Oracle® Communications

DSR Cloud Software Upgrade Guide

Release 9.2.0.0.0
G33393-01
September 2025

Oracle Communications DSR Cloud Software Upgrade Guide, Release 9.2.0.0.0

G33393-01

Contents

6 Site Upgrade Execution

7 Backout Procedure Overview

I Reset the SOAP Password

J Restore the Servers with Backout Errors

K Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

My Oracle Support

CAUTION: Use only the Installation procedure included in the Install Kit.

Before installing any system, access MOS(https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this procedure.

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

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

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

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

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

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

Emergency Response

In the event of a critical service situation, the users can avail emergency response by calling the CAS main number at 1-800-223-1711 (toll-free in the US), or 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 subhead, click the Oracle Communications documentation link. The Communications Documentation page appears. You can see most products covered by these documentation sets under the headings Network Session Delivery and Control Infrastructure or "Platforms."
4. Click your Product and then the Release Number. A list of the entire documentation set for the selected product and release appears. 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.

What's New in this Guide

This section introduces the documentation updates for Release 9.2.0.0.0.

Release 9.2.0.0.0 - G33393-01, September 2025

- Added the Workaround for Configuring GUI and MMI Using Label Format for FQDN/Realm section for the users who prefer to continue with label format for GUI and MMI configurations.
- Updated Supported Upgrade Paths to 9.2.0.0.0 section.

1 Introduction

This document describes methods and procedures to perform upgrades from the following releases.:

- 9.0.0.0.0
- 9.0.1.0.0
- 9.0.2.0.0

This document covers the upgrade of cloud deployments and provides instructions to perform any incremental or major cloud software upgrade. The implementation of this procedure assumes that the target DSR software load (ISO file, CD-ROM or other form of media) has already been delivered to the customer's premises. This includes delivery of the software load to the local workstation being used to perform this upgrade.

> **Note**
>
> - To understand the capacity and performance impact of this software release, refer to *DSR Cloud Benchmarking Guide*.
> - From DSR 9.0.0.0.0 and later, consider ISO as DIU ISO in all occurrences throughout this document.
> - From DSR 9.0.0.0.0 and later, consider DA-MP as DA-MP/vSTP in all occurrences throughout this document.

1.1 What is Not Covered in This Document

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

- Distribution of DSR software loads. It is recommended to contact My Oracle Support (MOS) for the software loads as described in My Oracle Support.
- Initial installation of DSR software. Refer to *DSR Cloud Installation Guide*.
- SDS installation. Refer to *SDS Cloud Installation Document*.

1.2 References

- *DSR Cloud Installation Guide*
- *SDS Cloud Installation Document*
- *Maintenance Window Analysis Tool*
- *Fast Deployment and Configuration Tool Technical Reference*
- *Cloud DSR Disaster Recovery Guide*
- *Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) in DSR by Enabling SCTP AUTH Extensions By Default*

- *DSR Alarms and KPIs Reference*
- *DSR Cloud Benchmarking Document*

1.3 Acronyms

The following table provides information about the acronyms used in this document.

Table 1-1 Acronyms

Acronym	Meaning
ASG	Automated Server Group Upgrade
ASU	Automated Site Upgrade
CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
DA	Diameter Agent
DAMP	Diameter Agent Message Processor
DB	Database
DIU	Dual Image Upgrade
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

Table 1-1 (Cont.) Acronyms

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

1.4 Terminologies

This section describes terminologies as they are used within this document.

Table 1-2 Terminologies

Term	Definition
Upgrade	The process of upgrading 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 8.6.x to 9.x.
Incremental Upgrade	An upgrade within a given DSR release e.g. 9.x to 9.x.
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 upgrading a DSR server from its current release to a newer release.
Backout	The process of converting a single DSR 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 preupgrade 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.

Table 1-2 (Cont.) Terminologies

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 on the DSR GUI and PM&C GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
Upgrade Ready	State that allows for graceful upgrade of a server without degradation of service. It is a state that a server is required to be in before upgrading a server. The state is defined by the following attributes: • Server is Forced Standby • Server is Application Disabled (signaling servers do not process any traffic)
UI	User interface.
Platcfg UI	Platform Configuration Utility User Interface, which is a text-based user interface.
N+0	Set up with N active DA-MP(s), but no standby DA-MP.
NOAM	Network OAM for DSR
SOAM	System OAM for DSR
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (active/standby) policy to N+ 0 (multiple active) policies.
Software Centric	The business practice of delivering an Oracle software product, while relying on 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, and so on) that enable a 3rd party entity to install, configure, and maintain Oracle products for Oracle customers.

2 Upgrade Overview

This document defines the step-by-step actions performed to perform an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 8.x to target release 9.0.x(Dual Hop Upgrade). An incremental upgrade advances the DSR from an earlier DSR 9.0.x source release to a more recent 9.2.0.0.0 target release.

> **Note**
>
> Advancing a DSR from 9.0.0.0.0_97.16.0 to 9.0.1.0.0_98.15.0 is an incremental upgrade. But, advancing a DSR running 8.6.x release to an 9.0.x target release constitutes a major upgrade.

2.1 Supported Upgrade Paths to 9.2.0.0.0

The following table provides information about the supported upgrade paths:

Source Release	Target Release
9.0.1.0.0	9.2.0.0.0
9.0.2.0.0	9.2.0.0.0
9.0.2.1.0	9.2.0.0.0
9.1.0.0.0	9.2.0.0.0

2.2 Geo-Diverse Site Configuration

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

2.3 Traffic Management During Upgrade

The upgrade of the NOAM and SOAM servers are 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 upgrade servers. The remaining servers continue to service traffic.

> **Warning**
>
> SCTP Datagram Transport Layer Security change.

Oracle introduced SCTP Datagram Transport Layer Security (DTLS) in DSR 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

DTLS Feature Activation Guide. These known impacts are managed by enabling SCTP AUTH Extensions. It is highly recommended that customers upgrading to Release 9.2.0.0.0 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 9.2.0.0.0. In this event, follow the procedure to enable or disable DTLS in *DSR Cloud Installation Guide*.

2.4 Automated Site Upgrade

You can upgrade a site using multiple methods. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. This feature upgrades an entire site (SOAMs and all C-level servers) with minimum user interaction. Once you initiate the upgrade, it automatically prepares the server(s), performs the upgrade, and sequences to the next server or group of servers. This action continues until all servers in the site are upgraded.

> **Note**
>
> The server upgrades are sequenced in a manner that preserves data integrity and processing capacity.

You can use Automated Site Upgrade only for upgrading DSR servers.

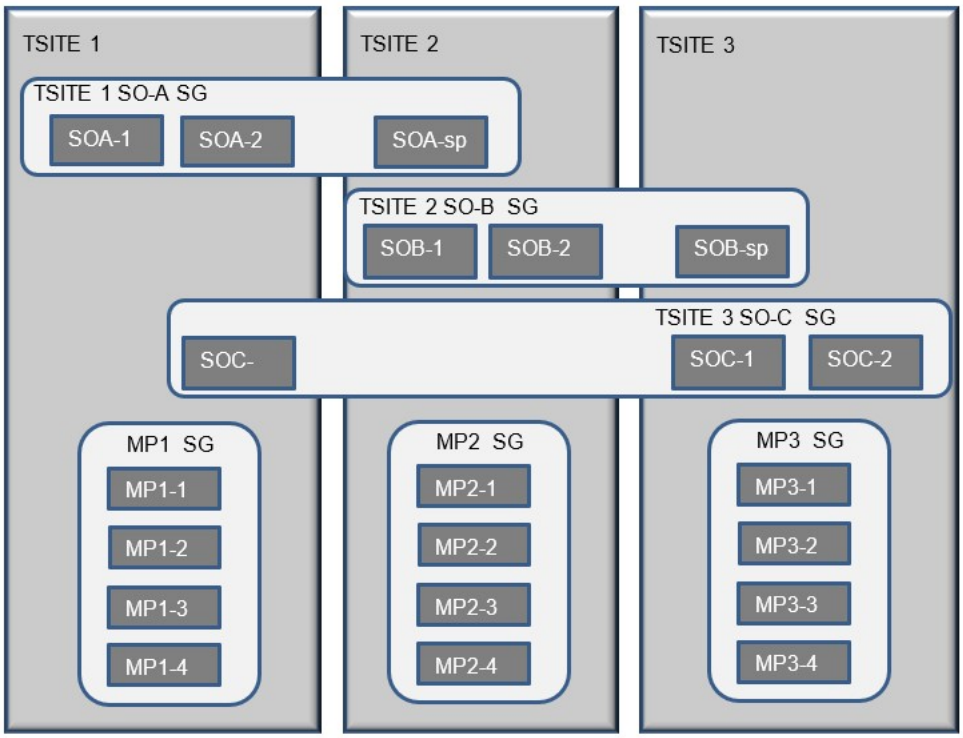
You can upgrade the DSR servers through the Automated Site Upgrade. A site is defined as a SOAM server group along with all the subtending servers of that server group, regardless of physical location. Fore more information, refer to Figure 2-1, which demonstrates three physical locations, labeled TSite 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, which despite being located at another site, is a member of the site that owns the server group. With the site upgrade, SOA-Sp upgrades with the Site 1 SOA server group, and SOB-sp upgrades 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 in Table 1-2.

1. With this feature, you can initiate a site upgrade 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 the availability setting and HA roles.
3. Immediately begin the upgrade of any other server groups which are also the children of SO-A SG. These upgrades begin in parallel with step 2.

Server groups that span across sites (for example, SOAMs and SBRs) are upgraded with the server group that the server belongs to. 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 Automated Site Upgrade of multiple sites in parallel manually.

Figure 2-1 Upgrade Perspective of DSR Site Topology

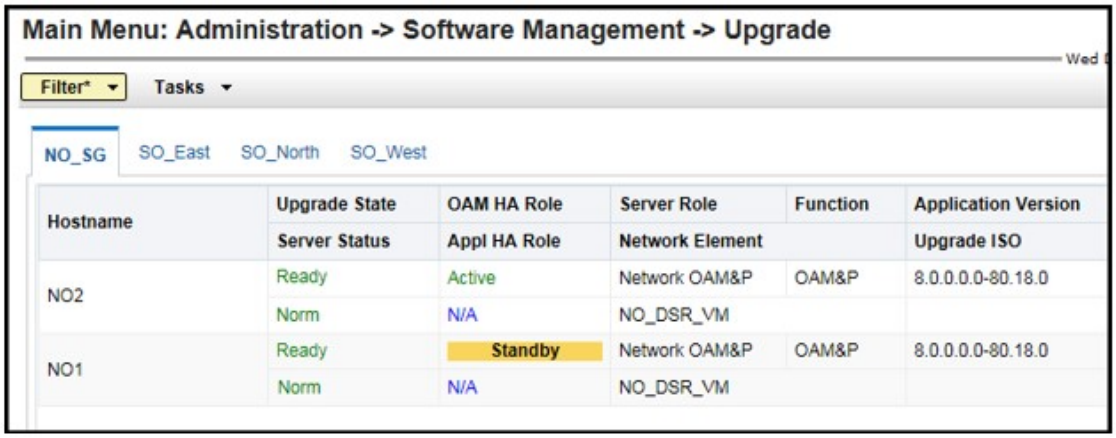


> ⚠ **Caution**
>
> Limitations in Create a Link for ComAgent for Automated Site Upgrade can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles, then manual upgrade method mentioned in Overview of Automated/Manual Server Group Upgrade should be used.

2.4.1 Site Upgrade Overview

With Auto Site Upgrade, the upgrade is initiated by navigating to **Administration**, then **Software Management,** and then **Upgrade GUI**. This GUI displays the NOAM server group and SOAM sites as shown in the following figure. On this screen, Auto Upgrade refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature is available once you select a SOAM server group tab. The SOAM server group tabs correspond to the topological sites (TSites).

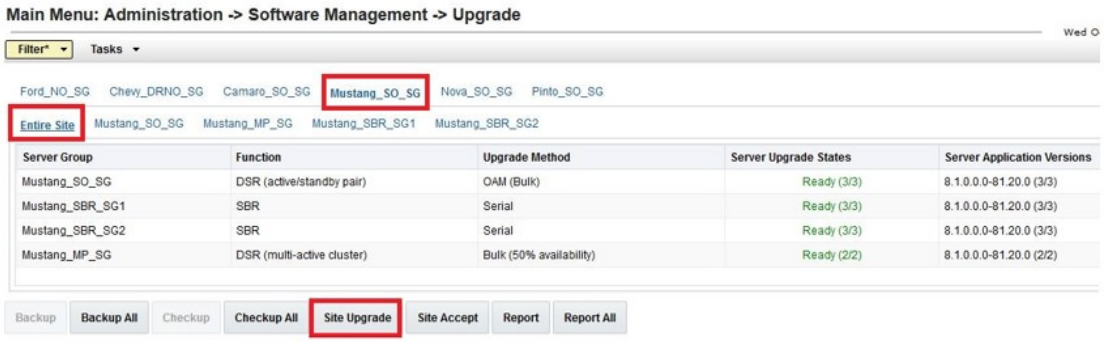
Figure 2-2 Site Upgrade – NOAM View



After selecting a SOAM site tab on the Upgrade Administration screen, the site summary screenappears as shown in Figure 2-3 Figure. The first link on the site summary screen displays the **Entire Site** view. In the **Entire Site** view, all the server groups for the site appears in table form, with each server group populating one row. You can can view the upgrade summary of the server groups 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. For more information on bulk availability, see Site Upgrade Options.
- The **Server Upgrade States** column groups the servers by state, indicating the number of servers in the server groups in each state.
- The **Server Application Versions**column indicates the current application version, indicating the number of servers in the server group existing in each version.

Figure 2-3 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

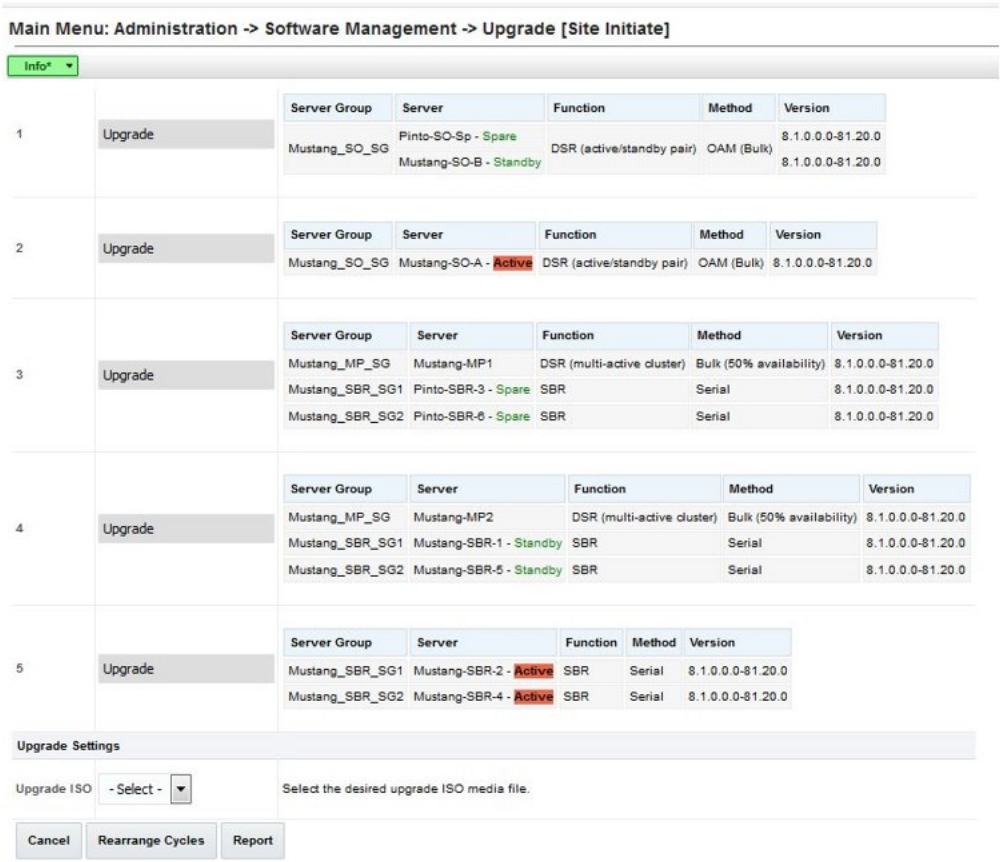
A site is eligible for Automated Site Upgrade when at least one server in the site is upgrade-ready.

Click **Site Upgrade** from the **Entire Site** screen to display the **Upgrade Site Initiate** screen as shown in Figure 2-4. The **Site Initiate** screen presents the **Site Upgrade** as a series of upgrade cycles. For the upgrade shown in Figure 2-4, Cycle 1 upgrades the spare and standby SOAMs in parallel.

> **Note**
>
> This scenario assumes default settings for the site upgrade options as described in Site Upgrade Options. The specific servers to be upgraded in each cycle are identified in the **Server** column of the **Site Initiate** screen. 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. As Cycle 2 is also atomic, Cycle 3 does not begin until Cycle 2 completes.

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

Figure 2-4 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 the above figure, Cycle 3 consists of IPFE1, IPFE3, MP1, MP4, and SBR3 because some servers can take longer to upgrade than others. Consequently, 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 the maintenance window efficiency. The primary reason for upgrading the C-level servers is the upgrade method for the server group function (for example, bulk by HA, serial). 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 in each upgrade cycle, particularly C-level, consideration is given to the server group function, the upgrade availability option, and the HA designation. The following table describes the server selection considerations for each server group function.

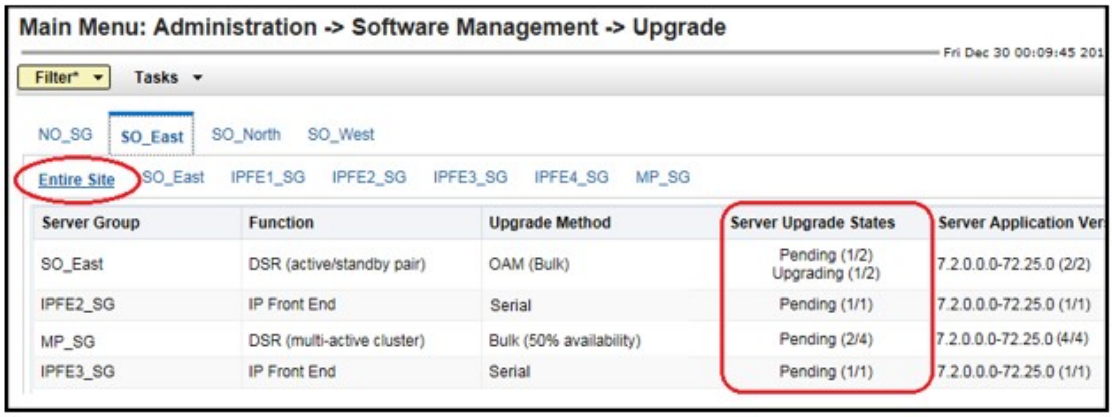
> **Note**
>
> The minimum availability option is a central component of the server selections for site upgrade . The effect of this option on server availability is described in detail in Minimum Server Availability.

Table 2-1 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 changes1.
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 Site Upgrade Options.
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. It is 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.

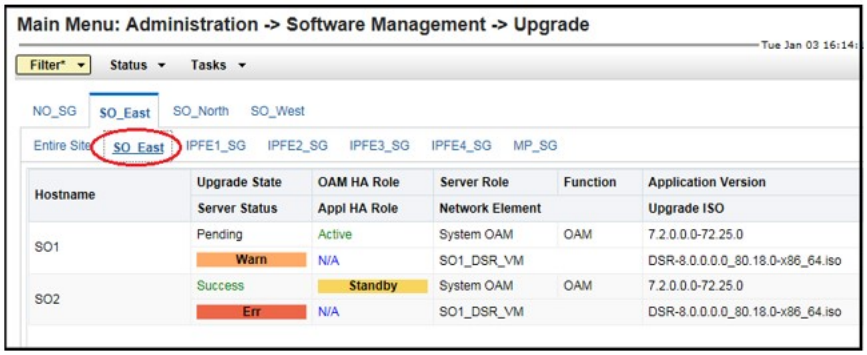
To initiate the site upgrade, you need to select a target ISO from the ISO picklist in the **Upgrade Settings** section of the **Site Initiate** screen. Once you click OK, the upgrade starts and control returns to the Upgrade Administration as shown in Figure 2-5 Figure. Once you select the **Entire Site** link, 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. Select the individual sever group links to obtain the detailed status. The server group view shows the status of each individual server within the selected server group.

Figure 2-5 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 as displayed in the following figure.

Figure 2-6 Server Group Upgrade Monitoring



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

2.4.2 Minimum Server Availability

The concept of Minimum Server Availability plays a key role during an upgrade using Automated Site Upgrade. The goal of server availability is to ensure that at least a specified percentage of servers (of any given type) remains 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 the other four upgrade. However, if there are nine servers 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, which allows for settings of 50%, 60%, and 75% minimum availability. There is also a setting of 0% for lab upgrade support. This option is described in detail in Site Upgrade Methodology.

The application of minimum server availability differs for the various server group functions. For some function types, it is calculated in percentage. However, for others, minimum availability does not apply due to overriding operational considerations. The following table describes the application of minimum server availability for the various server group functions.

Table 2-2 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 is calculated from the pool of in-service servers.

Table 2-2 (Cont.) Site Upgrade Availability vs. Server Group Function

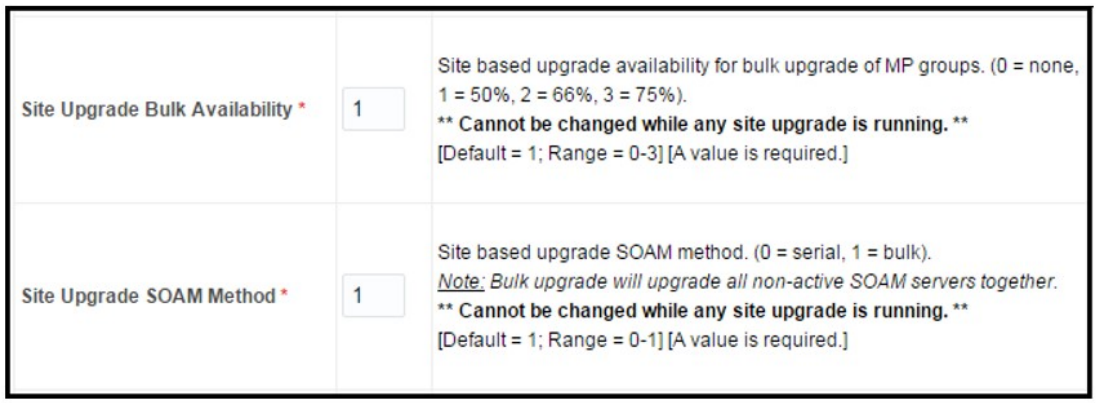
Server Group Function	Server Availability
SBR	Availability percentage does not apply to SBR server groups. SBRs are upgraded in a very specific order: spare – spare – standby – active.
IP Front End	IPFEs require special treatment during upgrade. The primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2.

When calculating the number of servers required to satisfy the minimum server availability, all servers in the server group (or server group cluster) are considered. Servers that are OOS or otherwise unable to perform their intended function, are included, as are servers that have already been upgraded. For example, cons ider a DA-MP server group with 10 servers; four have already been upgraded, one is OOS, and five are ready for upgrade. With a 50% minimum availability, only four of the servers that are ready for upgrade, can be upgraded in parallel. The four servers that have already been upgraded count toward the five that are needed to satisfy minimum availability. The OOS server cannot be used to satisfy minimum availability, so one of the upgrade-ready servers must remain in-service for minimum availability, thus leaving four servers to be upgraded together. Upgrading the last server would require an additional upgrade cycle.

2.4.3 Site Upgrade Options

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

Figure 2-7 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. 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.

The application of minimum server availability varies for the different types of C-level servers. For example, for a multi-active DA-MP server group, the minimum availability applies to all of the DA-MPs within the server group. This same setup applies to IPFEs as well. Table 2-2 defines how the Site Upgrade Bulk Availability setting on the General Options page affects the various server group function types.

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

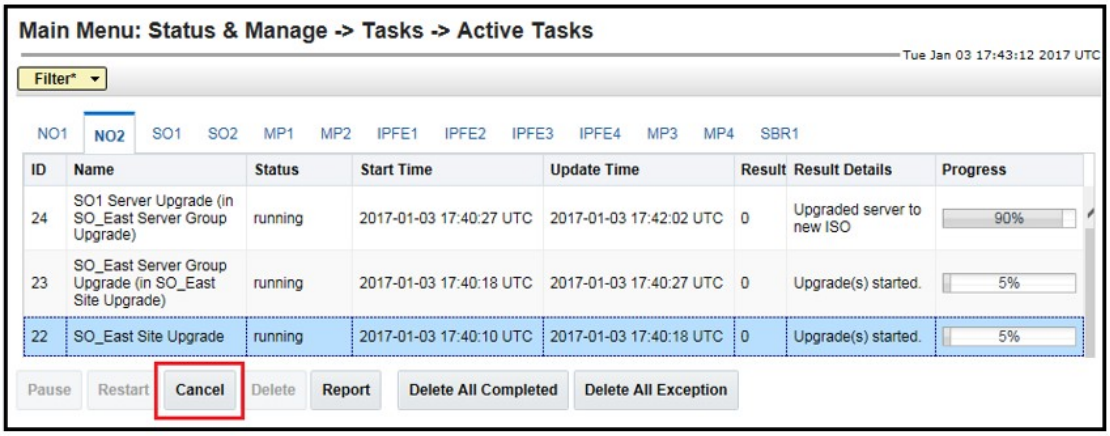
```
[Error Code xxx] - Option cannot be changed because one or more automated
site upgrades are in progress
```

2.4.4 Cancel and Restart Auto Site Upgrade

When an Auto Site Upgrade is initiated, several tasks are created to manage the upgrade of the individual server groups as well as the servers within the server groups. You can monitor and manage these tasks via the **Active Tasks screen**. Click **Status & Manage**, then **Tasks**, and then **Active Tasks**.

The naming convention **site_name** on the **Site Upgrade** screen identifies the main site upgrade controller task. In the following figure, the main task is task ID 22. This task controls the server group upgrade task (task ID 23), which in turn controls the server upgrade task (task ID 24).

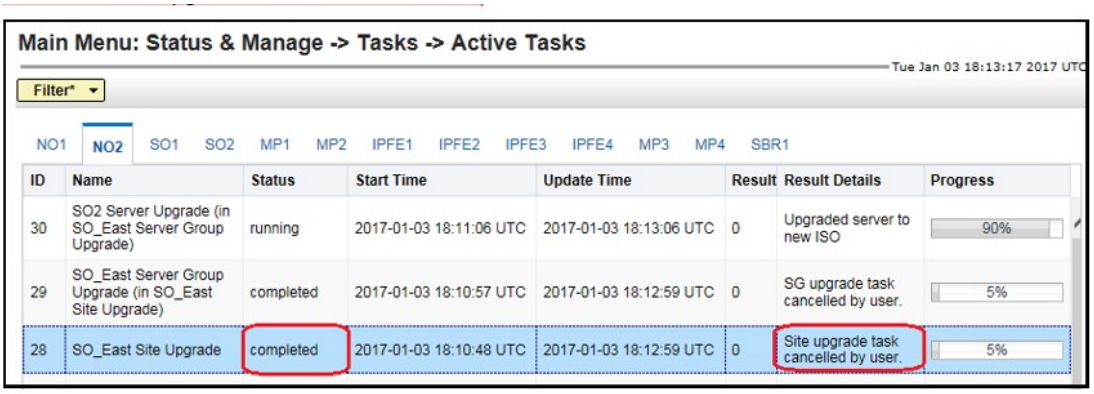
Figure 2-8 Site Upgrade Active Tasks



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 **Result 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. The following figure shows the **Active Tasks** screen after a site upgrade has been canceled.

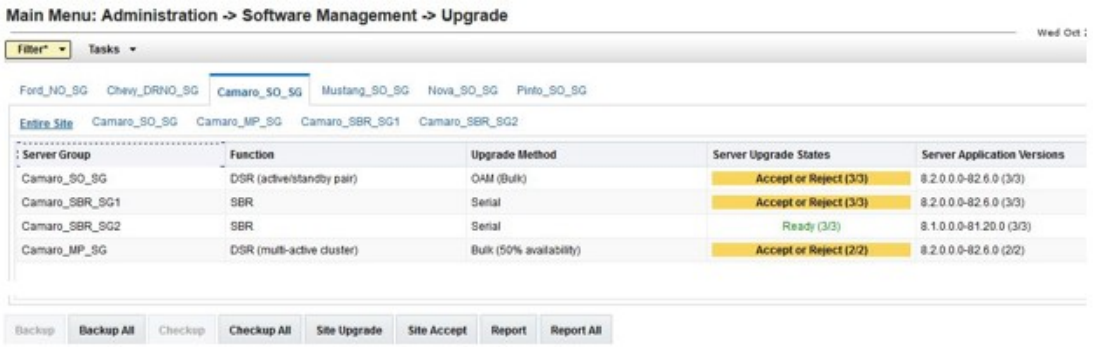
Once the site upgrade task is canceled, it cannot be restarted. However, the user can initiate the new site upgrade via the Upgrade Administration screen.

Figure 2-9 Canceled Site Upgrade Tasks



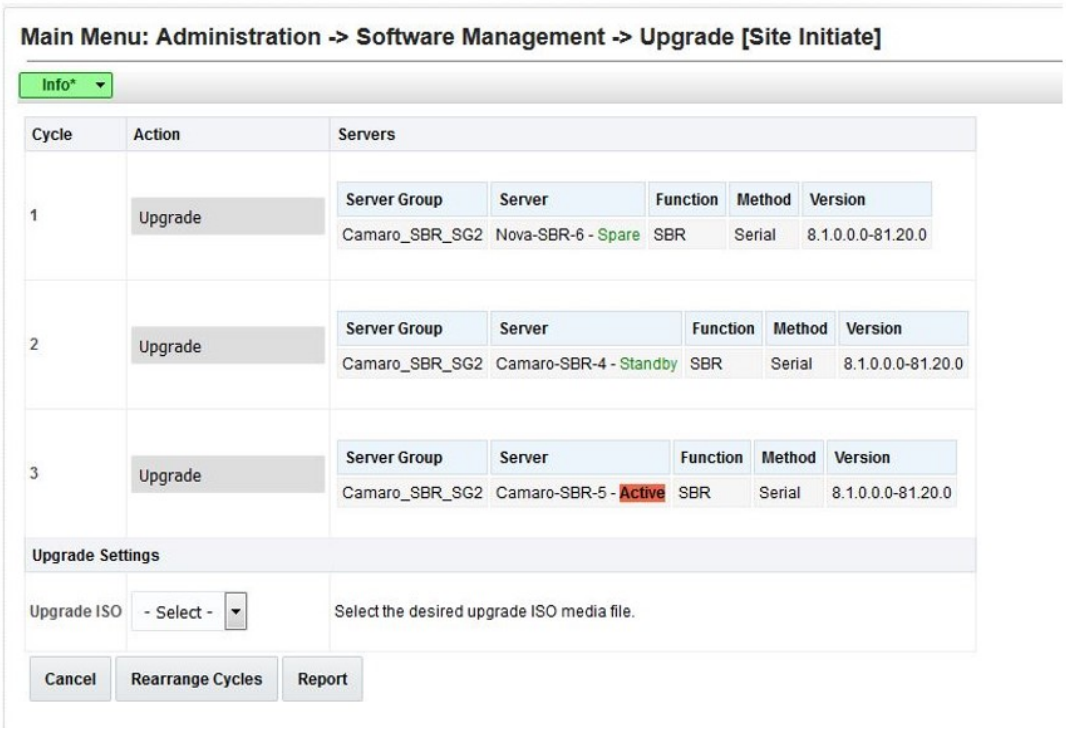
The following figure is representative of a site upgrade that was canceled before the site was completely upgraded. The servers that were undergoing upgrade when it was canceled continued to upgrade to the target release. These servers are now in the Accept or Reject state. The servers that were yet to be upgraded 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 2-10 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 2-9 Figure, only a single cycle is needed since the availability requirements can be met by the servers that have already been upgraded. Once the users select ISO and click OK, the site upgrade continues normally.

Figure 2-11 Restart Site Upgrade



2.5 Automated Server Group Upgrade

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

The purpose of ASG is to simplify and automate segments of the DSR upgrade. The DSR has long supported the ability to select multiple servers for upgrade. However, in doing so, it was

incumbent on the user to determine ahead of time which servers could be upgraded in parallel, considering traffic impact. If the servers were not carefully chosen, the upgrade could adversely impact system operations.

When a server group is selected for upgrade, ASG upgrades each of the servers serially, or in parallel, or a combination of both, while enforcing minimum service availability. The number of servers in the server group that are upgraded in parallel is user selectable. The procedures in this document provide the detailed steps specifying when to use ASG, as well as the appropriate parameters that should be selected for each server group type. ASG is the default upgrade method for most server group types associated with the DSR. However, there are some instances in which the manual upgrade method is utilized. In all cases where ASG is used, procedures for a manual upgrade are also provided.

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

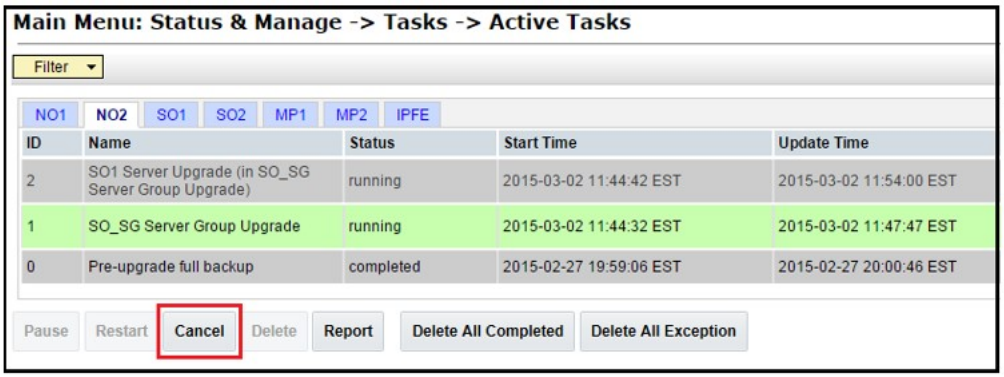
DSR continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

2.5.1 Cancel and Restart Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be manually canceled by navigating to **Status & Manage,** then **Tasks,** and then **Active Tasks** screen as shown in the following figure, if necessary. Once the task is canceled, it cannot be restarted. However, a new ASG task can be restarted via the Upgrade Administration screen.

For example, in the following Active Tasks Screen figure, task ID #1 (SO_SG Server Group Upgrade) is an ASG task, while task ID #2 is the corresponding individual server upgrade task. To cancel a specific ASG task, the users need to select it and click Cancel, as shown for task ID #1. It has no effect on the individual server upgrade tasks that were started by the ASG task (that is task ID #2 in the following figure). As the ASG task is canceled, no new server upgrades are initiated by the task.

Figure 2-12 Active Tasks Screen



In the event that a server fails to upgrade, it 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 canceled and no other servers in that server group are upgraded. Automatic cancelation triggers troubleshooting to correct the problem. Once the problem is solved, the users can again initiate a new server group upgrade on the upgrade screen.

2.5.2 Site Accept

You can accept the upgrade of some or all servers for a given site by clicking **Site Accept** on the upgrade GUI. When you click **Site Accept** a subsequent screen as shown in the following figure displays the servers that are ready for the Accept action. However, normal procedure calls for the Accept Upgrade to be applied to all 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, Click **OK** to confirm the intended action. 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.

3
Upgrade Planning

This section contains all the necessary information to carry out 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.
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 the procedures in Check Required Materials .

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

> **ⓘ Note**
>
> Be aware that once the upgrade starts and OAM level servers are on different releases than different sites, OAM level provisioning data is not replicated to sites that have not been upgraded. After the upgrade is completed, replication from OAM level server is restored and upgraded servers start receiving provisioning data.
>
> Refer to Automated Site Upgrade section for details and limitations/solutions while planning upgrade cycles.

There are some limitations with upgrading the DC server in a C-level server group that are upgraded in a group of servers, for example, DA-MP, vSTP MP(s). While manually upgrading, ensure the DC server is not upgraded in the first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix N and Identify the DC server. In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

You can access the DA-MP leader by navigating to the **Diameter Maintenance**, then **DA-MPs**, and then **Peer DA-MP** Status active SOAM, where MP Leader = Yes. Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration. Navigate to Main Menu, then MMI Guide to access the user guide.
2. Use the /vstp/mpleader MO. The result is the host name of the MP leader server.

> **Note**
>
> - If the Alarm 31149 - DB Late Write Nonactive appears on the screen, ignore it. This alarm does not have any effect on functionality.
> - If the upgrade is required from 8.x VM to 9.0.x, refer to Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible section.

3.1 Upgrade Check

- It is recommended to upgrade the SDS topology (NOAMs, SOAMs, DPs) before the DSR topology. See *SDS Software Upgrade Guide* for SDS upgrade documentation.

> **Caution**
>
> **SDS Upgrade**: If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes.

- If DSA or SFAPP is used with UDR, then it is recommended to upgrade the UDR topology (NOAMs, SOAMs, DPs) before the DSR topology. See *UDR Cloud Software Upgrade Guide* for UDR upgrade documentation.

> **Caution**
>
> **UDR Upgrade**: If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the UDR nodes.

3.2 Data Required for Upgrade

The following materials and information are needed to run an incremental upgrade:

- Target-release application DIU ISO image file or target-release application media.

> **Note**
>
> For a major upgrade, along with DIU ISO, the tar file and TPD OL7 DIU ISO is required.

- The capability to log into the network OAM servers with administrator privileges
- User logins, passwords, IP addresses, and other administration information. For more details, see Table 3-1
- VPN access to the customer's network is required if that is the only method to log in to the OAM servers.

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

3.2.1 Application ISO Image File

Obtain a copy of the target release and 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-9.2.0.0.0-102.16.0.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 Table 4-1.

3.2.2 Logins, Passwords, and Server IP Addresses

The following table identifies the information that is called out in the upgrade procedures such as server IP addresses and login credentials. While all of the information mentioned in the following table is required to complete the upgrade, there may be security policies in place that prevent the actual recording of this information in hard-copy form.

Table 3-1 Logins, Passwords, and Server IP Addresses

Item	Description
Target Release	Target DSR Upgrade Release
Credentials	GUI Admin Username
	GUI Admin Password
	DSR admusr Password
	DSR Root Password
VPN Access Details	Customer VPN Information (if needed)
NOAM	XMI VIP address
	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)

Table 3-1 (Cont.) Logins, Passwords, and Server IP Addresses

Item	Description
	Binding SBR SR2 Server Group Servers (Site 1)
	Binding SBR SR3 Server Group Servers (Site 1)
	Binding SBR SR4 Server Group Servers (Site 1)
PCA MP Server Group	PCA MP Server Group Servers (Site 1)
	PCA MP Server Group Servers (Site 1)
IPFE Server Groups(For PDRA)	PCA IPFE A1 Server Group Server (Site 1)
	PCA IPFE A 2 Server Group Server (Site 1)
	PCA IPFE B 1 Server Group Server (Site 1)
	PCA IPFE B 2 Server Group Server (Site 1)
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 2)
	Binding SBR SR2 Server Group Servers (Site 2)
	Binding SBR SR3 Server Group Servers (Site 2)
	Binding SBR SR4 Server Group Servers (Site 2)
PCA MP Server Group	PCA MP Server Group Servers (Site 2)
IPFE Server Groups (For PCA)	PCA IPFE A2 Server Group Server (Site 2)
	PCA IPFE B 1 Server Group Server (Site 2)
	PCA IPFE B 2 Server Group Server (Site 2)
vSTP MP Server Group	vSTP MP server(s)
Software	Target Release Number
	ISO Image (.iso) file name
Misc	Miscellaneous additional data

3.2.2.1 Expired Password Workaround Procedure

This section provides the procedures to handle password expiration during upgrade. This procedure 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 Expired Password Workaround Removal Procedure after the site is upgraded. Failure to remove the workaround inhibits password aging on the server.

3.2.2.1.1 Inhibit Password Aging

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

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

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

Expired Password Workaround Removal Procedure

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. Run the following command:

   ```
   clearCache
   ```

> **Note**
>
> For each server on which this workaround is enacted, the old expired password must be used for login. The new password used on the NOAM does not work on these servers.

> **Note**
>
> Repeat this step for the standby SOAM and all non-upgraded sites.

3.2.2.1.2 Enable Password Aging

The following procedure removes the password expiration workaround enabled in the Inhibit Password Aging procedure.

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. Run this command:

   ```
   $ sudo clearCache
   ```

4. Repeat sub-steps 1 to 3 for the standby SOAM.

> **Note**
>
> Repeat this procedure for all non-upgraded sites.

3.2.2.1.3 Password Reset

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

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. Run 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 in to the NOAM GUI using the new password. If the login is not successful, it is recommended to contact My Oracle Support (MOS) for guidance.

3.3 MySql User Accounts Password

This section provides the procedure to check for the presence of any forbidden special characters in the mysql passwords for **awadmin** and **root** user accounts.

Mysql password can contain the following:

- Upper case alphabets (A-Z)
- Lower case alphabets (a-z)
- Digits (0-9)
- 21 allowed special characters

Allowed Special Characters

There are a total of 32 special characters on the standard qwerty keyboard. Out of these 32 special characters, 21 characters are supported in the MySql passwords.

The following table provides the list of these 21 allowed special characters.

Table 3-2 Allowed Special Characters

Allowed Special Characters	Name
#	Octothorpe or hash or pound sign
!	Exclamation point
~	Tilde
%	Percent
^	Caret or circumflex
*	Asterisk
_	Underscore
-	Hyphen or dash
+	Plus
=	Equal
?	Question Mark
{	Open Braces
}	Close Braces
(	Open Parenthesis
)	Close Parenthesis
<	Open angle bracket or less than
>	Close angle bracket or greater than
|	Pipe or Vertical bar
.	Dot
,	Comma
;	Semi Colon

Forbidden Special Characters

There are a total of 32 special characters on the standard qwerty keyboard. Out of these 32 special characters, 11 characters are currently not supported in the MySql passwords. Usage of these forbidden special characters in the password will set the incorrect password in the database of MySql Server.

The following table provides the list of these 11 forbidden special characters.

Table 3-3 Forbidden Special Characters

Forbidden Special Characters	Name
@	Ampersat
$	Dollar
&	Ampersand
`	Backtick or backquote or grave accent
\	Backslash
/	Forward slash
[	Open Square Bracket
]	Close Square Bracket
'	Single quotation mark or apostrophe

Table 3-3 (Cont.) Forbidden Special Characters

Forbidden Special Characters	Name
“	Double quotation mark
:	Colon

3.3.1 Sanity Check on MySql Passwords

Perform the following procedure to sanity check MySql passwords.

1. Log in to the source server as `admusr`.

   ```
   Username: admusr
   Password: <current admin user password>
   ```

2. Verify the mysql passwords using the following commands.

   For `awadmin` user account:

   ```
   sudo /usr/TKLC/appworks/bin/aw.wallet credential get mysql default
   ```

   For `root` user account, use the following command:

   ```
   sudo /usr/TKLC/appworks/bin/aw.wallet credential get mysql root
   ```

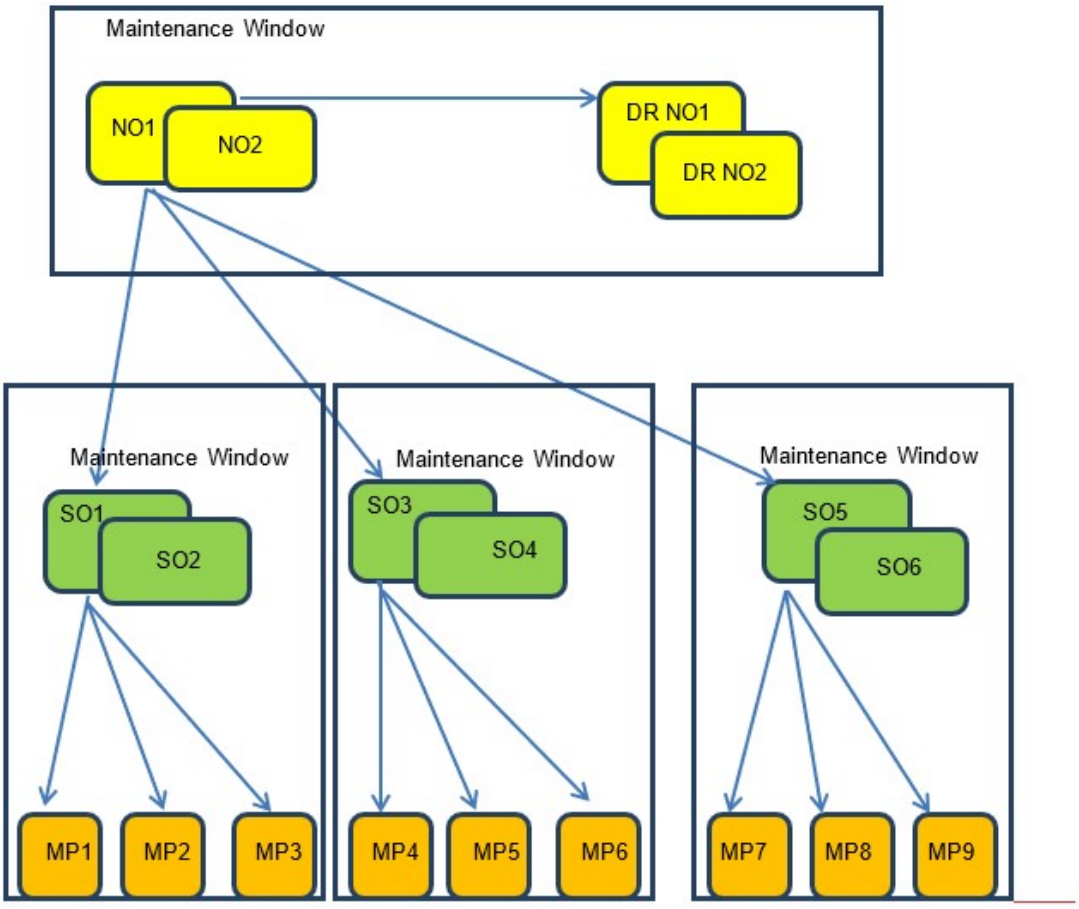
3. If passwords contain forbidden special characters mentioned in the Table 3-3 table, then reset the mysql password using the allowed special character mentioned in the Table 3-2 table.

> **Note**
>
> To reset the mysql password, see *Updating the MySQL Password* in *DSR Security Guide*.

3.4 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 all servers in a group are expected to be successfully upgrade in a single maintenance window. Use this high-level checklist to upgrade maintenance windows together with the detailed procedures that appear later in this document.

Figure 3-1 Upgrade Maintenance Windows for 3-Tier Upgrade



> **Note**
>
> Mated SOAM sites must be upgraded in separate maintenance windows.

3.4.1 Calculating Maintenance Windows

You can calculate the number of maintenance windows required for DSR setup and upgrade using the Maintenance Window Analysis Tool. For more information, see *Maintenance Window Analysis Tool* . It 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 *Maintenance Window Analysis Tool*.

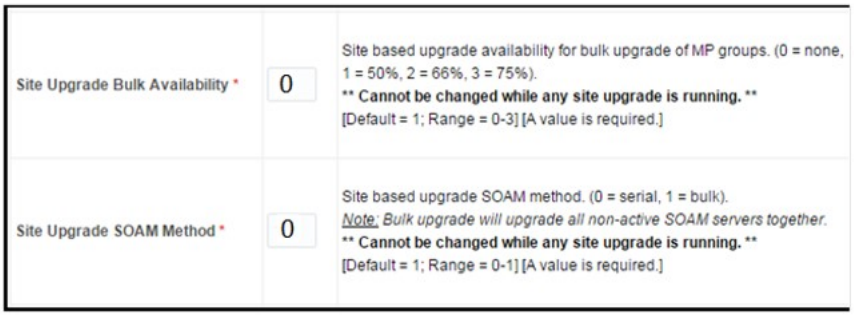
3.5 Site Upgrade Methodology

There are three primary methods for upgrading a DSR site:

- Auto Site Upgrade
- Auto Server Group Upgrade
- 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 provides more control of the upgrade process to the customer. of the upgrade process. The Automated Site Upgrade supports 0% availability that requires the least amount of time to upgrade the sites. This can be achieved by changing the following parameters: Site Upgrade SOAM Method setting to 0 - 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. Site Upgrade Bulk Availability setting to 0 - Changing the Site Upgrade Bulk Availability setting to 0 equates to 0% availability that means no servers are required to stay in service during the upgrade. This setting requires the minimum number of cycles, thus the least amount of time. This setting allows all of the DA-MPs to be upgraded at once .

Figure 3-2 Select Site Upgrade Methodology



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. The users can utilize a combination of upgrade methods to upgrade a given site to maximize efficiency with customer peace of mind. The following table is a checklist for determining which upgrade method meets the needs of the customer while ensuring compatibility with the DSR configuration. Upon completion of the checklist, a recommended upgrade method is identified.

Table 3-4 Traffic Analysis Checklist

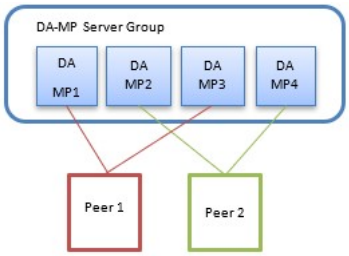
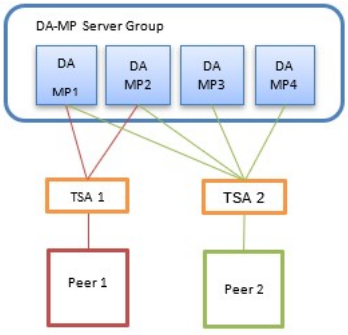
	Criteria	Yes/No	Notes
1	Do any of the site's DA-MPs have fixed diameter connections to any peer node, similar to this depiction? 		Automated Site Upgrade and Automated Server Group Upgrade, by default, do not consider fixed peer connections when selecting servers to upgrade. It is possible that all DA-MPs servicing a given peer (such as DA-MPs 1 and 3) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given peer are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to Rearrange Automated Site Upgrade Cycles to rearrange or add cycles for ASU or proceed to step 7 for a manual upgrade. If no, continue with step 2.
2	If peer nodes are configured via IPFE TSAs, are there any TSAs that are not distributed across all DA-MPs, similar to this depiction? 		Automated Site Upgrade and Automated Server Group Upgrade, by default, do not consider non-uniformly distributed TSAs when selecting servers to upgrade. It is possible that all DA-MPs servicing a given TSA (such as DA-MPs 1 and 2) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given TSA are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to Rearrange Automated Site Upgrade Cycles to rearrange or add cycles for ASU or proceed to step 7 for a manual upgrade. If no, continue with step 3.

Table 3-4 (Cont.) Traffic Analysis Checklist

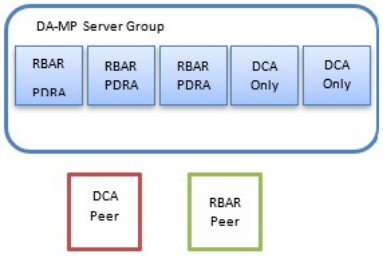
	Criteria	Yes/No	Notes
3	Do any of the site's DA-MPs have specialized distribution of DSR features, similar to this depiction? 		Automated Site Upgrade and Automated Server Group Upgrade, by default, do not consider non-uniform distribution of features when selecting servers to upgrade. It is possible that all DA-MPs hosting a given feature (such as DCA) could be upgraded simultaneously, thereby eliminating service functionality. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs hosting a given feature are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to Rearrange Automated Site Upgrade Cycles to rearrange or add cycles for ASU or proceed to step 7 for manual upgrade. If no, continue with step 4.
4	Automated Site Upgrade is a candidate for this system. Automated Site Upgrade supports 50% minimum server availability by default. A general option allows availability percentage settings of 66% or 75%. Is 50%, 66%, or 75% server availability during upgrade acceptable to the customer?		In general, a higher minimum availability setting increases the time required to upgrade a site. On the other hand, a lower minimum availability may reduce operational redundancy during the upgrade. If none of the minimum availability options are acceptable, Automated Site Upgrade should not be used to upgrade the site. If yes, continue with step 6. If no, proceed to step 7.
5	Is the customer comfortable with minimum user intervention (that is, user input) during the upgrade?		Once initiated, Automated Site Upgrade requires no additional user input to complete the upgrade. User control is limited to canceling the site upgrade task. If yes, Automated Site Upgrade is the recommended upgrade method. If no, proceed to step 7.
6	Automated Server Group Upgrade is a candidate for this system. Is the customer comfortable with the level of control afforded by the Automated Server Group upgrade?		Auto Server Group upgrade allows the user to initiate the upgrade of each server group, while the individual servers within the server group upgrade automatically. If yes, Auto Server Group upgrade is the recommended upgrade method. If no, proceed to step 7.

Table 3-4 (Cont.) Traffic Analysis Checklist

	Criteria	Yes/No	Notes
7	A manual upgrade affords the maximum level of control over upgrade sequencing. With this method, the upgrade of each server is individually initiated, allowing the user to control the level of parallelism and speed of the upgrade. **Note:** A site upgrade can include a combination of Automated Server Group upgrade and manual upgrades to improve efficiency. For example, SBRs can be upgraded with Automated Server Group upgrade, while the DA-MPs may be upgraded manually to control the order of upgrade for traffic continuity.		A manual upgrade is the recommended upgrade method.

3.5.1 DA-MP Upgrade Planning

If a manual upgrade is recommended by the Traffic Analysis Checklist, 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.

> **Note**
>
> If complete site upgrade is selected with 0% availability, then DA-MP upgrade planning is not required.

Table 3-5 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.

Customers need to 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 host names 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 host name 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.

You can access the DA-MP leader by navigating to **Diameter**, then **Maintenance**, then **DA-MPs**, and then **Peer DA-MP Status** on the active SOAM, where MP Leader = Yes. Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI from the MMI command using the REST Client for the vSTP configuration.

- Navigate to **Main Menu**, then **MMI Guide** to access the MMI user.
- Use the the /vstp/mpleader MO to obtain the host name of the MP Leader server.

> **Note**
>
> If needed, the users can upgrade DA-MPs serially, in which case, all host names would be listed in cycle 1. List the DA-MPs in the order in which they will be upgraded.

Table 3-5 DA-MP Upgrade Worksheet

	Host Names			
Upgrade Cycle 1 or Serial Upgrade				
Upgrade Cycle 2				
Upgrade Cycle 3				
Upgrade Cycle 4				

3.5.2 Pre-upgrade Validation

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

> **Note**
>
> This procedure resolves the inter-connectivity issue between the old-DC and non-DC MP at the time of upgrade for the BUG 27428669.

1. Check the Designated Coordinator (DC) node in the system by using the command:`ssh admusr@<MP_server> $ ha.info –d`
2. Before starting the MP server upgrade, disable the DSR application on current DC node, using the following command:
   a. On Active SOAM, go to **Status & Manage**, then **Server**.
   b. Disable the DSR application by selecting the MP (DC Node) and click **Stop**.
3. Select an MP to be upgraded:
   a. In cases where there is existing IPFE-based floating (Diameter) connections, choose an MP from TSA with more than 2 MPs. If there exists a TSA with just two MPs, and one having DC role, you should avoid using other MP (non-DC) in this TSA for upgrade at this step.
   b. In cases where there are MP based (Diameter) connection, select any MP except the MP having with DC role.
4. After upgrade, one of the upgraded MP with new release takes over the new -DC role.

5. The DSR application remains disabled on the old-DC node, as performed in Step 2.
6. The old-DC is upgraded in the next upgrade cycle.
7. When the upgrade is completed, from Active SOAM, navigate to **Status & Manage GUI** , then **Server** and check if the DSR application is Enabled on MP node (old-DC). If not, then Enable it by clicking **restart**.

3.5.3 Maintenance Window 1 for NOAM Site Upgrades

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

Maintenance Window 1 (NOAM Sites) Date: **Note:** You can view the form in DSR NOAM GUI by clicking **Configuration**, then **Network Elements**.	Record the Site **NE Name** of the DSR NOAM to be upgraded during Maintenance Window 1 in the space provided below. Verify if the upgrade is completed for the following servers: DR Standby NOAM (Guest): DR Active NOAM (Guest): Primary Standby NOAM (Guest): Primary Active NOAM (Guest):

3.5.4 Maintenance Window 2 for SOAM Site Upgrades and Rest of the Servers

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, georedundant PCA installations), copy and use the following form for the subsequent SOAM site upgrades.

> ⚠ **Caution**
>
> It is recommended that mated-pair SOAM sites are not upgraded in the same Maintenance Window.

Maintenance Window	Steps
SOAM Sites Date:	• Record the site NE Name of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided. • Verify if the upgrade is completed for the following sites: • SOAM Site: Spare SOAM1 (Guest): (if equipped) Spare SOAM2 (Guest): (if equipped): Standby SOAM (Guest): Active SOAM (Guest):

Maintenance Window	Steps
	DA-MP 1: DA-MP 2: DA-MP 3: DA-MP 4: DA-MP 5: DA-MP 6: DA-MP 7: DA-MP 8: DA-MP 9: DA-MP 10: DA-MP 11: DA-MP 12: DA-MP 13: DA-MP 14: DA-MP 15: DA-MP 16:
	IPFE1: IPFE 2: IPFE 3: IPFE 4:

Maintenance Window	Steps
	Binding Server Group 1 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 2 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 3 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 4 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 5 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 6 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 7 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped) Binding Server Group 8 Standby SBR: Active SBR: Spare SBR 1 (Mate): Spare SBR2 (Mate): (If equipped)

Maintenance Window	Steps
	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)

3.5.5 IDIH Upgrade

IDIH 9.2.0.0.0 supports only fresh installation.

4 Prerequisite Procedures

The pre-upgrade procedures shown in the following table are executed outside a maintenance window. 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.

4.1 Prerequisite Procedures Overview

Table 4-1 Prerequisite Procedures Overview

Procedure	Elapsed Time (hr:min)	Procedure Title
	This Step	Cum.
Check Required Materials	0:10-0:30	0:10-0:30
DSR ISO Administration	0:15-0:30	0:25-1:00
Verification of Configuration Data	0:20-0:30	0:55-1:30
Data Collection for Source Release 9.0 and Later	0:15-0:20	1:10-1:50
Back Up TKLCConfigData Files	0:15-0:30	1:30-3:05
Full Backup of DB Run Environment at Each Server	0:10-2:00	1:40-5:05

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.

> **Note**
>
> - Verify if the performance tuning parameters `txqueuelen`, `ring buffer`, and `multiqueue` are set appropriately before upgrade. For more information, see *Oracle Communications DSR Cloud Installation Guide*.
> - Performance tuning parameters on host machine may change after Oracle Linux upgrade on host machine. Verify these performance tuning parameters after upgrading Oracle Linux on host machine. For more information, see *Oracle Communications DSR Cloud Installation Guide*.
> - Prior to performing the upgrade, change all FQDN/Realm configurations to the standard FQDN format that is `label.label` format. In this instance, peer side configuration to be aligned with new FQDN/Realm configured at DSR. Edit operation on existing data can be performed using `GUI/MMI/importing CSV`. Existing data in DSR will work as is, if no modification is required in FQDN/Realm.
>   - In case of adding a new configuration, follow the standard format of FQDN/Realm.
>   - As an example, if FQDN is changed in peer with standard format then same has to be done in mediation and RBAR.

4.1.1 Check Required Materials

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

> **Note**
>
> Any third party software that the customer has installed will be removed after an upgrade.

Table 4-2 Check Required Materials

Step	Procedure	Description
1	Verify all required materials are present	Refer to Data Required for Upgrade to view the list of required materials.
2	Verify all administration data needed during upgrade	Double-check that all information in Upgrade Maintenance Windows is filled-in and accurate.
3	Contact My Oracle Support (MOS)	It is recommended to contact My Oracle Support and inform them of plans to upgrade this system. **Note:** Obtaining a new online support account can take up to 48 hours.

4.1.2 DSR ISO Administration

This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all the 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.
> - While upgrading from DSR 8.x to DSR 9.0.x before performing ISO Administration, see Extending the Partition for Dual Hop Upgrade `/var/TKLC/` size requirements.

1. Transfer through NOAM GUI using Active NOAM VIP

   Use the NOAM GUI upload function for ISO file transfer over the network. To upload the target release ISO image file to the File Management Area of the active NOAM server:

   a. Log in to the active NOAM GUI.
   b. Navigate to **Status & Manage**, then **Files**.
   c. Click the active NOAM server in the network to display all files stored in the file management storage area of this server.
   d. Ensure that this is actually the active NOAM server in the network by comparing the host name in the screen title vs. the host name in the session banner in the GUI. Verify they are the same and the status is Active in the session banner.
   e. Click **Upload**.

2. Upload active NOAM VIP.

   a. Click **Browse** to select the file to upload.
   b. Select the target release ISO image file and click **Open**.
   c. Click **Upload**.

3. Run the following commands on Active NOAM CLI.

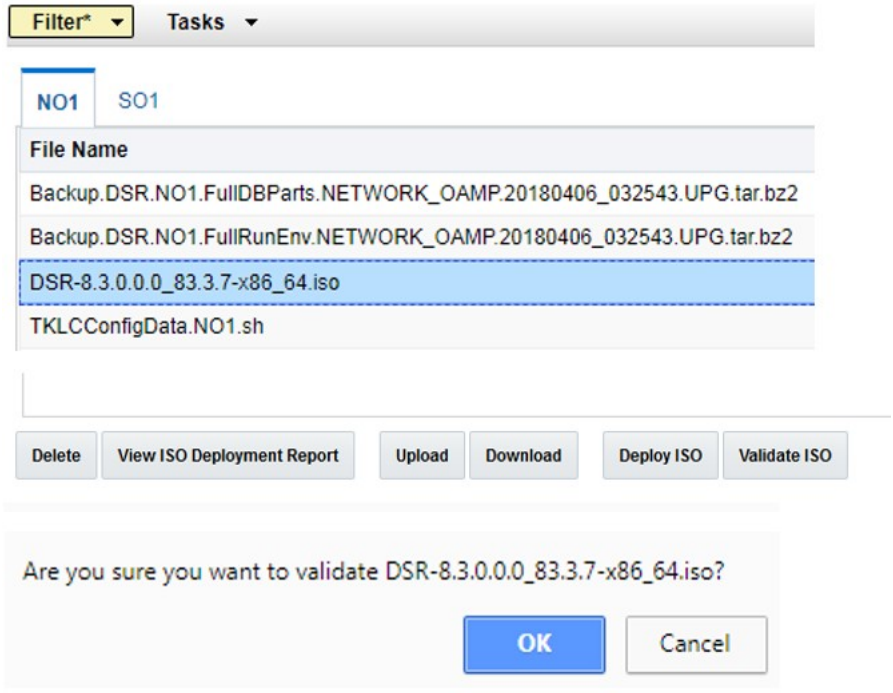
```
sudo sed -i '528i\ sleep(300);' /var/TKLC/appworks/services/SvrUpgrade.php


sudo sed -i '310s/validate_cd/validate_cd_tmp/' /var/TKLC/appworks/
services/FileManagement.php


sudo sed -i '294s/fwrite($file, $data);/fwrite($file,
json_encode($data));/' /var/TKLC/appworks/services/Diameter/
UpgradeHCplugin.php
```

> **Note**
>
> Perform the above step only if the base release is 9.0.0.0.0_97.16.0.

4. Change Permission of ISO using active NOAM CLI. Log in to the Active NOAM CLI and run the following command:

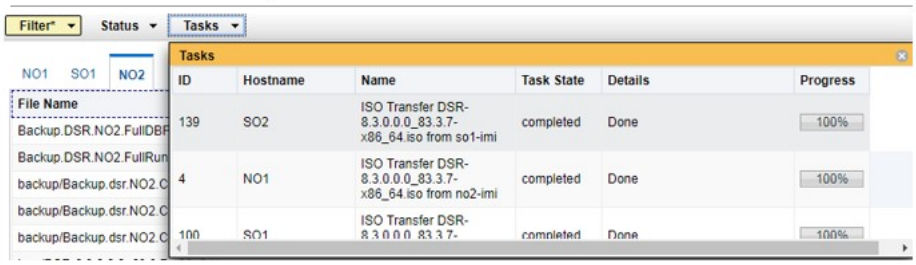
   ```
   sudo chmod 644 /var/TKLC/db/filemgmt/<DSR_ISO_Filename>
   ```

5. Deploy ISO to All the Servers to be Upgraded using NOAM GUI using active NOAM VIP.
   a. Navigate to **Status & Manage**, then **Files**.
   b. Click **Active NOAM** server tab. All files stored in the file management storage area of this server display on the screen.
   c. Select the target release ISO, and click **View ISO Deployment Report**.
   d. In the resulting report, determine if the ISO has been deployed to all servers in the system.
   e. If the ISO has been deployed to all servers, this procedure is complete. Proceed to the next procedure per Table 4-1.
   f. 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.
   g. 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, contact My Oracle Support.
   h. If the ISO is valid, select the ISO and click Deploy ISO. Click OK on the confirmation screen.

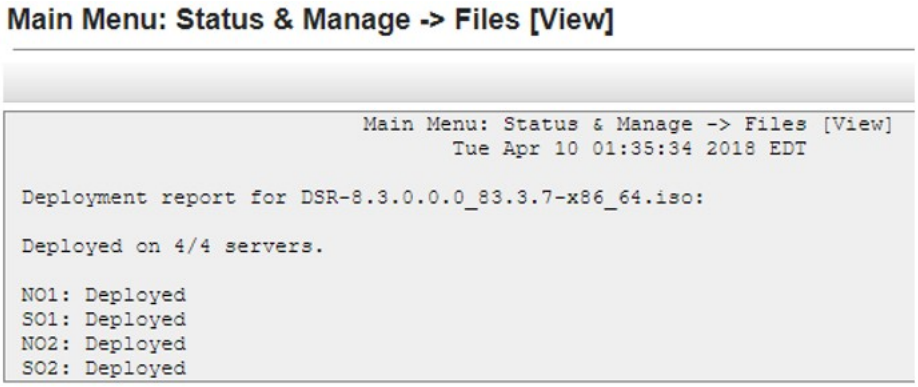


6. Monitor ISO Deployment using active NOAM VIP

a. Navigate to **Status & Manage**, select **Files**, and click **Tasks** to view the ISO deployment progress.



b. Select the target release ISO, and click **View ISO Deployment Report**. Verify the ISO has been deployed to all the servers in the system.



4.1.3 Data Collection - Verification of Global and Site Configuration Data

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

4.1.3.1 Verification of Configuration Data

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

Active NOAM VIP: Verify Application Version

1. Navigate to Administration, then Software Management, then Upgrade.
2. Verify the upgrade path to the target release is supported as documented in Supported Upgrade Paths to 9.2.0.0.0.
3. Select the NOAM Server Group and verify the Application Version.

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 to be installed. Rename the certificate, but note the original certificate pathname for use in Verify NOAM Post Upgrade Status.

> **Note**
>
> The following data collection procedures collect similar data. However, the collection method varies depending on the source release. Only Data Collection for Source Release 9.0 and Later procedure is to be executed for the pre-upgrade data collection.

4.1.3.2 Data Collection for Source Release 9.0 and Later

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 Verification of Configuration Data for guidance on which procedure to use. These procedures collect and archive system status data for analysis. Perform these procedures only if the source release is 9.0 and later.
If the Source Release is 9.0 and later use following procedure

1. Run the automated health checks on the active NOAM
   a. Navigate to Administration > Software Management > Upgrade.
   b. Select the active NOAM.
   c. Click **Checkup**.
   d. In the Health check options section, select the Advance Upgrade option.
   e. 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.
   f. Click OK. Control returns to the **Upgrade** screen.
2. Monitor Health Check Progress
   a. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **AdvanceUpgrade Health Check**.
   b. Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report.
   c. Click the hyperlink to download the Health Check report.
   d. Open the report and review the results.
3. 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.
   a. Navigate to **Status & Manage** and click **Files**.
   b. Select the **UpgradeHealthCheck.log** file and click **View**.
   c. Locate the log entries for the most recent health check.

d. Review the log for failures.

Analyze the failures and determine if it is safe to continue the upgrade. If necessary, contact My Oracle Support for guidance.

4. Initiate SOAM Health Check using Active NOAM VIP

This procedure runs the automated health checks on the active SOAM.

a. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.

b. Select the SOAM server group tab.

c. Select the active SOAM.

d. Click **Checkup**.

e. In the Health Check options section, select the **Advance Upgrade** option.

f. For a major upgrade, select the target release ISO from the Upgrade ISO option. Do not select an ISO for an incremental upgrade.

g. Click **OK**. Control returns to the Upgrade screen.

5. Monitor Health Check Progress using Active NOAM VIP

a. Click the Tasks option to view the currently executing tasks. The Health Check task name appears as <SOServerGroup> **AdvanceUpgrade Health Check**.

b. Monitor the Health Check task until the Task State is completed. The **Details** column displays a hyperlink to the Health Check report.

c. Click the hyperlink to download the Health Check report.

d. Open the report and review the results.

6. Analyze Health Check Failure using Active NOAM VIP

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.

a. Navigate to **Status & Manage**, then **Files**.

b. Select the active SOAM tab.

c. Select the UpgradeHealthCheck.log file and click **View**.

d. Locate the log entries for the most recent health check.

e. Review the log for failures.

Analyze the failures and determine if it is safe to continue the upgrade. If necessary, contact My Oracle Support for guidance.

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.

a. Analyze system topology data gathered in Verification of Configuration Data and steps 1 through 6 of the procedure. The Health Check reports from steps 3 and 6 can be found by navigating to **Status & Manage**, then **Files** on the active SOAM.

b. It is recommended to plan for MP upgrades by consulting My Oracle Support to assess the impact of out-of-service MP servers.

c. 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.

4.1.4 Back Up TKLCConfigData Files

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

Use the VIP address to access the primary NOAM GUI

Primary DSR NOAM VIP (GUI): Export Configuration Data for Each Server

1. Navigate to **Configuration**, then **Servers**.
2. Select each server in the topology and click **Export**.
3. Repeat this for all servers.

Primary SDS NOAM Server: Back Up TKLCConfig Data

1. Access the primary DSR NOAM server command line using ssh or a console. `ssh admusr@<NOAM_VIP>`
2. Transfer the TKLCConfigData files for all servers in the /var/TKLC/db/filemgmt directory to a remote location.`$ cd /var/TKLC/db/filemgmt $ scp TKLCConfigData.<Sever Hostname>.sh <username>@<remote-server>:<directory>`Example: scp TKLCConfigData.DSRNO1.sh <username>@<remote-server>:<directory>

4.1.5 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).

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

4.1.5.1 Full Backup of DB Run Environment for Release 9.0.x and Later

This procedure backs up the DB run environment when the active NOAM is on release 9.0.x and later. This procedure conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout.

> **Note**
>
> For 8.6.x release, backup files are created automatically when `./majorUpgrade.sh` script is used.

Active NOAM VIP: Start Backup of All Servers

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Administration** , then **Software Management,** and then **Upgrade**.
3. Click **Backup All**.

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.

Active NOAM VIP: Monitor Backup Progress

Select each server group tab and verify each server transitions from **Backup in Progress** to **Ready**.

Active NOAM VIP: Verify Backup Files on Each Server

1. Log in to the active NOAM.
2. Navigate to **Status & Manage**, then **Files**.
3. Click each server tab.
4. For each server, verify the following two files have been created:
   - `Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
   - `Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

4.1.5.2 Full Backup of DB Run Environment Using the backupAllHosts in GUI (Optional)

A manual backup can be run on each server individually, rather than using the GUI method.

> **Note**
>
> This is an alternative method.

Perform the following procedure:

1. Individually log into each server in the site.

2. Run the following command to generate a full backup on that server manually:

   ```
   sudo /usr/TKLC/appworks/sbin/full_backup
   ```

   Sample Output for 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`.

4.1.6 Software Upgrade Execution Overview

Before upgrading, users must perform data collection and system health check procedures in Prerequisite Procedures Overview. 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.

Please read the following notes on upgrade procedures:

- The completion time for all the procedures shown in this document are estimates. These estimates 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 host names.
  - 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.
- After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade must initiate each step. For procedures which are run multiple times, the checkbox displayed on the screen can be skipped, but the technician must initiate each iteration as a step is executed.
- Captured data is required for future support reference if a representative is not present during the upgrade.
- Answer these questions, and record:
  - What is the DSR Application version to be upgraded?
  - What is the DSR Application new version to be applied?
  - Is this a Major or Incremental Upgrade?
  - Are there IPFE servers to upgrade?

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

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

4.1.7 Accepting the Upgrade

After the upgrade of all the servers in the topology has been completed and an appropriate soak time, the post-upgrade procedures in Site Post-Upgrade Procedures are performed in a separate maintenance window to finalize the upgrade. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4.1.8 Checking the Network Adapter Settings

Perform the following procedure to check the Network Adapter settings before upgrading DSR from 8.x to 9.0.x:

> **Note**
>
> - This procedure is only applicable for VMware, not for OpenStack and KVM based systems.
> - If the Network Adapter settings output is in ascending order, skip this procedure.
> - The output may not always be in the ascending order. Perform the following procedure to verify the output.

1. Run the following command to verify that the hexa decimal number shown in bold in the output is in ascending order.

```
[root@LABVDSR03IPFE1 ~]# ls -l
    /sys/class/net
```

Figure 4-1 Output Example

```
[root@LABVDSR03IPFE1 ~]# ls -l /sys/class/net
total 0
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth0 ->
../../devices/pci0000:00/0000:00:16.1
/0000:0c:00.0/net/eth0
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth1 ->
../../devices/pci0000:00/0000:00:15.0
/0000:03:00.0/net/eth1
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth2 ->
../../devices/pci0000:00/0000:00:16.0
/0000:0b:00.0/net/eth2
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth3 ->
../../devices/pci0000:00/0000:00:17.0
/0000:13:00.0/net/eth3
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth4 ->
../../devices/pci0000:00/0000:00:18.0
/0000:1b:00.0/net/eth4
lrwxrwxrwx 1 root root 0 Apr  1 16:50 eth5 ->
../../devices/pci0000:00/0000:00:15.1
/0000:04:00.0/net/eth5
```

2. To obtain the hexa decimal number in ascending order, do the following:
   a. Run the following command to verify the parameters:

      ```
      [root@LABVDSR03IPFE1 ~]# lspci -v | grep
      ```

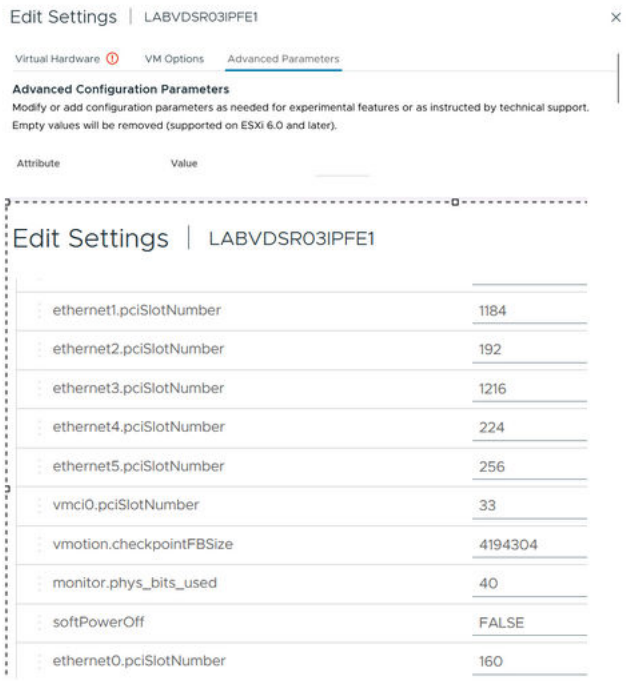
      The following image displays the output of the command:

Figure 4-2 Output Command

```
[root@LABVDSR03IPFE1 ~]# lspci -v | grep Ethernet -A2
03:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 160
        Flags: bus master, fast devsel, latency 0, IRQ 18
--
04:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 161
        Flags: bus master, fast devsel, latency 0, IRQ 18
--
0b:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 192
        Flags: bus master, fast devsel, latency 0, IRQ 19
--
0c:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 193
        Flags: bus master, fast devsel, latency 0, IRQ 19
--
13:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 224
        Flags: bus master, fast devsel, latency 0, IRQ 16
--
1b:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
        Subsystem: VMware VMXNET3 Ethernet Controller
        Physical Slot: 256
        Flags: bus master, fast devsel, latency 0, IRQ 17
```

3. After running the command, the user must shut down the VM, modify the parameters, and start the VM.
   a. To modify the parameters, from the **VMware GUI**, navigate to **VM**, and **Edit Settings**, and then click **Advanced Parameters**.
   b. Modify the pci slot number for the ascending order as shown in the output of the step 2.
   c. Modify or add the configuration parameters in the **Advanced Configuration Parameters** as shown in the following image:

Figure 4-3 Edit settings



5
Upgrading NOAM

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.

5.1 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 run 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 NOAM Upgrade procedure.
> - If syscheck fails on any server during pre-upgrade checks or in early checks stating that cpu: FAILURE:: No record in alarm table for FAILURE!, see Workaround to Resolve syscheck Error for CPU Failure procedure.
> - Increase the Maximum Number of Open Files As the number of servers in the topology grows, so does the need for additional files to handle data merge to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files. See Increase Maximum Number of Open Files to increase the maximum number of open files.

5.1.1 NOAM Health Check for Source Release 9.0 and Later

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 9.0 or later. This procedure must be executed on the active NOAM.

Active NOAM VIP: Verify DSR ISO upgrade transfer to all servers

1. Navigate to **Status & Manage,** then **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-9.0.2.0.0_98.15.0.iso:Deployed on 7/7 serversNO1: Deployed NO2: Deployed SO1: Deployed SO2: Deployed MP1: Deployed MP2: Deployed IPFE: Deployed`

Active NOAM VIP: Export and Archive the Diameter Configuration Data

1. Navigate to **Diameter Common**, then **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**, then **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.

Active NOAM VIP: Initiate NOAM Health Checks

This procedure runs the automated pre-upgrade health checks.

1. Navigate to **Administration**, then **Software Management**, and then **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.

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.

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**, then **Files**.
2. Select the **AdvancedUpgrade_HealthCheck_<NOAM SG>_<TIMESTMP>.txt file** and click View.
3. Locate the log entries for the most recent health check.
4. Review the log for failures.
5. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, contact My Oracle Support (MOS).

5.1.2 NOAM Pre-Upgrade Backup

This procedure takes a backup of the NOAM servers just prior to the upgrade.If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

> **Note**
>
> - If customer has changed MySQL password from default, refer to Sanity Check on MySql Passwords section to validate.
> - For further information on allowed and forbidden special charaters, see MySql User Accounts Password.

Active NOAM VIP: Backup All Global Configuration Databases for NOAM

This procedure is required for disaster recovery.

1. Navigate to **Status & Manage**, then **Database** to return to the Database Status screen.
2. Click to highlight the active NOAM server and click **Backup**.
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**.

Active NOAM VIP: Download/Save Database Files Backups for NOAM

This procedure is required for disaster recovery.

1. Navigate to **Status & Manage**, then **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**.

5.2 Increase Maximum Number of Open Files

Perform the following procedure to set the max open files limit to `tpdProvd`:

1. Add the following command in the `/usr/lib/systemd/system/tpdProvd.service` file, in the Service section after "UMask" value set, which is before `ExecStart` command:

   ```
   # Set limit to number of open files
   LimitNOFILE=32768
   #
   # Define the commands to start/stop the service.
   ExecStart=/usr/TKLC/plat/bin/tpdProvd --daemon
   ```

2. Run the following command:

   ```
   systemctl daemon-reload
   systemctl restart tpdProvd.service
   ```

```
Before change :
-----------------------

[admusr@sanityDSRNO92102a-DNO01 ~]$ ps -ef | grep -i tpdprovd
tpdProvd 6071 1 0 Jan16 ? 01:52:06 /usr/bin/perl -T /usr/TKLC/plat/bin/
tpdProvd --daemon
admusr 852030 849332 0 07:44 pts/1 00:00:00 grep --color=auto -i tpdprovd

[admusr@sanityDSRNO92102a-DNO01 ~]$ cat /proc/6071/limits | grep -i open
Max open files 1024 262144 files


After change:
--------------------

[admusr@sanityDSRNO92102a-DNO01 ~]$ ps -ef | grep -i tpdprovd
tpdProvd 852953 1 2 07:45 ? 00:00:00 /usr/bin/perl -T /usr/TKLC/plat/bin/
tpdProvd --daemon
admusr 853476 849332 0 07:46 pts/1 00:00:00 grep --color=auto -i tpdprovd

[admusr@sanityDSRNO92102a-DNO01 ~]$ cat /proc/852953/limits | grep -i open
Max open files 32768 32768 files
```

5.3 Disable Global Provisioning

The following procedure disables provisioning on the NOAM and Configuration Updates on the Entire Network. 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. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. Log in to the active NOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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)**

5.4 NOAM Upgrade

This procedure is used to upgrade the NOAM and DR NOAM servers. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

> **Note**
>
> If the upgrade is required from 8.x VM to 9.0.2, refer to Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible section.

1. Upgrade Primary DSR Standby NOAM

a. Upgrade the primary DSR standby NOAM server using Upgrade Single Server procedure.

   If the active NOAM is on DSR 9.x, follow the procedure in Upgrade Single Server – DSR 9.x.

b. After successfully completing the procedure from Upgrade Single Server – DSR 9.x, return to this point and continue with the next step.

   The active NOAM server may have some or all of the following expected alarms:

   Alarm ID = 10008 (Provisioning Manually Disabled)

   Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)

   Alarm ID = 31101 (DB Replication to slave DB has failed)

   Alarm ID = 31106 (DB Merge to Parent Failure)

   Alarm ID = 31107 (DB Merge from Child Failure)

   Alarm ID = 31225 (HA Service Start Failure)

   Alarm ID = 31226 (HA Availability Status Degraded)

   Alarm ID = 31233 (HA Path Down)

   Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)

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

   If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action.

2. Upgrade Second DSR NOAM
   a. Upgrade the second DSR NOAM server using the Upgrade Single Server procedure in Upgrade Single Server – DSR 9.x
   b. After successfully completing the procedure in Upgrade Single Server – DSR 9.x, return to this point and continue with the next step.
3. Upgrade Standby DR NOAM
   a. Upgrade the standby DR NOAM server using the Upgrade Single Server procedure in Upgrade Single Server – DSR 9.x
   b. After successfully completing the procedure in Upgrade Single Server – DSR 9.x, return to this point and continue with the next step.
4. Upgrade Active DR NOAM
   a. Upgrade the active DR NOAM server using the Upgrade Single Server procedure in Upgrade Single Server – DSR 9.x
   b. After successfully completing the procedure in Upgrade Single Server – DSR 9.x, return to this point and continue with the next procedure.

5.5 Verify NOAM Post Upgrade Status

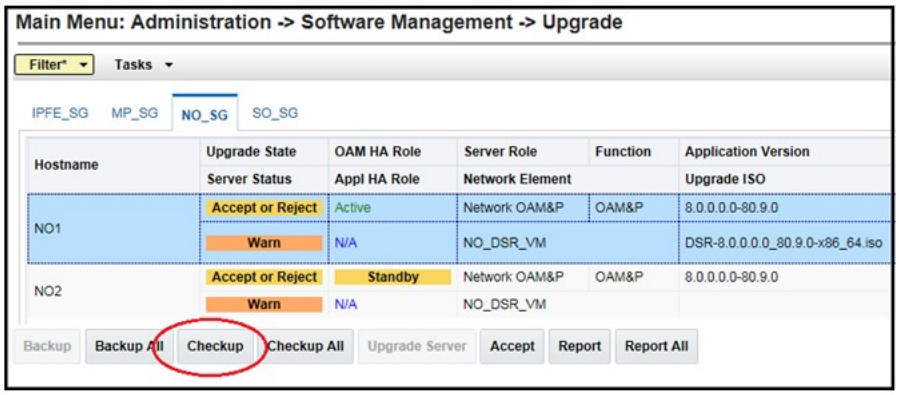
This procedure determines the validity of the upgrade and the health and status of the network and servers. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

Active NOAM VIP: Post-upgrade Health Checks

This procedure runs the automated post-upgrade health checks.

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
2. Select the active NOAM.

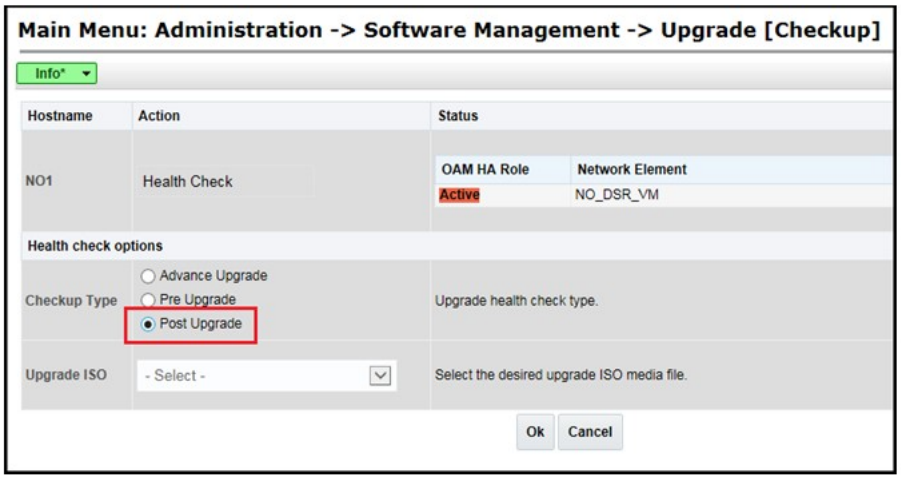
Figure 5-1 Active NOAM VIP Upgrade State



3. Click **Checkup**.
4. Under Health check options, select the **Post Upgrade** option.
5. Click **OK**.

   Control returns to the Upgrade screen.

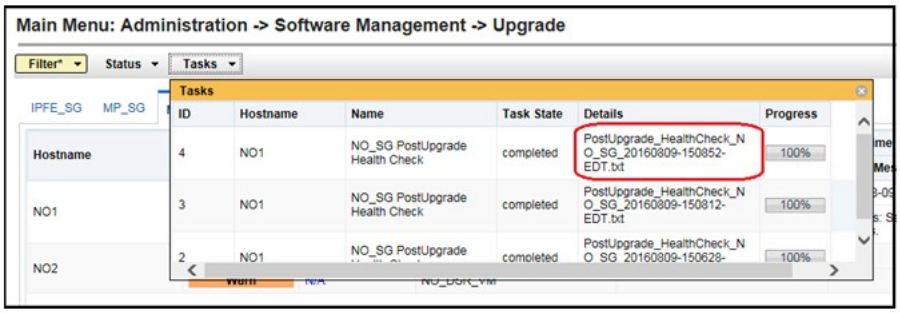
Figure 5-2 NOAM Upgrade Screen



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.

Figure 5-3 Active NOAM VIP Health Check Progress



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**, then **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, contact My Oracle Support (MOS) for guidance.

5.6 Allow Provisioning

The following procedure enables Global Provisioning after the NOAM upgrade for the NOAM and DR NOAM servers.

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

5.6.1 Active NOAM VIP: Enable Global Provisioning and Configuration Updates on the Entire Network

1. Log in to the active NOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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 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.

5.6.2 Active NOAM VIP: Add New Network Element

Perform this procedure only if you want to add a new network element 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 NOAMs. Follow the release specific installation procedures from *DSR Cloud Installation Guide* to install the software on the new servers and add the new network element under the existing NOAMs.

Skip the sections of the installation procedure related to installing and configuring the NOAMs. This adds a new DSR SOAM site under the existing NOAMs.

5.7 SNMP Configuration Update (Post NOAM Upgrade)

Apply SNMP workaround in following cases:

- If SNMP is not configured in DSR.
- If SNMP is already configured and SNMPv3 is selected as enabled version.

This can be checked by navigating to **Administration > Remote Servers >SNMP Trapping** screen using GUI session of NOAM server VIP IP address.

6
Site Upgrade Execution

This section contains the procedures for upgrading an entire site, starting with the preupgrade 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 maximum extent possible.

The Automated Site Upgrade procedures are explained in Automated Site Upgrade. Use the procedures in this section if the Automated Site Upgrade was recommended in Site Upgrade Methodology. For more details, see Rearrange Automated Site Upgrade Cycles.

The manual site upgrade procedures are in Overview of Automated/Manual Server Group Upgrade. Use the procedures in this section if the manual upgrade was recommended in Site Upgrade Methodology.

> **Note**
>
> Refer to Automated Site Upgrade for details and limitations/solutions while planning for upgrade cycles.

6.1 Site Preupgrade Activities

This section contains the procedures for site upgrade planning, preupgrade backups, health checks, and disabling site provisioning. Following are the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use the following list for determining the order in which the procedures are to be executed.

- Site Preupgrade Backups
- Site Preupgrade Health Check for Release 9.0 and Later
- Site Upgrade Options Check
- Disable Site Provisioning
- Site Upgrade Pre-Checks
- Automated Site Upgrade
- Rearrangement of upgrade cycles for Automated Site Upgrade
- Rearrangement of upgrade cycles for Automated Site Upgrade

6.1.1 Site Preupgrade 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 used to conduct 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. It is recommended that this procedure be executed no earlier than 36 hours before the upgrade starts.

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. This is an alternate procedure that can be used to backup a site using the command line. It should only be used as per the directions from My Oracle Support.

Active SOAM VIP: Back Up Site Configuration Data

This procedure is required for disaster recovery.

1. Log in to the SOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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**, then **HA** and identifying which server is currently assigned the VIP in the **Active VIPs** field. The server having VIP assigned is **Active**.

Active SOAM VIP: Download and Save Database Backup Files

This procedure is required for disaster recovery.

1. Navigate to **Status & Manage**, then **Files**.
2. Click the active **SOAM server** tab.
3. Select the configuration database backup file and click **Download**.
4. If a confirmation window appears, 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**.

Active NOAM VIP: Upgrade and Back Up DB Run Environment for Site

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
3. Click **Backup All**.

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 **Backup** 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 preupgrade 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.

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 four are complete.

Active NOAM VIP: Verify Backup Files are Present on Each Server

1. Log in to the active NOAM or SOAM GUI.
2. Navigate to **Status & Manage**, then **Files**.
3. Click 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.bz2Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
5. Repeat sub-steps one through four for each site being upgraded.

6.1.2 Site Preupgrade Health Check

This section provides procedures to verify the health of the SOAM site prior to upgrade. This is the primary procedure to be executed on the active SOAM . Alternate release-specific procedures are also provided, to be used as directed. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

> **Note**
>
> If syscheck fails on any server during preupgrade checks or in early checks stating that **cpu: FAILURE:: No record in alarm table for FAILURE!**, see the Workaround to Resolve syscheck Error for CPU Failure.

1. Run Site Health Checks (Phase 1)
   a. Select the SOAM on which health checks are run.
   b. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
   c. Select the tab of the site to be upgraded.
   d. Select the SOAM server group link.
   e. Select the active SOAM.
   f. Click **Checkup**.
2. Run site health checks (Phase 2)
   a. Click **Checkup**.
   b. In the Health Check options section, select the **Pre Upgrade** option.
   c. Use the **Upgrade ISO** option to select the target release ISO.
   d. Click **OK** to initiate the health check.

      Control returns to the Upgrade Administration screen.
3. Monitor Health Check Progress for Completion
   a. Click the **Tasks** option to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PreUpgrade Health Check**.
   b. Monitor the Health Check task until the Task State is completed.

      The Details column displays a hyperlink to the Health Check report.
   c. Click the hyperlink to download the Health Check report.
   d. Open the report and review the results.
4. 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.
   a. Navigate to **Status & Manage**, then **Files**.
   b. Select the active SOAM tab.
   c. Select the **UpgradeHealthCheck.log** file and click **View**.
   d. Locate the log entries for the most recent health check.
   e. Review the log for failures.

      Analyze the failures and determine if it is safe to continue the upgrade. If necessary, contact My Oracle Support (MOS) for guidance.
5. Export and Archive the Diameter Configuration Data on Active SOAM GUI
   a. Navigate to **Diameter Common**, then **Export**.
   b. Capture and archive the Diameter data by selecting the **All** option for the Export Application.
   c. Click **OK**.
   d. Verify the requested data is exported by clicking Tasks at the top of the screen.
   e. 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.

Capture data for each configured SOAM site.

6.1.3 Check Site Upgrade Options

Automated Site Upgrade provides user-configurable options that control certain upgrade behaviors. To find these options, navigate to SOAM's **Administration**, then **General Options** screen and are described in detail in Site Upgrade Options. 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.

1. Log in to the active SOAM GUI.
2. Navigate to **Administration**, then **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.

6.1.4 Disable Site Provisioning

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

> **Note**
>
> This procedure may only be performed in the maintenance window immediately before the start of the SOAM site upgrade.

1. Log in to the SOAM GUI of the site to be upgraded.
2. Navigate to **Status & Manage**, then **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)

   > **Note**
   >
   > Repeat this procedure for each configured SOAM site to be upgraded.

6.2 Site Upgrade Pre-Checks

This procedure verifies that the system is prepared for Automated Site Upgrade. It verifies the traffic status and verifies that Site Provisioning is disabled, in preparation for upgrading the site.

The following procedures must be completed before the start of automated site upgrade:

- Site Preupgrade Backups
- Site Preupgrade Health Check
- Check Site Upgrade Options
- Disable Site Provisioning
- Site Upgrade Pre-Checks

Also read Automated Site Upgrade section for details. Upgrade cycles are created when using the Automated Site Upgrade. Limitations in Limitations of Automated Server Group and Automated Site Upgrade 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 Overview of Automated/Manual Server Group Upgrade.

1. View KPIs to Verify Traffic Status in active SOAM VIP
   a. Log in to the active SOAM GUI using the VIP.
   b. Navigate to **Status & Manage**, then **KPIs**.
   c. Inspect KPI reports to verify traffic is at the expected condition.
2. Verify site provisioning is disabled
   a. Verify that Site Provisioning was properly disabled in Disable Site Provisioning section.
   b. In the GUI status bar, where it says Connected using …, check for the message Site Provisioning disabled.

> **Note**
>
> If the message is present, continue with the next procedure; otherwise, follow Disable Site Provisioning procedure.

6.2.1 Initiate Automated Site Upgrade

This procedure upgrades an entire site using the Automated Site Upgrade option. If this procedure fails, it is recommended to contact My Oracle Support and ask for assistance.

1. Review Site Upgrade Plan and Site Readiness

   Review the site upgrade plan created in Upgrade Maintenance Windows . This step verifies that the servers and server groups to be upgraded are in the appropriate state.
   a. Log in to the NOAM GUI using the VIP.
   b. Select **Administration**, then **Software Management**, and then **Upgrade**.
   c. Select the SOAM tab of the site to be upgraded.
   d. 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.

The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including **Accept or Reject**, **Ready**, **Backup Needed**, **Failed**, or **Not Ready**. Only the servers in the **Ready** or **Failed** state are upgrade eligible

2. Initiate Site Upgrade
   a. Verify no server groups are selected on the upgrade administration screen. The Site Upgrade button is not available if a server group is selected.
   b. Click **Site Upgrade**.
   c. Review the upgrade plan as presented on the Site Initiate screen.

> **Note**
>
> - 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.
> - Review the upgrade plan again and ensure all concerns noted in Table 6 have been addressed with the upgrade plan shown on the screen.

If you need to rearrange the upgrade cycle, see Rearrange Automated Site Upgrade Cycles. Otherwise, continue with the next step. There are some limitations with upgrading the DC server during its server group upgrade, which are upgraded in a group of servers. This is applicable for all upgrade options, for example DA-MP, vSTP MP(s). Hence, make sure the DC server is not upgraded in first upgrade cycle of the C-Level servers in its server group. Identify the DC server. If the DC server displays by default in the first upgrade cycle of its server group, then rearrange the upgrade cycles by referring to Rearrange Automated Site Upgrade Cycles section such that the DC server is not upgraded in the first upgrade cycle of its server group. vSTP MPs should be divided in cycles to avoid a network outage. In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

You can acces the DA-MP leader by navigating to **Diameter**, then **Maintenance**, then **DA-MPs**, and then **Peer DA-MP Status**, where MP Leader = Yes. Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

   i. From the MMI command using the REST Client for the vSTP configuration. The MMI user guide can accessed by navigating to **Main Menu**, then **MMI Guide**
   ii. Use the /vstp/mpleader MO.
   The result is the hostname of the MP leader server.
   iii. In the Upgrade Settings section of the form, use the Upgrade ISO options to select the target ISO.
   iv. Click OK to start the upgrade sequence.
   Control returns to the Upgrade Administration screen.

3. View the Upgrade Administration Form to Monitor Upgrade Progress

After selecting the **Entire Site** link , a summary of the upgrade status for the selected site appears. This summary identifies the server group(s) currently upgrading, the number of

servers within each server group that are upgrading, and the number of servers that are pending upgrade. Use this view to monitor the upgrade status of the overall site.
More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.
During the upgrade, the servers may have a combination of the following expected alarms.

- 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)
- Alarm ID = 31149 (DB Late Write Nonactive)
- Do not accept any upgrades at this time.
- If the upgrade fails, do not proceed. Refer to Recover from a Failed Upgrade for failed server recovery procedures.

4. 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) and refer to My Oracle Support and provide these files. Refer to Recover from a Failed Upgradefor failed server recovery procedures.

   When upgrade failure issue is identified and resolved, then Auto Site upgrade can be started again without executing any failed server recovery procedure.

5. Post Upgrade Verification

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

6.2.2 Rearrange Automated Site Upgrade Cycles

This procedure provides details to rearrange the Automated Site Upgrade cycles if required. Automated Site Upgrade provides an option to rearrange servers in the cycles thus eliminating

the risks of a potential network outage. ASU provides the flexibility to user to order the servers within the cycles without breaking the Minimum Availability and DA-MP Leader/vSTP MP leader criteria. .

1. Rearrange the Upgrade Cycle as Needed

   Click Rearrange Cycles.

2. Rearrange Servers in Cycles

   a. Automated Site Upgrade Cycles across the sites.

   > **Note**
   >
   > You can rearrange only DA-MPs and vSTPs. Re-arranging SBR and IPFE servers is restricted.

   b. When a server needs to be removed from cycle and needs to be added in an existing cycle or a new cycle, perform the following steps:

      i. Select the desired server in the list and click **Remove from Cycle**.

      > **Note**
      >
      > The server moves to the Free Pool on the right side.

      ii. Add the servers in Free Pool to another existing cycle or new cycle.

      > **Note**
      >
      > If there is no need to add a new cycle, then the procedure to rearrange the cycle is complete.

3. Add New Cycle (If needed)

   a. Click **Add Cycle**.

      After adding new cycle, servers available in free pool can be added in new cycle.

   b. Click **OK**.

6.3 Overview of Automated/Manual Server Group Upgrade

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.

The following 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 information to upgrade the SOAMs. The first cycle upgrades the standby SOAM, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, vSTP MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions

in -service to process traffic. The fourth cycle upgrades the second half of the DA-MPs, and IPFEs to complete the site upgrade.

Table 6-1 Non-PCA/PDRA Site Upgrade Plan

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

The following table details the site upgrade plan for a PCA/PDRA system with two-site redundancy. This upgrade plan is divided into five cycles. The first two cycles consist of upgrading the SOAMs - the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers. The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, IPFEs, and vSTP servers are upgraded in parallel with all of the spare SBRs. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the standby SBRs. The fifth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 6-2 Two-Site Redundancy PCA Site Upgrade Plan

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

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

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

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

The first two cycles consist of the information to upgrade the SOAMs – the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures the OAM controllers are always upgraded before any C-level servers. The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, and IPFEs are upgraded in parallel with one spare SBR. This leaves the remaining server functions in-service to process traffic. The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the second spare

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

Table 6-3 Three-Site Redundancy PCA Site Upgrade Plan

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

6.3.1 Site Upgrade Planning

The upgrade of the site servers involve multiple automated upgrades using the Automated Server Group upgrade feature, along with manual upgrades that are a comparatively less automated.

For the server groups that are upgraded using ASG, the only planning necessary is to record the name of the server group. ASG automatically selects the individual servers to upgrade. The IPFE and vSTP (if equipped) server groups must be upgraded manually since there is only one server per server group. Planning is necessary for these server groups to ensure traffic continuity. Record the host name of the servers to be upgraded in each iteration. vSTP MPs should be divided in cycles to avoid a network outage. While choosing ASG and Manual upgrades for multi-active MP servers, see the limitations in Limitations of Automated Server Group and Automated Site Upgrade for the Automated Server Group upgrade option.

While choosing ASG and Manual upgrades for multi-active MP servers, see the limitations in Limitations of Automated Server Group and Automated Site Upgrade for the Automated Server Group upgrade option. If your network aligns with any of the scenarios listed in Limitations of Automated Server Group and Automated Site Upgrade, then do NOT use the Automated Server Group. This eliminates the risks of a potential network outage.

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

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

Access the DA-MP leader on the active SOAM by navigating to **Diameter**, then **Maintenance**, then **DA-MPs**, and then Peer DA-MP Status, where **MP Leader** = **Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI from the MMI command using the REST Client for the vSTP configuration. Complete this procedure by performing the following steps:

1. Access the MMI user guide by navigating to **Main Menu**, then **MMI Guide**.
2. Use the **/vstp/mpleader** MO.
   The result is the hostname of the MP leader server.

> **Note**
>
> In iteration 1, if a spare SOAM exists, the spare and standby SOAMs are upgraded manually. Otherwise, the SOAMs are upgraded with ASG.
> In iteration 2, the active SOAM is upgraded either manually or by ASG.
>
> In iteration 3 and 4, ASG automatically selects DA-MPs for upgrade in DA-MP Group 1 and DA-MP Group 2 respectively. ASG also automatically selects the spare SBR(s) for upgrade. However, IPFE 1 Hostname and IPFE 3 Hostname are upgraded manually.
>
> In iteration 5, ASG automatically selects the active SBR(s) for upgrade.

6.3.2 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. The above shows the estimated execution times for the SOAM upgrade. Manual SOAM Upgrade (Active/Standby/Spare) is recommended for upgrading the SOAMs when there is no spare SOAM. ASG automatically upgrades the standby SOAM followed by the active SOAM.

Manual SOAM Upgrade (Active/Standby/Spare) procedure is also recommended when the site has a spare SOAM.The manual upgrade procedure upgrades the standby and spare SOAMs in parallel, followed by the active SOAM.

> **Note**
>
> For information on SOAM VM profile for increased MP Capacity, refer to Create a Link for ComAgent.

6.3.3 Upgrade SOAMs

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, the SOAMs are upgraded manually so that the spare and standby SOAMs can be upgraded concurrently. This reduces the time required to upgrade the SOAMs. Regardless of which SOAM upgrade option is used, refer to SOAM Upgrade Pre-Checks section to ensure site provisioning is disabled. If the site does not include a spare SOAM, refer to Automated SOAM Upgrade (Active/Standby) section. If the site does include a spare SOAM, refer to Manual SOAM Upgrade (Active/Standby/Spare) section.

> **Note**
>
> Site Preupgrade Backups, Site Preupgrade Health Check and disable Site Provisioning procedures must be completed before the start of SOAM upgrade.

Active SOAM VIP: View KPIs to Verify Traffic Status

This procedure verifies the traffic status by viewing the KPIs.

1. Log in to the active SOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **KPIs**.
3. Inspect KPI reports to verify traffic is at the expected condition.

Active SOAM VIP: Verify Site Provisioning is Disabled

This procedure verifies that site provisioning is disabled.

1. Verify that Site Provisioning was properly disabled. In the GUI status bar, where it says **Connected using …**, check for the message **Site Provisioning disabled**.
2. If the message is present, continue with the next procedure. Otherwise, perform Disable Site Provisioning procedure.

6.3.3.1 Automated SOAM Upgrade (Active/Standby)

This procedure is the recommended method for upgrading the SOAMs if the site does not include a spare SOAM. If the site has a spare SOAM, refer to Manual SOAM Upgrade (Active/Standby/Spare) section and upgrade. Upon completion of this procedure, proceed to Rearrange Automated Site Upgrade Cycles section, Upgrade Iteration 3.

Upgrade SOAM Server Group

This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option.

1. Upgrade the SOAM server group using the Upgrade Multiple Servers procedure with the following options:
   a. Use the Automated Server Group Upgrade option
   b. Select the Serial Upgrade mode
2. Execute Appendix D Upgrade Multiple Servers – Upgrade Administration.

After successfully completing the procedure in Appendix D, return to this point and proceed to Upgrade Iteration 3 section.

> **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 replicatiochannel to the C-level server is inhibited due to the difference in release versions.

6.3.3.2 Manual SOAM Upgrade (Active/Standby/Spare)

This procedure upgrades the SOAM server group if the site includes a spare SOAM. If the SOAM server group was upgraded via Automated SOAM Upgrade (Active/Standby) section, then do not perform this procedure; proceed to Upgrade Iteration 3 section.

Upgrade Standby and Spare SOAMs in parallel using the Upgrade Multiple Servers Procedure

This procedure upgrades the SOAMs in a DSR manually. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

- Execute Appendix D Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.

Upgrade Active SOAM using Upgrade Single Server Procedure

This procedure upgrades the SOAMs in a DSR manually. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

- Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and proceed to Upgrade Iteration 3.

6.3.4 Upgrade Iteration 3

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

> **Note**
>
> - The estimated time required to upgrade the C-level servers for iteration 3 is 0:40-1:00, and this procedure upgrades ½ of the DA-MPs, ½ of the IPFEs, ½ of the vSTPs, and the spare SBR(s).
> - This procedure upgrades a portion of the C-level servers for iteration 3. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

> **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 Site Upgrade Methodology Selection section, do not use ASG to upgrade the DA-MPS in this iteration. Alternate upgrade procedures are provided in Appendix F.3.

1. Select the DA-MP server group to view preupgrade status of DA-MPs
   a. Log in to the NOAM GUI using the VIP.
   b. Navigate to **Administration**, select **Software Management**, and click **Upgrade**.
   c. Select the SOAM tab of the site being upgraded.
   d. Select the DA-MP Server Group link.
   e. For the DA-MP servers to be upgraded in iteration 3, verify the application version value is the expected source software release version.

2. View preupgrade status of DA-MP servers on active NOAM VIP
   a. 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**.
   b. Verify the **OAM Max HA Role** is in the expected condition (either standby or active). This depends on the server being upgraded.
3. Verify if upgrade status is ready for the server to be upgraded.

> **Note**
>
> This may take a minute if a backup is in progress. 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. Initiate the Automated Server Group upgrade of the DA-MP Servers (Part 1)
   a. To use the Automated Server Group upgrade option, verify no servers in the server group are selected.
   b. Click **Auto Upgrade**.
5. Initiate the Automated Server Group upgrade of the DA-MP Server (Part 2)
   a. The **Upgrade Settings** section of the Initiate screen controls the behavior of the server group upgrade. Select **Bulk** mode.
   b. Select 50% for the **Availability** setting.
   c. Select the appropriate ISO from the **Upgrade ISO** options.
   d. Click **OK** to start the upgrade.
6. View the upgrade administration form to monitor upgrade progress.

a. Observe the upgrade state of the DA-MP servers. Upgrade status displays under the Status Message column.

b. While the DA-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.

7. Identify the IPFE server group(s) to upgrade

   From the data captured in Site Upgrade Planning section, identify the IPFE server group(s) to upgrade in iteration 3.

8. View preupgrade status of IPFEs

   a. Navigate to Administration, select **Software Management** Upgrade.

   b. Select the SOAM tab of the site being upgraded.

   c. Select the link for each IPFE server group to upgrade.

   d. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version.

   e. 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**.

   f. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded.

9. Verify Upgrade Status is Ready for the server to be upgraded

   > **Note**
   >
   > 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 appears. Navigate to the IPFE server group being upgraded.

   Servers may have a combination of the following expected alarms:

   > **Note**
   >
   > Not all servers have all alarms.

   - Alarm ID = 10008 (Provisioning Manually Disabled)
   - Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)
   - Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)
   - Alarm ID = 32515 (Server HA Failover Inhibited)
   - Alarm ID = 31101 (DB Replication to slave DB has failed)
   - Alarm ID = 31106 (DB Merge to Parent Failure)
   - Alarm ID = 31107 (DB Merge From Child Failure)
   - Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)

- Alarm ID = 31114 (DB Replication over SOAP has failed)
- Alarm ID = 31225 (HA Service Start Failure)

10. Initiate IPFE Upgrade (Part 1)
    a. Select the Upgrade Server method.
    b. From the Upgrade Administration screen, select the server to upgrade.
    c. Click **Upgrade Server**.
11. Initiate IPFE Upgrade (Part 2)
    a. Select target ISO.
    b. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options.
    c. Click **OK** to start the upgrade.
12. View the upgrade administration form to monitor upgrade progress.

    Observe the upgrade state of the IPFE server. Upgrade status displays under the Status Message column.
13. Identify the SBR Server Group(s) to Upgrade

    From the data captured in Site Upgrade Planning section, identify the SBR server group(s) to upgrade in iteration 3.

> **Note**
>
> ASG steps (Auto Upgrade), mentioned in the next steps, do not provide any liberty to the operator to verify observations during the upgrade. If a manual upgrade was recommended for the SBR upgrade, do not use ASG to upgrade all the SBR servers from the same server group in this single iteration. Alternate upgrade procedures are provided in Manual SBR Upgrade section. Spare SBR server(s) need to be upgraded. If the Manual Upgrade is used, skip ASG steps 15. to 19.

14. View preupgrade status of SBRs to upgrade.
    a. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
    b. Select the SOAM tab of the site being upgraded.
    c. Select the link for each SBR server group to upgrade.
    d. For the SBR servers to be upgraded in iteration 3, verify the application version value is the expected source software release version.
    e. 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.
    f. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded.
15. Verify upgrade status is Ready for the server to be upgraded.

> **Note**
>
> This procedure defines the steps to verify that the 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 appears. Navigate to the SBR server group being upgraded.

Servers may have a combination of the following expected alarms. However, 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)

16. Initiate SBR Upgrade (Part 1)
    a. Select the Auto Upgrade method.
    b. To use the Automated Server Group upgrade option, select the SBR server group to upgrade.
    c. Verify no servers in the server group are selected.
    d. Click Auto Upgrade.
17. Initiate SBR Upgrade (Part 2)
    a. The Upgrade Settings section of the Initiate screen controls the behavior of the automated upgrade. Select **Serial** mode.
    b. Set upgrade options and start the Automated Server Group Upgrade.
    c. Select the appropriate ISO from the Upgrade ISO options.
    d. Click **OK** to start the upgrade.
18. 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.
19. View Pre-upgrade Status of vSTP MP Servers
    a. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
    b. Select the SOAM tab of the site being upgraded.
    c. Select the link for each vSTP server group to upgrade.
    d. For the vSTP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.
    e. If a server is in **Backup Needed s**tate, 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**.

f. Verify the **OAM Max Ha Role** is the expected condition (either standby or active). This depends on the server being upgraded.

20. Verify upgrade status is Ready for the server to be upgraded.

> **Note**
>
> 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.

> **Note**
>
> Servers may have a combination of the following expected alarms. However, 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)

21. Initiate vSTP MP Upgrade (Part 1) on active NOAM VIP
    a. Select the Upgrade Server method.
    b. From the Upgrade Administration screen, select the server to be upgraded.
    c. Click **Upgrade Server**.
22. Initiate vSTP Upgrade (Part 2) on active NOAM VIP
    a. Select target ISO
    b. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options.
    c. Click **OK** to initiate the upgrade.
23. 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.
24. View the upgrade administration form to monitor upgrade progress

> **Note**
>
> If the upgrade of a server fails section for instructions if the upgrade fails, or if execution time exceeds 60 minutes. 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.

a. Navigate to **Administration**, select **Software Management**, and click **Upgrade**.

b. Select the SOAM tab of the site being upgraded.

c. 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.

- 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**
>
> 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 Limitations of Automated Server Group and Automated Site Upgrade to resolve this issue.

25. 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
```

> **Note**
>
> It is recommended to contact My Oracle Support (MOS) and provide these files. Refer to Appendix I for failed server recovery procedures.

6.3.5 Upgrade Iteration 4

Upgrade iteration 4 continues the upgrade of the site C-level servers. Iteration 4 consists of details to upgrade the second half of the DA-MPs, vSTPs, and IPFEs, as well as the standby SBR(s), if equipped. The procedures in this section provide the steps to upgrade, ½ of the vSTPs servers and ½ of the IPFEs. ASG automatically upgrades the DA-MPs and SBRs.

From the data captured in Site Upgrade Planning section, identify the IPFE server group(s) to be upgraded in iteration 4.

Active NOAM VIP: View Pre-upgrade Status of IPFEs

1. Navigate to Administration, and select **Software Management** and click **Upgrade**.
2. Select the NOAM 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.

6.3.6 Upgrade Iteration 5

1. At iteration 5, the active SBR is upgraded, causing the standby to become active.
2. 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.

   a. Navigate to **Administration**, select **Software Management**, and click **Upgrade**.
   b. Select the SOAM tab of the site being upgraded.
   c. 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.

- 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 Limitations of Automated Server Group and Automated Site Upgrade to resolve this issue.

Wait for the SBR upgrades to complete. The Status Message column displays **Success**. This step takes approximately 20 to 50 minutes.

3. If the upgrade of a server fails, access the server command line (through ssh or a console), and collect the following files:

   [1]

   If any upgrade fails, do not proceed. It is recommended to consult with on the best course of action. Refer to Recover from a Failed Upgrade for failed server recovery procedures.

6.4 Upgrade Single Server – DSR 9.x

The following procedures upgrade a single DSR server of any type (For example: NOAM, SOAM, MP) when the active NOAM is on DSR 9.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 this procedure to mark up, or keep another form of written record of the steps performed.
> - If the upgrade is required from 8.x VM to 9.0.2, refer to Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible section.

[1] /var/TKLC/log/upgrade/upgrade.log

/var/TKLC/log/upgrade/ugwrap.log

/var/TKLC/log/upgrade/earlyChecks.log

/var/TKLC/log/platcfg/upgrade.log

1. View the preupgrade status of servers in active NOAM VIP
   a. Log in to the NOAM GUI using the VIP.
   b. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
   c. Select the Network Element of the server to be upgraded (NOAM or site).

      The active NOAM server may have some or all of these expected alarms:

      Alarm ID = 10008 (Provisioning Manually Disabled)

      Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
2. Verify Status of Server to be Upgraded
   a. Identify the server to be upgraded (NOAM, SOAM, MP, and so on) and record hostname.
   b. Verify the Application Version value is the expected source software release version.
   c. If the server is in the **Backup Needed** state, select the server and click Backup.
   d. On the Upgrade Backup screen, click **OK**.

      The Upgrade State changes to **Backup in Progress**.
   e. Verify the **OAM Max HA Role** is the expected condition (either standby or active). This depends on the server being upgraded.
   f. When the backup is complete, verify the server state changes to **Ready**.
3. Initiate the Server Upgrade
   a. From the Upgrade Administration screen, select the server to be upgraded.
   b. Click **Upgrade Server**.

      The Initiate Upgrade form appears.
4. Select Upgrade ISO
   a. Initiate the server upgrade. 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.
      > 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.

   b. Click **OK**.

      The upgrade begins and control returns to the Upgrade Administration screen.

      > **Note**
      >
      > Do not omit this step.

   c. 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. View the Upgrade Administration Form to Monitor Upgrade Progress

   a. Observe the upgrade status of the site on the Upgrade Administration screen by selecting the Entire Site link. An upgrade status summary of each server group in the site displays in the Server Upgrade States column.

      Servers may have a combination of the following expected alarms. However, 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 tTo Parent Failure)

      Alarm ID = 31107 (DB Merge fFrom Child Failure)

      Alarm ID = 31233 (HA Secondary Path Down)

      Alarm ID = 31101 (DB Replication tTo 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)

   b. Wait for the upgrade to complete. The Status Message column displays Success. This step takes approximately 20 to 50 minutes.

> **Note**
>
> - In the unlikely event that after the upgrade, if the Upgrade State of server is Backout Ready or Failed and the Status Message displays Server could not restart the application to complete the upgrade, then perform the stepms mentioned in Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade.
> - Perform Create a Link for ComAgent to create a link of Comagent. If the upgrade fails, do not proceed. It is recommended to consult with Create a Link for ComAgent on the best course of action. Refer to Recover from a Failed Upgrade for failed server recovery procedures.
>   See Server CLI: (Optional) View in progress status from command line of server section for an optional method of monitoring upgrade progress.
>   See Server CLI: If the upgrade fails section for instructions if the upgrade fails.

6. View In Progress Status from Command Line of Server in Server CLI

> **Note**
>
> This is an optional method to view the 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@DsrDemoUpg-DNO00 ~]$ appRev
Install Time: Tue Oct 10 04:01:33 2023
Product Name: DSR
Product Release: 9.0.2.0.0_98.15.0
Base Distro Product: TPD
Base Distro Release: 8.6.0.2.0_110.14.0
Base Distro ISO: TPD.install-8.6.0.2.0_110.14.0-OracleLinux8.6-x86_64.iso
ISO name: DSR-9.0.2.0.0_98.15.0-x86_64.iso
OS: OracleLinux 8.6
```

> **Note**
>
> If the upgrade fails, do not proceed. It is recommended to consult with on the best course of action. Refer to Recover from a Failed Upgrade for failed server recovery procedures.

7. If the upgrade of a server fails, access the server command line (through 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
   ```

   > **Note**
   >
   > It is recommended to contact My Oracle Support by referring to Create a Link for ComAgent of this document and provide these files. Refer to Recover from a Failed Upgrade for failed server recovery procedures.

8. Verify post upgrade status using active NOAM VIP.
   a. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.

b. Select the tab of the NOAM or site being upgraded.

c. Verify the Application Version value for this server has been updated to the target software release version.

d. Verify the Upgrade State of the upgraded server is Accept or Reject.

9. Verify if the Server was Successfully Upgraded

   Navigate to **Alarm & Events**, then **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.

6.5 Upgrade Multiple Servers – Upgrade Administration

The procedures in this section upgrade 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 D to mark up or keep another form of written record of the steps performed.
> - If the upgrade is required from 8.x VM to 9.0.2, refer to Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible section.

1. View Preupgrade Status of the Servers

   Repeat the steps listed in Active NOAM VIP: View Preupgrade Status of the Servers.

2. Verify status of servers to be upgraded

   Repeat the steps listed in Active NOAM VIP: Verify Status of Servers to be Upgraded.

3. 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.

- 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
   a. To upgrade multiple servers in parallel using the manual option, perform Active NOAM VIP: Initiate upgrade (part 1) and Active NOAM VIP: Initiate upgrade (part 2).
   b. To upgrade a server group using the Automated Server Group Upgrade option, proceed to Active NOAM VIP: Initiate (part 1) – Automated Server Group Upgrade option.
5. Initiate Upgrade (Part 1)
   a. From the Upgrade Administration screen, select the servers to upgrade.
   b. Click Upgrade Server

   The Initiate Upgrade form displays on the **Administration**, then **Software Management**, and then **Upgrade Initiate** screen.
6. Initiate Upgrade (Part 2) – Select ISO Form
   a. From the Upgrade Settings – Upgrade ISO options, select the ISO to use in the server upgrade.
   b. Click **OK**

      The upgrade begins and control returns to the Upgrade Administration screen.
   c. Proceed to Active NOAM VIP: Initiate (part 2) – Automated Server Group Upgrade procedure to complete this procedure.
7. Initiate Part 1 – Automated Server Group Upgrade Option
   a. To utilize the Automated Server Group upgrade option, verify no servers in the server group are selected.
   b. Click **Auto Upgrade**.
8. Initiate Part 2 – Automated Server Group Upgrade
   a. 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.

b. Select the appropriate ISO from the **Upgrade ISO** options.

c. Click **OK** to start the upgrade.

9. View the Upgrade Administration Form to Monitor Upgrade Progress.

   Repeat the steps mentioned in Active NOAM VIP: View the Upgrade Administration Form to Monitor Upgrade Progress

> **Note**
>
> See Server CLI: (Optional) View in-progress status from command line procedure for an optional method of monitoring upgrade progress.
> See Server CLI: If upgrade fails procedure for instructions if the Upgrade fails, or if execution time exceeds 60 minutes.

10. View In-Progress Status from Command Line

    Repeat the Server CLI: View In-Progress Status from Command Line procedure.

11. If Upgrade Fails

    Repeat the Server CLI: If Upgrade Fails procedure.

12. Verify Post-Upgrade Status

    Repeat the Active NOAM VIP: Verify Post-Upgrade Status procedure.

13. Verify the Upgrade

    Repeat the Verify the Upgrade procedure.

6.6 Manual Completion of Server Upgrade

This procedure provides the details about manual completion of server upgrade.

In the unlikely event that after the upgrade, if the Upgrade State of server is Backout Ready and the Status Message displays Server could not restart the application to complete the upgrade, then perform this procedure to restore the server to full operational status and return to this step to continue the upgrade. Perform the steps in Create a Link for ComAgent.

NOAMP VIP GUI: Log in to the Server (If Not Already Done)

1. Establish a GUI session on the NOAM server using the VIP IP address of the NOAM server. Open the web browser and enter the following URL:

   `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in to the NOAM GUI as the guiadmin user.

NOAMP VIP GUI: Verify Server Status

1. Navigate to **Status and Manage**, then **HA**.
2. Locate the server you want to upgrade.
3. Verify the Max Allowed HA Role is Standby.
4. Click **Edit**.

NOAMP VIP GUI: Change the Role

1. Change the Max Allowed HA Role to Active.
2. Click **OK**.

NOAMP VIP GUI: Verify Change

- Verify the **Max Allowed HA Role** changes to **Active**.

NOAMP VIP GUI: Restart the Server

1. Navigate to **Status & Manage**, then **Server**.
2. Select the server to be upgraded.
3. Click **Restart**.

   After a few minutes, the Appl State changes to **Enabled**.

NOAMP VIP GUI: Verify Status

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
2. Verify the Upgrade State changes to **Accept** or **Reject** and the Status Message changes to **Success: Server manually completed**.

6.7 Site Post-Upgrade Procedures

You need to perform the post-upgrade procedures after all 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.

> **Note**
>
> Allow Site Provisioning and Site Post-Upgrade Health Check procedures must be executed at the completion of each SOAM site upgrade.
> After all SOAM sites in the topology have completed upgrade, the upgrade may be accepted using the Accept Upgrade procedure.

6.7.1 Allow Site Provisioning

This procedure enables Site Provisioning for SOAM and MP servers. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

Active SOAM VIP: Enable Site Provisioning

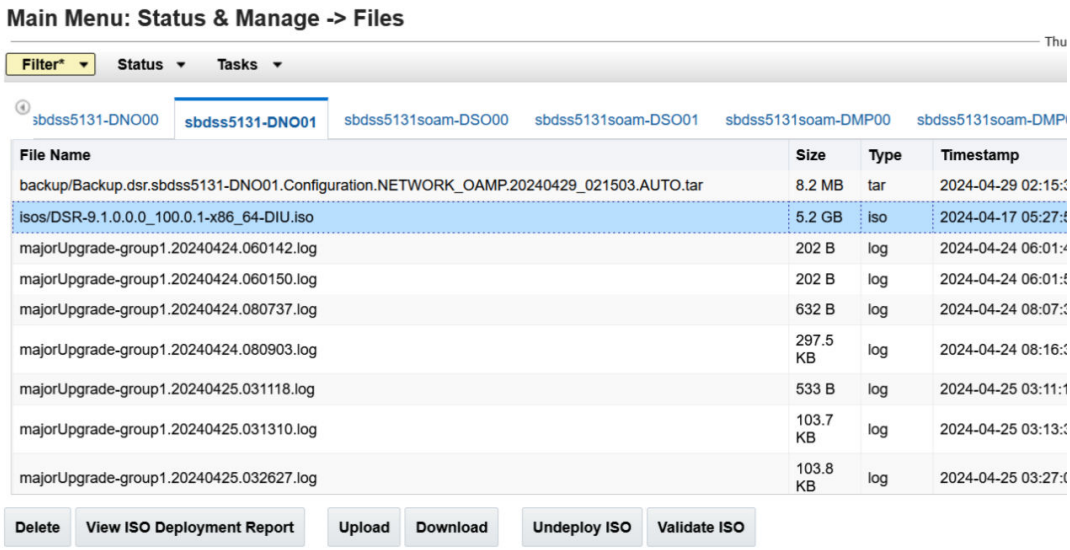
1. Log in to the SOAM GUI of the site just upgraded using the VIP.
2. Navigate to **Status & Manage**, then **Database**.
3. Click **Enable Site Provisioning**.
4. Confirm the operation by clicking **OK** on the screen.
5. Verify the button text changes to **Disable Site Provisioning**.

6.7.2 Undeploy the ISO from Active NOAM

To upgrade the servers, deployment of ISO is required, after the successful upgrade of all the servers you can undeploy the ISO by performing the following procedure:

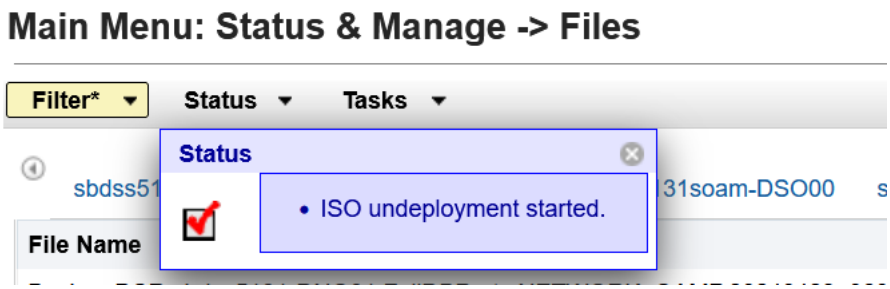
1. Log in to **Active NOAM** using your login credentials.
2. From the **Main Menu**, click **Status and Manage**, and then click **Files**.
3. From the **Active NOAM** tab, select the target release **DSR ISO** which is located in the `/isos` folder.

Figure 6-1 Undeploy ISO



4. Click **Undeploy ISO**.

Figure 6-2 ISO Undeployment



6.7.3 Post-Upgrade Health Checks

This section provides procedures to verify the validity and health of the site upgrade. It consists of the procedures that determine the validity of the upgrade as well as the health and status of the network and servers. If the 10054 - Device Deployment Failed alarm displays after the upgrade for any server, refer to Appendix S Workaround to Resolve Device Deployment Failed Alarm corrective steps.

> **Note**
>
> If syscheck fails on any server during preupgrade checks or in early checks stating that cpu: FAILURE: No record in alarm table for FAILURE!, see Workaround to Resolve syscheck Error for CPU Failure procedure.

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.

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.

Active NOAM VIP: Analyze Health Check Results

Follow this procedure to 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**, then **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.

> **Note**
>
> 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.
> If the health check log contains the Unable to Execute Health Check on <Active NOAM hostname> message, perform the health checks in Alternate SOAM Post-Upgrade Health Check procedure.

Active SOAM VIP: Export and Archive the Diameter Configuration Data

1. Navigate to **Diameter Common**, then **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**, then **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**, then **Maintenance**, and then **Applications**.
6. Verify Operational Status is Available for all applications.

Active SOAM Server: Verify if the Setup has an Apache Certificate

Check if the setup has a customer supplied Apache certificate installed and is protected with a passphrase, which was renamed before starting with upgrade.

- If the setup has a customer-supplied Apache certificate installed and is protected with passphrase before the start of the upgrade. Refer to Verification of Configuration Data procedure and rename the certificate back to the original name.

Active SOAM Server: Compare Health Check Data to PRe-Upgrade Health Check Data

Verify that the health check status of the upgraded site is the same as the preupgrade health checks taken in Preupgrade Health Checks section. If system operation is degraded, it is recommended to contact My Oracle Support (MOS).

6.7.3.1 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 Post-Upgrade Procedures section.

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 Logins, Passwords, and Server IP Addresses section.

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.

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. The FIPS integrity verification test failed message may display when the upgradeHealthCheck command runs. This message can be ignored.

Active SOAM CLI: View DA-MP Status

1. Enter the following command:

   ```
   $ upgradeHealthCheck daMpStatus
   ```

   This command outputs the status on 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.

Compare Data to the Pre-Upgrade Health Check

Compare data to the pre-upgrade health check to verify if the system has degraded after the second maintenance window.

- 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 Pre-Upgrade Health Checks section 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 in Site Pre-Upgrade Activities section must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.

6.7.4 Post-Upgrade Procedures

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

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 9.0.2.0.0 and later releases. See *Release Notes* section for more details.

1. Navigate to **Diameter**, then **Maintenance**, and then **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.

6.7.5 Diameter Custom Applications Post Upgrade Tasks

After upgrading all the sites, upgrade the DCA applications to ensure that the code of DCA applications is up-to-date with the DSR release.

DSA, RSA, SoR, and ZBA are few of the DCA applications. For more information about upgrading DSA, RSA, SoR, and ZBA refer to the following guides:

- For DSA, see *Oracle Communications Diameter Signaling Router Diameter Security Application User Guide with UDR*.
- For RSA, see *Oracle Communications Diameter Signaling Router Rx ShUDR Application User's Guide*.
- For SoR, see *Oracle Communications Diameter Signaling Router Roaming Steering Guide*.
- For ZBA, see *Oracle Communications Diameter Signaling Router Zero Balance Application User's Guide*.

7

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 and Normal Backout.

The emergency backout overview procedures back out the target release software in the fastest possible manner, without regard to traffic impact. The normal backout overview 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 the following tables are only estimates as the reason to run 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.
> - Backout is not supported if the upgrade was performed from 8.x to 9.x release.

Table 7-1 Emergency and Normal Backout Procedure Overview

Procedure	Elapsed Time (This Step)	Elapsed Time (Cum.)	Procedure Title	Impact
Backout Health Check	0:10-0:30	0:10-0:30	Backout Health Check The reason to run 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
Disable Global Provisioning	0:01	0:11-0:31	Disable Global Provisioning	Disables global provisioning

Table 7-1 (Cont.) Emergency and Normal Backout Procedure Overview

Procedure	Elapsed Time (This Step)	Elapsed Time (Cum.)	Procedure Title	Impact
Emergency Site Backout	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.
Backout Multiple Servers	See Note	See Note	Backout 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.
Emergency NOAM Backout	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.
Post-Backout Health Check	0:01-0:05	Varies	Post-Backout Health Check	None

7.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to My Oracle Support (MOS) before executing any of these procedures. Run this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.

> ⚠ **Caution**
>
> Before attempting to perform these backout procedures, it is recommended to first contact My Oracle Support (MOS). Backout procedures cause traffic loss.

> ⓘ **Note**
>
> These recovery procedures are provided for the backout of an Upgrade only (i.e., from a failed 9.2.0.0.0 release to the previously installer release). Backout of an initial installation is not supported.

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

Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)

Alarm ID = 31109 (Topology config error)

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

Alarm ID = 31106 (DB Merge tTo Parent Failure)

Alarm ID = 31134 (DB replication to slave failure)

Alarm ID = 31102 (DB replication from master failure)

Alarm ID = 31282 (HA management fault)

7.2 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.

Active NOAM VIP: Run the Automated Post-upgrade Health Checks for Backout

Use this procedure to perform a Health Check on the site prior to backing out the upgrade.

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
2. Select the SOAM tab of the site being backed out.
3. Select the SOAM server group link for the site being backed out.
4. Select the active SOAM.
5. Click **Checkup**.

6. Under Health check options, click **Post Upgrade.**
7. Click **OK**.

   Control returns to the Upgrade screen.

Active NOAM VIP: Monitor Health Check Progress for Completion

This procedure details the steps to monitor the rogress of health check .

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.

Active NOAM VIP: Analyze Health Check Results

Follow the steps in this procedure to 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**, then **Files**.
2. Select the active NOAM tab.
3. Select the UpgradeHealthCheck.log file and click **View**.
4. Locate the log entries for the most recent health check.

Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance.

Active NOAM VIP: Identify IP Addresses of Servers to be Backed Out

1. Navigate to **Administration**, then **Software Management** , and then **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**, then **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 run 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.

Active NOAM VIP: Verify Backup Archive Files

1. Navigate to **Status & Manage**, then **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 3.4.4, 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`

Active NOAM CLI: Verify Disk Usage

This procedure lists the steps to verify the disk usage.

Starting with the active NOAM, log in to 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 NOAM.`ssh admusr@<server IP>`

   `password: <enter password>`
   Answer yes if you are asked to confirm the identity of the server.

2. Enter the command:`[admusr@EVO-NO-1 ~]$ df`

   Sample output (abridged):

   ```
   Filesystem 1K-blocks Used Available Use% Mounted on /dev/mapper/
   vgroot-plat_root 999320 294772 652120 32% / tmpfs 12303460 0
   12303460 0% /dev/shm /dev/vda1 245679 41967 190605 19% /boot /dev/
   mapper/vgroot-plat_tmp 999320 1548 945344 1% /tmp /dev/mapper/
   vgroot-plat_usr 5029504 2962552 1804824 63% /usr /dev/mapper/
   vgroot-plat_var 999320 558260 388632 59% /var /dev/mapper/vgroot-
   plat_var_tklc 3997376 2917284 870380 78% /var/TKLC
   ```

3. Observe the line for the /var and /usr partition. If the Use% column is 70% or less, this procedure is complete. Continue with the back out per Table 22 (Emergency) or Table 23 (Normal).

   If the Use% of the /var and /usr partition is at 70% or greater, search the partition for files that can be safely deleted. Use extreme caution in selecting files to be deleted. The deletion of critical system files could severely impair the DSR functionality.

4. Repeat this step for all servers to be backed out.

7.3 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.

Active NOAM VIP: Disable global provisioning and configuration updates on the entire network

This procedure lists the steps to disable global provisioning and configuration updates on the entire network.

1. Log in to the active NOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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)

7.4 Perform Emergency Backout

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 the 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..

7.4.1 Emergency Site Backout

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

> **Note**
>
> 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.

Active NOAM VIP: Identify all the servers that require backout (within a site)

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
3. Select the NOAM 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.

Active SOAM VIP: Disable site provisioning for the site to be backed out

1. Log in to the SOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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)

Backout all C-level Servers

For all configurations, backout all C-level servers (IPFEs, SBRs, SBRs, and DA-MPs) identified in Active NOAM VIP:

1. Identify all servers that require backout (within a site) procedure in this section and perform Backout Multiple Servers procedure.

   > **Note**
   >
   > This process results in a total loss of all traffic being processed by this DSR.

2. After all the servers in a particular server group are backed out, revert back the changes for the SBR server by performing the steps in Create a Link for ComAgent additional post backout steps.
3. Back out the standby and spare DSR SOAM servers: If standby and spare SOAM servers are present, perform Backout Multiple Servers procedure. If only a spare SOAM server is present, perform Backout Single Server procedure.
4. Perform Backout Single Server procedure to backout the active DSR SOAM server.

   After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s).

Active SOAM VIP: Enable site provisioning

1. Log in to the SOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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 Emergency Backout Procedure Overview section in another maintenance window.

7.4.2 Emergency NOAM Backout

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. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. Perform Backout Single Server procedure to:

- Back out the standby DR NOAM server (if equipped)
- Back out the active DR NOAM server (now the standby) (if equipped)
- Back out the standby DSR NOAM server (as applicable)
- Back out the active DSR NOAM server (now the standby)

2. After all the servers in a particular server group are backed out, revert back the changes for the NOAM server(s) by performing additional Post-Backout Steps.
3. **Active NOAM VIP:** Enable global provisioning and configuration updates on the entire network
   a. Log into the NOAM GUI using the VIP.
   b. Navigate to **Status & Manage**, then **Database**.
   c. Click **Enable Provisioning**.
   d. Verify the button text changes to **Disable Provisioning**.
4. **Active NOAM VIP:** Remove Ready state for any backed out server
   a. Navigate to **Status & Manage**, then **Servers**.
   b. If any backed-out server Application Status is Disabled, then navigate to the server row and click Restart.
   c. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
   d. 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.
   e. Click **OK**.

      This removes the Forced Standby designation for the backed-out server.

      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.
5. Verify the Application Version value for servers has been downgraded to the original release version.

7.5 Perform Normal Backout

Run the following procedures to perform a normal backout only when 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.

7.5.1 Normal Site Backout

The procedures in this section back out an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, IPFEs, and SBRs.

Active NOAM VIP: Identify all Servers That Require Backout (Within a Site)

Repeat the steps mentioned in Active NOAM VIP: Identify all servers that require backout (within a site) procedure in Emergency Site Backout.

Active SOAM VIP: Disable Site Provisioning for the Site to be Backed Out

Repeat the steps mentioned in Active SOAM VIP: Disable site provisioning for the site to be backed out procedure in Emergency Site Backout.

Back out First Set of C-level Servers

Follow these steps to backout the first set of C-level servers, as applicable.

- The following C-level servers can be backed out in parallel, as applicable:
  - ½ of all DA-MPs for N+0 (multi-active) configuration
  - Standby SBR(s)
  - Spare SBR(s)
  - ½ of all IPFEs

> **Note**
>
> Run Backout Single Server procedure for each standby/spare C-level server identified.
>
> In a PCA System, the spare SBR server is located at the mated site of the site being backed out.

Active NOAM VIP: Verify Standby SBR Server Status

If the server being backed out is the standby SBR, run this step. Otherwise, continue with Backout remaining C-level servers, as applicable procedure mentioned in this section.

1. Navigate to **SBR**, then **Maintenance**, and then **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**.

Active NOAM VIP: Verify Bulk Download is Complete

Perform this procedure to verify the bulk download is complete between the active SBR in the server group to the standby and spare SBRs.

1. Navigate to **Alarm & Event**, then **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.

Backout Remaining C-level Servers

Run Backout Single Server procedure to backout the remaining servers in parallel, as applicable:

- ½ of all DA-MPs for N+0 (multi-active) configuration
- Active SBR(s)
- ½ of all IPFEs
- Backout the standby DSR SOAM server
- Backout spare DSR SOAM server, if applicable
- Backout active DSR SOAM server

> **Note**
>
> After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s) by performing the steps in Create a Link for ComAgent.

Active SOAM VIP: Enable Site Provisioning

1. Log in to the SOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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 Emergency Table 7-1 in another maintenance window.

7.5.2 Normal NOAM Backout

This procedure is used to perform a normal backout of the DSR application software from the NOAM servers.

- Repeat steps 1 to 3 in Emergency NOAM Backout Emergency NOAM Backout procedure.

7.6 Backout Single Server

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

> **Note**
>
> This procedure is executed as a component of the Emergency Site Backoutor Normal Site Backout. This procedure should never be executed as a standalone procedure.

7.6.1 Active NOAM VIP: Prepare the Server for Backout

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
2. Select the NOAM 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.

> **Note**
>
> Make the server Backout Ready as follows:

5. To make the server backout ready, navigate to **Status & Manage,** then **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**
>
> 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 Q to have the NOAMP HA switchover.

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**, then **Server**.
12. Select the server to backout and click **Stop**.
13. Click **OK** to confirm the operation and verify the Appl State changes to **Disabled**.
14. Navigate to **Administration**, then **Software Management,** and then **Upgrade**.
15. Select the NOAM 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.

7.6.2 Server CLI: SSH to Server

- Use an SSH client to connect to the server (e.g., ssh, putty):

```
ssh admusr@<server address>
password: <enter password>
```

> **Note**
>
> If direct access to the IMI is not available, or if TVOE is installed on a blade, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

7.6.3 Server CLI: Execute the Backout

- Execute this command to find the state of the server to be backed out:

```
ha.mystate
sudo /var/TKLC/backout/diUpgrade --reject
```

> **Note**
>
> The reject command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.

> **Note**
>
> If back out asks to continue, answer y.

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

7.6.4 Server CLI: SSH to Server

1. Use an SSH client to connect to the server (e.g., ssh, putty):

   ```
   ssh admusr@<server address>
   ```

   password: <enter password>
2. Perform Create a Link for ComAgent.

7.6.5 Server CLI: Restore the Full DB Run Environment

1. After the restart check the file`/var/TKLC/appw/logs/Process/upgrade.log`, and wait till the following `postReject` is completed `grep -i "REJECT COMPLETE" /var/TKLC/appw/logs/Process/upgrade.log`.
2. Execute the backout_restore utility to restore the full database run environment:

   ```
   $ sudo /var/tmp/backout_restore
   ```
3. If asked to proceed, answer y.

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

7.6.6 Server CLI: Verify the Backout

1. Examine the output of the following command 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 errors occurred in the initial upgrade.

2. Disregard the following **TKLCplat.sh** error:

```
[root@NO1 ~]# verifyUpgrade

ERROR: TKLCplat.sh is required by upgrade.sh!

ERROR: Could not load shell library!

ERROR: LIB: /var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh
```

ERROR: RC: 1

Also, disregard this error:

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

ERROR: 1513202476::zip error: Nothing to do!

/usr/share/tomcat6/webapps/ohw.war

This command displays the current sw rev on the server:

```
$ appRev

Install Time: Wed Apr 4 05:03:13 2023

Product Name: DSR

Product Release: 9.0.2.1.0-99.16.0

Base Distro Product: TPD

Base Distro Release: 8.6.0.2.0_110.14.0

Base Distro ISO: TPD.install-8.6.0.2.0_110.14.0-OracleLinux8.6-
x86_64.iso

ISO name: DSR-9.0.2.1.0-99.16.0-x86_64.iso

OS: OracleLinux 8.6
```

3. Run the following command.

   ```
   $ sudo verifyBackout
   ```
   The verifyBackout command searches the upgrade log and report all errors found.
4. If the backout is successful (no errors or failures reported), then proceed to Server CLI: Reboot the Server procedure in this section.
5. 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>-9.0.2.1.0-99.16.0 : 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

   RCS_VERSION=1.12

   ERROR: Backing out changes from BACKOUT_SERVER on backwards...

   ERROR: Backout was unsuccessful!!!
   ```

```
ERROR: Trouble when running backout command!
ERROR: CMD: /var/TKLC/backout/ugwrap --backout
ERROR: Failed to reject upgrade.
Rebuilding RPM database. This may take a moment...
rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format
Cleaning up chroot environment...
Stopping remoteExec background process
Shutting down /var/TKLC/backout/remoteExec...
/usr/TKLC/plat/sbin/savelogs_plat logs:
1530516317::ERROR: TKLCdpi-8.0.33-8.0.1.0.0_80.28.0: Adding the DSR
helpset failed!
1530516320::error: %post(TKLCdpi-0:8.0.33-8.0.1.0.0_80.28.0.x86_64)
scriptlet failed, exit status 1
```

Examine the upgrade log at `/var/TKLC/log/upgrade/upgrade.log` for errors that occurred during the backout.

> **Note**
>
> If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) for further instructions.

7.6.7 Server CLI: Reboot the Server

Enter the following command to reboot the server:

```
$ sudo init 6
```

This step can take several minutes.

> **Note**
>
> If in case the following alarms are found, then delete core files from `/var/TKLC/core` directory and restart the server using above command:
>
> ```
> >database health impacted.
> >persistent database failure
> >writing the database to disk failed.
> > server core file detected.
> ```

7.6.8 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 systemctl status httpd.service
   ```

   The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):

   ```
   httpd <process IDs will be listed here> is running...
   ```

   If httpd is not running, repeat sub-steps 3 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further instructions.
4. Verify if the file id_rsa has required ownership:
   a. Check the ownership of the file:

      ```
      sudo ls –ltr /home/awadmin/.ssh/
      ```

      The file permission should be defined as shown:
   b. If the file ownership is not set for awadmin, then change the permission:

      ```
      sudo chown awadmin:awadm /home/awadmin/.ssh/id_rsa
      ```
   c. Verify file ownership is changed to awadmin awadm.

7.6.9 Active NOAM VIP: Verify Server State is Correct after Backout

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade** to observe the server upgrade status.
2. Select the SOAM tab of the site being backed out.
3. Select the link of the server group containing the server being backed out.

   If the server status is Not Ready, proceed to the next step; otherwise, proceed to Active NOAM VIP: Verify application version is correct for the backed out server procedure in this section.

7.6.10 Active NOAM VIP: Change/Correct the Upgrade State on Backed out Server to Ready

1. Navigate to **Status & Manage**, then **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**, then **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**, then **Software Management**, and then **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.

7.6.11 Active NOAM VIP: Verify Application Version is Correct for the Backed Out Server

1. Navigate to **Administration**, then **Software Management**, and then **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.

> **Note**
>
> To support backout for major upgrade paths on the NOAM, SOAM, and SBR server(s), follow the steps in Additional Backout Steps.

7.7 Backout Multiple Servers

This section provides the procedures to backout the application software on multiple servers. These procedures back out the upgrade of DSR 9.2.0.0.0 application software for multiple servers. Any server requiring a backout can be included, such as DA-MPs, IPFEs, and SBRs.

> **Note**
>
> This procedure is executed as a component of the Emergency Site Backout or Normal Site Backout. This procedure should never be executed as a standalone procedure.

7.7.1 Active NOAM VIP: Prepare the Server for Backout

Follow the steps listed in this procedure to prepare the server for backout.

- Repeat the steps listed in Active NOAM VIP: Prepare the Server for Backout section to complete this procedure.

7.7.2 Server CLI: Log in to the Server(s)

- Use an SSH client to connect to the server (for example, ssh, putty):

  ```
  ssh admusr@<server address>
  password: <enter password>
  ```

> **Note**
>
> If direct access to the IMI is not available, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.

7.7.3 Server CLI: Execute the Backout

1. Determine the state of the server to be backed out. The server role must be either **Standby** or **Spare**.
2. Run the following command to find the server role:

   ```
   $ ha.mystate
   ```

   In this example output, the HA state is **Standby**.

   ```
   [admusr@SO2 ~]$ ha.mystate
   resourceId role node subResources lastUpdate
   DbReplication Stby B2435.024 0 0127:113603.435
   VIP Stby B2435.024 0 0127:113603.438
   SbrBBaseRepl OOS B2435.024 0 0127:113601.918
   SbrBindingRes OOS B2435.024 0 0127:113601.918
   SbrSBaseRepl OOS B2435.024 0 0127:113601.918
   SbrSessionRes OOS B2435.024 0 0127:113601.918
   CacdProcessRes OOS B2435.024 0 0127:113601.918
   DA_MP_Leader OOS B2435.024 0 0127:113601.917
   DSR_SLDB OOS B2435.024 0-63 0127:113601.917
   VIP_DA_MP OOS B2435.024 0-63 0127:113601.917
   EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917
   DSR_Process OOS B2435.024 0-63 0127:113601.917
   CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272
   DSROAM_Proc OOS B2435.024 0 0128:081123.951
   ```

   If the state of the server is Active, then return to Active NOAM VIP: Prepare the server for backout. Run the reject command to initiate the backout:

> **Note**
>
> Many informational messages display to the terminal screen as the backout proceeds. After backout is complete, the server automatically reboots.

7.7.4 Server CLI: Restore the Full DB Run Environment

Follow this procedure to restore the full DB run environment.

- Repeat the steps listed in Server CLI: Restore the Full DB Run Environment.

7.7.5 Server CLI: Verify the Backout

Follow this procedure to verify backout has been carried out.

- Repeat the steps listed in Server CLI: Verify the Backout.

7.7.6 Server CLI: Reboot the Server

Enter the following command to reboot the server:

```
$ sudo init 6
```

This step can take several minutes.

> **Note**
>
> If in case the following alarms are found, then delete core files from `/var/TKLC/core` directory and restart the server using above command:
>
> ```
> >database health impacted.
> >persistent database failure
> >writing the database to disk failed.
> > server core file detected.
> ```

7.7.7 Server CLI: Verify OAM Services Restart (NOAM/SOAM Only)

- Repeat the steps listed in Server CLI: Verify OAM Services Restart (NOAM/SOAM Only)

> **Note**
>
> To support backout for incremental upgrade paths, run Appendix K (Additional Backout Steps).

7.7.8 Active NOAM VIP: Verify Server State is Correct after Backout

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade** to observe the server upgrade status.
2. If the active NOAM server status is **Not Ready**, proceed to the next step; otherwise, proceed to Active NOAM VIP: Verify application version is correct for the backed out server procedure.

7.7.9 Active NOAM VIP: Change/Correct the Upgrade State on Backed Out Server to Ready

1. Repeat steps 1 to 12 from Active NOAM VIP: Change/Correct the Upgrade State on Backed Out Server to Ready.

2. Proceed to Active NOAM VIP: Verify application version is correct for the backed out server procedure to complete this procedure.

7.7.10 Active NOAM VIP: Remove Upgrade Ready Status

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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.

7.7.11 Active NOAM VIP: Correct Upgrade Status on the Backed Out Server

Correct the upgrade status on the backed out server.

1. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
2. If the servers just backed out show an Upgrade State of **Ready** or **Success**, then select the backed-out server and click **Complete**. If the servers just backed out show Upgrade State of **Not Ready**, then proceed to the next step.
3. Leave the Action set to the default value of **Complete** on the Upgrade Complete screen.
4. Click **OK**. This updates the Max Allowed HA Role of the backed-out server to active, which causes the server's Upgrade State to change to **Not Ready**.

> **Note**
>
> 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.

7.7.12 Active NOAM VIP: Verify Application Version is Correct for the Backed Out Server

1. Navigate to **Administration**, then **Software Management**, and then **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.

> **Note**
>
> To support backout for incremental upgrade paths on the NOAM, SOAM, and SBR server(s), follow the steps in Additional Backout Steps.

7.8 Additional Backout Steps

This procedure provides the details about additional backout steps for NOAM, SOAM, and SBR server(s) to support backout for incremental upgrade release paths.

Server CLI: Log in to the Server

- Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to the server under backout:

  ```
  ssh admusr@<server address>
  ```

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

  Answer yes if you are asked to confirm the identity of the server.

  If the server is NOAM or SOAM server, run tasks 2 to 5 in this procedure and if server is SBR server, run tasks 6. to 7. Please note down the host name of the server on which these steps are executed. Once all the servers in a server group will be backed out then the additional post-backout steps will be executed to revert back the changes done in this procedure.

Server CLI: Set the Resource as Optional for OAM Servers Only

1. Check for the resource:

   ```
   iqt -E HaResourceCfg where "name='<resource_name>'"
   ```

2. Run this command:

   ```
   iset -W -foptional='Yes' HaResourceCfg where "name='DSROAM_Proc'"
   ```

   These commands change/update the results of some records.

> **Note**
>
> Make sure the resource being set is in system. Some of the resources shown are introduced in different releases. If the resource is not in the system, presence check will not result any output records. In this case, skip updating these fields for the resource not in the system.

Server CLI: Restart the HTTPD Service (For OAM Servers Only)

- Run this command:

  ```
  sudo systemctl restart httpd.service
  ```

Active NOAM/SOAM Server CLI: Log in to the Server

- Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to the Active NOAM/SOAM server in the same server group, in which server is under backout:

  ```
  ssh admusr@<server address>
  ```

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

Answer yes if you are asked to confirm the identity of the server.

Server CLI: Verify that the Replication is Working Appropriately (For OAM Servers Only)

1. Run this command on an active NOAM/SOAM server in the same server group being backed out:

   ```
   irepstat
   ```

2. Verify the irepstat command displays a replication row for the server which is being backed out.

   Note the replication status is Active before proceeding. If it is Audit, then wait until replication becomes Active.

   If this step is missed, data is lost and is unrecoverable.

   Example:

   Here Ford-B-NO is Active NOAM Server and Ford-A-NO is backed out.

   ```
   Ford-B-NO A3301.157 Ford-B-NO 09:32:17 [Rw]

   Policy 0 ActStb [DbReplication]
   ---------------------------------------

   AA To P0 Ford-A-NO Active 0 0.00 1%R 0.12%cpu 1.88k/s

   AA To P1 Chevy-DRNO-B Active 0 0.00 1%R 0.08%cpu 1.89k/s

   AB To D0 Camaro-SO-B Active 0 0.00 1%R 0.09%cpu 1.89k/s

   AB To D0 Nova-SO-B Active 0 0.00 1%R 0.08%cpu 1.90k/s

   AB To D0 Pinto-SO-B Active 0 0.00 1%R 0.10%cpu 1.89k/s

   AB To D0 Mustang-SO-B Active 0 0.00 1%R 0.10%cpu 2.14k/s
   ```

3. Press q if you want to exit the irepstat command output.
4. Run `irepstat` again, if required.

Server CLI: Set the Resource as Optional (For SBR Servers Only)

- If a resource is not in the system, presence check does not result in any output records. In this case, do not update the fields for the resource.

  Resource presence can be checked using:

  ```
  iqt -E HaResourceCfg where "name='<resource_name>'"
  ```

  For example:

  ```
  iqt -E HaClusterResourceCfg where "resource='uSbrRes'"
  ```

  Run this command for Session SBR only:

  ```
  iset -W -foptional='Yes' HaResourceCfg where "name='pSbrSBaseRepl'"

  iset -W -foptional='Yes' HaClusterResourceCfg where
  "resource='uSbrRes'"

  iset -W -foptional='Yes' HaClusterResourceCfg where
  "resource='pSbrSessionRes'"
  ```

Run this command for Binding SBR only:

```
iset -W -foptional='Yes' HaResourceCfg where "name='pSbrBBaseRepl'"
```

```
iset -W -foptional='Yes' HaClusterResourceCfg where
"resource='uSbrRes'"
```

```
iset -W -foptional='Yes' HaResourceCfg where
"name='pSbrBindingRes'"
```

These commands change/update the results of some records.

> **Note**
>
> Make sure the resource being set is in the system. Some of the resources listed below are introduced in different releases.

Server CLI: Verify that the Replication is Working Appropriately (For SBR Servers Only)

1. Run this command on an active SBR server in the same server group as the server being backed out:

   ```
   irepstat
   ```

2. Verify the irepstat command displays a replication row for the server which is being backed out.

   Note the replication status is Active before proceeding, if it is Audit, then wait until replication becomes Active.

   If this step is missed, data is lost and is unrecoverable.

   Example:

   Here Pinto-SBR-2 is Active SBR Server and Pinto-SBR-1 is backed out.

   Also, on Binding SBR, resource will be pSbrBindingPolicy.

   And on Session SBR, resource will be pSbrSessionPolicy.

   ```
   Pinto-SBR-2 C3783.034 Pinto-SBR-2 13:39:38 [Rw]

   Policy 0 ActStb [DbReplication]
   ---------------------------------------

   BC From D0 Pinto-SO-B Active 0 0.10 ^0.10%cpu 67.0/s

   CC To P0 Pinto-SBR-1 Active 0 0.10 1%S 0.31%cpu 30.9/s

   CC To P1 Mustang-SBR-3 Active 0 0.10 1%S 0.28%cpu 39.6/s

   Policy 21 pSbrBindingPolicy [pSbrBBaseRepl]
   ---------------------------

   CC To P0 Pinto-SBR-1 Active 0 0.10 1%S 0.63%cpu 186k/s

   CC To P1 Mustang-SBR-3 Active 2 0.13 1%S 0.55%cpu 189k/s
   ```

3. Press q if you want to exit the irepstat command output.
4. Run `irepstat` again, if required.

7.9 Additional Post-Backout Steps

This procedure provides the details about additional post-backout steps for NOAM, SOAM, and SBR server(s) to support backout for incremental upgrade release paths.

Server CLI: Log in to the Server (If Not Already Done)

- Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout:

  ```
  ssh admusr@<server address>
  ```

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

  Answer **yes** if you are asked to confirm the identity of the server.

  If the server is an NOAM or SOAM server, run step 2.

  If the server is an SBR server, run steps 3.

  > **Note**
  >
  > The host name of the server on which these steps are executed. Once all servers in a server group are backed out, additional post-backout steps are executed to revert the changes done in this procedure. Run the following commands on servers where the services are in pending state:

  Run the following commands on servers where the services are in pending state:

  ```
  rm –rf /etc/ld.so.cache
  ```

  ```
  echo "/usr/TKLC/dsr/lib" | sudo tee -a /etc/ld.so.conf.d/dsr.conf
  ```

  ```
  sudo cat /etc/ld.so.conf.d/dsr.conf
  ```

  ```
  sudo ldconfig
  ```

  Check for configured libraries, for example:

  ```
  sudo ldconfig -p | grep -i pdra
  ```

  Output must have the following information:

  ```
  libPdraTraps.so (libc6,x86-64) => /usr/TKLC/dsr/lib/libPdraTraps.so
  ```

  Check whether all the services are up:

  ```
  pl
  ```

Server CLI: Set the Resource as Optional (For OAM Servers Only)

- Repeat the steps listed in Server CLI: Set the Resource as Optional (For OAM Servers Only) .

Server CLI: Set the Resource as Optional (For SBR Servers Only)

- Repeat the steps listed in Server CLI: Set the Resource as Optional (For SBR Servers Only).

7.10 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.

Active NOAM VIP: Verify Server Status is Normal

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Status & Manage**, then **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 Critical and Major Alarms Analysis 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.

Active NOAM VIP: Log All Current Alarms in the System

1. Navigate to **Alarms & Events**, then **View Active**.
2. Click Report to generate an Alarms report.
3. Save the report and print the report. Keep these copies for future reference.

8
Critical and Major Alarms Analysis

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

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

1. Log/View all current alarms at the NOAM
   a. Navigate to **Alarms & Events**, then **View Active**.
   b. Click **Report** to generate an Alarms report.
   c. Save the report and/or print the report.
2. Analyze the Active Alarms Data

   Refer to the Table 8-1 and Table 8-2 for the list of alarms.

   > **Note**
   >
   > If any alarms listed in the Table 8-1 and Table 8-2 displays in the system, resolve the alarms before starting the upgrade.

   Refer to *DSR Alarms and KPIs Reference* for specific alarm in-depth details.

   Following are the two categories of alarms.

   - **High impact alarms**
     It's almost certain that 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 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 8-1 High Impact Alarms

Alarm ID	Name
5010	Unknown Linux iptables command error
5011	System or platform error prohibiting operation
10000	Incompatible database version
10134	Server Upgrade Failed
10200	Remote database initialization in progress
19217	Node isolated - all links down
19805	Communication Agent Failed to Align Connection
19855	Communication Agent Resource Has Multiple Actives
19901	CFG-DB Validation Error
19902	CFG-DB Update Failure
19903	CFG-DB post-update Error
19904	CFG-DB post-update Failure
22223	MpMemCongested
22950	Connection Status Inconsistency Exists
22961	Insufficient Memory for Feature Set
22733	SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration
22734	Policy and Charging Unexpected Stack Event Version
25500	No DA-MP Leader Detected
25510	Multiple DA-MP Leader Detected
31101	Database replication to slave failure
31116	Excessive shared memory
31117	Low disk free
31125	Database durability degraded
31128	ADIC Found Error
31133	DB Replication Switchover Exceeds Threshold
31215	Process resources exceeded
31288	HA Site Configuration Error
32100	Breaker Panel Feed Unavailable
32101	Breaker Panel Breaker Failure
32102	Breaker Panel Monitoring Failure
32103	Power Feed Unavailable
32104	Power Supply 1 Failure
32105	Power Supply 2 Failure
32106	Power Supply 3 Failure
32107	Raid Feed Unavailable
32108	Raid Power 1 Failure
32109	Raid Power 2 Failure
32110	Raid Power 3 Failure
32111	Device Failure
32112	Device Interface Failure
32113	Uncorrectable ECC memory error
32114	SNMP get failure
32115	TPD NTP Daemon Not Synchronized Failure
32116	TPD Server's Time Has Gone Backwards

Table 8-1 (Cont.) High Impact Alarms

Alarm ID	Name
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
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

Table 8-1 (Cont.) High Impact Alarms

Alarm ID	Name
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
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

Table 8-1 (Cont.) High Impact Alarms

Alarm ID	Name
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 8-2 Medium Impact Alarms

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

Table 8-2 (Cont.) Medium Impact Alarms

Alarm ID	Name
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
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

Table 8-2 (Cont.) Medium Impact Alarms

Alarm ID	Name
8202	RclItrPoolCongested
8203	RclTxTaskQueueCongested
8204	RclEtrPoolCongested
22016	Peer Node Alarm Aggregation Threshold
22017	Route List Alarm Aggregation Threshold
22056	Connection Admin State Inconsistency Exists
22200	MpCpuCongested
22201	MpRxAllRate
22202	MpDiamMsgPoolCongested
22203	PTR Buffer Pool Utilization
22204	Request Message Queue Utilization
22205	Answer Message Queue Utilization
22206	Reroute Queue Utilization
22207	DclTxTaskQueueCongested
22208	DclTxConnQueueCongested
22214	Message Copy Queue Utilization
22221	Routing MPS Rate
22222	Long Timeout PTR Buffer Pool Utilization
22349	IPFE Conneetion Alarm Aggregation Threshold
22350	Fixed Connection Alarm Aggregation Threshold
22407	Routing attempt failed duto internal database inconsistency failure
22500	DSR Application Unavailable
22501	DSR Application Degraded
22502	DSR Application Request Message Queue Utilization
22503	DSR Application Answer Message Queue Utilization
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

Table 8-2 (Cont.) Medium Impact Alarms

Alarm ID	Name
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
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

Table 8-2 (Cont.) Medium Impact Alarms

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

9 Workarounds

9.1 Workaround to Resolve DB Site Replication Alarms

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

1. Server CLI: Log in to the server.
   - Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to the active NOAM:

     ```
     ssh admusr@<server address>
     ```

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

     Answer **yes** if you are asked to confirm the identity of the server.
2. Server CLI: Check if the replication links are up.
   - Run this command:

     ```
     irepstat
     ```

     Some of the B-C and C-C replications links may be down.
3. Server CLI: Resolve replication issue
   - Run this command:

     ```
     sudo pm.kill inetrep
     ```

> **Note**
>
> Repeat this procedure on each affected server.

9.2 Workaround to Resolve Device Deployment Failed Alarm

This procedure resolves the device deployment failed alarm i.e. 10054. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

NOAMP VIP GUI: Log In

1. Open the web browser and enter the following URL:

   ```
   http://<Primary_NOAM_VIP_IP_Address>
   ```
2. Log in to the NOAM GUI as the guiadmin user.

NOAMP VIP GUI: Identify Server(s) and Interface(s) with Alarm

Navigate to current alarm details and identify the server and interface where the **10054 - Device Deployment Failed** alarm is displayed.

1. Navigate to **Alarms & Events**, then **View Active**.
2. Look for the 10054 alarm and make a list of the server(s) and interface(s).

NOAMP VIP GUI: Corrective Action for Alarm 10054

Interfaces like XMI and IMI are in locked state and do not allow editing as a corrective action. For XMI and IMI interfaces, first unlock the interface and for other interfaces skip steps 1 to 4 below.

1. Navigate to **Configuration**, then **Networking**, and then **Networks**, select the respective "Network element" tab used for the server configuration.
2. Click the Network Name row.
3. Click **Unlock**. Click the checkbox to confirm it and click **OK**.
4. To unlock the network for the particular device, navigate to **Configuration**, then **Networking**, and then **Devices**.
5. Click the Server tab from the list in task 2 in this procedure.
6. Select each interface row one by one for which alarm is showing and click **Edit**.
7. Click **OK**.

> **Note**
>
> Give some time to the system to auto correct the condition to clear the alarm. Once this step is done, lock the network back again which were unlocked above.

For XMI and IMI interfaces, lock the interface back, for other interfaces skip 1 to 4 below.

8. To lock the network for a specific device, navigate to **Configuration**, then **Networking**, and then **Networks**, select the respective Network element tab used for the server configuration.
9. Click the **Network Name** row.
10. Click **Lock**. Click the checkbox to confirm it and click **OK**.

9.3 Workaround to Resolve syscheck Error for CPU Failure

This procedure details the workaround to resolve syscheck error for CPU failure.

Log in to the server using CLI on which syscheck is failing

- Use the SSH command (on UNIX systems – or putty if running on windows) to log in to the server identified:

  ```
  ssh admusr@<SERVER_XMI>
  ```

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

Answer yes if you are asked to confirm the identity of the server.

Server CLI: Execute Workaround

1. Edit the cpu config file.

   ```
   $ sudo vim /usr/TKLC/plat/lib/Syscheck/modules/system/cpu/config
   ```

2. Comment out the all the text that reads: EXPECTED_CPUS= by putting # at the beginning of the line, for example:

   ```
   # EXPECTED_CPUS=2
   ```

3. Save the cpu config file.
4. Reconfig the syscheck by running these commands:

   ```
   sudo syscheck --unconfig
   sudo syscheck --reconfig
   sudo syscheck
   CPU related errors do not display.
   ```

9.4 Workaround to Resolve the Server HA Switchover Issue

The following procedure resolves the HA switchover issue. It restarts the cmha process on the server that has HA switchover issue.

1. Server CLI: Log in to the server.
   - Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to 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).
   - Run this command:

     ```
     sudo pm.kill cmha
     ```
3. Repeat this procedure on each affected server.

9.5 Workaround for Errors During Dual Image Upgrade

Fatal Errors

During any fatal errors the server will not be recoverable and must be rebuilt. Rebuild the server with the same DSR release of its mate server.

Failures

During typical failures the system can be recovered by running the following commands and then restart the server.

```
/var/TKLC/backout/diUpgrade --clearError
```

```
sudo /usr/TKLC/appworks/sbin/backout_restore
```

```
sudo init 6
```

Early Check Failure

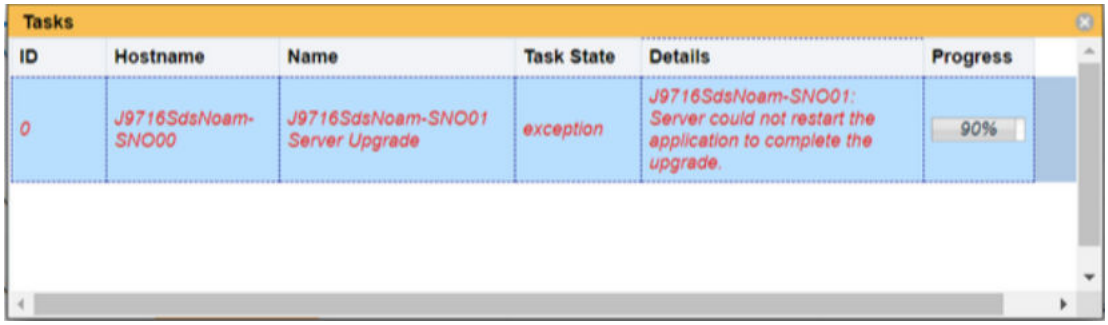
In case the upgrade fails due to an early check, restart the server before retrying the upgrade.

9.6 Workaround to Resolve Failed Upgrade

Error: Upgrade failed from 9.x to 9.0.2 with error: "Server could not restart the application to complete the upgrade".

Following are the steps to resolve a failed upgrade:

Figure 9-1 Failed upgrade



1. Set **Max HA Role** to **Active** for the failed server on **HA** screen.
2. Restart the server on the server screen.

9.7 Workaround To Resolve Alarms while upgrading from build 8.5 to 9.0.2.0.0_99.13.0

Following are the alarms received while upgrading from the build 8.5 to 9.0.2.0.0_99.13.0:

- 14152 MAJOR Failed to transfer file from remote host, see trace log for details.
- 31214 MINOR Scheduled Process Fault.

Resolution

To resolve the alarm, run the following command

```
sudo irem RecentAlarmEv.0 where "eventNumber=14152"
```

.

9.8 Workaround to resolve DSR process restart when multiple sites have both DSR and vSTP MP

Workaround for DSR process restart when the user is upgrading from 9.x to 9.2.

Resolution:

Run the following commands on DA-MP post upgrade and then restart the MP Server.

```
iset -fcntl=off PmControl where "procTag='traceoam'"
```

```
sudo init 6
```

9.9 Workaround to Resolve False Alarms for DA MP and vSTP MP

The following critical alarms raised for DA MP (Diameter Agent Message Processor), vSTP MP in DSR or vSTP for combined deployments with multiple sites can be ignored:

- 25500 - No DA MP Leader Detected
- 70371 - No vSTP MP Leader Detected

If required, perform the following procedure to resolve the below alarms:

1. On DSR SOAM, run the following commands:

   ```
   iset -fcntl=off PmControl where "procTag='vstpoam'"
   iset -fcntl=respawn PmControl where "procTag='dsroam'"
   ```

2. On vSTP SOAM, run the following commands:

   ```
   iset -fcntl=off PmControl where "procTag='dsroam'"
   iset -fcntl=respawn PmControl where "procTag='vstpoam'"
   ```

> **Note**
>
> In future, if the system is restarted, the alarms will not be restored.

9.10 Workaround for Configuring GUI and MMI Using Label Format for FQDN/Realm

For the users who prefer to configure with a single label format instead of the label.label format for FQDN/Realm, perform the following procedure for GUI and MMI configuration changes:

> **Note**
>
> By default, thecode is compliant.

1. Navigate to the `cd /usr/TKLC/dpi/prod/maint/scripts/` folder.
2. Run the following command:

   ```
   sudo ./rfcRealmFqdn.sh
   ```

3. Select an option from the list and proceed with the FQDN/Realm configuration:
   a. Non-Compliant: Allow RFC (Request for Comments) Non-Compliant label format.
   b. Compliant: Allow RFC Compliant label format.
   c. Quit

   > **Note**
   >
   > To continue with the switchover, this manual step must be performed on every OAM server.

A

Alternate Server Upgrade Procedures

The following procedure provides alternative ways of upgrading various server types, using an array of differing methods. All of the procedures in this section are secondary to the upgrade methods provided in previous sections. These procedures should be used only when directed by or by other procedures within this document.

A.1 Alternate Pre-Upgrade Backup

This procedure is an alternative to the normal pre-upgrade backup provided in Site Preupgrade Backups. This procedure is a manual alternative backup. It 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.

1. Log into the Active SOAM

   Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to the active SOAM:

   ```
   ssh admusr@<SOAM_VIP>
   ```

2. Start a Screen Session.

   Enter the command:

   ```
   $ screen
   ```

   The screen tool creates a no-hang-up shell session, so the command continues to run if the user session is lost.

3. Backup all servers managed from the SOAM to be upgraded.

   Run 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:

   > ⚠ **Caution**
   >
   > Failure to include the --site parameter with the backupAllHosts command results in overwriting the NOAM backup file created in Back Up TKLCConfigData Files. Backing out to the previous release is not possible if the file is overwritten.

   ```
   $ /usr/TKLC/dpi/bin/backupAllHosts --site=<NEName>
   ```

   where <NEName> is the Network Element Name (NEName) as seen using the following command:

   ```
   $ iqt NetworkElement
   ```

   This output displays when executing either of the options:

```
Do you want to remove the old backup files (if exists ) from all
the servers (y/[n])?y
```

It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.

Do not proceed until the backup on each server is completed.

Output similar to the following indicates successful completion:

```
HOSTNAME | STATUS

-------------------------------------------

HPC3blade02 | PASS

HPC3blade01 | 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. 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 to run backup on individual server

This is an alternative backup method that can be executed on each individual server instead of using the backupAllHosts script. A manual backup can be executed on each server individually, rather than using the script. To do this, log in to each server in the site individually and run 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. Verify Backup Files are Present on Each Server
   a. Log in to the active NOAM GUI using the VIP.
   b. Navigate to **Status & Manage**, then **Files**.
   c. Click each server tab.
   d. For each server, verify the following (2) files have been created:
   e. Repeat steps 1 to 4 for each site.

A.2 Server Upgrade Using platcfg

The following procedure enables a server to be upgraded using the Platform Configuration (platcfg) utility.

1. Log in to 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. Enter the platcfg menu

   Switch to the platcfg user to start the configuration menu:

   ```
   $ sudo su – platcfg
   ```

   From the Main Menu, select **Maintenance**.

3. Perform Upgrade Checks
   a. From the Maintenance Menu, select **Dual Image Upgrade**.
   b. From the Dual Image Upgrade Menu, select **Early Upgrade Checks**.

4. Select the Upgrade Media
   a. 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!
      ```

   b. Verify early upgrade checks pass. In case of errors, it is recommended to contact My Oracle Support (MOS).

c. Press **q** to exit the screen session and return to the platcfg menu.

d. From the Choose Upgrade Media Menu, select **Exit**.

5. Initiate the Upgrade.

   From the Dual Image Upgrade Menu, select **Initiate Background Upgrade**.

6. Select the Upgrade Media

   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.

7. Exit from **Upgrade Media Menu** and select **Dual Image Upgrade Menu**.

8. Select **Apply Upgrade**.

   > **Note**
   >
   > If **Apply Upgrade** option does not appear, exit from the platcfg and then again navigate to platcfg.

   After the upgrade is complete, the server reboots.

   ```
   A reboot of the server is required.

   The server will be rebooted in 10 seconds
   ```

9. Log in to 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.

   Once server comes us and post apply scripts are completed, verify this by running the following command:

   ```
   tail -f /var/TKLC/log/upgrade/upgrade.log
   ```

   > **Note**
   >
   > Post apply scripts takes 10 to 15 minutes to get completed.

10. Check for Upgrade Errors

    a. 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
       ```

    b. Examine the output of the command to determine if any errors were reported.

    c. 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
```

d. It is recommended to contact My Oracle Support by referring to Create a Link for ComAgent and provide these files.

11. Verify the Upgrade

a. Check the upgrade log for the upgrade complete message:

```
grep "APPLY COMPLETE" /var/TKLC/log/upgrade/upgrade.log
```

b. Verify the APPLY COMPLETE message displays. If not, it is recommended to contact My Oracle Support:

```
[admusr@NO2 ~]$ grep "APPLY COMPLETE" /var/TKLC/log/ upgrade/
upgrade.log

1407786220:: APPLY COMPLETE
```

B

Recover from a Failed Upgrade

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

Active NOAM VIP: Select Affected Server Group Containing the Failed Server

1. Log in to the NOAM GUI using the VIP.
2. Navigate to **Administration**, then **Software Management**, and then **Upgrade**.
3. Select the server group tab for the server to be recovered.

> **Note**
>
> If the failed server was upgraded using the Upgrade Server option, then skip to step 7 of this procedure.
> If the failed server was upgraded using the Auto Upgrade option, then continue with step 2 of this procedure.

Active NOAM VIP: Navigate to the Active Tasks Screen to View Active Tasks

- Navigate to **Status & Manage**, then **Tasks**, and then **Active Tasks**.

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**.

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 host name of the active NOAM server.
2. Locate the task for the **Server Group Upgrade**. It shows a the status as paused.

> **Note**
>
> Consider the case of an upgrade cycle where it is seen that the upgrade of one or more servers in the server group have status as exception (i.e., failed), while the other servers in that server group have upgraded successfully. However, the server group upgrade task still shows as running. In this case, please cancel the running (upgrade) task for that server group before reattempting ASU for the same.

> **Caution**
>
> Before clicking Cancel for the server group upgrade task, ensure the upgrade status of the individual servers in that particular server group should have has 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.

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.

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**.

Failed Server CLI: Inspect Upgrade Log

1. Log in to the failed server to inspect the upgrade log for the cause of the failure.
2. 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.

3. View or edit the upgrade log at **/var/TKLC/log/upgrade/upgrade.log** for clues to the to identify the cause of the upgrade failure.
4. If the upgrade log contains a message similar to the followingone shown below, 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
```

> **⚠ Caution**
>
> 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).
>
> Do not proceed to the next procedure until the alarm condition has been cleared.

Failed Server CLI: Verify Platform Alarms are Cleared from the Failed Server

- Use the alarmMgr utility to verify all platform alarms have been cleared from the system.

  ```
  $ sudo alarmMgr --alarmstatus
  ```

  Example output:

  ```
  [admusr@SO2 ~]$ sudo alarmMgr --alarmstatus
  SEQ: 2 UPTIME: 827913 BIRTH: 1458738821 TYPE: SET ALARM:
  TKSPLATMI10|tpdNTPDaemonNotSynchronizedWarning|
  1.3.6.1.4.1.323.5.3.18.3.1.3.10|32509|Communications|Communications
  Subsystem Failure
  ***user troubleshoots alarm and is able to resolve NTP sync issue
  and clear alarm***
  [admusr@SO2 ~]$ sudo alarmMgr --alarmstatus
  [admusr@SO2 ~]$
  ```

Active NOAM VIP: Re-execute the Server Upgrade

- Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option.

> **ⓘ Note**
>
> Once a server has failed while using the Automated Server Group Upgrade option, the Auto Upgrade option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the Upgrade Server option.

C

Identify the DC Server

This procedure provides the details to identify the DC server.

NOAMP VIP GUI: Login

- Repeat the steps listed in .NOAMP VIP GUI: Log in to the server (if not already done).

NOAMP VIP GUI: Select an MP Server

1. Navigate to **Configuration**, then **Server Groups**.
2. Select an MP server from the server group that needs to be upgraded.

Log in to MP Server using CLI SSH to MP Server Chosen Above

1. Use the SSH command (on UNIX systems – or putty if running on windows) to log into the MP server identified in task 1.

   ```
   ssh admusr@<MP_SERVER_XMI>
   ```

   ```
   password: <enter password>
   ```
2. Answer **yes** if you are asked to confirm the identity of the server.

MP Server CLI: Find DC Server

- Identify the DC server in the server group with this command:

  ```
  ha.info -d
  ```

D

Limitations of Automated Server Group and Automated Site Upgrade

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

> **Note**
>
> Oracle's recommendation for any customer whose network aligns with any of the following scenarios is that the Automated Server Group upgrade should NOT be used on multi-active DA-MP server groups. Use of ASG risks a potential network outage. For Automated Site Upgrade, following limitations can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles then in that case manual upgrade procedure from section 5.3 method should be used.

Specialized Fixed Diameter Connections

In this scenario, each peer node is configured to connect to two specific DA-MPs for local redundancy (Figure 18). With ASG/ASU setup for 50% minimum availability, three of the DA-MPs in the server group are upgraded in parallel. However, it is not possible to determine in advance which three DA-MPs are selected. Although the DSR has redundant connections to the peer nodes, an unfortunate selection of servers for upgrade could result in an outage. Upgrade cycle 1 takes out both DA-MPs connected to the unhappy peer. This peer is isolated for the duration of the upgrade. The happy peer is connected to DA-MPs that are selected by ASG/ASU for different upgrade cycles. This peer is never isolated during the upgrade.

Specialized Floating Diameter Connections

In this scenario, each peer node is configured to connect to an IPFE TSA address hosted by a set of DA MPs. When any particular TSA contains only a subset of the server group MPs, and the DSR upgrade logic happens to select that subset of MPs for simultaneous upgrade, then there is a signaling outage for that TSA. This scenario is depicted in Figure 19. TSA1 is distributed across the first three DA-MPs, whereas TSA2 is distributed across all six DA-MPs. If ASG/ASU is initiated with 50% minimum availability, the DSR could select all three of the DA-MPs hosting TSA1 in the first upgrade cycle. The unhappy peer is isolated for the duration of upgrade cycle 1. The happy peer is connected to TSA2, which is hosted by the DA-MP servers in such a way that the TSA is evenly hosted in both upgrade cycles. This peer is never isolated during the upgrade.

Specialized Distribution of DSR Features

In this scenario, the customer has decided to enable P-DRA and RBAR on four DA-MP servers and DCA on two DA-MP servers, consistent with expected traffic load. With ASG setup for 50% minimum availability, the DA-MP server group is upgraded in two cycles. RBAR and P-DRA

happen to be hosted by DA-MP servers selected by ASG/ASU to be in different upgrade cycles, albeit unbalanced. The RBAR peer is only marginally happy because during upgrade cycle 1, only 25% of RBAR and P-DRA capacity is available, even though the customer specified 50% availability. DCA happens to be hosted by DA-MP servers selected by ASG/ASU to be in upgrade cycle 2. In this event, the DCA peer is unhappy because DCA is completely unavailable during upgrade cycle 2.

E

Advanced Health Check Procedure

This procedure verifies the UDP/TCP port 53 is open between NOAM and each DR-NOAM site, NOAM, and each SOAM site, and between MPs and each name server of the file /etc/resolv.conf.

Verify if the UDP/TCP Port 53 is Open Between NOAM and Each DR-NOAM Site

1. From the command prompt of the server with the alarm, issue the sudo nmap -sTU -p 53 <DR-NOAM hostname> command.
2. Verify that the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:

```
[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-DRNOAM-A

Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:57 EST

Nmap scan report for Icepick-DRNOAM-A (10.75.202.173)

Host is up (0.00025s latency).

rDNS record for 10.75.202.173: Icepick-DRNOAM-
A.platform.cgbu.us.oracle.com

PORT STATE SERVICE

53/tcp open domain

53/udp open domain

MAC Address: 02:05:39:E0:60:8A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds

[admusr@Icepick-NO-A ~]$
```

   If port is reported as any state other than “Open”, then inform the customer before accepting the upgrade.

> **Note**
>
> If the ports are reported as “Closed” it may be because no services are running on the far end. Check with the customer if the firewall has been configured to allow DNS traffic on port 53.
> If the port is reported as “Filtered” then the port is likely blocked by a Firewall and the upgrade must not be accepted until the customer confirms that their network will allow DNS traffic on port 53.

Verify if the UDP/TCP Port 53 is Open Between NOAM and Each SOAM Site

1. From the command prompt of the server with the alarm, issue the sudo nmap -sTU -p 53 <SOAM hostname> command.
2. Verify that the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:

```
[admusr@Icepick-NO-A ~]$ sudo nmap -sTU -p 53 Icepick-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 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.

Verify if the UDP/TCP Port 53 is Open Between MP and Each Name Server of the /etc/resolv.conf file

1. List the contents of the file /etc/resolv.conf via the “sudo cat etc/resolv.conf” command.
2. Verify that the Customer Firewall is configured to allow DNS traffic on UDP/TCP port 53 to the addressed from the file /etc/resolv.conf:

```
[admusr@Icepick-DAMP-1 ~]$ sudo cat /etc/resolv.conf (lookups)

domain platform.cgbu.us.oracle.com

nameserver 10.240.50.134

nameserver 10.240.50.133
```

```
search platform.cgbu.us.oracle.com 500lab.com labs.tekelec.com
labs.nc.tekelec.com

[admusr@Icepick-DAMP-1 ~]$

[admusr@Icepick-DAMP-1 ~]$ sudo nmap -sTU -p 53 10.240.50.134
10.240.50.133

Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-02 17:46 EST

Nmap scan report for Icepick-SO-B-imi.platform.cgbu.us.oracle.com
(10.240.50.134)

Host is up (0.00022s latency).

PORT STATE SERVICE

53/tcp open domain

53/udp open domain

MAC Address: 02:17:B4:4F:DA:B6 (Unknown)

Nmap scan report for Icepick-SO-A-imi.platform.cgbu.us.oracle.com
(10.240.50.133)

Host is up (0.00025s latency).

PORT STATE SERVICE

53/tcp open domain

53/udp open domain

MAC Address: 02:EE:13:E2:2C:EF (Unknown)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.66 seconds

[admusr@Icepick-DAMP-1 ~]$
```

If port is reported as any state other than “Open” then inform the Customer before accepting the upgrade.

> **Note**
>
> If the ports are reported as “Closed” it may be because no services are running on the far end. Verify with the Customer that the firewall has been configured to allow DNS traffic on port 53.
> If the port is reported as “Filtered” then the port is likely to be blocked by a Firewall and the upgrade must not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

F

Create a Link for ComAgent

This procedure provides the details about creating a symbolic link of Comagent.

Server CLI: Log in to the Server (if not already done)

- Use the SSH command (on UNIX systems – or putty if running on Windows) to log in to the server under backout:

  ```
  ssh admusr@<server address>
  ```

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

  Answer **yes** if you are asked to confirm the identity of the server.

Server: Create a Link for ComAgent

1. Navigate to /var/TKLC/appworks/library.

   ```
   $ cd /var/TKLC/appworks/library
   ```

2. Create a link.

   ```
   $ sudo ln -s /usr/TKLC/comagent-gui/gui/ Comagent
   ```

G

Change SOAM VM Profile for Increased MP Capacity on an OpenStack System

This procedure provides the details about changing SOAM VM profile for increased MP Capacity. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. Log in to Openstack GUI horizon dashboard.
2. Go to the corresponding Instance and select the **Shut Off Instance** option from the list.
3. Once the instance is in **Shutoff** state, select the **Resize Instance** option from the list.
4. Select the **New Flavor** that meets the standard VCPUs size and memory configuration.
5. Click **Resize**.

> **Note**
>
> For information on the recommended vCPUs size and memory, refer to *DSR Cloud Benchmarking document*.

H

Change SOAM VM Profile for Increased MP Capacity on a VMware system

This procedure describes how to change the SOAM VM profile on a VMware system.

Log in to Active NOAM

1. Log in to the Active NOAM GUI using the VIP.
2. Navigate to **Main Menu**, then **Status & Manage**, and then **HA**.
3. Confirm that at least one SOAM has **OAM HA Role** of **Active**.
4. Identify the Active and Standby SOAM server based upon the **OAM HA Role** column.

Check System Alarms

1. Navigate to **Main Menu**, then **Alarms & Events** , and then **View Active**.
2. Confirm that there are no alarms related to Replication, Merging, system health, or SOAMs.
3. In case of any alarms, stop the activity, identify the cause of alarms, and resolve them, and then continue to the next steps when the alarms are cleared.

Take Standby SOAM Out of Service in HA

1. Navigate to **Main Menu**, then **Status & Manage**, and then **HA**.
2. Press the Edit button in lower-left corner of the page.
3. Take the SOAM identified as Standby in Step 1 to Max Allowed HA Role of OOS.
4. Click **OK**.

   Information displays information banner Pre-Validation passed-Data Not Committed.
5. Press **OK**.

   The system goes back to the previous screen with the Standby SOAM now Showing OOS in Max Allowed HA Role and OAM HA Role. At this point, the server is ready to be turned off for any change.

Stop/Shut Down the VM

1. Log in to Command Line Interface of the SOAM taken out of service.
2. Run the `sudo init 0` command.

Modify the vCPU and Memory

1. Confirm that the virtual machine is powered off.

2. Click the virtual machine.
3. Go to Settings.
4. Edit System Settings to change:

   vCPU: 8

   RAM/Base Memory: 14,336 (14GB, 14 x 1024)

> **Note**
>
> The exact steps may be different depending on the VM Manager. Contact your VM Manager for any help on the exact steps.

Start the VM

- Set Power State of VM to Power ON in the VM Manager and wait for a few minutes.

Log in to SOAM using CLI

1. Use the SSH command to log in to the respective SOAM identified.

   ```
   ssh admusr@<SERVER_XMI>
   password: <enter password>
   ```

2. Answer **yes** when prompted to confirm the identity of the server.

Confirm that the SOAM is Sowing 8 vCPU

- On the SOAM CLI, run the mpstat -P ALL command.

  The output should be one line for each vCPU. Confirm that for vCPU=8, the output shows 8 lines.

Check Memory (RAM) Size is 14 GB

- On the SOAM CLI, run the following command:

  ```
  cat /proc/meminfo
  vmstat -s
  ```

  Sample output:

  ```
  admusr@labNOAM ini]$ cat /proc/meminfo
  MemTotal: 14007172 kB
  [admusr@labNOAM ini]$ vmstat -s
  14007172 total memory
  ```

Increase Measurement Memory and Queue Size

1. Run the following command:

```
sudo sh /usr/TKLC/dsr/prod/maint/loaders/install/load.AppwMeasMem
```

2. Verify if the MeasMem.inifile is created for measurement memory size of 3072 MB:

   ```
   cat /var/TKLC/appworks/ini/MeasMem.ini
   ```

   > **Note**
   >
   > INI entry should be aw.measure.maxmem = 3072.

3. Verify that the measurement queue size is set to 2 in LongParam table where the parameter name "measurementMaxQueues" is 2:

   ```
   iqt -pE LongParam | grep measurementMaxQueues
   ```

Bring Back SOAM in to Service

1. Log in to the Active NOAM GUI using the VIP.
2. Navigate to **Main Menu**, then **Status & Manage** , and then **HA**.
3. Press **Edit** in the lower-left corner of the page.
4. Take the modified SOAM to Max Allowed HA Role of ACTIVE.
5. Press **OK**.

   Information displays information banner Pre-Validation passed-Data Not Committed.
6. Press **OK**.

   The system goes back to the previous screen with the Standby SOAM now showing **Active** in **Max Allowed HA Role**.
7. Wait for the time till this SOAM shows **Standby** in the **OAM HA Role**.

   At this point, the server is back to the normal operating status.

Take Active SOAM Out of Service in HA

1. Navigate to **Main Menu**, then **Status & Manage**, and then **HA**.
2. Press **Edit** in the lower-left corner of the page.
3. Take the SOAM identified as Active in Step 1 to **Max Allowed HA Role** of OOS.
4. Press **OK**.

   Information displays the information banner Pre-Validation passed-Dat Not Committed.
5. Press **OK**.

   The system goes back to the previous screen with the Active SOAM showing OOS in **Max Allowed HA Role** and **OAM HA Role**.
6. Confirm that the SOAM that was Standby earlier is now Active in **Max Allowed HA Role** and **OAM HA Role**.

   At this point, the server is ready to be turned off for any change.

Note

Repeat all the tasks from Stop/Shut down the VM to Bring Back SOAM into service.

Reset the SOAP Password

Perform the following procedure to reset the SOAP password for Active NOAM Server:

Log in to the Active NOAM Server

1. Log in as admusr on the active NOAM server.
2. Retrieve the TPD web service password in plaintext by executing:

   ```
   $ /usr/TKLC/appworks/bin/aw.wallet credential get cmsoapa password
   ```

   The command will print the current plaintext configuration web service password.

   For example:

   7w57q9U0OvOtKtgtLVTMajDcXfhCj2F4nyXw45qK6EXNHA9jACyQ

J

Restore the Servers with Backout Errors

This workaround resolves a backout failure error. Run this procedure on the failed server.

1. Recognize the rpm (dsr/dpi) which yielded the scriptlet failure. Examine the upgrade log at /var/TKLC/log/upgrade/upgrade.log for errors that occurred during the backout.

   ```
   $ rpm –qa <rpm_name>
   ```

   Example:

   ```
   $ rpm – qa <TKLCdsr.x86_64>
   ```

   > **Note**
   >
   > There will be two rpms, identify the newer rpm.

2. Uninstall the newer version of the rpm:

   ```
   rpm –e <rpm_name>
   ```

3. Run this command:

   ```
   $ rpm –qa <rpm_name>
   ```

   > **Note**
   >
   > There must be a single rpm.

4. Run the `sudo /var/tmp/backout_restore` command to restore the database and restart the server.

K

Dual Hop Upgrade from DSR-8.x to DSR-9.0.x Using Ansible

This section provides information and the procedure for Dual Hop Upgrade from release 8.x VM to DSR 9.0.x VM or above release.

Points to be considered during Dual Hop upgrade:

- Use only `admusr` as username for all the commands.
- Do not perform ISO deployment for Dual Hop Upgrade.
- During "Fatal Error", the server cannot be restored, a new server build is required. The server must be rebuilt using the same DSR release of its mate server.
- During typical failure, the system can be restored using the following command: `/var/TKLC/backout/diUpgrade --clearError`
- In case of upgrade failure due to an early check, restart the server prior to retrying the upgrade.
- This procedure is applicable for VSTP installation as well.
- SDS must be upgraded before DSR.
- For the User Data Repository upgrade, refer to User Data Repository upgrade document.
- Backout is not supported for OL6 to OL8 Upgrade (DSR-8.x to DSR-9.0.x).
- `majorUpgrade.sh` will run the dual hop upgrade command and copy the ISO file to the required path. In order to perform the upgrade, it will also install Ansible RPM.

Prerequisites

- DSR 9.x requires more disk space and RAM capacity. Hence, create flavor to resize the instance and refer to *Diameter Signaling Router Cloud Benchmarking Guide* for flavor details.
- Ensure the instance which must be upgraded does not contain any alarms. To check the alarm status before triggering the upgrade, run the following command:

  ```
  alarmMgr --alarmStatus
  ```

- Space utilization should be less than 70% for all partitions and no hard disk alarm should be present. Run the following command to check:

  ```
  df -kh
  ```

- Download the `dualHopUpgrade.tar.gz` file from Oracle Software Delivery Cloud (OSDC) site. Extract the file to retreive the following files, which are required to perform this upgrade:
  - `pre_upgrade_check.sh`
  - `extend_partition.sh`
  - `post_partition.sh`

- `diuMajHosts`
- `vault.yml`
- `majorUpgrade.sh`

> **Note**
>
> Backout is not supported for OL6 to OL8 upgrade (DSR 8.x to 9.0.x).

The following table provides the time required by each task while performing Dual Hop Upgrade (DIU) from DSR 8.x VM to DSR 9.0.x VM.

Table K-1 Time Required for Dual Hop Upgrade

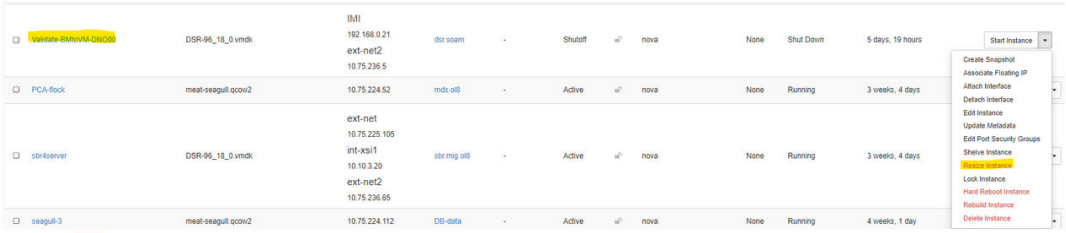
Procedure	Time Required (hr:min)	Reference
Step 1	0:10 - 0:20 for each VM	Resizing all the Instances in the Setup
Step 2	0:10 - 0:20 for each VM	Extending the Partition
Step 3	0:20 - 0:30	Setting up the Active NOAM as Controller
Step 4	0:40 - 0:60	Upgrading Standby NOAM
Step 5	0:05 - 0:10	Configuring Upgraded Standby NOAM
Step 6	0:05 - 0:10	Setting up Active NOAM as Controller
Step 7	0:40 - 0:60 for each Group	Upgrading Other Servers

K.1 Resizing all the Instances in the Setup

> **Note**
>
> For procedure to resizing instances if the setup used is in KVM environment, see Resizing Instances if Setup is in KVM Environment.

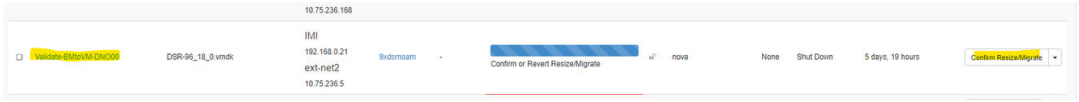
1. Login to OpenStack GUI.
2. Shutdown the instance.
3. Select **Resize Instance** option and configure the required flavour.

Figure K-1 Resizing Instance



4. Select the instance and click **Confirm Resize**.

Figure K-2 Confirm Resize



5. Start the instance.

K.1.1 Resizing Instances if Setup is in KVM Environment

> **Note**
>
> Perform this procedure on the Host where VM is deployed.

1. Shutdown VM by running the following command:

   ```
   virsh shutdown <VM Name>
   ```

   Wait for the VM to shut down.

2. Run the following commands:

   ```
   virsh dumpxml <VM Name> | grep 'disk type' -A 5
   ```

   Output:

   ```
   [root@ol-server ~]# virsh dumpxml Dsrtestsetup-Noam1 | grep 'disk type' -A
   5
   <disk type='file' device='disk'>
   <driver name='qemu' type='qcow2'/>
   <source file='/mnt/data/ova/Dsrtestsetup-Noam1.qcow2'/>
   <target dev='vda' bus='virtio'/>
   <address type='pci' domain='0x0000' bus='0x05' slot='0x00' function='0x0'/>
   </disk>
   ```

   ```
   qemu-img info {{ path with image name }}.qcow2
   ```

   Output:

   ```
   [root@ol-server ~]# qemu-img info /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
   image: /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
   file format: qcow2
   virtual size: 120 GiB (128849018880 bytes)
   disk size: 7.56 GiB
   cluster_size: 65536
   Format specific information:
       compat: 1.1
       compression type: zlib
       lazy refcounts: false
   ```

```
    refcount bits: 16
    corrupt: false
```

```
qemu-img resize {{ path with image name }}.qcow2 +<additional required
size>G
```

Output:

```
[root@ol-server ~]# qemu-img resize /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
+40G
Image resized.
```

3. Verify VM sixe, by running the following command:

```
qemu-img info {{ path with image name }}.qcow2  (To verify VM size)
```

Output:

```
[root@ol-server ~]# qemu-img info /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
image: /mnt/data/ova/Dsrtestsetup-Noam1.qcow2
file format: qcow2virtual size: 160 GiB (171798691840 bytes)
disk size: 7.56 GiB
cluster_size: 65536
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
    extended l2: false
```

4. Start VM by running the following command:

```
virsh start <VM Name>
```

K.2 Extending the Partition

1. Provide `chmod 777` permission to all the scripts.
2. Download the scripts from the tar file and place it in `/home/admusr` directory.
3. Run the following command:

```
sudo ./extend_partition.sh
```

4. Restart the server.

```
sudo init 6
```

5. Run the following commands:

```
sudo ./post_partition.sh.
```

```
sudo ./pre_upgrade_check.sh
```

> **Note**
>
> This is a manual step and must be executed on all the servers.

6. Switchover the roles from Standby to Active and Active to Standby.

> **Note**
>
> - Resize new standby, by performing Resizing all the Instances in the Setup and Extending the Partition procedures.
> - For NOAM, SOAM, and IPFE, perform Resizing all the Instances in the Setup and Extending the Partition procedures on both Standby and Active.
> - For DAMP, perform Resizing all the Instances in the Setup and Extending the Partition procedures except Switchover step.

K.2.1 Resizing /var/TKLC/ Directory

Resizing is required in the following scenarios, when a 5.4G iso is attempting to copy to a directory that has an average 3.5G of free space, which results in upgrade failure in locating or opening .iso file in `/var/TKLC/upgrade/` directory:

- When the 5.4G DSR-9.0.2 iso file is copied by the ISO deployment from `/var/TKLC/db/filemgmt` directory to the `/var/TKLC/db/filemgmt/isos/` directory.
- When running the beginning of the `majorUpgrade.sh` script, during OL8 upgrade attempts to copy the 1.5G TPD.install-8.0 DIU iso to `/var/TKLC/upgrade/` directory.

In some cases, resizing `/var/TKLC/` by adding 8G is required. Increasing the `/var/TKLC/` directory (`/dev/mapper/vgroot-plat_var_tklc`) from 3.9G to 11.9G allows room for the 5.4G DSR-9.01 iso file and 1.5G TPD.install-8.0 DIU iso. The DSR-9.0.2 upgrade allows resizing the `/var/TKLC/` directory for 7.8G.

Perform the following procedure to resize `/var/TKLC/` directory:

1. To confirm enough free space exists, run the following command to verify there is free PE / Size: with the following command to increase `/var/TKLC/` by 8G

```
sudo vgdisplay
```

Output:

```
[admusr@MP-2 ~]$ sudo vgdisplay
  --- Volume group ---
  VG Name               vgroot
  System ID
```

```
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  27
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                12
  Open LV               12
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               105.44 GiB
  PE Size               32.00 MiB
  Total PE              3374
  Alloc PE / Size       1825 / 57.03 GiB
  Free  PE / Size       1549 / 48.41 GiB
  VG UUID               xydJnb-5LDn-leFp-J2qO-tLrW-gAsn-n1SajJ
```

2. Verify `/var/TKLC/` directory size, by running the following command:

```
[admusr@MP-2 ~]$ df –h /var/TKLC/
Filesystem                          Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_var_tklc  3.9G  194M  3.5G   6% /var/TKLC
```

3. Use the following commands to increase the `/var/TKLC/` directory size:

```
sudo lvresize -L +8G /dev/mapper/vgroot-plat_var_tklc


sudo resize2fs /dev/mapper/vgroot-plat_var_tklc
```

4. Verify the free PE `/ Size after /var/TKLC/` resize, by running the following command:

```
[admusr@MP-2 ~]$ sudo vgdisplay
  --- Volume group ---
  VG Name               vgroot
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  27
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                12
  Open LV               12
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               105.44 GiB
  PE Size               32.00 MiB
  Total PE              3374
  Alloc PE / Size       1825 / 57.03 GiB
  Free  PE / Size       1549 / 40.41 GiB
  VG UUID               xydJnb-5LDn-leFp-J2qO-tLrW-gAsn-n1SajJ
```

5. Verify `/var/TKLC/` size, by running the following command:

```
[admuse@MP-2 ~]$ df -h /var/TKLC
Filesystem                          Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_var_tklc  11.8G  194M 10.2G  2% /var/TKLC
```

K.2.2 Run ISO Administration

Refer to DSR ISO Administration to deploy the DSR 9.0.2 target release ISO image file.

K.3 Setting up the Active NOAM as Controller

1. Place the TPD OL7 DIU ISO and DSR DIU ISO on `/var/TKLC/db/filemgmt` of Active NOAM.
2. Create diuMajHosts file in `/home/admusr` of Active NOAM.

> **Note**
>
> **Description of diuMajHosts file:**
>
> - image_name_tpd: TPD OL7 DIU ISO name should be given
> - image_name_dsr: DSR DIU ISO name should be given
>
> **For DSR dual hop upgrade, use the groups as mentioned below:**
>
> - Divide the servers into the groups with the XMI IP of the servers, which are required to be upgraded.
> - group1: We have included IP of Standby NOAM in group1, as this would be the first server that must be upgraded.
> - group2: In this group Active NOAM IP is included (Standby NOAM after switchover).
> - group3: This group contains the IP of Standby SOAM.
> - group4: This group contains the IP of Active SOAM.
> - group5 and group6: These groups contains the 50% of IP's of C level servers respectively.
>
> There can be n number of groups in the below file.
>
> Host name (host1, host2....) must be different for different groups.

For example:

```
[all:vars]
image_name_tpd=TPD.install-8.0.0.0.0_90.12.0-OracleLinux7.4-x86_64-DIU.iso
image_name_dsr=DSR-9.0.2.0.0_98.5.0-x86_64.iso

[group1]
host1 ansible_host=<XMI IP of StandBy NOAM> ansible_user=admusr
ansible_port=22
```

```
[group2]
host2 ansible_host=<XMI IP of Active NOAM> ansible_user=admusr
ansible_port=22

[group3]
host3 ansible_host=<XMI IP of Standby SOAM> ansible_user=admusr
ansible_port=22

[group4]
host4 ansible_host=<XMI IP of Active SOAM> ansible_user=admusr
ansible_port=22

[group5]
host5 ansible_host=10.75.237.93  ansible_user=admusr ansible_port=22  -----
> DMP00
host6 ansible_host=10.75.236.97  ansible_user=admusr ansible_port=22  -----
> DIP00
.
.
.
[group6]
host7 ansible_host=10.75.237.141ansible_user=admusr ansible_port=22  -----
> DMP01
host8 ansible_host=10.75.237.161ansible_user=admusr ansible_port=22  -----
> DIP01
.
.
.
```

3. Create the `vault.yml` file in `/home/admusr` of Active NOAM.

   ```
   ansible_ssh_pass: secret_password(password for admusr)
   ```

4. Place the `majorUpgrade.sh` script in `/var/TKLC/db/filemgmt` of Active NOAM.
5. Run the following command:

   ```
   chmod 777 /var/TKLC/db/filemgmt/majorUpgrade.sh
   ```

K.4 Upgrading Standby NOAM

- Run the following commands on the Active NOAM Shell.

  ```
  cd /var/TKLC/db/filemgmt


  ./majorUpgrade.sh upgrade group1
  ```

K.5 Verifying Upgrade

Perform the following steps to verify whether the upgrade is successful on a particular host.

1. To print the logs, and verify if the upgrade is successful, run the `majorUpgrade.sh` script.

> **Note**
>
> Before starting with the next step, run the `majorUpgrade.sh` script on every group.

2. Run the following command on the instance which was upgraded:

```
sudo verifyUpgrade
ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!
ERROR: 1721303654::Use of uninitialized value in pattern match (m//)
at /usr/TKLC/plat/lib/Security/Freeze.pm line 98.
1721303654::Use of uninitialized value in pattern match (m//) at /usr/TKLC/
plat/lib/Security/Freeze.pm line 98.
1721303654::ERROR: /etc/pam.d/system-auth is not in the list of known auth
files!
1721303654::ERROR: Parsing an unknown auth file is not supported!
1721303654::ERROR: /etc/pam.d/system-auth is not in the list of known auth
files!
1721303654::ERROR: Parsing an unknown auth file is not supported!
1721303795::Use of uninitialized value in pattern match (m//) at /usr/TKLC/
plat/lib/Security/Freeze.pm line 98.
1721303795::Use of uninitialized value in pattern match (m//) at /usr/TKLC/
plat/lib/Security/Freeze.pm line 98.
1721303795::ERROR: /etc/pam.d/system-auth is not in the list of known auth
files!
1721303795::ERROR: Parsing an unknown auth file is not supported!
1721303795::ERROR: /etc/pam.d/system-auth is not in the list of known auth
files!
1721303795::ERROR: Parsing an unknown auth file is not supported!
```

   If the upgrade is successful, the above command would not return any output or would return the following expected error.

```
ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!
ERROR: 1721989552::ERROR: Command Failed!
1721989553::ERROR: Child process has exited with:
1721989553::ERROR: Failed to load shared secret keys post diu
```

K.6 Configuring Upgraded Standby NOAM

1. Login to Active NOAM.
2. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
3. Click **Edit** and update the **Max Allowed HA Role** value of Active NOAM to `Standby`, then click **Ok**.
4. Login to Standby NOAM from GUI, which is now the Active NOAM.
5. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
6. Click **Edit** and update the **Max Allowed HA Role** value of Standby NOAM to `Active`, then click **Ok**.

K.7 Setting up Active NOAM as Controller

1. Copy `majorUpgrade.sh` file from Standby NOAM to Active NOAM in `/var/TKLC/db/filemgmt` path, by performing the following steps:
   a. SSH to Standby NOAM console.
   b. Navigate to `/var/TKLC/db/filemgmt` path.
   c. Run the following command to copy the `majorUpgrade.sh` script to file management path of Active NOAM:

      ```
      scp majorUpgrade.sh admusr@<Active Noam IP>:/var/TKLC/db/filemgmt
      ```

2. Copy `diuMajHosts` and `vault.yml` files from Standby NOAM to Active NOAM in `/home/admusr` path, by performing the following steps:
   a. SSH to Standby NOAM console.
   b. Navigate to `/home/admusr/` path.
   c. Run the following command to copy the `diuMajHosts` and `vault.yml` files to `/home/admusr` path of Active NOAM:

      ```
      scp diuMajHosts admusr@<Active Noam IP>:/home/admusr
      ```

      ```
      scp vault.yml admusr@<Active Noam IP>:/home/admusr
      ```

K.8 Upgrading Other Servers

- Run the following commands to upgrade remaining servers:

  ```
  cd /var/TKLC/db/filemgmt
  ```

  ```
  ./majorUpgrade.sh upgrade group2
  ```

  ```
  ./majorUpgrade.sh upgrade group3
  ```

  > **Note**
  >
  > Run this command for all remaining groups.