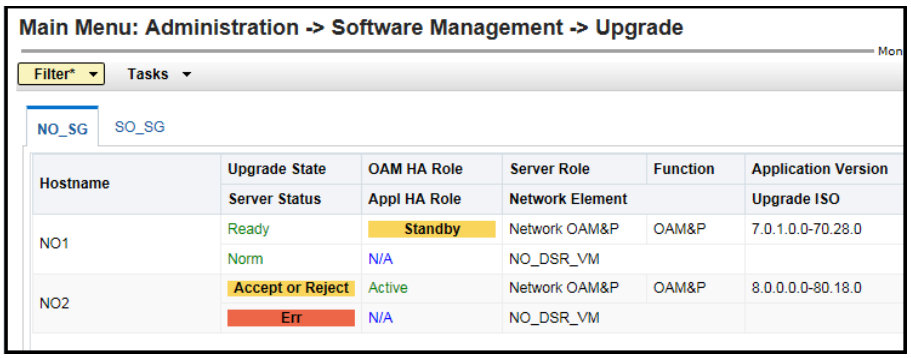
9. ☐	**Active NOAM CLI**: Estimate PCRF pooling migration completion
	Optional
		If the PCRF pooling migration is not complete, the user may get an estimate of when the PCRF pooling migration is complete.
		Execute the PCRF Pooling Migration Completion Estimate tool using the following command:
		`./verifyPCRFPoolingMigration.sh --estimateMigrationCompletionTime`
		Note: Once complete, this command displays the estimated PCRF pooling migration in days, hours, minutes, and seconds.
		Example:
		`Estimated total time for migration completion for all binding servers is: 3 days 4 hours 45 minutes 34 seconds.`

Appendix D. Upgrade Single Server – DSR 8.x

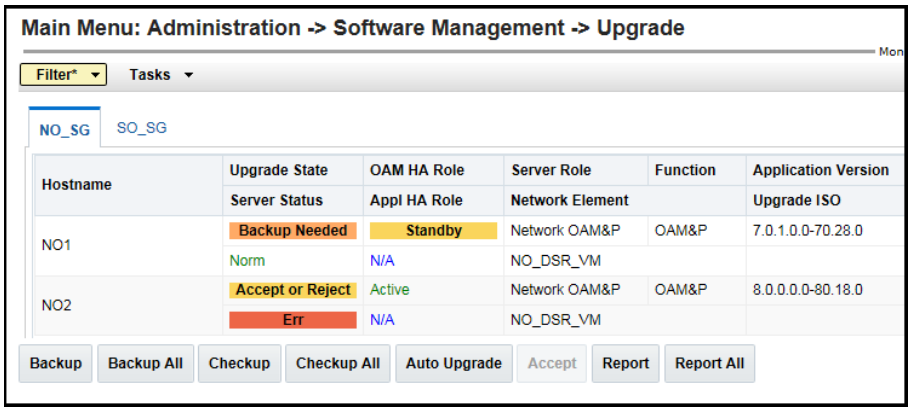
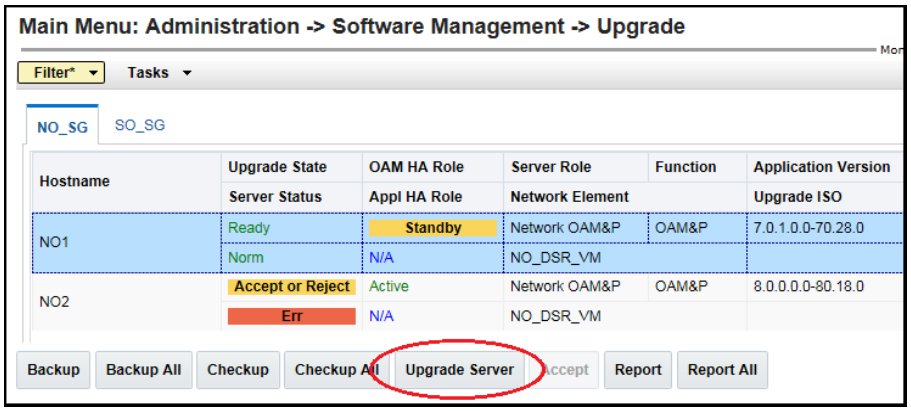
This appendix upgrades a single DSR server of any type (NOAM, SOAM, MP, etc.) when the active NOAM is on DSR 8.x.

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 D to mark up, or keep another form of written record of the steps performed.

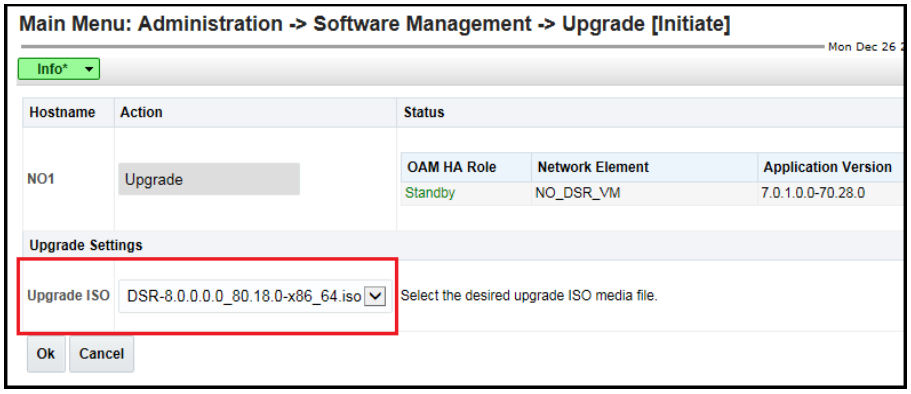
Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

S T E P #		
	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 My Oracle Support (MOS) 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)**

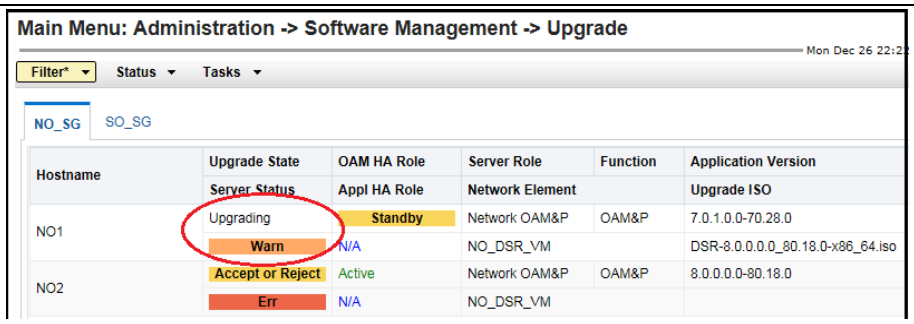
Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

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.  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. 

Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

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.  *** 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.

Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x



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 = 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.

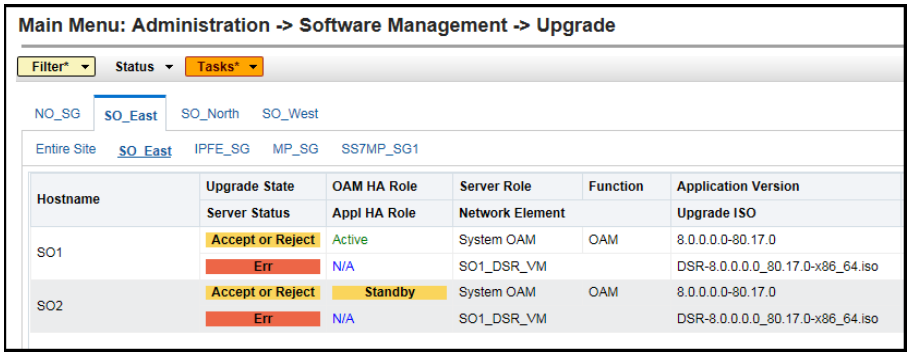
   If the upgrade fails, **do not proceed**. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K 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 My Oracle Support (MOS) by referring to Appendix P of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

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.

Procedure 55. Upgrade Single Server – Upgrade Administration – DSR 8.x

10. ☐	**Server CLI**: Update the tuned profile	After successful upgrade has been verified above, access the server on command line (via ssh or console), and update the tuned profile:
		`$ sudo /usr/TKLC/dsr/bin/tuned.sh`
		Now, verify whether tuned profile has been successfully set to “comcol_app”:
		`$ sudo tuned-adm active`
		Sample Output:
		`[admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`
		`[admusr@SOAM1 ~]$`
		The single server upgrade is now complete.
		Return to the DSR upgrade procedure step that directed the execution of Appendix D.

Appendix E. Upgrade Single Server – Pre-DSR 8.0

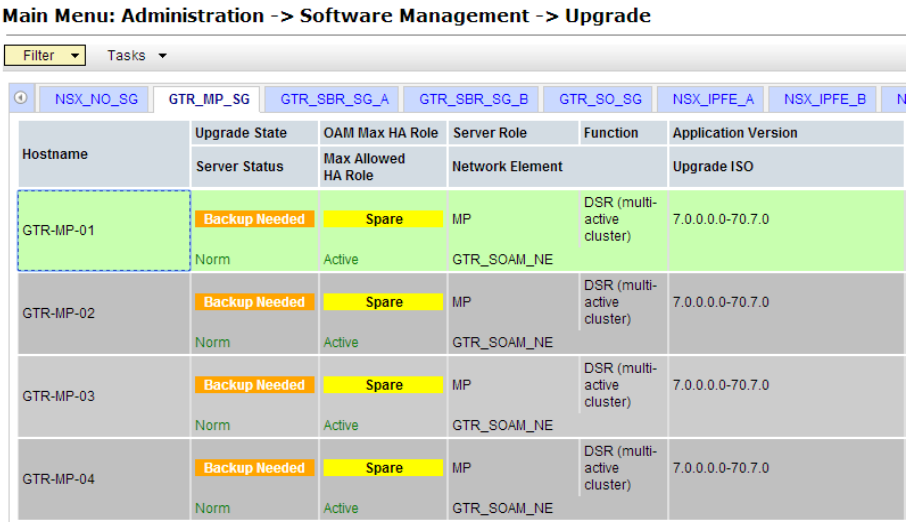
This appendix upgrades a single DSR server when the active NOAM is on DSR 6.x.y or 7.x.y. This procedure upgrades the standby NOAM only. The remaining servers are upgraded using Procedure 55.

Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

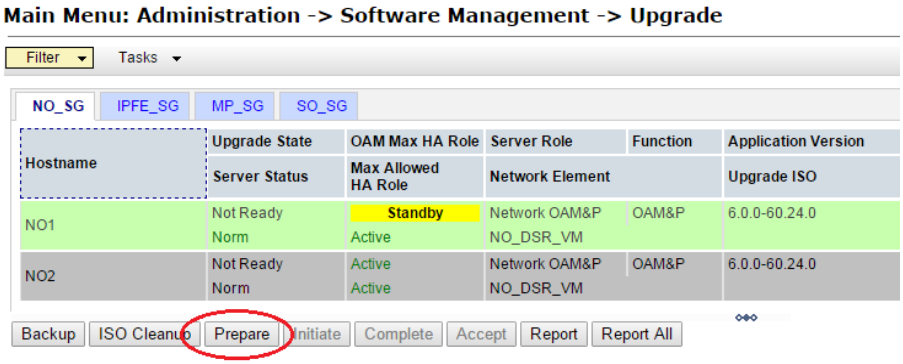
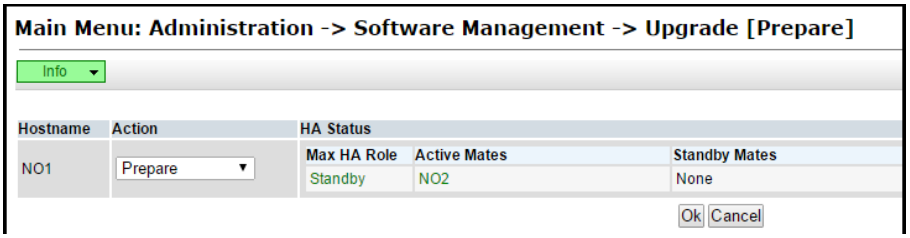
S T E P #	This procedure executes the Upgrade Single Server when the active NOAM is on a release prior to DSR 8.x. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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

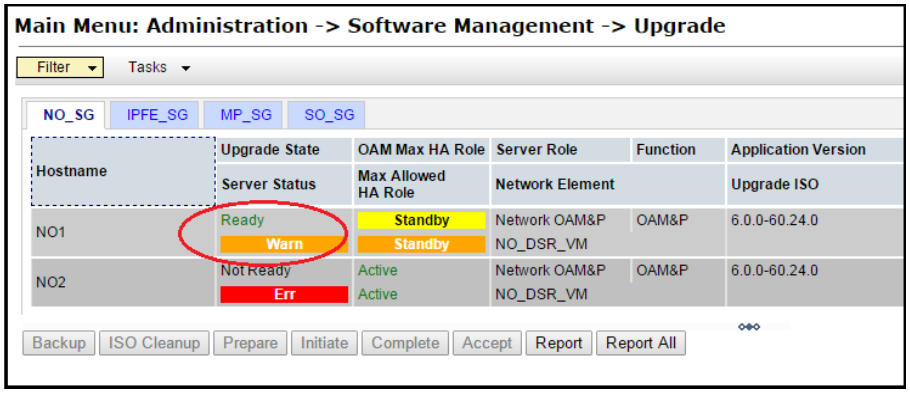
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

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. **For active NOAM on release 7.0.x** • When the backup is complete, verify the server state changes to **Not Ready**. • Perform steps 3 through 10. **For active NOAM on release 7.1.x and later** • When the backup is complete, verify the server state changes to **Ready**. • Proceed to step 11.

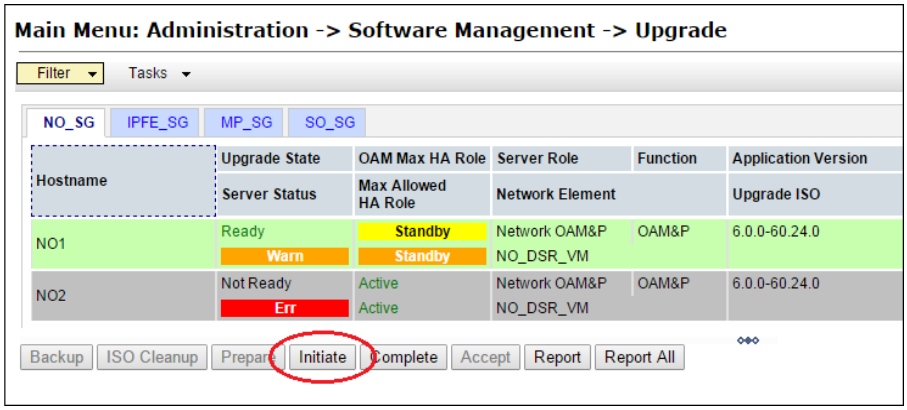
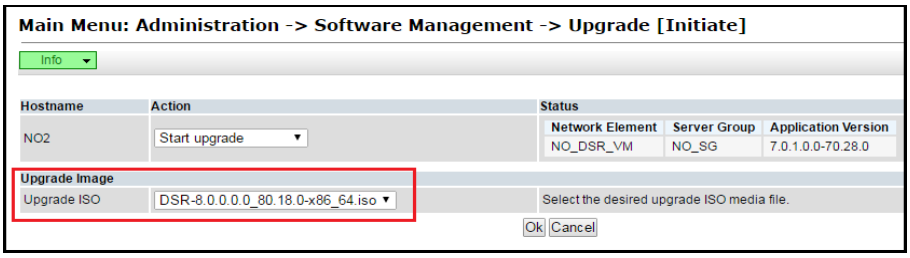
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

3. ☐	**Active NOAM VIP**: Prepare the server for upgrade (step 1) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only**. On the Upgrade form, make the server **Upgrade Ready** by selecting the server to be upgraded and clicking **Prepare**. In this example, an NOAM with name NO2 is made ready for upgrade. 
4. ☐	**Active NOAM VIP**: Prepare the server for upgrade (step 2) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** The **Upgrade Prepare** form displays.  For the Max HA Role: 1. Verify the selected server status **is the expected condition (either Standby** or **Active)** (this depends on the server being upgraded). 2. If the state of the server to be upgraded is as expected, click **OK**.

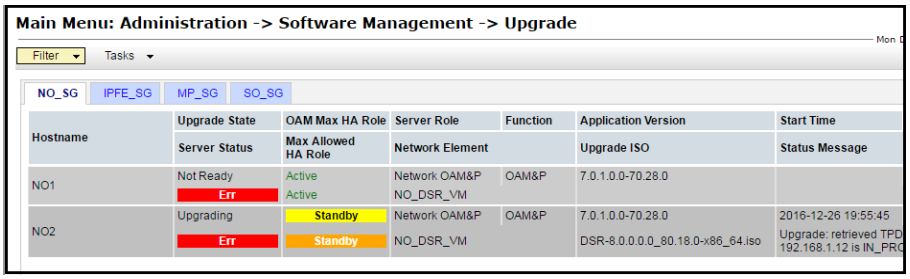
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

5. ☐	**Active NOAM VIP**: Verify upgrade status is **Ready** **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** Verify the server upgrade status is ready. When preparing the selected server, the Upgrade Administration form refreshes and the server to upgrade displays Upgrade State = **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 = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** **Alarm ID = 31101 (DB Replication to slave DB has failed)** **Alarm ID = 31107 (DB Merge From Child Failure)** **Alarm ID = 31106 (DB Merge to Parent Failure)** **Alarm ID = 31114 (DB Replication over SOAP has failed)** **Alarm ID = 31225 (HA Service Start Failure)**

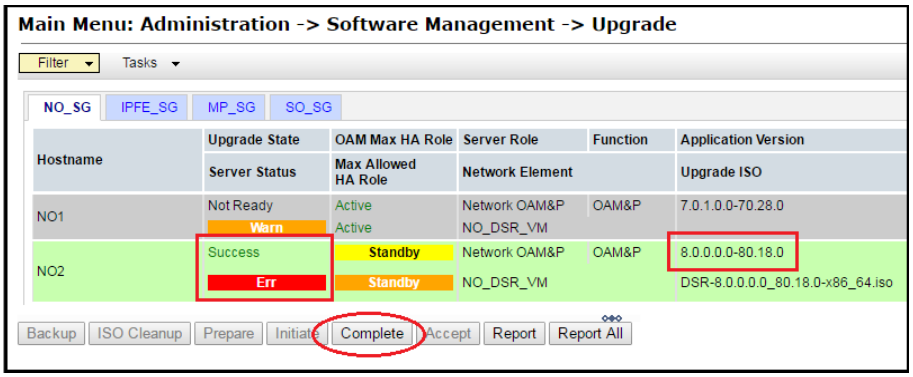
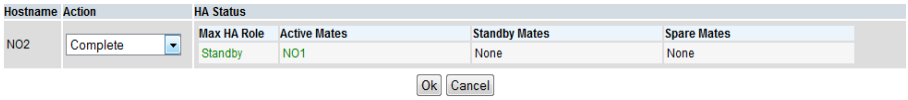
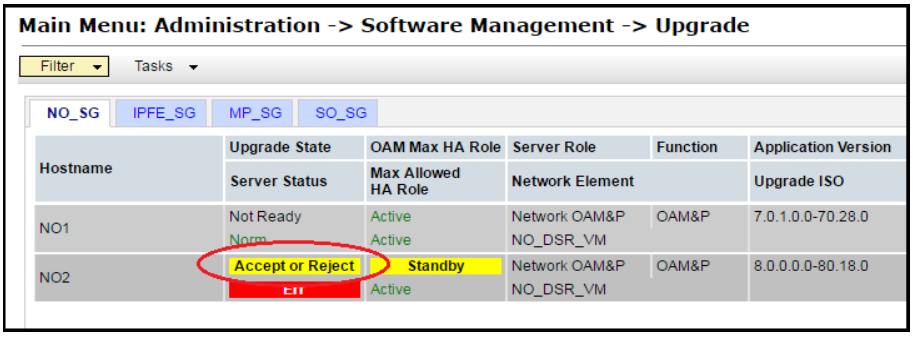
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

6. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 1) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click **Initiate**. 
7. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 2) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** The Initiate Upgrade form displays on the **Administration > Software Management > Upgrade Initiate** screen. 1. From the **Upgrade Image – 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. 

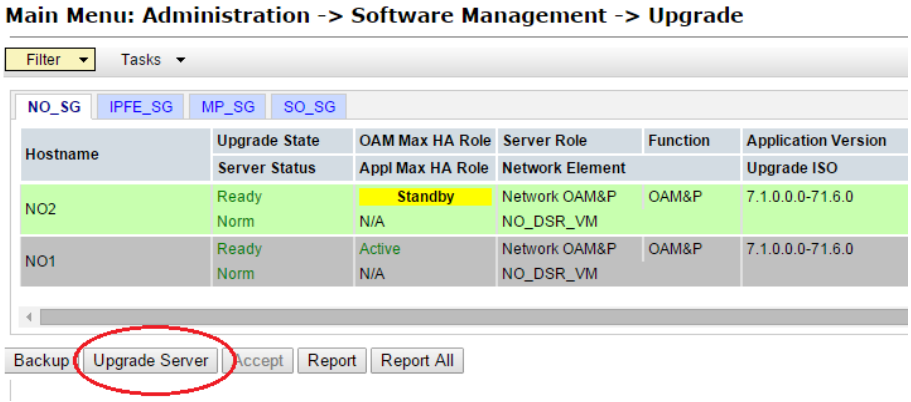
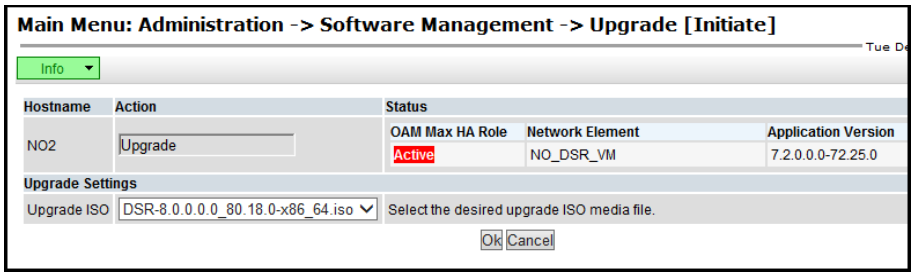
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

8. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** See step 15 for an optional method of monitoring upgrade progress. See step 16 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. Observe the Upgrade State of the server of interest. Upgrade status displays under the Status Message column.  Main Menu: Administration -> Software Management -> Upgrade Filter Tasks NO_SG IPFE_SG MP_SG SO_SG Hostname / Server Status / Upgrade State / Max Allowed HA Role / OAM Max HA Role / Network Element / Server Role / Function / Upgrade ISO / Application Version / Status Message / Start Time NO1: Not Ready, Err, Active, Active, Network OAM&P, NO_DSR_VM, OAM&P, 7.0.1.0.0-70.28.0 NO2: Upgrading, Err, Standby, Standby, Network OAM&P, NO_DSR_VM, OAM&P, 7.0.1.0.0-70.28.0, DSR-8.0.0.0.0_80.18.0-x86_64.iso, 2016-12-26 19:55:45, Upgrade: retrieved TPD 192.168.1.12 is IN_PRG 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. If the upgrade fails – do not proceed. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

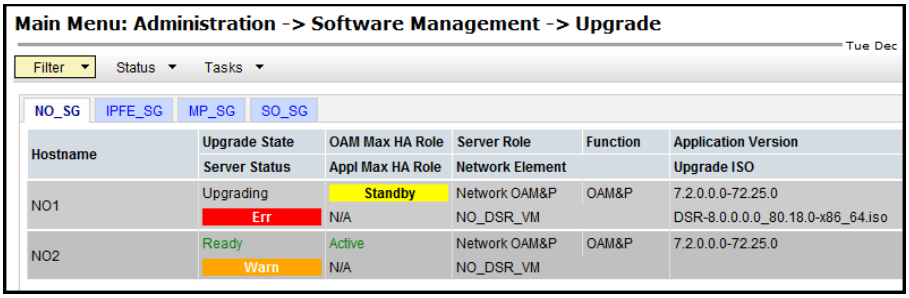
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

9. ☐	**Active NOAM VIP**: Take the upgraded server out of the upgrade SUCCESS state (part 1) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** This step applies to all servers, regardless of type. 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 server that was upgraded is **Success**. 4. Select the server that was upgraded. 5. Click **Complete**. 
10. ☐	**Active NOAM VIP**: Take the upgraded server out of the upgrade SUCCESS state (part 2) **For active NOAM on release 7.0.x only**	**This step is for an active NOAM on release 7.0.x only.** The Upgrade Complete screen displays. 1. Click **OK** on the Upgrade Complete screen.  This completes the upgrade action on the server. 2. Wait for the screen to refresh and show the Upgrade State as **Accept or Reject**. It may take up to 2 minutes for the Upgrade State to change to **Accept or Reject**.  3. Proceed to step 18. to complete this procedure.

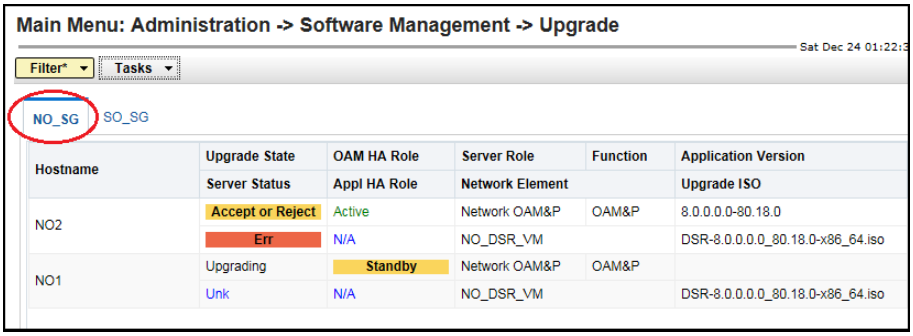
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

11. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 1) **For active NOAM on release 7.1.x and later**	**This step is for an active NOAM on release 7.1.x or later.** 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.
12. ☐	**Active NOAM VIP**: Initiate the server upgrade (part 2) – Select ISO form **For active NOAM on release 7.1.x and later**	**This step is for an active NOAM on release 7.1.x or later.** 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.

Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

13. ☐	**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.  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. If the upgrade fails, **do not proceed**. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

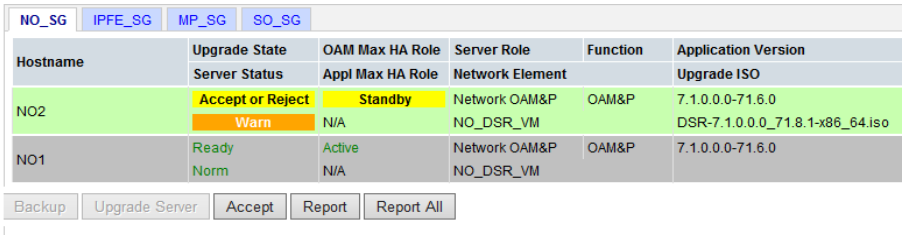
Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

14. ☐	**Active NOAM VIP**: View the upgrade administration form to monitor upgrade progress **For active NOAM on DSR 8.1 only**	This step monitors the 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 8.0/8.1. See step 15. for an optional method of monitoring upgrade progress. See step 16. 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. If the upgrade fails, **do not proceed**. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

15. ☐	**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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

16. ☐	**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 My Oracle Support (MOS) by referring to Appendix P of this document and provide these files. Refer to Appendix K for failed server recovery procedures.

17. ☐	**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. **If the active NOAM is on release 7.0.x** Verify the Status Message indicates **Success**. **If the active NOAM is on release 7.1.x or later** Verify the Upgrade State of the upgraded server is **Accept or Reject**. 

Procedure 56. Upgrade Single Server – Upgrade Administration – Pre-DSR 8.x

18. ☐	**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 E.

Appendix F. Upgrade Multiple Servers – Upgrade Administration

This appendix 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 F to mark up or keep another form of written record of the steps performed.

Procedure 57. Upgrade Multiple Servers – Upgrade Administration

S T E P #		
	This procedure executes the Upgrade Multiple Servers – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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)**

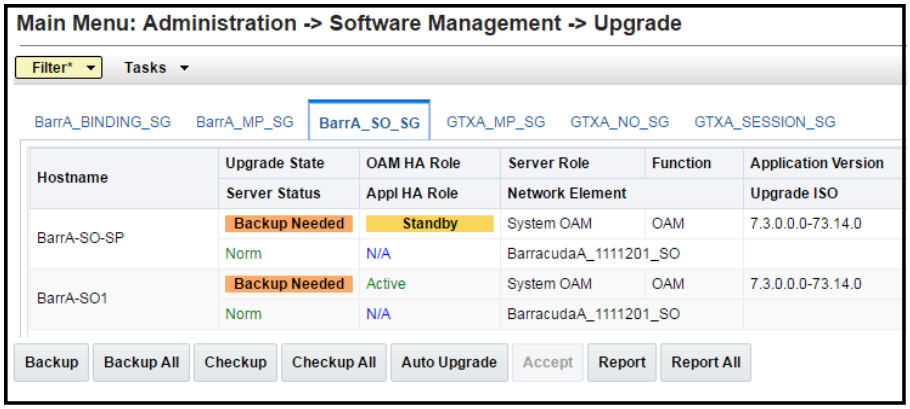
Main Menu: Administration -> Software Management -> Upgrade

Filter ▾ Tasks ▾

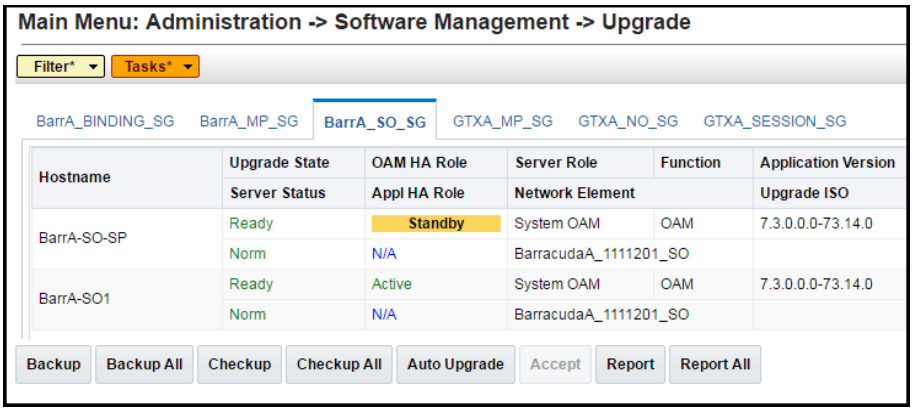
NSX_NO_SG | GTR_MP_SG | GTR_SBR_SG_A | GTR_SBR_SG_B | GTR_SO_SG | NSX_IPFE_A | NSX_IPFE_B

Hostname	Upgrade State 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

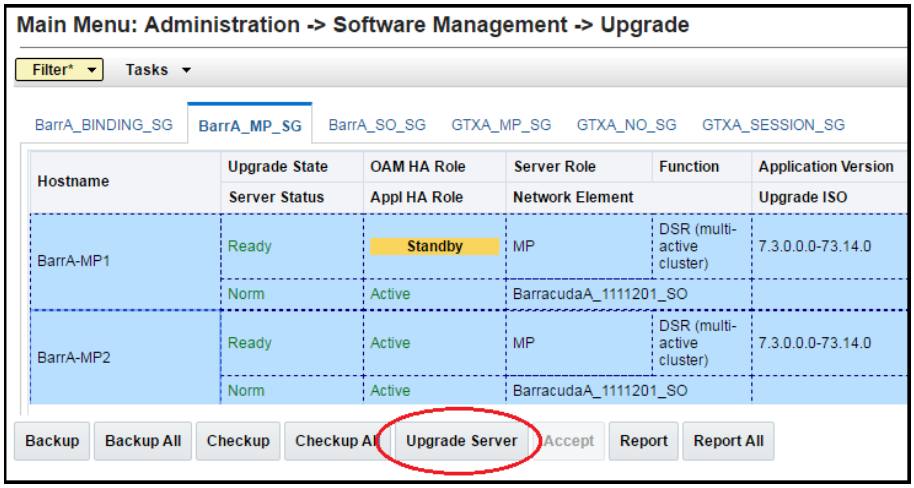
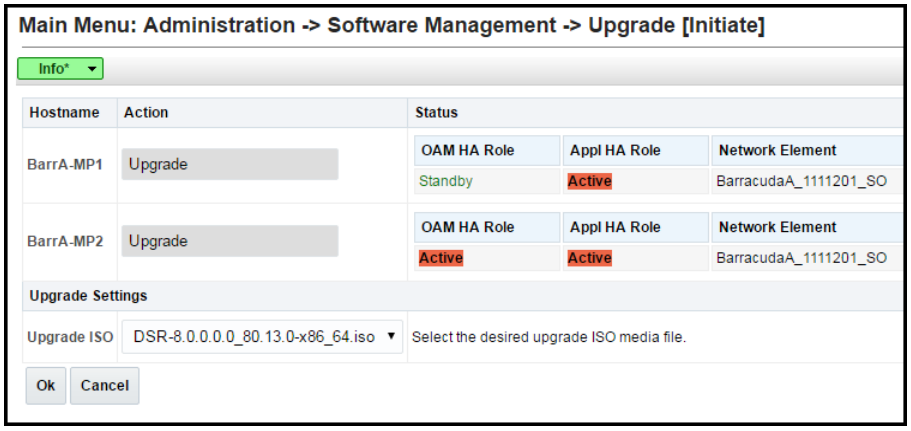
Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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.

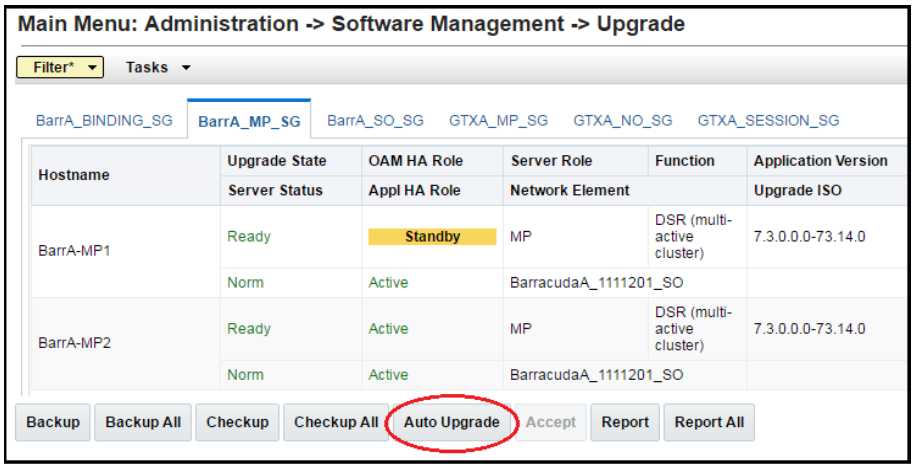
Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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.

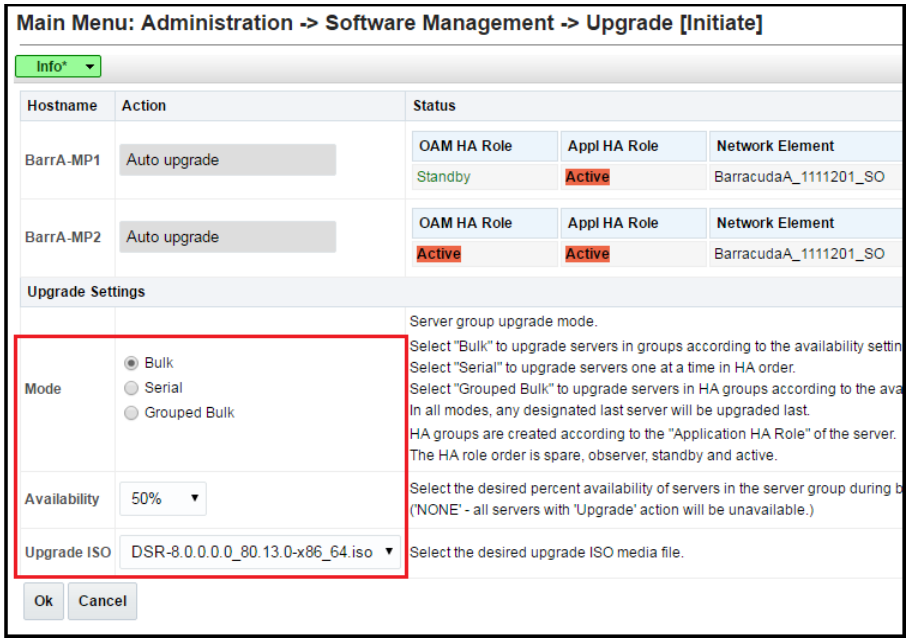
Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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.

Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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**.

Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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 form to monitor upgrade	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.

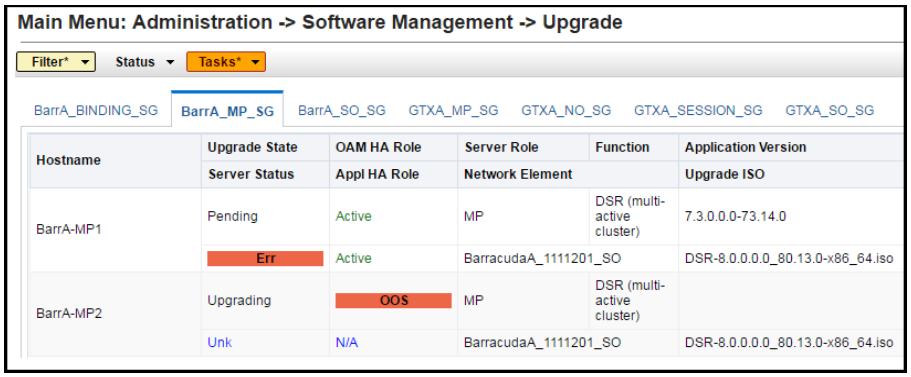
Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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.



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)

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 35.

Alarm ID = 25607 (DSR Signaling Firewall is administratively Disabled)

If the upgrade fails – do not proceed. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K for failed server recovery procedures.

Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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 Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		If the upgrade fails, **do not proceed**. It is recommended to consult with My Oracle Support (MOS) on the best course of action. Refer to Appendix K 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 My Oracle Support (MOS) on the best course of action. Refer to Appendix K 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**.

Procedure 57. Upgrade Multiple Servers – Upgrade Administration

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.

14. ☐	**Server CLI**: Update the tuned profile	After successful upgrade has been verified above, access the server on command line (via ssh or console), and update the tuned profile:
		`$ sudo /usr/TKLC/dsr/bin/tuned.sh`
		Now, verify whether tuned profile has been successfully set to **comcol_app**:
		`$ sudo tuned-adm active`
		Sample Output:
		`[admusr@SOAM1 ~]$ sudo tuned-adm active`
		`Current active profile: comcol_app`
		`Service tuned: enabled, running`
		`Service ktune: enabled, running`

Appendix G. Alternate Server Upgrade Procedures

The procedures in this section provide 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 4.6. These procedures should be used only when directed by My Oracle Support (MOS) or by other procedures within this document.

Appendix G.1. Alternate Pre-Upgrade Backup

This procedure is an alternative to the normal pre-upgrade backup provided in Procedure 22. It is recommended that this procedure be executed only under the direction My Oracle Support (MOS).

Procedure 58. Alternate Pre-Upgrade Backup

S T E P #	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 My Oracle Support (MOS) 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.

Procedure 58. Alternate Pre-Upgrade Backup

		Output similar to the following indicates successful completion:
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`
		`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.

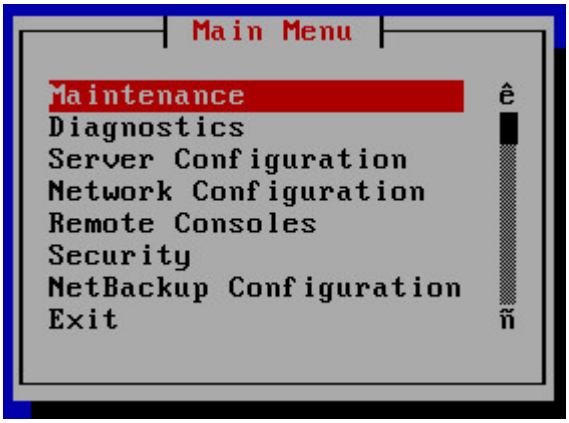
Appendix G.2. Server Upgrade Using platcfg

The procedure provided in this appendix enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of My Oracle Support (MOS).

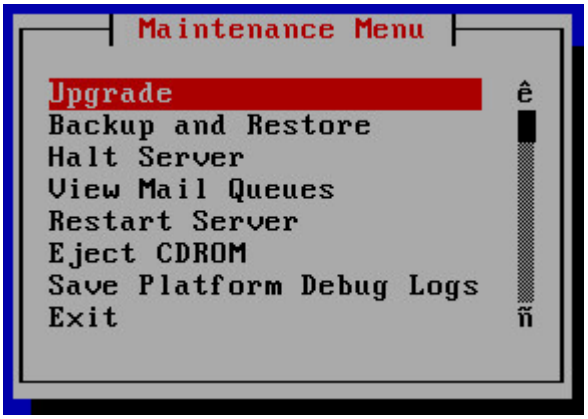
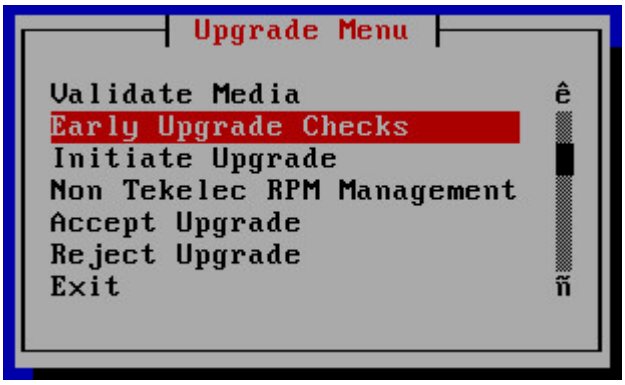
Procedure 59. Server Upgrade Using Platcfg

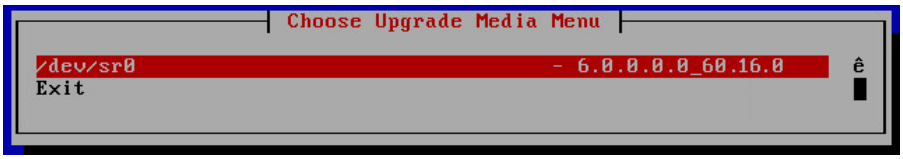
S T E P #		
	This procedure upgrades a server using the platcfg utility. ***Note***: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step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

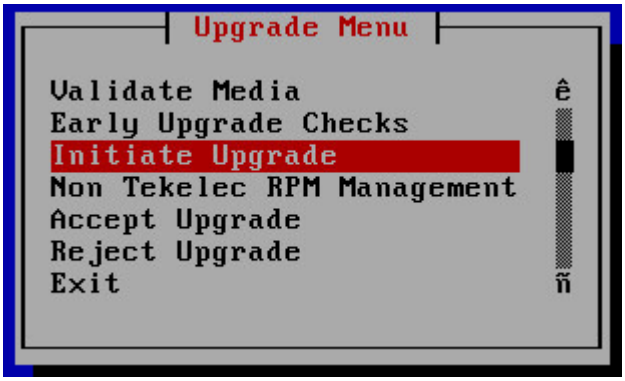
2. ☐	**Server CLI**: Enter the platcfg menu	Switch to the platcfg user to start the configuration menu. `$ sudo su - platcfg` From the Main Menu, select **Maintenance**. 

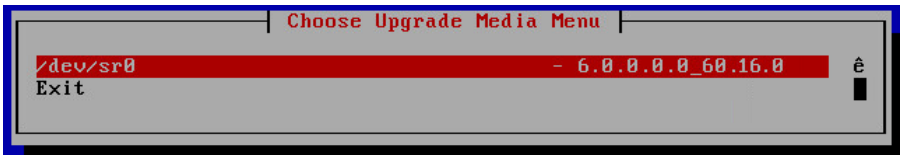
Procedure 59. Server Upgrade Using Platcfg

3. ☐	**Server CLI**: Select upgrade	From the Maintenance Menu, select **Upgrade**. 
4. ☐	**Server CLI**: Select early upgrade checks	From the Upgrade Menu, select **Early Upgrade Checks**. 

5. ☐	**Server CLI**: Select the upgrade media	1. 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!`
		2. Verify early upgrade checks pass. In case of errors, it is recommended to contact My Oracle Support (MOS).
		3. Press **q** to exit the screen session and return to the platcfg menu.
		4. From the Choose Upgrade Media Menu, select **Exit**.

Procedure 59. Server Upgrade Using Platcfg

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

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.

Procedure 59. Server Upgrade Using Platcfg

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 My Oracle Support (MOS) by referring to Appendix P 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 My Oracle Support (MOS).
		`[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

Procedure 60 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 4.6.

Procedure 60 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 60 must be executed four distinct times.

Procedure 60. Manual DA-MP (N+0) Upgrade Procedure

S T E P #	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 My Oracle Support (MOS) 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.

Procedure 60. Manual DA-MP (N+0) Upgrade Procedure

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 F Upgrade Multiple Servers – Upgrade Administration. 2. After successfully completing the procedure in Appendix F, 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. Manual DA-MP (1+1) Upgrade Procedure

Procedure 61 is used to manually upgrade an active/standby DA-MP server group. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 4.6.

Procedure 61. Manual DA-MP (1+1) Upgrade Procedure

S T E P #	This procedure upgrades an active/standby 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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	Upgrade the standby DA-MP server using the Upgrade Single Server procedure	1. Execute Procedure 55 Upgrade Single Server – Upgrade Administration – DSR 8.x. 2. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
2. ☐	Upgrade the active DA-MP server using the Upgrade Single Server procedure	Execute Procedure 55 Upgrade Single Server – Upgrade Administration – DSR 8.x.

Appendix G.5. ASG SBR Upgrade Procedure

Procedure 62 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 4.6.

Procedure 62. ASG SBR Upgrade

S T E P #		
	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 My Oracle Support (MOS) 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 F 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.6. Manual SBR Upgrade Procedure

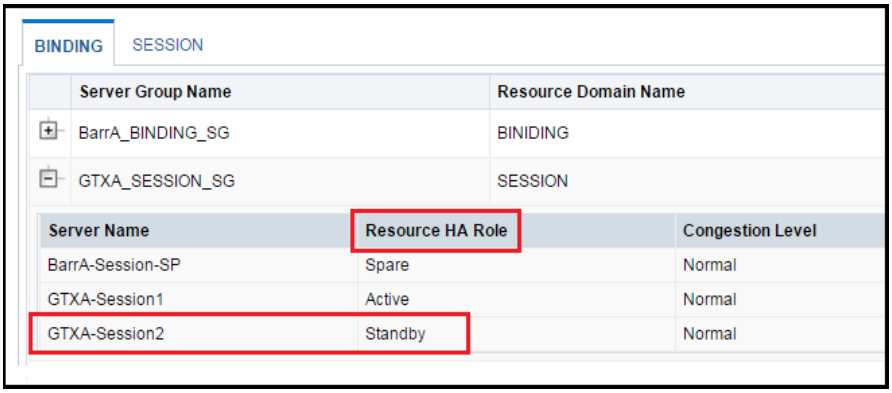
Procedure 63 is used to upgrade the SBR server group manually. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 4.6.

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 data.

Procedure 63. Manual SBR Upgrade Procedure

S T E P #		
	This procedure upgrades an SBR server group using the manual 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. ☐	**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

Procedure 63. Manual SBR Upgrade Procedure

		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 / Resource Domain Name BarrA_BINDING_SG / BINIDING GTXA_SESSION_SG / 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).

Procedure 63. Manual SBR Upgrade Procedure

2. ☐	**Active NOAM VIP**: Upgrade spare SBR server identified in step 1 of this procedure	***Note***: The spare SBRs of this server group are located at different sites. 1. Execute Appendix D Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix D, 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 D, 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 through 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	1. Execute Appendix D Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix D, 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	1. Navigate to **Policy and Charging >Maintenance > SBR Status**. Open the tab of the server group being upgraded. ***Note***: After executing Appendix D, 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**. 2. 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**.

Procedure 63. Manual SBR Upgrade Procedure

5. ☐	**Active NOAM VIP**: Verify bulk download from the active SBR to the standby and spare SBRs completes	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. ☐	Upgrade active SBR server as identified in step 1 of this procedure	1. Execute Appendix D Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
7. ☐	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 handles password expiration during upgrade. Procedure 64 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 **Error! Reference source not found.** after the site is upgraded. Failure to remove the workaround inhibits password aging on the server.

Appendix H.1. Inhibit Password Aging

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

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

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

Procedure 64. Expired Password Workaround Procedure

S T E P #	This procedure disables password aging on a server, allowing “expired” credentials to be used for login. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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`

Procedure 64. Expired Password Workaround Procedure

		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

This procedure removes the password expiration workaround that is enabled by Procedure 64.

Procedure 65. Enable Password Aging

S T E P #	This procedure removes the password aging workaround and re-enables password aging on a server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) 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

Procedure 66 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 66. Expired Password Reset Procedure

S T E P #	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 My Oracle Support (MOS) 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 My Oracle Support (MOS) for guidance.

Appendix I. Network IDIH Compatibility Procedures

The procedures in this appendix are used to provide IDIH compatibility when upgrading to release 8.x. Procedure 67 is performed on a release 8.x IDIH to make the trace data viewable on prior release IDIH systems, as described in section 1.7.5. 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 68 must be executed on every IDIH on which Procedure 67was previously performed.

Procedure 67. Enable IDIH 8.x Compatibility

S T E P #	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 My Oracle Support (MOS) 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 68. Disable IDIH 8.x Compatibility

S T E P #	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 My Oracle Support (MOS) 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.

Procedure 68. Disable IDIH 8.x Compatibility

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. 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 69	1:15-1:45	1:15-1:45	Oracle Guest Upgrade	None
Procedure 70	0:30-0:45	1:45-2:30	Upgrade the Mediation and Application Guests	None

Appendix J.1. Oracle Guest Upgrade

The Oracle Guest is upgraded first.

Procedure 69. Oracle Guest Upgrade

S T E P #	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 My Oracle Support (MOS) 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 My Oracle Support (MOS) for guidance.

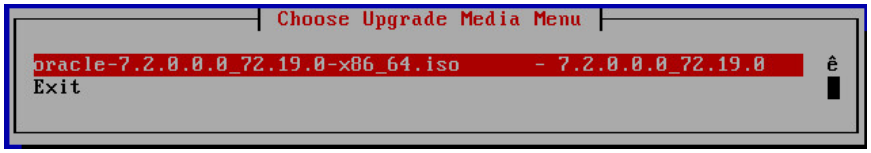
Procedure 69. Oracle Guest Upgrade

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

4. ☐	Move Oracle ISO	Use a file transfer tool to copy the Oracle ISO to the Oracle guest as **admusr**.
		Example:
		`$ scp oracle-8.0.0.0.0_80.21.0-x86_64.iso`
		`admusr@<ora-guest-ip>:/var/TKLC/upgrade`

Procedure 69. Oracle Guest Upgrade

5. ☐	**IDIH CLI**: Start Oracle guest upgrade	The Oracle guest is upgraded using the Platform Configuration utility. 1. Start 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**. 
6. ☐	**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.
7. ☐	**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 J.2. Upgrade the Mediation and Application Guests

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

Procedure 70. Upgrade the Mediation and Application Guests

STEP #	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 My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Cloud GUI**: Remove existing Application Server	Use the hpyervisor-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].

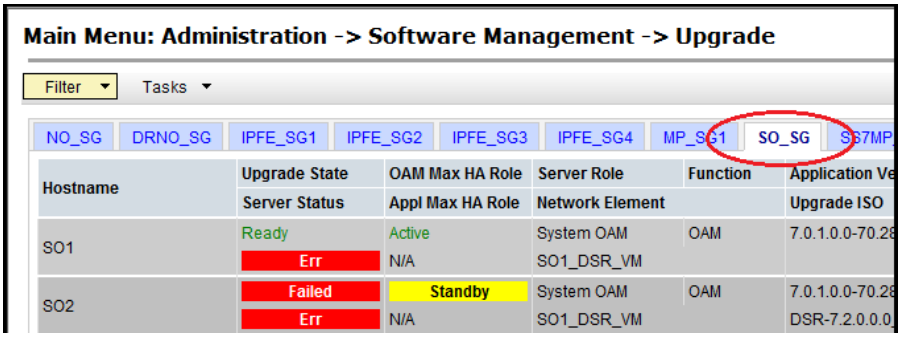
Procedure 70. Upgrade the Mediation and Application Guests

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].

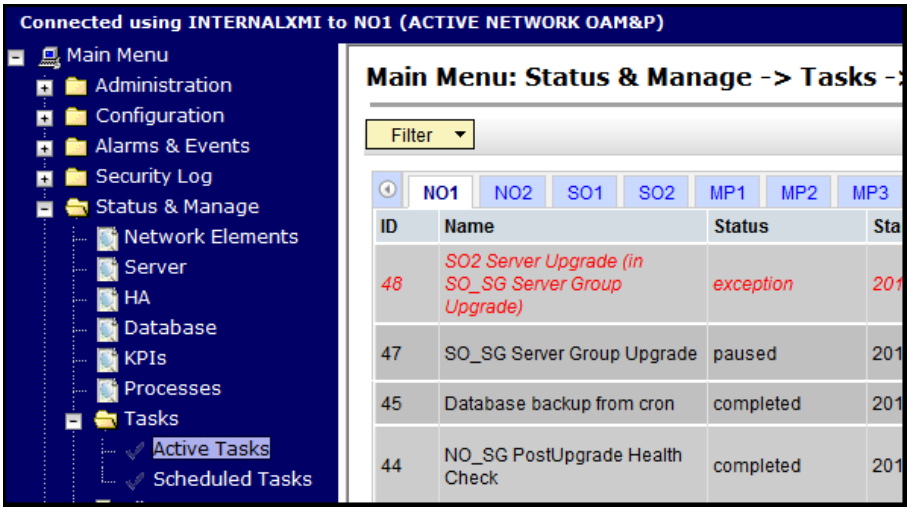
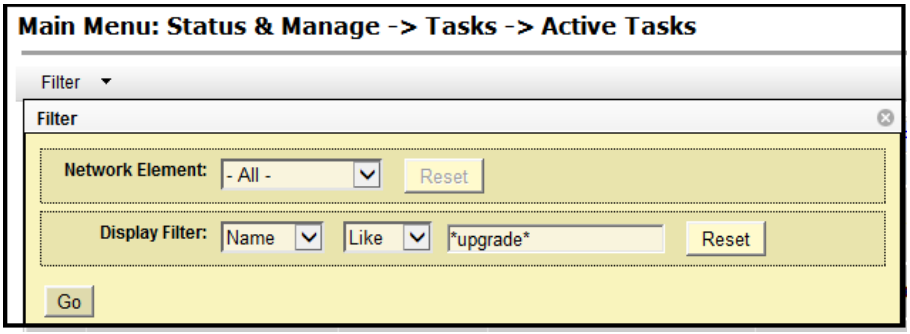
Appendix K. Recover From a Failed Upgrade

This 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 My Oracle Support (MOS) for guidance while executing this procedure.

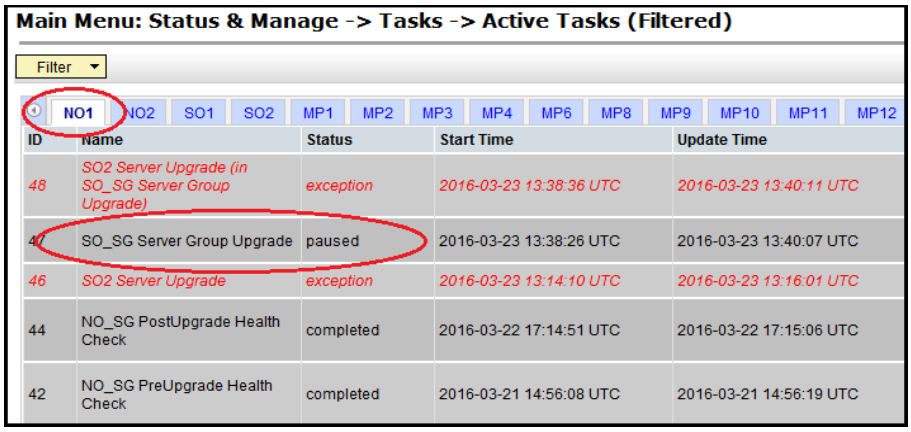
Procedure 71. Recover from a Failed Upgrade

S T E P #	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 My Oracle Support (MOS) 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 the next step of this procedure.

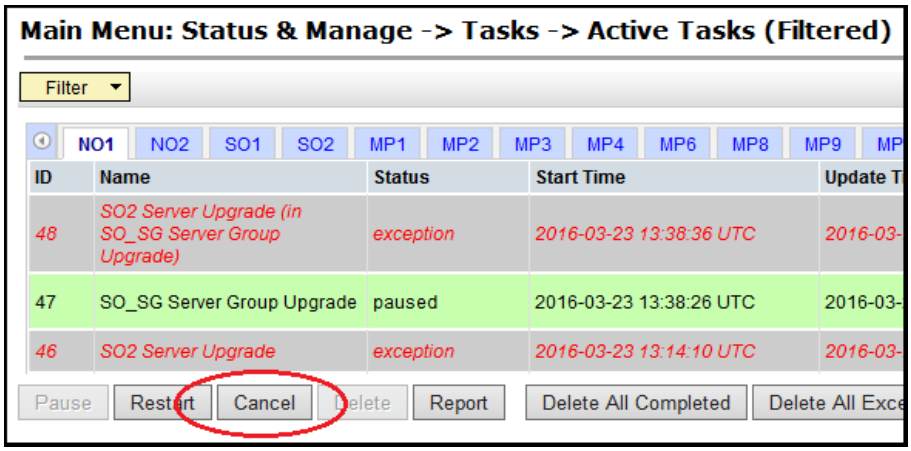
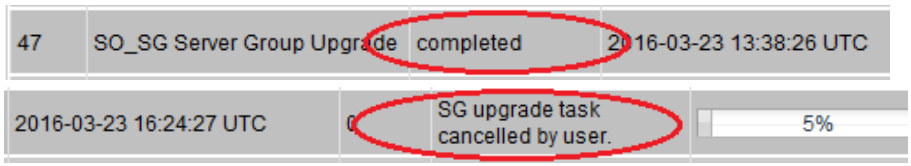
Procedure 71. Recover from a Failed Upgrade

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**. 

Procedure 71. Recover from a Failed Upgrade

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 (that is, 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.

Procedure 71. Recover from a Failed Upgrade

5. ☐	**Active NOAM VIP**: Cancel the Server Group Upgrade task	1. Click the Server Group Upgrade task to select it. 2. Click **Cancel** to cancel the task. 3. 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`

Procedure 71. Recover from a Failed Upgrade

<table>
<tr><td colspan="3">

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 My Oracle Support (MOS) as described Appendix P.
Do not proceed to the next step of this procedure until the alarm condition has been cleared!
</td></tr>
<tr><td>8. ☐</td><td>Failed Server CLI: Verify platform alarms are cleared from the failed server</td><td>Use the alarmMgr utility to verify all platform alarms have been cleared from the system.
<code>$ sudo alarmMgr --alarmstatus</code>
Example output:
<code>[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus</code>
<code>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</code>
user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm
<code>[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus</code>
<code>[admusr@SO2 ~]$</code></td></tr>
<tr><td>9. ☐</td><td>Active NOAM VIP: Re-execute the server upgrade</td><td>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.</td></tr>
</table>

Appendix L. Critical and Major Alarms Analysis

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

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

Procedure 72. Verify Critical and Major Alarms in the System Before the Upgrade

S T E P #	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 My Oracle Support (MOS) 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 [8] 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

Alarm ID	Name
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 Failover 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
32107	Raid Feed Unavailable
32108	Raid Power 1 Failure

Alarm ID	Name
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
32324	Breaker panel feed error
32325	Breaker panel breaker error

Alarm ID	Name
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
32508	Server core file detected
32509	Server NTP Daemon not synchronized

Alarm ID	Name
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

Alarm ID	Name
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
19250	SS7 process CPU utilization
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
19250	SS7 process CPU 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 incosistency 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
33000	MAP-to-Diameter Service Registration Failure on DA-MP
33001	Diameter-to-MAP Service Registration Failure on DA-MP
33003	Insufficient memory for DM-IWF
33004	DM-IWF Transaction Response Queue Utilization
33005	DM-IWF PTR Pool Utilization
33007	MD-IWF Error
33050	MD-IWF Ingress Message Rate
33051	MD-IWF Application Degraded or Unavailable
33052	MD-IWF Notified that DM-IWF Service Status is Down
33053	MD-IWF DiamTrans Task Queue Utilization
33054	MD-IWF MapTrans Task Queue Utilization
33055	MD-IWF DAMPInterface Task Queue Utilization
33056	MD-IWF ComAgent Provider Registration Failure on SS7-MP
33057	MD-IWF ComAgent User Registration Failure on SS7-MP
33058	MD-IWF DiamToMap PTR Utilization
33059	MD-IWF MapToDiam PTR Utilization

Alarm ID	Name
33062	Insufficient Memory for MD-IWF
33076	MD-IWF received Diameter Answer from unexpected DA-MP
33103	GLA Communication Agent Error
33105	Routing Attempt failed due to queue exhaustion
33106	GLA Communication Agent Timeout
33120	Policy SBR Binding Sub-Resource Unavailable
33121	GLA pSBR-B Response Task Message Queue Utilization
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 M. Advanced Health Check

Procedure 73. Advanced Health Check

S T E P #		
	This procedure verifies if UDP/TCP port 53 is open between NOAM and each DR NOAM site, NOAM site, and each SOAM site; and between MPs and each name server of the **/etc/resolv.conf** file. 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. ☐	Verify if UDP/TCP port 53 is open between NOAM and each DR-NOAM site	1. From the command prompt of the server with the alarm, type:
		`sudo nmap -sTU -p 53 <DR-NOAM hostname>`
		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-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.

Procedure 73. Advanced Health Check

2. ☐	Verify if UDP/TCP port 53 is open between NOAM and each SOAM site	1. From the command prompt of the server with the alarm, execute:
		`sudo nmap -sTU -p 53 <SOAM hostname>`
		2. Verify the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
		Example:
		`[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`
		If the port is in any state other than **Open**, then inform the customer before accepting the upgrade.
		Note: If the ports are **Closed**, it may be because no services are running on the far end. Check with the customer to make sure the firewall has been configured to allow DNS traffic on port 53.
		If the port is **Filtered,** then the port is likely blocked by a firewall and the upgrade MUST not be accepted until the customer confirms their network allows DNS traffic on port 53.

3. ☐	Verify if UDP/TCP port 53 is open between MP and each name server of the file /etc/resolv.conf	1. List the contents of the /etc/resolv.conf file.
		`sudo cat etc/resolv.conf`
		2. Verify 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 ~]$`
		`[admusr@Icepick-DAMP-1 ~]$ 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-`

Procedure 73. Advanced Health Check

		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 If the port is in any state other than **Open**, then inform the customer before accepting the upgrade. ***Note***: If the ports are **Closed**, it may be because no services are running on the far end. Check with the customer to make sure the firewall has been configured to allow DNS traffic on port 53. If the port is **Filtered,** then the port is likely blocked by a firewall and the upgrade MUST not be accepted until the customer confirms their network allows DNS traffic on port 53.

Appendix N. Workaround to Resolve DB Site Replication Alarms

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

Procedure 74. Restart the inetrep Process on the Affected Server(s)

S T E P #	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 My Oracle Support (MOS) 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.

Procedure 74. Restart the inetrep Process on the Affected Server(s)

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 O. Workaround to Resolve Server HA Failover

This procedure resolves the HA switchover issue.

Procedure 75. Resolve the HA Switchover Issue on Affected Server(s)

S T E P #	This procedure restarts the cmha process on the server with the 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 My Oracle Support (MOS) 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 P. 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, 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.