Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management 12.1.x/12.2.x to 12.3 Upgrade Procedure Non-CMP Georedundancy Disabled

E85337-01

Augtust 2017

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

Before upgrading any system, please access Oracle's Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

Refer to C for instructions on accessing this site.

Contact the Oracle Customer Care Center and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

EMAIL: support@oracle.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures performed to upgrade the Oracle Communications Policy Management Release 12.2.x to Release 12.3 when georedundancy on non-CMP components (that is, MPE/MRA/Mediation) is disabled.

Firmware upgrades may be required, but are not covered in this document.

The non-georedundant MPE/MRA/Mediation cluster scheme only has two servers, active and standby, that are co-located on one site.

Two sites may be used in Policy Management deployments, namely, a Site1 or Primary Site and a Site2 or Secondary Site. The primary MRA/MPE/Mediation cluster of the active and standby resides on Site1 while the secondary MRA/MPE/Mediation cluster of active and standby resides on Site2 for disaster recovery.

1.2 Acronyms

Acronym	Meaning
CMP	Configuration Management Product **NOTE:** It usually refers to the CMP on the primary site
DR-CMP	Configuration Management Platform for Disaster Recovery **NOTE:** It refers to the CMP on the secondary site
DSR	Diameter Signaling Router
GUI	Graphical User Interface
LVM	Logical Volume Manager
MPE	Multimedia Policy Engine
MPE-LI	MPE for Lawful Intercept - a type of Multimedia Policy Engine
MRA	Multiprotocol Routing Agent (also referred to as Policy Front End or PFE)
PC	Policy Counter
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rules Function–An Oracle Communications Policy Management system
PM&C	Platform Management and Configuration
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment

1.3 Terminology

- Primary Site (Site1)

  A site where the MPE/MRA/Mediation primary cluster exists with co-located Active and Standby servers

- Secondary Site (Site2)

  A site where the MPE/MRA/Mediation secondary cluster exists with co-located active and standby servers for disaster recovery

- Segment

  A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster may be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.

1.4 Software Release Numbering

- PM&C: 6.0.3
- TVOE: 3.0.3
- TPD: 7.0.3
- COMCOL: 6.4
- Policy Management Release 12.3
- Oracle Firmware: 3.1.5
- HP Firmware: Firmware Upgrade Pack 2.2.9

2. UPGRADE OVERVIEW

This section lists the required materials and information to perform Policy Management Release 12.3 software upgrades.

2.1 Upgrade Status Values

Status	Condition
OK	All servers are up-to-date and no alarms are present.
Info	No alarms are present, but a condition (such as out-of-date) is present that you should be made aware of.
Minor	At least one minor alarm is present.
Major	At least one major alarm is present.
Offline	The server cannot be reached.
Degraded	At least one server in the cluster cannot be reached.
Critical	At least one critical alarm is present.
Active	The server is active.
Standby	The server is in standby mode as part of normal operations.
Forced Standby	The server is in standby mode because it has been placed into that state via direct intervention or as part of the upgrade.
Offline	The server cannot be reached.
Zombie	The server is in a state where it cannot recover automatically and requires direct intervention.

2.2 Upgrade Path

This upgrade document supports the following upgrade paths:

Policy Management 12.1.x to 12.3

Policy Management 12.2.x to 12.3

2.3 Upgrade Information

2.3.1 Upgrade Sequence

An upgrade procedure applies to an Active/Standby pair of servers. This pair of servers is referred to as a cluster. A cluster can be of different types: CMP, MRA, MPE, or Mediation depending on the mode. For a CMP cluster, the cluster status may also be Primary site and/or Secondary site.

A deployment may consist of multiple clusters.

2.3.2 Required Cluster Upgrade Sequence

Policy Server software upgrades are performed on a cluster by cluster basis at the primary and secondary sites within the same maintenance window.

The following is the general upgrade sequence, specific procedures/steps can further be documented by an Oracle provided MOP.

Software Upgrade Procedure
The following are the steps for a Policy Management system upgrade procedure (process for specific installations are documented by an Oracle provided MOP):

1. Upgrade PM&C Server at Site 1–Needed if version is older than what is listed in section 1.4
2. Upgrade PM&C Server at Site 2–Needed if version is older than what is listed in section 1.4
3. Firmware upgrade–If needed (not covered in this document)
4. Upgrade Primary (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Upgrade MPE/MRA/Mediation (see note below)

NOTE: MPE/MRA/Mediation clusters can be upgraded in parallel, a maximum of 4 at a time (except for upgrades from 12.1.x where 8 clusters can be upgraded in parallel).

2.3.3 Policy Release Mixed-Version Operation and Limitation

The general expectation is that a system that is running in a mixed version configuration should support features and perform at a level of the previous version. Thus, a system that is running pre-12.3 release and 12.3 release in mixed configuration would support the performance and capacity of the pre-12.3 release. The mixed version Policy Management configuration would also support pre-12.3 features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the Release 12.3 CMP is managing MRA/MPE/Mediation servers in a pre-12.3 release. In this mixed version configuration, a Release 12.3 CMP does not prevent configuring anything that can be configured in a previous release and all configuration items from the previous release are available. However, the configuration changes during the upgrade of Policy Management system are discouraged and have limited support.

In the mixed version, a Release 12.3 CMP has the following limitations while running in a mixed version environment:

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.
- As a general guideline, policy rules should not be changed while running in a mixed version environment. If it is necessary to make changes to the policy rules while running in a mixed version environment changes that do not utilize new conditions and actions for the release could be installed, but should be jointly reviewed by the you and Oracle before deployment to verify that these policies indeed do not use new conditions or actions.
- The support for configuration of MPE/MRA/Mediation servers is limited to parameters that are available in the previous version. Specifically:
    - Network Elements can be added

Mixed-version configurations supported

Policy Management system components on	CMP R12.3	MRA R12.3	MPE R12.3	Mediation R12.3
CMP R12.2.x	Yes	No	No	No

Policy Management system components on	CMP R12.3	MRA R12.3	MPE R12.3	Mediation R12.3
MRA R12.2.x	Yes	Yes	Yes	N/A
MPE R12.2.x	Yes	Yes	Yes	Yes
Mediation R12.2.x	Yes	N/A	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP to Release 12.3. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.3.

2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the Standby server, switching over from the Active to the Standby, and upgrading the second server (that is, the new Standby). The switchover of each cluster has a small impact on traffic being processed at that cluster, as in the past releases upgrades.

2.5 Rollback/Backout

The full pre-upgrade server image is stored on the server during the upgrade, and can be restored in the event of a problem discovered during or after upgrade.

2.6 TPD Version

The Tekelec Product Distribution (TPD) version needed for this release is included in the Policy Application software upgrade ISO, and TPD is upgraded to version 7.0.3 as part of this procedure.

In the case of IPM or clean install of a new server, the supported baseline TPD version 7.0.3 should be installed prior to upgrading to Policy Release 12.3.

2.7 Server Hardware Platforms

The Policy Management Release 12.2 software upgrade can be applied on any server that previously had Policy Management Release 12.2.x

2.8 Loading Application software

For upgrade of server application software, the recommended method is to copy the application ISO images to the servers using **scp** or **ftp**. If the system is HP c-Class using a PM&C Server, the application software must also be loaded into the PM&C software management library to support new installs and FRU activities.

NOTE: PM&C is not used during the upgrade and backout procedures.

2.9 Required Materials and Remote Access

1. Policy 12.3 software ISO files and TPD software ISO file
2. Policy 12.3 software upgrade Release Notes.
3. TVOE, PM&C upgrade/installation documentation, software ISO files, and TPD ISO file. (If applicable)
4. Firmware Upgrade Pack 2.2.9 (or higher) documentation and ISOs. (If applicable)

5. The capability to remote login to the target server as admusr.

   NOTE: The remote login can be done through SSH, local console, or iLO maintenance port. Ensure the network firewall policy allows the required application and corresponded ports.

6. The capability to secure copy (SCP) from the local workstation being used to perform this upgrade to the target server, or otherwise be able to transfer binary files to the target server.
7. User logins, passwords, IP addresses and other administration information.
8. VPN access to the network is required if that is the only method for remote logging into the target servers. It must be also possible to access the Policy Manager GUI, and the PM&C GUI.

2.9.1 Upgrade Media

See the release notes for the list of ISO image files required for the Policy Management upgrade you are installing.

2.9.2 Login Users and Passwords

Logins, passwords and server IP addresses

The IP address assignments for each site, from the appropriate Oracle Network IP Site Survey/NAPD, must be available. This ensures that the necessary administration information is available prior to an upgrade.

Further, need to confirm login information for key interfaces, and document in Table-1.

It is assumed that the logins are common among the sites. If not, record the password for each site.

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

Table-1: Logins, Passwords and Server IP Addresses

Item	Value
CMP servers	GUI Administrator Login User/Password:
	admusr password:
MRA/MPE servers	admusr password:
Target iLO	iLO Administrator Login: User/Password
Target OA	OA Administrator Login: User/Password
PM&C server	GUI Administrator Login User/Password:
	admusr password:
Software upgrade target release[1]	Target Release Number:
	Policy 12.3 software ISO Image (.iso) filenames.

[1] The ISO image filenames should match those referenced in the Release Notes for the target release.

3. THEORY OF OPERATION

3.1 Upgrade Manager Page

The Upgrade Manager represents a significant shift from some of the previous upgrade pages. In the past, it was up to you with assistance from an MOP to know the correct sequence of server selects and menu options. The Upgrade Manager takes a different approach. It determines the next course of action to either:

1. Begin/continue upgrading a cluster
2. Begin/continue backing out a cluster.

There is an important point implicit in the list above:

> Upgrade is now presented from a cluster perspective, instead of a server perspective.

The shift in perspective has a number of ramifications, most noticeably it is no longer possible to select individual servers or bulk select a group of servers. In fact, in order to perform any operation, it is necessary to select a cluster first.

Another major shift is that certain operations are performed automatically. These operations are not even presented as an option. However, you can see what has been performed by viewing the upgrade log.

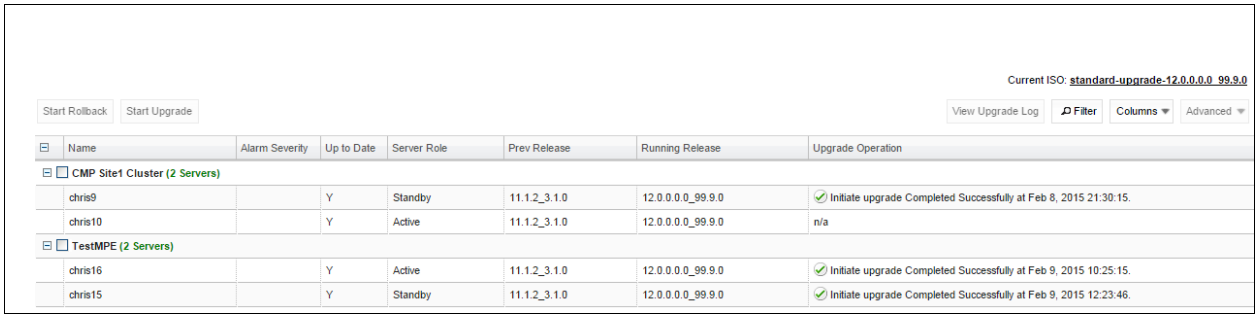


Figure 1: Sample display of the Upgrade Manager page.

For the most part, the items in the display are fairly self-explanatory. With that said, there are three items that deserve a deeper discussion.

- Start Rollback/Start Upgrade buttons (upper left)–If these buttons are greyed out, it means that there is not an appropriate action to take at this time. However, if a button is not greyed out, then it means that there is a preferred action that can be taken to upgrade (or backout) the cluster. Normally, upgrading a cluster is a well-defined fixed procedure. However, in some cases there are a number of valid sequences. Selecting the preferred step causes the Upgrade Director to choose the default sequence. It is strongly recommended to exclusively use these buttons to upgrade/backout a cluster.
- Alarm Severity–This column is used to indicate if there are alarms associated with a server. If so, it displays the severity of the most severe alarm here. It is important to explain the intent of this column. The intent is to give a visual indication that the particular server is experiencing alarms. This is not a reason to panic: During the upgrade we expect servers to raise alarms:
  - The CMP raises alarms to indicate that it is initiating upgrade activity.
  - Servers report alarms to indicate that their mate servers are offline.

However, if alarms are asserted for a server, it is good practice to look at the alarms prior to initiating upgrade activity on them.

- Up to Date–This column is used to indicate the state of the code on the server.
  - N

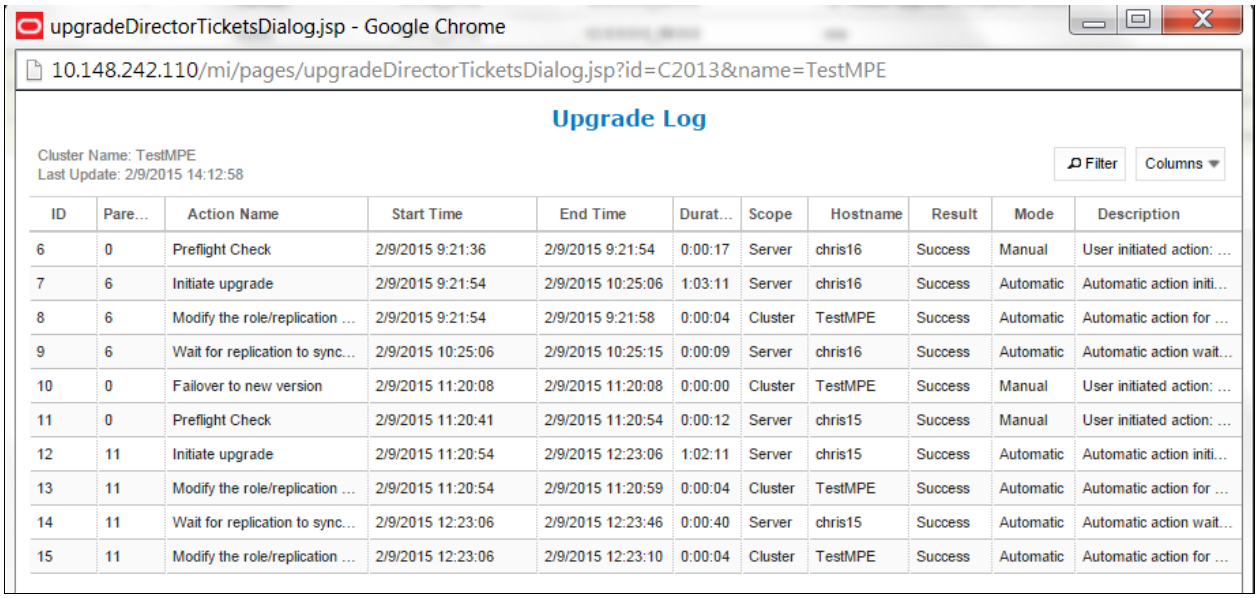
    The server is running old code needs to be upgraded
  - Y

    The server is running new code.
  - N/A

    Upgrade is not appropriate and/or the server is in a bad state

3.1.1 The Upgrade Log

You can access the upgrade log using the Upgrade Manager page. This displays attributes of the various actions (manual and automatic) that have been performed on the selected cluster. It is important to note that this is NOT the audit log. The audit log tracks what the has been done. This log captures the sequence of upgrade activity–whether it was initiated by you or automatically triggered.



ID	Pare...	Action Name	Start Time	End Time	Durat...	Scope	Hostname	Result	Mode	Description
6	0	Preflight Check	2/9/2015 9:21:36	2/9/2015 9:21:54	0:00:17	Server	chris16	Success	Manual	User initiated action: ...
7	6	Initiate upgrade	2/9/2015 9:21:54	2/9/2015 10:25:06	1:03:11	Server	chris16	Success	Automatic	Automatic action initi...
8	6	Modify the role/replication ...	2/9/2015 9:21:54	2/9/2015 9:21:58	0:00:04	Cluster	TestMPE	Success	Automatic	Automatic action for ...
9	6	Wait for replication to sync...	2/9/2015 10:25:06	2/9/2015 10:25:15	0:00:09	Server	chris16	Success	Automatic	Automatic action wait...
10	0	Failover to new version	2/9/2015 11:20:08	2/9/2015 11:20:08	0:00:00	Cluster	TestMPE	Success	Manual	User initiated action: ...
11	0	Preflight Check	2/9/2015 11:20:41	2/9/2015 11:20:54	0:00:12	Server	chris15	Success	Manual	User initiated action: ...
12	11	Initiate upgrade	2/9/2015 11:20:54	2/9/2015 12:23:06	1:02:11	Server	chris15	Success	Automatic	Automatic action initi...
13	11	Modify the role/replication ...	2/9/2015 11:20:54	2/9/2015 11:20:59	0:00:04	Cluster	TestMPE	Success	Automatic	Automatic action for ...
14	11	Wait for replication to sync...	2/9/2015 12:23:06	2/9/2015 12:23:46	0:00:40	Server	chris15	Success	Automatic	Automatic action wait...
15	11	Modify the role/replication ...	2/9/2015 12:23:06	2/9/2015 12:23:10	0:00:04	Cluster	TestMPE	Success	Automatic	Automatic action for ...

Figure 2: Upgrade Log

3.1.2 Optional actions

It is possible to perform every step in the upgrade process just using the **Upgrade** and **Backout** buttons. When you click these buttons, the Upgrade Director performs the next preferred action. However, there are times that you may want to take a slightly different–but legal–action. For example, the Upgrade Director has a preferred order in which it upgrades a cluster. However, if the you want to deviate from that default procedure–say to restrict upgrade to servers in a particular site–then you can use the optional actions menu. It is important to note that this menu is ONLY be populated with legal/reasonable actions. Actions that are wrong/inconsistent are not displayed.

If the you select an optional action, you can go back to using the default/preferred actions at any time

3.1.3 The ISO select

In the upper right hand corner, there is an item called the current ISO. In some respects the term ISO is misleading. A better description might be upgrade procedure. This item shows the upgrade procedure that is being used. In common cases, this is going to work out to either;

- A standard (full) upgrade to version XXX
- An incremental upgrade to version XXX

To start a upgrade, click this item. The Upgrade Director searches for valid upgrade procedures. In order to minimize confusion, these upgrade procedures are usually embedded within a CMP ISO. This way, the CMP ISO is tightly tied to the corresponding upgrade procedure.

When you select a new ISO, you are telling the Upgrade Director to abandon its current upgrade procedure in favor of a new procedure.

3.1.4 Introducing Upgrade Director behavior

The Upgrade Director is a component that tracks the state of the servers, cluster and system during an upgrade. The Upgrade Director is mostly hidden. However, there are conventions/operating principles that have visible effects.

3.1.4.1 Alarm philosophy

In general, the Upgrade Director raises alarms if:

1. A server is impaired.
2. An activity expected.

Table 2 summarizes the alarms that can be raised in 12.3.

Table 2 12.3 possible alarms

Alarm ID	Name	Description
70500	SYSTEM_MIXED_VERSION	The servers in the topology are running different versions of software. Upgrade of the system is not complete.
70501	CLUSTER_MIXED_VERSION	The servers in the specified cluster are running different versions of software. The upgrade of the cluster is not complete.
70502	REPLICATION_INHIBITED	Replication is inhibited to the specified server. It is not receiving session information.
70503	SERVER_FORCED_STANDBY	The specified server has been placed in forced standby and cannot provide service.
70506	UPGRADE_OPERATION_FAILED	An upgrade operation failed on the specified server.
70507	UPGRADE_IN_PROGRESS	An upgrade/backout is currently in progress on the server. It may leave the cluster, become unreachable or even reboot.
70508	ZOMBIE_SERVER	The server is in an indeterminate state and needs to be repaired by support.

3.1.4.2 General upgrade procedure

In general, the upgrade of a server goes through 3 steps.

1. Preflight checks–look for certain conditions which guarantee a failed upgrade. If such conditions are detected, fail. There are two principles behind the preflight checks
    a. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.
    b. Preflight checks are VERY narrow. We do not want a false positive preventing an otherwise valid upgrade.
2. The upgrade itself
3. Wait for replication to synchronize.

This procedure is in place so that it should not be necessary for you to login to the target server to verify conditions. They should be able to comfortably stay on the Upgrade Manager page.

3.1.4.3 Unreachable servers

During the course of an upgrade, servers can go unreachable. This is expected and the Upgrade Manager tries to be graceful about unreachable servers. However, if the CMP experiences a failover when another server is unreachable, this runs into limits. The Upgrade Director does not have the full history/context. It waits until it can contact the unreachable server before it takes action on the server.

3.1.4.4 Reversing directions

In general, it should be possible to reverse directions at any time. You should be able to upgrade a server in a cluster, back it out, upgrade it, upgrade its mate, back that out, and so on. In this sense, upgrade/backout should be fully reversible. However, you are permitted to reverse direction if there is an ongoing action: You cannot start a backout of a server if another server in the cluster is being upgraded. You have to wait for the upgrade to finish.

3.1.4.5 Mixed version and forced standby

As a general rule, if a cluster is in mixed version, then every server that is NOT running the same version as the active server needs to be in forced standby. This way, a simple failover does not cause a change in the version of code that is providing service.

3.1.4.6 Failure handling and recovery

Failures fall into two categories:

- Failures that the Upgrade Director is able to recover from.
- Failures that the Upgrade Director cannot automatically recover from.

Any failure should generate an UPGRADE_OPERATION_FAILED alarm. In such cases, the operation can be attempted again. Ideally, the original failure is investigated before repeating. However, if the server is in an indeterminate state, the server is declared a ZOMBIE and no further action can be taken on the server. It requires direct action by support/engineering to repair.

For the current release, recovery or even deep failure diagnosis, is not something that we expose via the GUI.

4. UPGRADE PREPARATION

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

4.1 Overview:

1. Upgrade TVOE and PM&C Server at Site 1 (if applicable)
2. Upgrade TVOE and PM&C Server at Site 2 (if applicable)
3. Firmware (if applicable)
4. Upgrade Primary (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Segment 1 Site 1:
    c. Upgrade MPE clusters
    d. Upgrade MRA clusters
    e. Upgrade Mediation clusters (If needed, recommend to upgrade UDR clusters first to compatible version)
7. Segment 1 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation clusters
8. Segment 2 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation clusters
9. Segment 2 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation clusters

4.1 Pre-requisites

Procedure 1 verifies that all required prerequisite steps needed to be performed before the upgrade procedure begins.

NOTE: TVOE, PM&C, and firmware might need to be upgraded prior to the upgrade to Policy Management Release 12.3.

Procedure 1 Prerequisite steps

Step	Procedure	Description
1. ☐	Verify all required materials are present	As listed in section: *2.9 Required Materials and Remote Access*
2. ☐	Review Release Notes	Review Policy Release 12.3 for the following information: • Individual Software components and versions included in target release • New features included in target release • Issues (Oracle BUGs) resolved in target release • Known Issues with target release • Any further instructions that may be required to complete the software upgrade for the target release. In particular, the supported browsers: **NOTE:** In release 12.3, only Mozilla Firefox and Google Chrome are fully supported.

4.2 TVOE and PM&C Server Upgrade

Policy Release 12.3 requires PM&C version 6.0.3 to support the IPM of TPD 7.0.3 on c-Class blades.

PM&C shall IPM TPD on a c-Class if the a blade is introduced either for disaster recovery (DR) or adding blades to an enclosure (foe example, capacity expansion).

Appendix A describes in detail the upgrade of TVOE and PM&C.

4.3 Firmware Upgrade

See the release notes for the list of ISO image files required for the firmware upgrade you are installing.

4.4 Plan and Track Upgrades

The upgrade procedures in this document are divided into the following three main sequential steps:

1. Upgrade TVOE and PM&C Server and deploy firmware upgrade if necesssary
2. Upgrade CMP clusters
3. Upgrade non-CMP clusters

Procedure 2 can be completed first before performing the upgrade, to identify the clusters to be upgraded and plan the work. It can also be used to track the completion of the upgrades, and assign work to different engineers.

NOTES:

- Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.
- Time estimates are for upgrade procedures without backout procedure. Backout procedure time is typically same as, or less than the upgrade procedure.

Procedure 2 Cluster information

Step	Procedure	Result	Engineer	Time
1. ☐	Use the following checklist to plan the cluster upgrades for the entire system.	Maintenance windows are planned		
2. ☐	Upgrade Site A and Site B TVOE/PM&C	Site Names _____ and _____		3 hrs
3. ☐	Upgrade Site1 and Site2 CMP clusters	Site Names _____ and _____		3 hrs
4. ☐	Upgrade Site1 non-CMP clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site2 clusters for Segment-1	Site Names _____ Cluster List:		2 hrs

Step	Procedure	Result	Engineer	Time
6. ☐	Upgrade Site1 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs
7. ☐	Upgrade Site2 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs

4.5 Convert to Using Interval Statistics

Prior to Release 12.3, Oracle Communications Policy Management offers two methods for gathering statistics: Manual and Interval statistics. They operate as follows:

- Manual. When configured to use this method, CMP records the cumulative values from the time the blade becomes active or when the statistics are manually reset. Statistics which represent maximum values contain the peak value since the blade became active or was reset. This is the system default.
- Interval. When configured to use this method, all counters reset automatically at the beginning of every interval and write the cumulative values at the end of the interval. Statistics which represent maximum values contain the peak value which occurred during the interval. The definable interval length can be 5, 10, 15, 20, 30 or 60 minutes. The default interval is 15 minutes.

In Oracle Communications Policy Management Release 12.3, Manual statistics are no longer be available. You must migrate to Interval statistics before upgrading to Release 12.3. Upon upgrade to R12.3, Oracle Communications Policy Management uses only Interval statistics and any Manual statistics not saved are lost.

Statistics affected by this change are reset to zero when migrating to Interval statistics. This affects both the information presented by the CMP GUI and the information returned using the OSSI interface. The values for statistics which are not counters, such as active session counts, are the same in both cases. The behavior of KPIIntervalStats is the same in both cases.

It is recommended that the following actions are taken in advance of the upgrade procedure:

1. Review your current configuration to determine which statistics method is currently being used by navigating to **GLOBAL CONFIGURATION → Global Configuration Settings → Stats Settings**.
2. If Manual is being used, change the Stats Reset Configuration parameter to Interval.
3. Review any systems which access this information via OSSI to determine whether they must be modified.

For completeness and assuredness, it is recommended to collect at least 24 hours of interval statistics before upgrading to 12.3

For addition information, see the following publications:

- *Configuration Management Platform User's Guide*
- *OSSI XML Interface Definitions Reference*

4.6 Perform System Health Check

This procedure determines the health and status of the servers to be upgraded and must be performed at least once within the time frame of 24 to 36 hours prior to the start of a maintenance window.

Step	Procedure	Result
1. ☐	CMP GUI access	Open a supported browser (Mozilla Firefox or Google Chrome) to access the Primary CMP GUI on its VIP address and login to verify access.
2. ☐	View active alarms	Identify the cause of any existing active alarms, and determine if these may have impact on the upgrade. Export current alarms to save into a file. ***IMPORTANT: Before starting any upgrade activity, ensure that all active alarms are resolved.***
3. ☐	View KPI reports	Verify that the system is running within expected parameters. Export current KPIs to save into a file.

4. ☐	Confirm NTP servers reachable from all the servers (CMP and non-CMP) to be upgraded
	NOTE: If the time across the servers is out of synch, fix it first and re-validate this step, before starting the upgrade procedures.
		1. Validate the IP connectivity between the server and NTP servers with **`ping`** command.
		2. Confirm that time is synchronized on each server with CLI shell command of:
		`ntpq -np`
		3. Confirm the date is correct on each server.
		4. Check that BIOS clock is synchronized with the clock using the shell command:
		`hwclock`

THIS PROCEDURE HAS BEEN COMPLETED		

4.7 Deploy Policy Upgrade Software

Software should be deployed to each policy server `/var/TKLC/upgrade` directory before the actual upgrade activities. This is typically done using the Upgrade Manager. Because of the large size of the software ISOs, sufficient time should be planned to accomplish this step. For Policy Release 12.3, each ISO image size is approximately 1.0 Gigabytes.

4.7.1 Deploying Policy Upgrade Software to Servers

There are several possible software images in this upgrade (CMP, MPE, MPE-LI, MRA, and Mediation). A single image must be deployed to the upgrade (`/var/TKLC/upgrade`) directory of each server to be upgraded. The image must be the correct type for that server. For example, the CMP software image must be deployed to CMP servers, the MPE image must be deployed to the MPE servers, the MRA image must be deployed to the MRA servers and so on.

IMPORTANT: If the deployed image type (CMP, MPE, MRA, Mediation,and so) does not match the existing installed software type, the upgrade fails. Example: an attempt to upgrade a CMP with an MPE software image fails during the upgrade action.

NOTE: To change a server from one application type to another, the server must first be cleaned of all application software by an Install OS action via the PM&C GUI, and then the new application type installed.

If multiple images are copied into the `/var/TKLC/upgrade` directory, the upgrade fails.

4.7.2 Copy ISO image files to the Management Server (PM&C)

NOTE: Not all Policy Management systems use a PM&C server. If you do not use PM&C, skip to section *4.7.3*.

This procedure transfers software upgrade ISO files to the PM&C servers at each site to be upgraded, and loads ISO files into the PM&C Software Image repository. This is done as a placeholder for future use of the software.

PM&C is not used for the upgrade activities. The purpose of this step is to be prepared for server recovery activities in case a server needs to be re-installed with software.

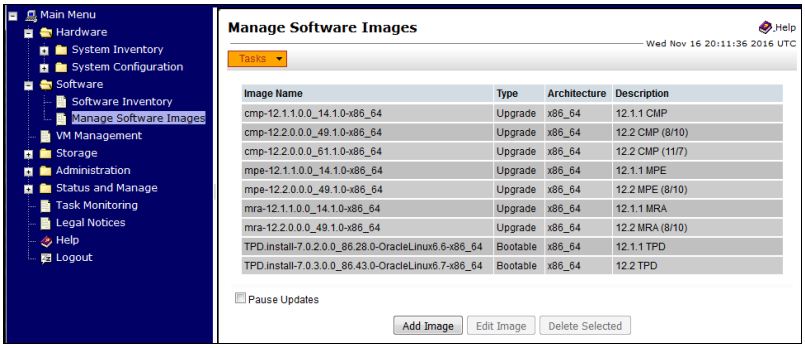
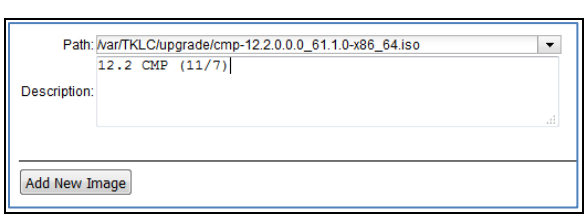
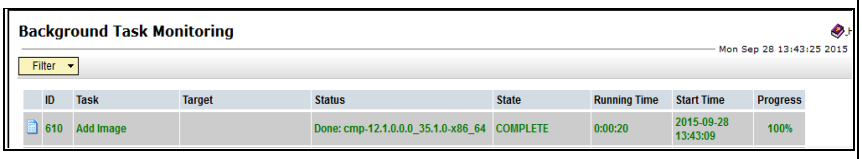
NOTE: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

NOTE: Because the ISO images are large, the procedure includes instructions to check space available in the `/var/TKLC/upgrade` directory before copying the ISOs to this directory. After the Add Image action on the PM&C, the ISO images are registered in PM&C, and stored in the `/var/TKLC/smac/image/repository` directory which is very large.

Step	Procedure	Result
1. ☐	**PM&C GUI:** Verify no Release 12.3 ISO files exist.	1. Log on to the PM&C Server GUI 2. Navigate to **Software → Manage Software Images**. 3. Confirm no release 12.3 ISO files already exist. If there are, remove them.

2. ☐	SSH to PM&C server as admusr	1. Log on as admusr to the PM&C server.
		2. Change target directory to `/var/TKLC/upgrade` and ensure there is at least of 3.0 GB free disk space available.
		`$cd /var/TKLC/upgrade`
		`$df –h /var/TKLC`
		NOTE: There may be ISOs in the `/var/TKLC/upgrade` directory, they can be removed to free up disk space or added to the PM&C repository.

3. ☐	Copy Release 12.3 ISO files to the target directory in the PM&C server	Transfer all required Release 12.3 ISO files (CMP, MPE/MPE-Li, MRA, Mediation) into directory `/var/TKLC/upgrade` via either the following methods: • SCP/WGET command in the following steps outline in this Procedure • USB drive

Step	Procedure	Result
4. ☐	**PM&C GUI:** Adding Release 12.3 ISO files	1. Navigate to **Software → Manage Software Images**. 2. Click **Add Image** to select the ISO files that are just transferred into PM&C server.   3. Click **OK** on the pop-up
5. ☐	**PM&C GUI:** Verify the ISO files are added successfully	Navigate to **Software → Manage Software Images**. The status of the image being added can be monitored via the Task Monitoring menu with the screen display as the following:  **NOTE:** The added ISO files are now stored in the `/var/TKLC/smac/image/repository` directory.
THIS PROCEDURE HAS BEEN COMPLETED		

4.7.3 Distribute Application ISO image files to servers

This procedure applies to all server types. It assumes that the ISO image files are electronically copied to the sites 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. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

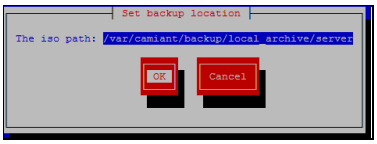
Step	Procedure	Result

1. ☐	Transfer ISOs to Policy Servers.	Transfer release 12.3 ISO files (CMP and non-CMP) into the directory `/var/TKLC/upgrade` on the respective server via either of the following methods:
		• SCP/WGET command
		• USB drive
		Or, if the images are on a server on the same network, scp via CLI.
		Copy CMP software ISO to ONE of the other CMP servers:
		`$sudo scp 872-* <cmp-12.3x>:/var/TKLC/upgrade/`
		Copy MPE software ISO to ONE of the other MPE servers:
		`$sudo scp 872-* <mpe-12.3x>:/var/TKLC/upgrade/`
		Copy MPE-Li software ISO to ONE of the other MPE-Li servers:
		`$sudo scp 872-* <mpe-li-12.3x>:/var/TKLC/upgrade/`
		Copy MRA software ISO to ONE of the other MRA servers:
		`$sudo scp 872-* <mra-12.3x>:/var/TKLC/upgrade/`
		Copy Mediation software ISO to ONE of the other Mediation servers:
		`$sudo scp 872-* <mediation-12.3.x.x.x>:/var/TKLC/upgrade/`
		NOTE: After copying the ISO to one of the respective servers, the ISO Maintenance option is used to upload to the remaining servers.

THIS PROCEDURE HAS BEEN COMPLETED		

4.7.4 Backups and Backup Locations

Step	Procedure	Result

1. ☐	**SSH CLI/ iLO**: Access the server to be backed up
	
	NOTE: System Backup is done on Active CMPs ONLY
		IMPORTANT: Server backups (for all CMP and non-CMP active and standby servers), and the system backup (from the active CMP), must be collected and readily accessible for recovery operations.
		
		1. Login into the ACTIVE Primary CMP server.
		2. Open the platcfg utility.
		`$sudo su-platcfg`
		3. Navigate to **Policy Configuration→Backup and Restore→Server Backup**.
		Enter the ISO backup filename (or use the suggested one) in the default backup location path:
		`/var/camiant/backup/local_archive/serverbackup/<serverbackup.iso>`
		 
		4. Click **OK**.
		5. Go back to the previous menu (**Policy Configuration→Backup and Restore**) and select **System Backup**
		6. Provide a tarball backup filename (or use the suggested one) in the default backup location path:
		`/var/camiant/backup/local_archive/systembackup/<systembackup.tar.gz>`

2. ☐	**SSH CLI/iLO:** Verify the backup file	If the default location is accepted in the previous step, change directory to the following and verify file exists:
		`$ cd /var/camiant/backup/local_archive/serverbackup`
		`$ ls <hostname>-<servertype>_x…x-serverbackup-<yyyy><mm><dd><hhmm>.iso`
		And:
		`$ cd /var/camiant/backup/local_archive/systembackup`
		`$ ls <hostname>-cmp_x…x-systembackup-<yyyy><mm><dd><hhmm>.tar.gz`

Step	Procedure	Result

3. ☐	Copy backup files.	Copy the ISO and tarball files to a safe location, for example, for a server backup file:
		`$sudo scp -p /var/camiant/backup/local_archive/serverbackup/<serverbackup>.iso <remoteserverIP>:<destinationpath>`
		Another option is to scp the server and system backup files to your local workstation.
		After copying to remote server/workstation, remove the backup files from the server.
		`$sudo rm <serverbackup>.iso`

4. ☐	Identify backup location	Backup location is: _____ Instructions to access to backups are as follows: _____ _____ _____
THIS PROCEDURE HAS BEEN COMPLETED		

4.7.5 Changing Non-Default root and admusr Passwords

4.7.5.1 Improve Password Security

The default password hash prior to Policy 12.0 is MD5. MD5 is now considered a weak hash that can be brute-force cracked in a reasonable amount of time. The best hash to use is SHA512. This is currently the strongest hash supported on the platform. Due to this change, during upgrade all non-default passwords are automatically expired. This may cause issues during upgrade from pre-12.2 to 12.3 and above. To prevent those issues, the following procedure has been created.

4.7.5.2 Impact

After this procedure is run, the root and admusr password are hashed with the strongest possible method, SHA512.

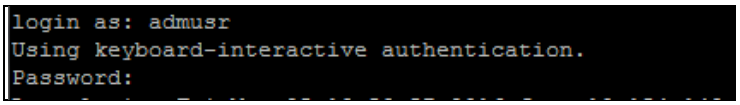
This procedure only addresses root and admusr passwords. Other users should also update their password to benefit from the new hashing. If they are not changed prior to the upgrade to 12.3, they are expired post upgrade.

The following procedure must be perfromed prior to the upgrade to 12.3 only if the root or admusr passwords are non-default.

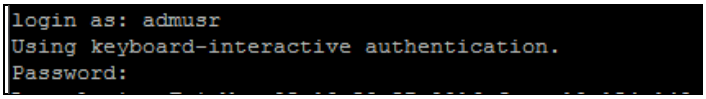
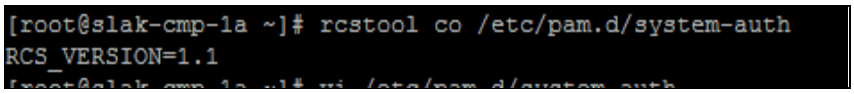
Order to perform this procedure on an In-Service Policy Management

1. Standby CMPs
2. Active CMPs
3. Standby MPEs/MRAs/Mediations

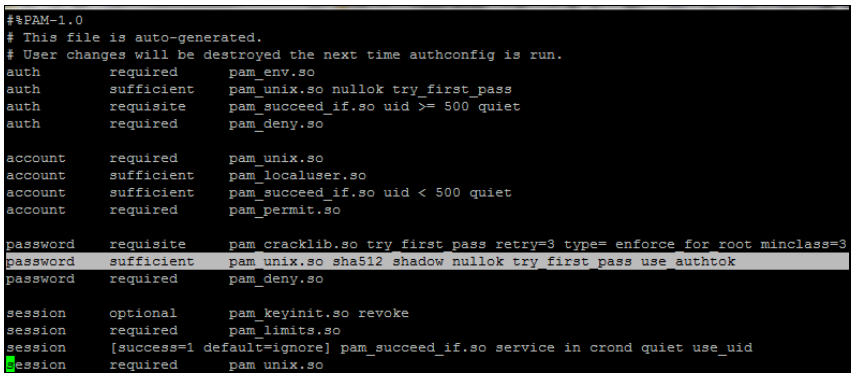
4. Active MPEs/MRAs/Mediations

Step	Procedure	Result
1. ☐	Login to the every server	Login as admusr and change to root using the following command: `$sudo su` 

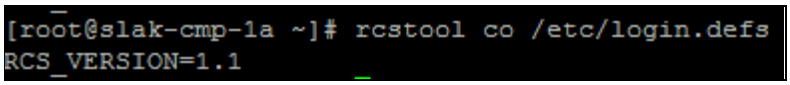
2. ☐	Check the password field of root and admusr	Issue the following
		`#egrep '^(root|admusr)' /etc/shadow`
		Example output:
		`root:$6$mErKrEsA$83n5G8dR3CgBJjMEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc.Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7:::`
		`admusr:$6$mUstAfa$gn2B8TsW1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825::::::`
		If the first two characters after the colon (:) is $6, then this procedure is not needed on this server. Skip to section 5.
		If the first two characters after the colon are not $6, then it is probably $1 (MD5) and this procedure should be followed for this server. Continue on with step 4

3. ☐	Order to perform the change	Perform steps 4 through 17 in the following order: 1. Standby CMPs 2. Active CMPs 3. Standby non-CMP servers 4. Active non-CMP servers
4. ☐	Login to the server as admusr	Login as admusr and change to root using the following command: `$sudo su` 
5. ☐	Checkout revisions	Issue the following command. `#rcstool co /etc/pam.d/system-auth` 

Step	Procedure	Result

6. ☐	Modify the `system-auth` file	1. Open the `system-auth` file:
		`#vi /etc/pam.d/system-auth`
		2. Modify the file. Change the following line from md5 to sha512
		Modify the below line with sha512 instead of md5 (Current line indicates currently configured in server. Modified Line indicates modification which needs to be implemented)
		Current Line:
		`password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok`
		Modified Line:
		`password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok`
		 

7. ☐	Save the file	If the file required changing
		`#rcstool ci /etc/pam.d/system-auth`
		If the file was already configured
		`#rcstool unco /etc/pam.d/system-auth`

8. ☐	Checkout revisions for `login.defs`	`#rcstool co /etc/login.defs` 

9. ☐	Edit login.defs	Shadow password suite configuration.
		1. Open the `login.defs` file:
		`#vi /etc/login.defs`
		2. Modify the below line with SHA512 instead of MD5
		Current Line: ENCRYPT_METHOD MD5
		Modified Line: ENCRYPT_METHOD SHA512
		NOTE: The line to edit is at the bottom of the file
		3. Comment out the following line if necessary:
		`MD5_CRYPT_ENAB yes`

Step	Procedure	Result

10. ☐	Save the File	If the file required changing
		`#rcstool ci /etc/login.defs`
		if the file already was configured
		`#rcstool unco /etc/login.defs`

11. ☐	Checkout revisions for `libuser.conf`	`# rcstool co /etc/libuser.conf`
		`[root@slak-cmp-1a ~]# rcstool co /etc/libuser.conf`
		`RCS_VERSION=1.1`

12. ☐	Edit `libuser.conf`	1. Open the `libuser.conf` file: `#vi /etc/libuser.conf` 2. Modify the below line with sha512 instead of md5 **Current Line:** crypt_style = md5 **Modified Line:** crypt_style = sha512 **NOTE:** The line to edit is close to the top of the file.

13. ☐	Save the File	If the file required changing
		`#rcstool ci /etc/libuser.conf`
		if the file already was configured
		`#rcstool unco /etc/libuser.conf`

14. ☐	Set the admusr and root passwords	For root user
		`#passwd root`
		For admusr user
		`#passwd admusr`

15. ☐	Verify	Logout of the current session and re-login using the new password credentials.
THIS PROCEDURE HAS BEEN COMPLETED		

5. PRE-UPGRADE TASKS (12.2.X TO 12.3)

5.1 Accepting Previous Upgrade

This is ONLY applicable if any previous Policy Management upgrade on all clusters has not been accepted, otherwise skip this section and go directly to the next section. If a previous upgrade was not accepted, after the first server of a cluster is upgraded, upgrade of the second server fails validation.

Use Accept Upgrade to accept the previous upgrade. This function removes backout information. After upgrade is accepted for any server in a cluster, that cluster cannot be rolled back.

This procedure must be done during Maintenance hours to avoid any possible interruption to the Policy operation. Some of the steps may impact the Session processing during the execution.

NOTE: If a server fails after an upgrade is accepted, you must accept the upgrade again for the replacement server.

This procedure accepts the previous upgrade for a cluster.

PREREQUISITES:

If a upgrade status for the server is Pending and the alarm 32532 (Upgrade Pending Accept/Reject) is active as shown in the screenshot below, then this procedure is required for the clusters. Otherwise, skip this section and goto the next procedure of performing CMP clusters upgrade.

Navigate to CMP GUI: **System Wide Reports →Alarms→ Active Alarms**.

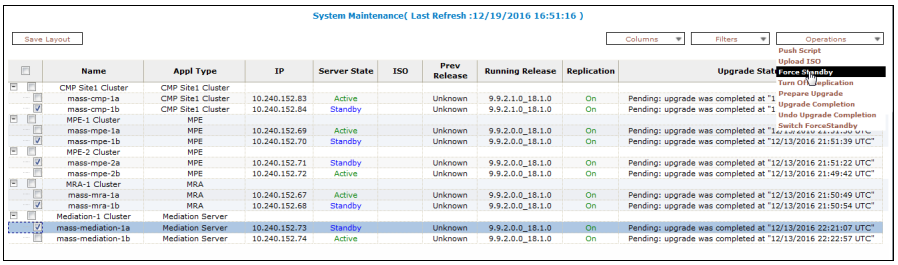
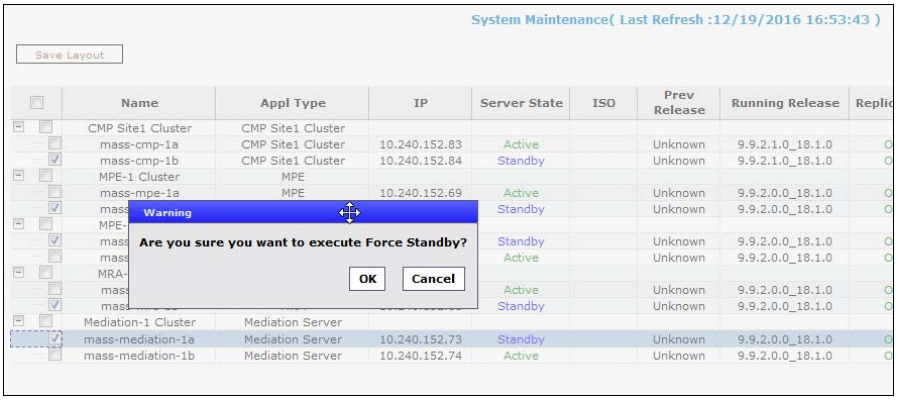
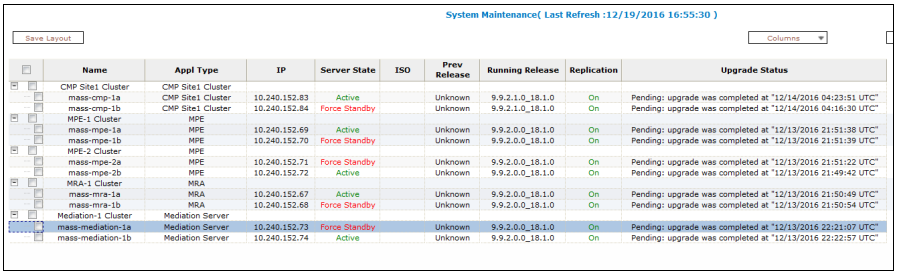
Dec 14, 2016 05:35 PM EST	Minor	32532	Server Upgrade Pending Accept/Reject		mass-mediation-1b 10.240.152.74	
Dec 14, 2016 05:27 PM EST	Minor	32532	Server Upgrade Pending Accept/Reject		mass-mediation-1a 10.240.152.73	

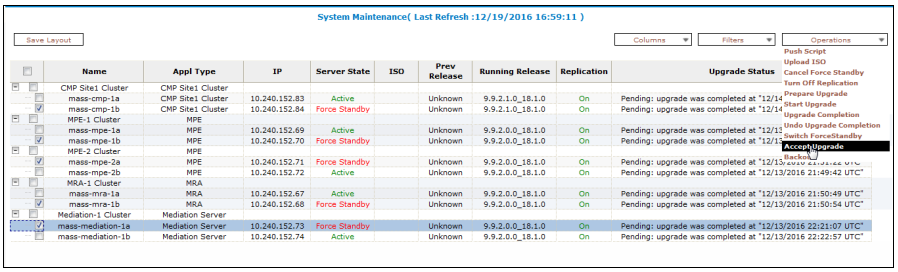
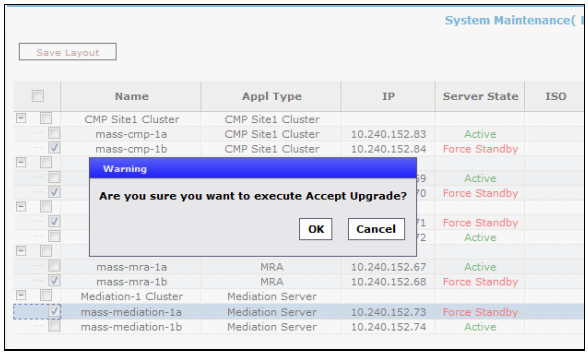
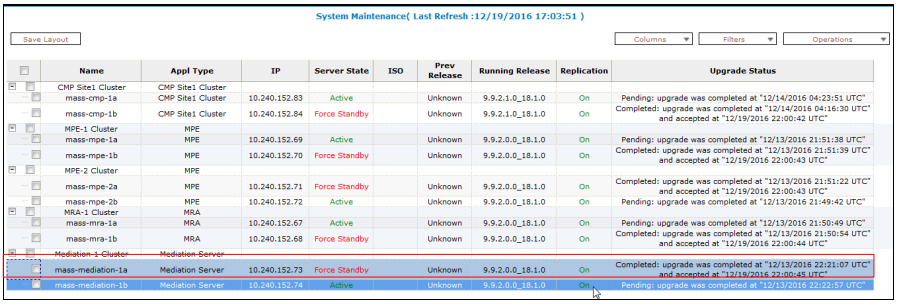
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **Upgrade → System Maintenance**. 2. Confirm the existing alarm 32532 (Upgrade Pending Accept/Reject) as shown in the example below, and note the impacted clusters.

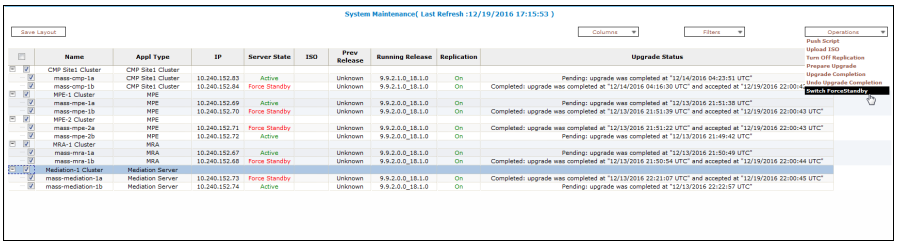
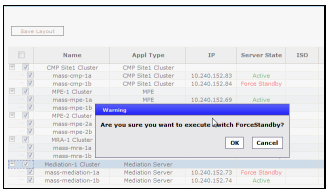
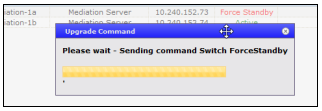
System Maintenance(Last Refresh :12/19/2016 16:49:10)

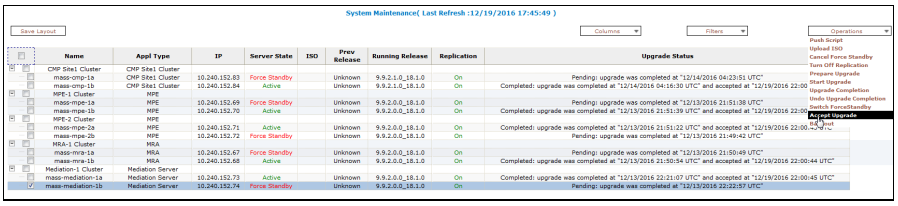
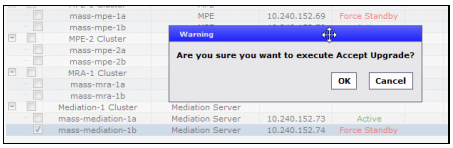
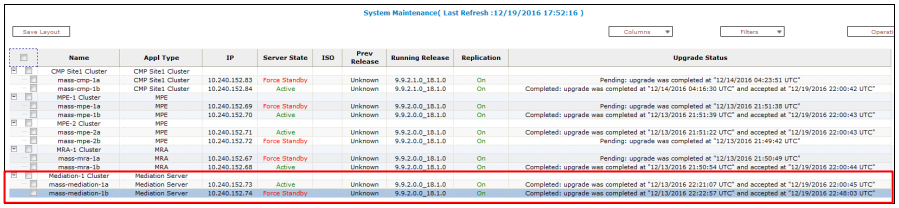
Save Layout | Columns

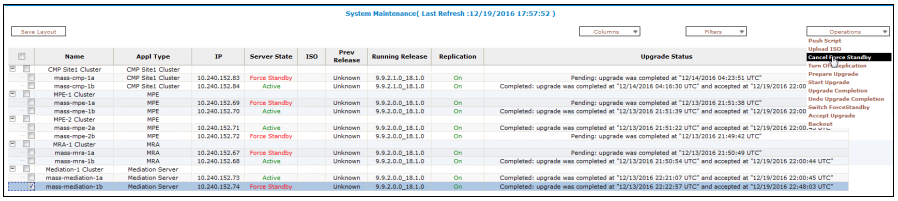
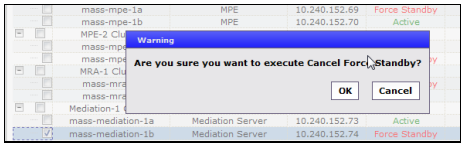
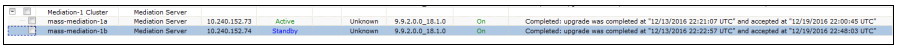
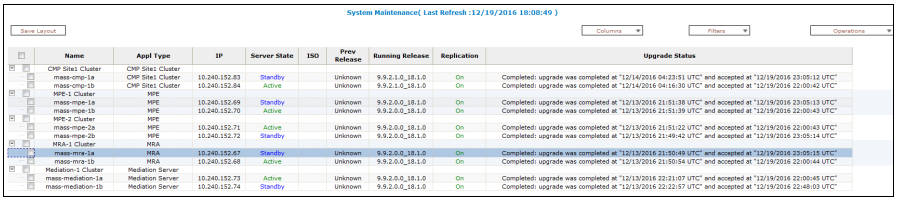
Name	Appl Type	IP	Server State	ISO	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster							
mass-cmp-1a	CMP Site1 Cluster	10.240.152.83	Active		Unknown	9.9.2.1.0_18.1.0	On	Pending: upgrade was completed at "12/14/2016 04:23:51 UTC"
mass-cmp-1b	CMP Site1 Cluster	10.240.152.84	Standby		Unknown	9.9.2.1.0_18.1.0	On	Pending: upgrade was completed at "12/14/2016 04:16:30 UTC"
MPE-1 Cluster	MPE							
mass-mpe-1a	MPE	10.240.152.69	Active		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:51:38 UTC"
mass-mpe-1b	MPE	10.240.152.70	Standby		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:51:39 UTC"
MPE-2 Cluster	MPE							
mass-mpe-2a	MPE	10.240.152.71	Standby		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:51:22 UTC"
mass-mpe-2b	MPE	10.240.152.72	Active		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:49:42 UTC"
MRA-1 Cluster	MRA							
mass-mra-1a	MRA	10.240.152.67	Active		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:50:49 UTC"
mass-mra-1b	MRA	10.240.152.68	Standby		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 21:50:54 UTC"
Mediation-1 Cluster	Mediation Server							
mass-mediation-1a	Mediation Server	10.240.152.73	Standby		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 22:21:07 UTC"
mass-mediation-1b	Mediation Server	10.240.152.74	Active		Unknown	9.9.2.0.0_18.1.0	On	Pending: upgrade was completed at "12/13/2016 22:22:57 UTC"

Step	Procedure	Result
2. ☐	**CMP GUI:** Put the impacted server into force-standby	1. Navigate to **Upgrade → System Maintenance**. 2. Select the Standby server of the impacted cluster with the alarm 32532. 3. Select **Operations → Force-Standby.**  4. Click **OK** to proceeed and wait for few seconds or so to have the status changed.  5. Verify that the server is now in Force Standby status. 

Step	Procedure	Result
3. ☐	**CMP GUI:** Accept the upgrade on the Force Standby server	1. Navigate to **Upgrade → System Maintenance**. 2. Select the server with the Force Standby status. 3. Select **Operations → Accept Upgrade.**  4. Click **OK** to proceeed and wait for few seconds or so to have the status changed.  **NOTE:** After the Accept Upgrade completes, alarm 32532 (Upgrade Pending Accept/Reject) on the impacted servers is cleared, while the remaining servers have the alarm. Continue with the following steps to clear the alarm. 5. Verify the highlighted server is associated with Completed: upgrade was completed at < *timestamp* > and accepted at <*timestamp*> message. 

Step	Procedure	Result
4. ☐	**CMP GUI**: Switch the Force-Standby servers	1. Navigate to **Upgrade → System Maintenance**. 2. Select the server with the Force Standby status. 3. Select **Operations → Switch ForceStandby**.  4. Click **OK** to proceeed and wait for a minute or so to have the status changed.   **NOTE:** The previously Forced-Standby server becomes the active server now and the previously active server becomes the Forced-Standby server now. During this time, thereis a critical alarm 70001 raised, This is expected and is cleared after the successful switchover. There could be Policy session processing interruption.

Step	Procedure	Result
5. ☐	**CMP GUI:** Accept the upgrade on the switched Force Standby server	1. Navigate to **Upgrade → System Maintenance**. 2. Select the server with the Force Standby status. 3. Select **Operations → Accept Upgrade.**  4. Click **OK** to proceed. Wait until the status changes.  **NOTE:** After the Accept Upgrade is completed, the alarm 32532 (Upgrade Pending Accept/Reject) on the impacted servers is cleared similar to the last step. The remaining servers have the alarm. Continue with the following steps to clear the alarm. 5. Verify that both servers of this same cluster are now associated with the Completed: upgrade was completed at < *timestamp* > and accepted at <*timestamp*> message. 

Step	Procedure	Result
6. ☐	**CMP GUI:** Cancel Force-Standby on the server	1. Navigate to **Upgrade → System Maintenance**. 2. Check the server with the Force Standby status and select **Operations → Cancel Force-Standby** as shown in the example below.  3. Click **OK** to proceeed and wait for few seconds or so to have the status changed to Standby as shown in the example below.  4. Verify that the server shown in the highlighted Upgrade Status message as shown in the example below. 
7. ☐	Continue to perform Accept Upgrade to the remaining impacted clusters	Repeat steps 2 through 6 for each cluster that requires this procedure. All alarm 32532 (Upgrade Pending Accept/Reject) should be cleared after the Accept Upgrade procedure is applied to all impacted clusters as shown in the example below . 

6. UPGRADE CMP CLUSTERS (12.2.X TO 12.3)

Following the upgrade sequence outlined in previous Section 2.3, the Primary CMP cluster are upgraded first, and followed by the Secondary CMP cluster (if applicable). If the Policy system is deployed with only one CMP cluster, then the subsequent upgrade sequence of the Secondary CMP cluster can be skipped.

6.1 Upgrade CMP Clusters Overview

6.1.2 Upgrade Sequence For Primary CMP cluster

1. Use the CMP GUI–System Maintenance (12.2.x) place Primary Standby CMP server into Frc-Stby.
2. Use the CMP GUI–System Maintenance (12.2.x), to upgrade the Primary Frc-Stby CMP server
3. Use the CMP GUI–System Maintenance (12.2.x), to perform Switch Frc-Stby on the Primary CMP cluster
4. Log back into the CMP GUI and upgrade the remaining Frc-Stby Primary CMP server using the 12.3 Upgrade Manager

6.1.3 Upgrade Sequence For Secondary CMP cluster (if applicable)

Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the Secondary CMP cluster.

1. Start Upgrade
2. Continue Upgrade—Failover
3. Continue Upgrade

This procedure should not be service affecting, but it is recommended to perform during the Maintenance hours.

It is assumed that the CMPs may be deployed as 2 Geo-Redundant clusters, identified as Site1 and Site2 as displayed on the CMP GUI. When deployed as such, one site is designated as the Primary site (which is the site that is managing the Policy system), and the other is as Secondary site (this site is ready to become Primary site, if needed).

Identify the CMPs sites to be upgraded here, and verify which sites are Primary and Secondary:

CMP Sites Status	Operator Site Name	Site Designation from Topology Form (Site1 or Site2)
Primary Site		
Secondary Site		

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP _____

Server-A Status _____

Server-B Hostname _____

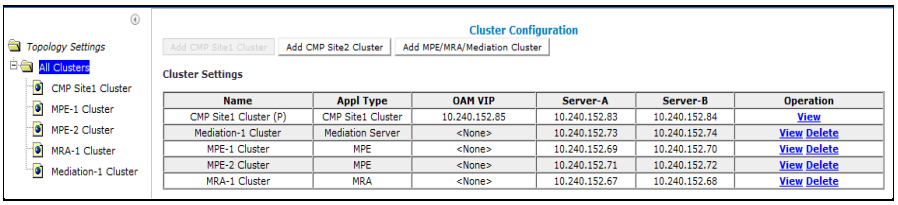
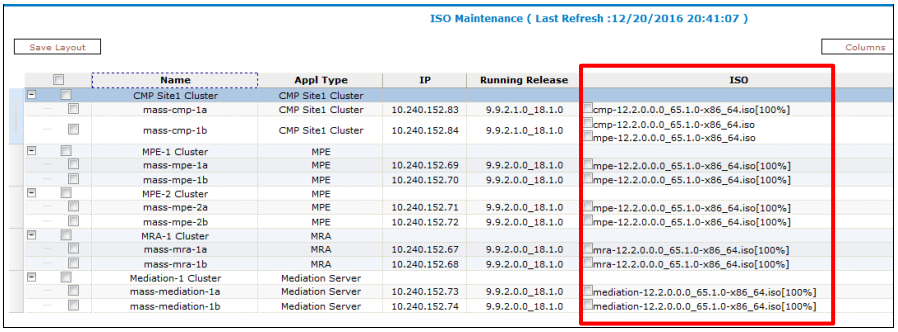
Server-B IP _____

Server-B Status _____

IMPORTANT:

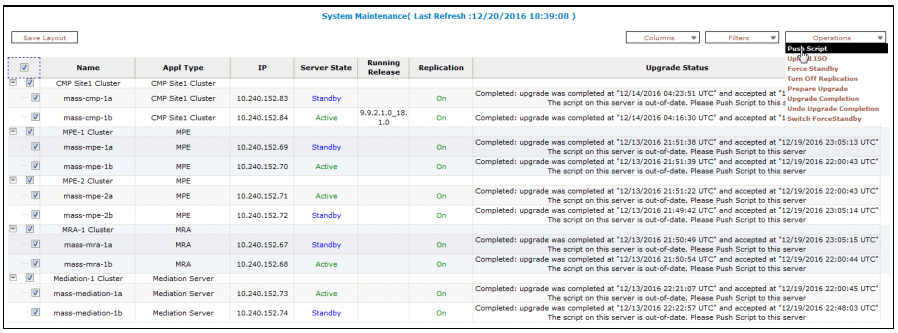
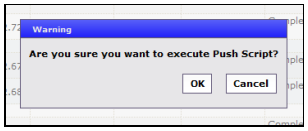
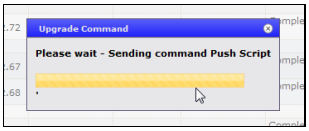
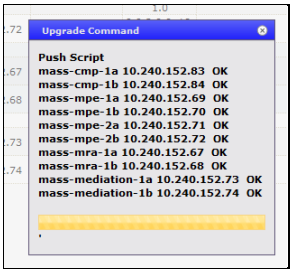
- CMP servers MUST be upgraded first, before the MPE, MRA and Mediation (Mediation) clusters
- Primary CMP cluster MUST be upgraded to the new release first, before the Secondary CMP cluster (if applicable)

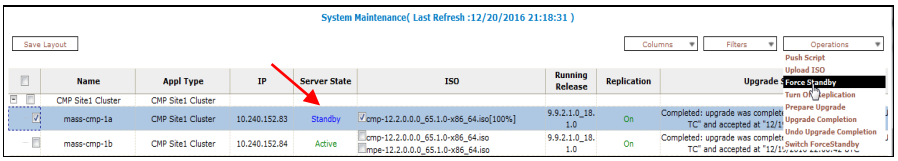
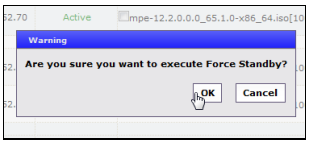
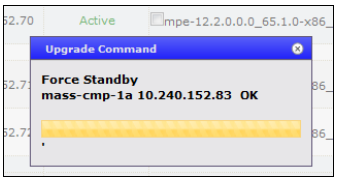
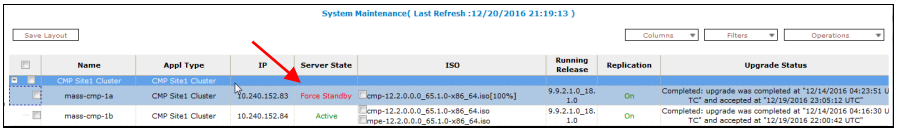
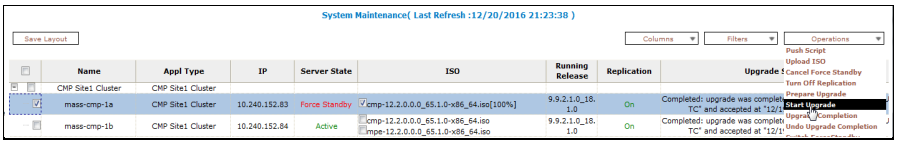
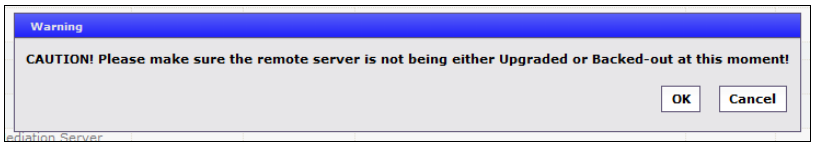
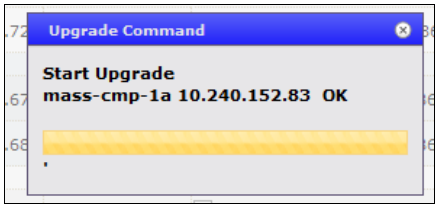
6.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **System Wide Reports →Alarms→ Active Alarms**. 2. Confirm that any existing alarm displayed on the Primary active CMP server has no impact to the upgrade procedure. 3. Capture a screenshot and save it into a file for reference.
2. ☐	**CMP GUI:** Identify and Record the CMP cluster(s)	1. Navigate to **Platform Settings → TOPOLOGY Settings**.  2. Note the Primary CMP cluster is labelled as a (P), and if applicable, the Secondary CMP cluster is labelled as a (S). 3. Save the screenshot for future reference.
3. ☐	**CMP GUI**: Verify status of Primary CMP cluster	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Confirm the Primary CMP cluster has the following: - The servers have both the Active and Standby status - Running Release of 12.2.x version. **NOTE:** The CMP is on the patch version labelled as 12.2.x. - Replication ON - Corresponding Release 12.3 ISO files have already been copied[1] to all cluster types (CMP/MRA/MPE/Mediation) as shown in the screenshot example below. **NOTE:** Assuming the Release 12.3 ISO files were already successfully transferred from Section 4.6 Procedure. 

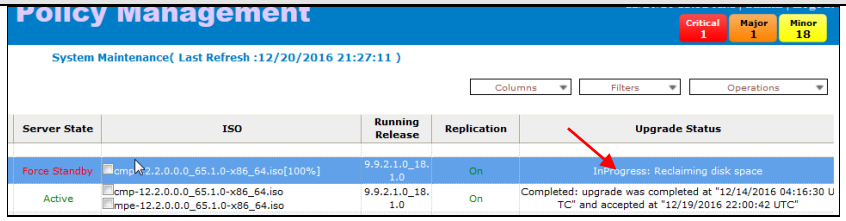
Step	Procedure	Result

4. ☐	**SSH CLI Primary Active CMP:** Acquire Release 12.2 upgrade scripts and Exchange SSH keys	1. Login to Active Primary CMP with root privilege.
		2. Mount the Release 12.3 CMP ISO as shown in the example below -
		`# mount -o loop /var/TKLC/upgrade/< R12.3 CMP ISO filename> /mnt/upgrade/`
		3. Copy the upgrade scripts with the following commands -
		`# cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		4. Unmount the /mnt/upgrade NFS link
		`# cd /`
		`# umount /mnt/upgrade`
		5. Exchange SSH keys with the remaining clusters with login as admusr with the following shell command and expected results as shown in the screenshot example below.
		`# qpSSHKeyProv.pl --prov --user=admusr`
		`[root@mass-cmp-1b /]# qpSSHKeyProv.pl --prov --user=admusr`
		`The password of admusr in topology:`
		`Connecting to admusr@mass-mra-1b ...`
		`Connecting to admusr@mass-mpe-2b ...`
		`Connecting to admusr@mass-cmp-1a ...`
		`Connecting to admusr@mass-mpe-2a ...`
		`Connecting to admusr@mass-cmp-1b ...`
		`Connecting to admusr@mass-mpe-1a ...`
		`Connecting to admusr@mass-mediation-1b ...`
		`Connecting to admusr@mass-mediation-1a ...`
		`Connecting to admusr@mass-mpe-1b ...`
		`Connecting to admusr@mass-mra-1a ...`
		`[1/10] Provisioning SSH keys on mass-mpe-2b ...`
		`[2/10] Provisioning SSH keys on mass-mra-1b ...`
		`[3/10] Provisioning SSH keys on mass-cmp-1a ...`
		`[4/10] Provisioning SSH keys on mass-mpe-2a ...`
		`[5/10] Provisioning SSH keys on mass-cmp-1b ...`
		`[6/10] Provisioning SSH keys on mass-mpe-1a ...`
		`[7/10] Provisioning SSH keys on mass-mediation-1b ...`
		`[8/10] Provisioning SSH keys on mass-mediation-1a ...`
		`[9/10] Provisioning SSH keys on mass-mpe-1b ...`
		`[10/10] Provisioning SSH keys on mass-mra-1a ...`
		`SSH keys are OK.`

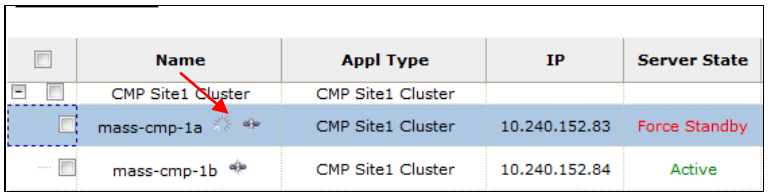
Step	Procedure	Result
5. ☐	**CMP GUI**: Push the Release 12.3 upgrade scripts to all clusters in the segment topology	1. Navigate to **Upgrade Manager → ISO Maintenance**. 2. Select all the clusters in the Topology as shown and select **Operations → Push Scripts**.  3. Click **OK** to continue the operation.   Script push operation successful as shown in the example below. 

Step	Procedure	Result
6. ☐	**CMP GUI**: Set Force-Standby mode on the Standby server at Primary CMP cluster	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Check the Standby CMP Server at Primary CMP cluster and select **Operations → Force Standby.**  3. Click **OK** to confirm and continue with the operation.   The Standby CMP server state changes to Force Standby. 
7. ☐	**CMP GUI:** Upgrade the Primary Force-Standby CMP server **NOTE:** Each server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Select the Force-Standby CMP server at the Primary CMP cluster. 3. Select **Operations → Start Upgrade**.  4. Click **OK** to continue with the operation.   In the Upgrade Status column, it shows the InProgress:… message along with the various upgrade activities. This process typically takes aboutapproximately 40 minutes to complete.

Step	Procedure	Result



NOTE: There are a spinner and Sync-broken icons displayed next to the CMP server being upgraded as expected.



The following alarms are expected during the course of upgrade in-progress.

Expected Critical Alarm

31283 High availability server is offline

Expected Major Alarms

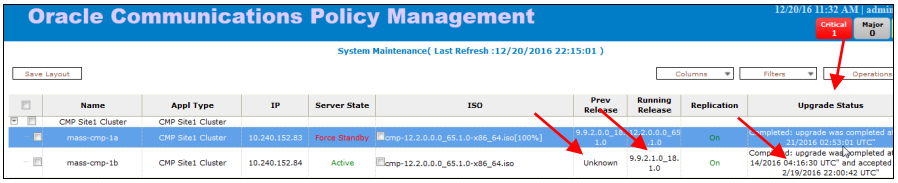
31233 HA Path Down
70004 The QP processes have been brought down for maintenance.
70021 The MySQL slave is not connected to the master

Expected Minor Alarms

31114 DB Replication of configuration data via SOAP has failed
31106 DB merging to the parent Merge Node has failed
31107 DB merging from a child Source Node has failed
31101 DB replication to a slave DB has failed

After the upgrade is completed successfully, the following displays changed:

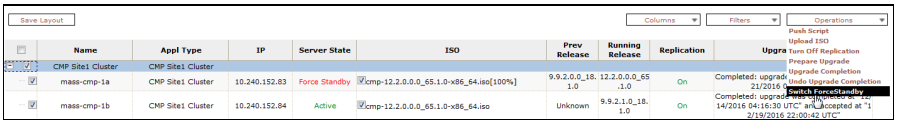
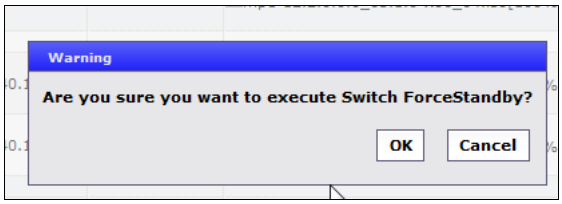
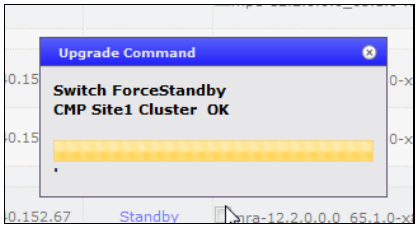
- Upgrade Status column displays the Completed: upgrade was completed at… message
- Running Release column shows Release 12.3 version
- Prev Release column shows the previous version

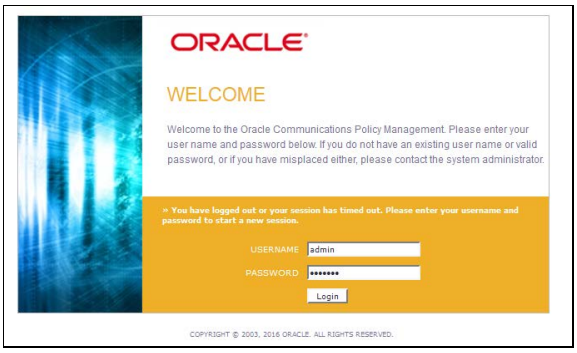
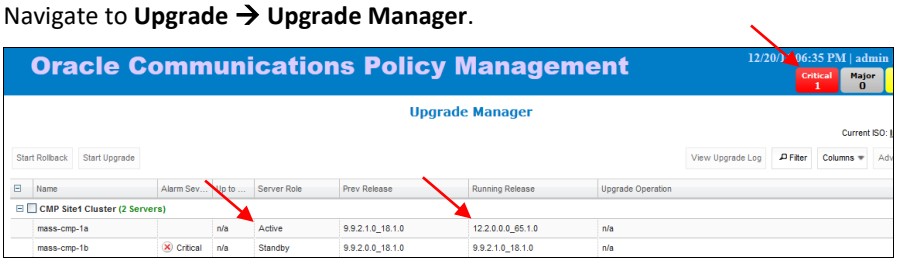


The critical alarm 70025 (The MySQL slave has a different schema version than the master) is expected to remain, whereas the remaining alarms should be cleared.

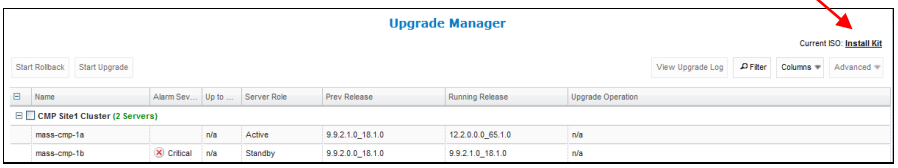
NOTE: Both the Spinner and Sync-broken icons display disappeared as expected.

If there is a status message other than the Upgrade complete…, **STOP HERE** and contact Oracle Technical Services to troubleshoot and determine if a rollback should be performed.

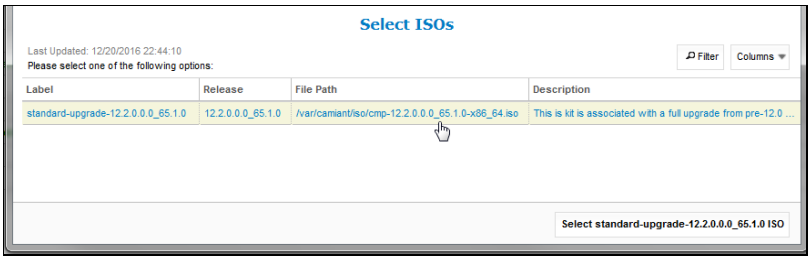
Step	Procedure	Result
8. ☐	**CMP GUI:** Perform Switch ForceStandby of Upgraded Release 12.3 CMP server	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Select the Primary CMP cluster to be switched. 3. Select **Operations → Switch ForceStandby**.  4. Click **OK** to continue with the operation and a successful message displays.   **NOTE:** At this point, the current CMP GUI browser connection is lost. If it is the primary CMP cluster, you must login again as illustrated in the next step.

Step	Procedure	Result
9. ☐	**CMP GUI:** Re-login to the Primary CMP server VIP address	1. Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Release 12.3 CMP GUI Login screen opens. 2. Login and password credentials are the same as before the upgrade.  3. Navigate to **Help → About**. 4. Validate that the CMP server version is now showing the release 12.3. 
10. ☐	**CMP GUI:** Verify the Policy Release 12. 3 CMP server is Active	Navigate to **Upgrade → Upgrade Manager**.  **NOTE:** The critical alarm 70025 (The MySQL slave has a different schema version than the master) is expected to remain.

Step	Procedure	Result
11. ☐	**CMP GUI:** Install the Current ISO Release 12.3 Install Kit	1. Navigate to **Upgrade → Upgrade Manager → Current ISO: Install Kit.**

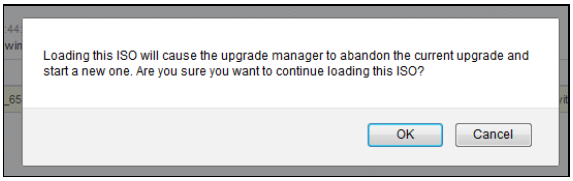


2. Click **Install Kit.** This opens a dialog box that lists the contents of ISO file located in the `/var/camiant/iso` directory.

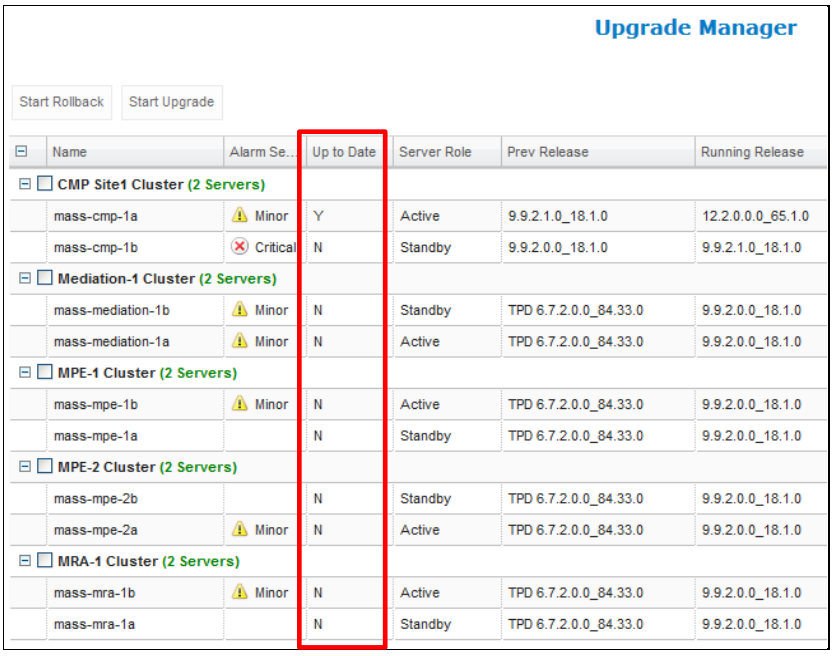


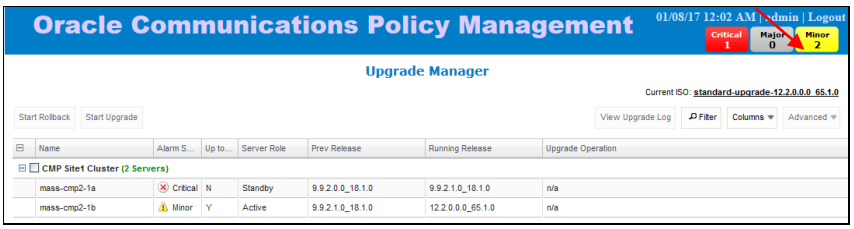
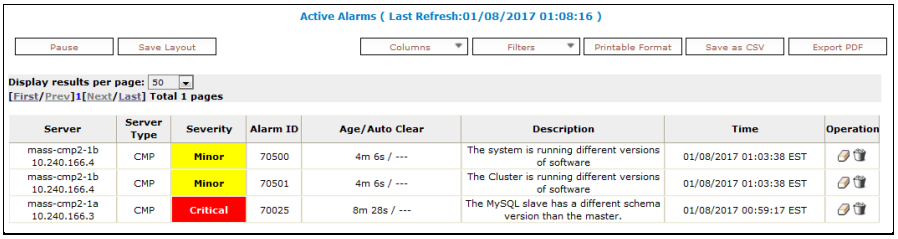
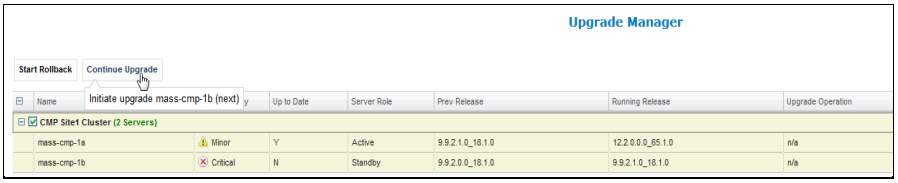
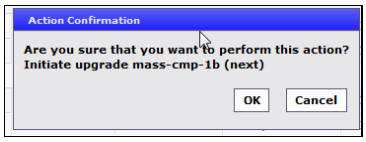
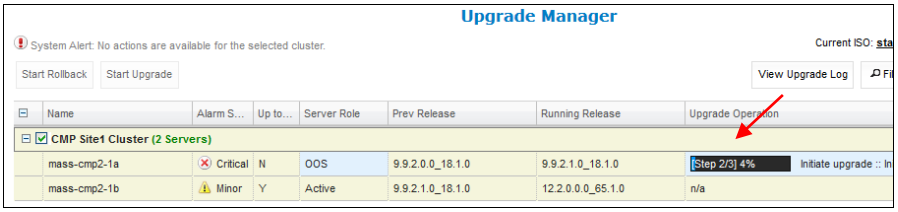
3. Highlight the Release 12.3 ISO file and click the button labeled as **Select standard-upgrade-12.3xxxx** in the bottom right hand corner.

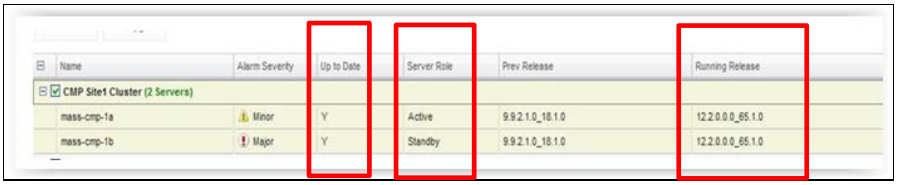
4. Click **OK** to proceed.



The Up to Date column transitions from n/a to Y (meaning up-to-date) or N (meaning needs upgrade).



Step	Procedure	Result
12. ☐	**CMP GUI:** New minor alarms introduced in Release 12.3.0	The following minor alarms of 70500 and 70501 are added, along with the existing critical alarm of 70025 which are now shown in the Upgrade Manager.  
13. ☐	**CMP GUI:** Complete the Upgrade of the remaining of the Primary CMP cluster **NOTE:** Each server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Check the Primary CMP cluster and both the **Continue Upgrade** and **Start Rollback** buttons become available. In the case of this upgrade, click **Continue Upgrade** button.  3. Click **OK** to proceed with the upgrade.  **NOTE:** The Upgrade Operation status column displays the in-progress status bar during the upgrade.  **NOTE**: This upgrade process takes approximately 40 minutes to complete. During this time, the Server Role of the upgrading server would be OOS as expected. The following alarms are to be expected during the upgrade process - **<u>Expected Critical Alarms</u>** **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline

Step	Procedure	Result
		70001 The qp_procmgr process has failed. **70025** QP Slave database is a different version than the master **Expected Major Alarms** **31233** High availability path loss of connectivity **70004** The QP processes have been brought down for maintenance. **70021** The MySQL slave is not connected to the master **70022** The MySQL slave failed synchronizing with the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed
14. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	1. Navigate to **Upgrade Manager → Upgrade Manager**. 2. Successful Upgrade Operation status shows the following: - Both servers running the Release 12.3.0 in the Running Release column. - There are Active and Standby server roles to both servers in this Primary CMP cluster. - The Up to Date column status is updated to Y for both CMP servers 
15. ☐	Proceed to next applicable upgrade procedure	• At this point, the Primary Site1 CMP cluster is running Release 12.3.0 • The remaining MPE, MRA, and Mediation clusters are on Release 12.2.x
THIS PROCEDURE HAS BEEN COMPLETED		

7. UPGRADE CMP CLUSTERS (12.2.X TO 12.3) WIRELESS MODE

This procedure upgrades the Site1 CMP cluster first, and if needed, upgrade the Site2 CMP cluster.

7.1 Upgrade CMP Clusters Overview

7.2 Upgrade Primary CMP cluster

1. Use the CMP GUI–System Maintenance (12.2.x) to place Primary Standby CMP into Frc-Stby
2. Use the CMP GUI–System Maintenance (12.2.x) to upgrade the Primary Frc-Stby CMP server
3. Use the CMP GUI–System Maintenance (12.2.x) to perform Switch Frc-Stby on the Primary CMP cluster
4. Log back into the CMP GUI and upgrade the remaining Frc-Stby Primary CMP server using the 12.3 Upgrade Manager

7.3 Upgrade the Secondary CMP cluster (if applicable)

Use the CMP GUI, navigate to **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2

a. Start Upgrade

b. Continue Upgrade--Failover

c. Continue Upgrade

This procedure should not be service affecting, but it is recommended to perform this in a Maintenance Window

It is assumed that the CMPs may be deployed as 2 Geo-Redundant clusters, identified as Site1 and Site2 as displayed on the CMP GUI. When deployed as such, one site is designated as the Primary Site (which is the site that is managing the Policy system), and the other is as Secondary site (this site is ready to become Primary site, if needed).

If the System is deployed with only ONE CMP, then the upgrade of the Secondary CMP can be skipped.

Identify the CMPs sites to be upgraded here, and verify which sites are Primary and Secondary:

CMP Sites Geo-Redundant Status	Operator Site Name	Site Designation from Topology Form (Site1 or Site2)
Primary Site		
Secondary Site		

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP _____

Server-A Status _____

Server-B Hostname _____

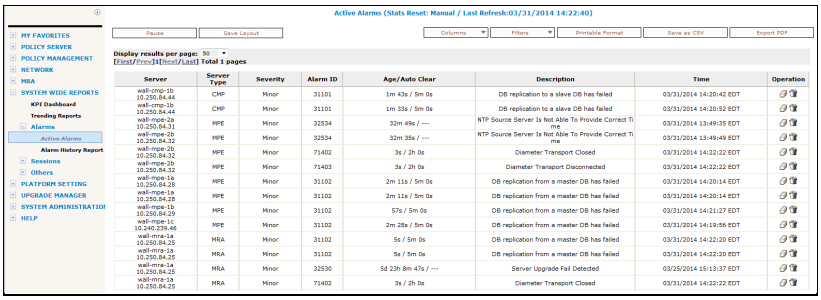
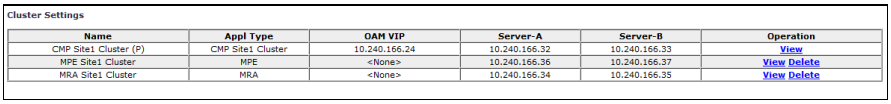
Server-B IP _____

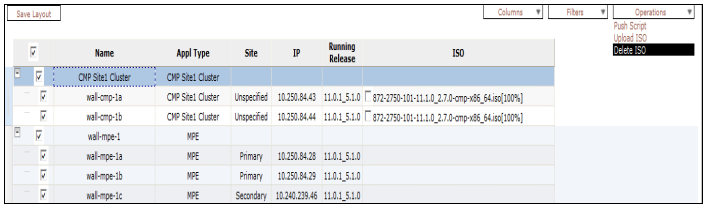
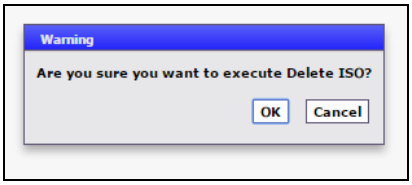
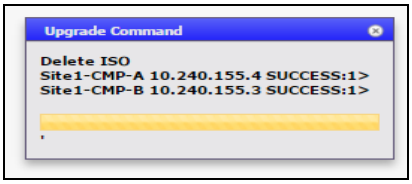
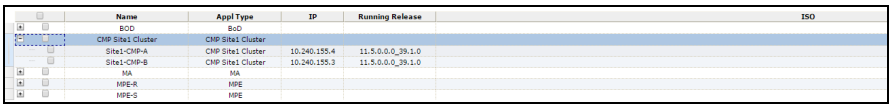
Server-B Status _____

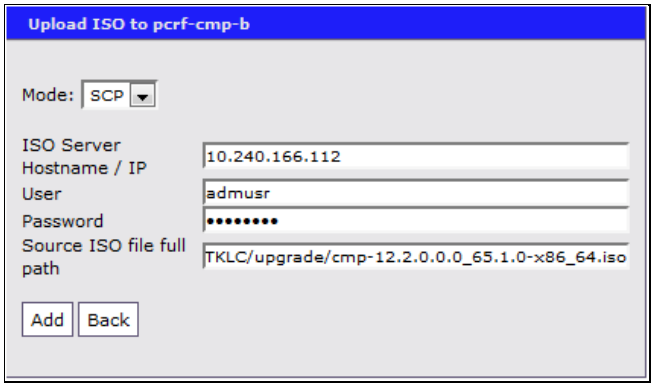
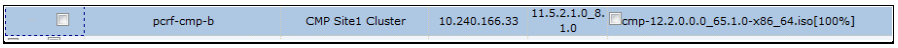
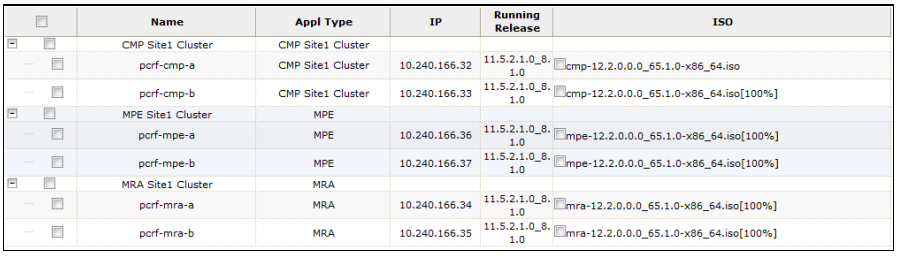
IMPORTANT:

- CMP servers MUST be upgraded first, before the MPE or MRA clusters
- Site1 CMP MUST be upgraded to the new release first, before the Site2 CMP (if applicable)

7.3.1 Upgrade primary CMP Cluster

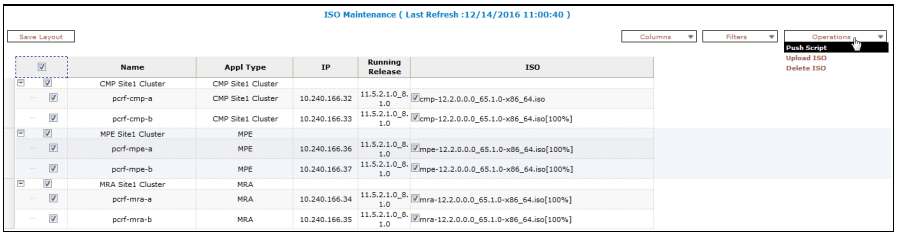
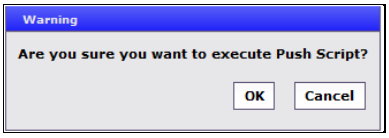
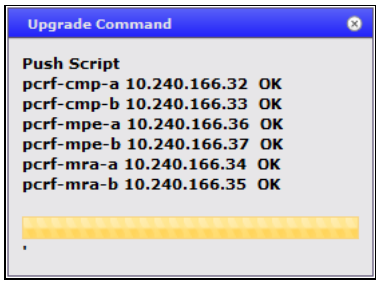
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **System Wide Reports →Alarms→ Active Alarms**. 2. Confirm that any existing alarm has no impact to the upgrade procedure. 3. Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and record the CMP clusters	1. Navigate to **Platform Settings →TOPOLOGY Settings → All Clusters.**  Name / Appl Type / OAM VIP / Server-A / Server-B / Operation CMP Site1 Cluster (P) / CMP Site1 Cluster / 10.240.166.24 / 10.240.166.32 / 10.240.166.33 / View MPE Site1 Cluster / MPE / <None> / 10.240.166.36 / 10.240.166.37 / View Delete MRA Site1 Cluster / MRA / <None> / 10.240.166.34 / 10.240.166.35 / View Delete 2. Note which cluster is the primary and which is the secondary. The Primary CMP is noted with a (P) in parenthesis and a Secondary CMP is noted with an (S) in parenthesis. 3. Save a screenshot for future reference.
3. ☐	**CMP GUI**: Verify Status of CMP clusters	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Confirm the CMP clusters have the following: - Active/Standby status - Running Release of 12.2.X version - Replication ON - Corresponding Release 12.3 ISO files copied to at least one of each server types (CMP/MRA/MPE)–Meaning, a copy of the MPE ISO is on one of the MPE servers, an MRA ISO is on one of the MRA servers and a copy of the CMP ISO is on one CMP server

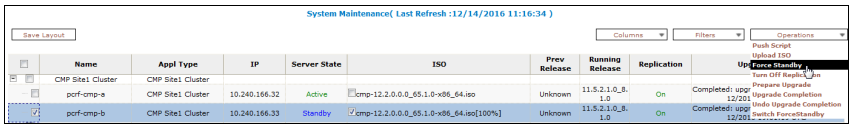
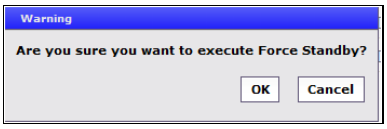
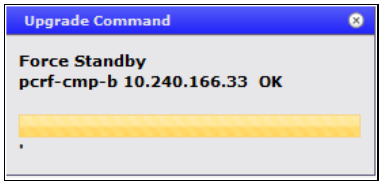
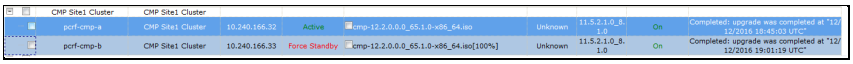
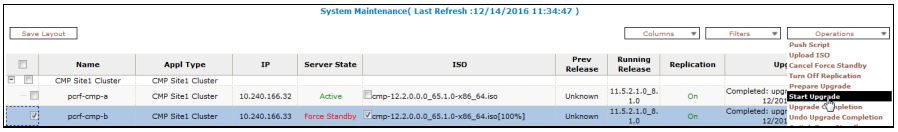
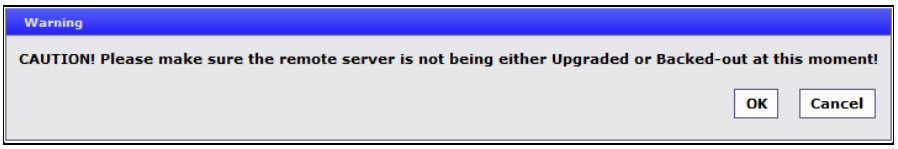
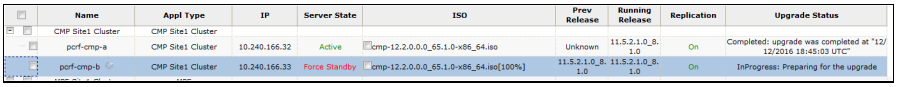
Step	Procedure	Result
4. ☐	**CMP GUI Access** into Primary CMP Server—Remove old ISO files from servers.	1. Navigate to **Upgrade Manager → ISO Maintenance**. 2. Select the servers that show old ISO files. 3. Select the server cluster and select **Operations→ Delete ISO** for any of the older ISO files in the list.  4. Click **OK** to continue  5. Wait until the successful deletion message displays.  6. Wait until the **ISO Maintenance** page refreshes showing that the ISO column blank 

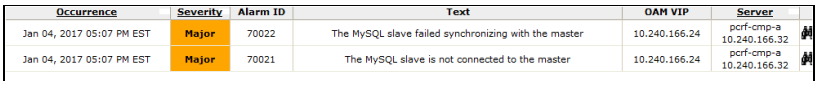
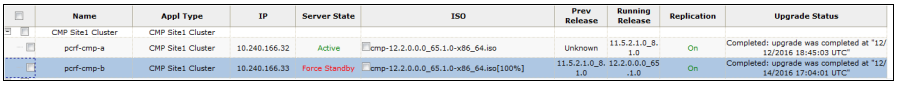
Step	Procedure	Result
5. ☐	**CMP GUI:** Upload relevant upgrade ISO file to each CMP/MPE/MRA server **NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly.	**Upgrade Manager → ISO Maintenance** 1. (Optional but Preferred) Filter CMP/MPE/MRA servers 2. One application at a time, select one server type (CMP/MPE/MRA) to upload its upgrade ISO file. 3. Select **Operations → Upload ISO**  4. Fill in the dialog with the following information: Mode: Select **SCP** ISO Server Hostname/IP: <*IP_address_where_ISO_files_are_located*> User: admusr Password: <*admusr_password_for_the_server*> Source ISO file full path: `/var/TKLC/upgrade/<ISO file>`  5. Click **Add** and wait until the filename displays in the ISO column and the file is 100% transferred:  6. When completed for all servers, the ISO column are populated with the ISO filename and indication of 100% transfer completion  **NOTE:** For those servers where the ISO file was transferred from the local machine, there is not a 100% indicator. This indicator is only available when transferring ISO files using the ISO management screen of CMP GUI.

Step	Procedure	Result

6. ☐	**SSH CLI Primary Active CMP:** Copy latest upgrade scripts and Exchange keys	1. Ssh to active CMP, login as admusr user then mount the upgrade iso file to copy the latest upgrade scripts as follows:
		`$sudo mount -o loop /var/TKLC/upgrade/cmp-12.3.x-x86_64.iso /mnt/upgrade/`
		`$sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		`$sudo umount /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.2.0.0.0_65.1.0-x86_64.iso /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		`[admusr@pcrf-cmp-a ~]$ sudo umount /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$`
		2. Run the following command to exchange the SSH keys with all servers in the topology:
		`$sudo qpSSHKeyProv.pl --prov`
		NOTE: You need to supply the PASSWORD of admusr for command to process
		`[admusr@pcrf-cmp-a ~]$ sudo qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:`
		`Connecting to admusr@pcrf-mpe-a ...`
		`Connecting to admusr@pcrf-mra-b ...`
		`Connecting to admusr@pcrf-cmp-a ...`
		`Connecting to admusr@pcrf-cmp-b ...`
		`Connecting to admusr@pcrf-mra-a ...`
		`Connecting to admusr@pcrf-mpe-b ...`
		`[1/6] Provisioning SSH keys on pcrf-mpe-a ...`
		`[2/6] Provisioning SSH keys on pcrf-mra-b ...`
		`[3/6] Provisioning SSH keys on pcrf-cmp-b ...`
		`[4/6] Provisioning SSH keys on pcrf-cmp-a ...`
		`[5/6] Provisioning SSH keys on pcrf-mra-a ...`
		`[6/6] Provisioning SSH keys on pcrf-mpe-b ...`
		`SSH keys are OK.`
		`[admusr@pcrf-cmp-a ~]$`
		3. Verify that the Keys are exchanged successfully with all the server clusters as follows :
		`[admusr@pcrf-cmp-a ~]$ sudo qpSSHKeyProv.pl --check`
		`The password of admusr in topology:`
		`Connecting to admusr@pcrf-mpe-a ...`
		`Connecting to admusr@pcrf-mra-b ...`
		`Connecting to admusr@pcrf-cmp-a ...`
		`Connecting to admusr@pcrf-cmp-b ...`
		`Connecting to admusr@pcrf-mra-a ...`
		`Connecting to admusr@pcrf-mpe-b ...`
		`[1/6] Checking SSH keys on pcrf-mpe-a ...`
		`[2/6] Checking SSH keys on pcrf-mra-b ...`
		`[3/6] Checking SSH keys on pcrf-cmp-b ...`
		`[4/6] Checking SSH keys on pcrf-cmp-a ...`
		`[5/6] Checking SSH keys on pcrf-mra-a ...`
		`[6/6] Checking SSH keys on pcrf-mpe-b ...`
		`SSH keys are OK.`
		`[admusr@pcrf-cmp-a ~]$`

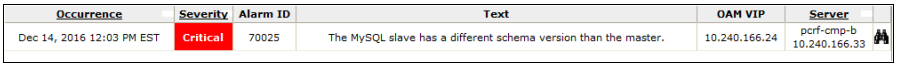
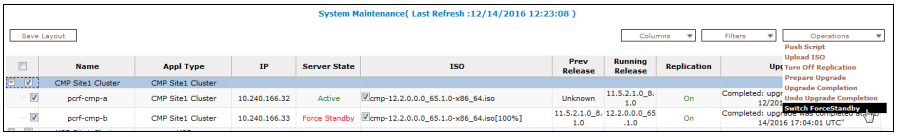
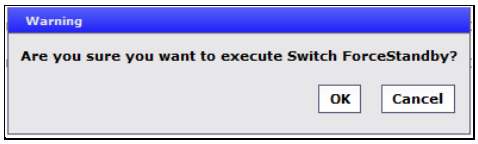
Step	Procedure	Result
7. ☐	**CMP GUI**: Push the Release 12.3 upgrade Scripts to all servers in the segment topology	1. Login to CMP GUI. 2. Navigate to **Upgrade Manager → ISO Maintenance** 3. Select all the servers in the Topology as shown. 4. Select **Operations → Push Scripts**. (It is safe to run the push script multiple times as needed).  5. Click **OK** to continue the operation.  6. Operation successful.  **NOTE:** Give the push script a minute to complete

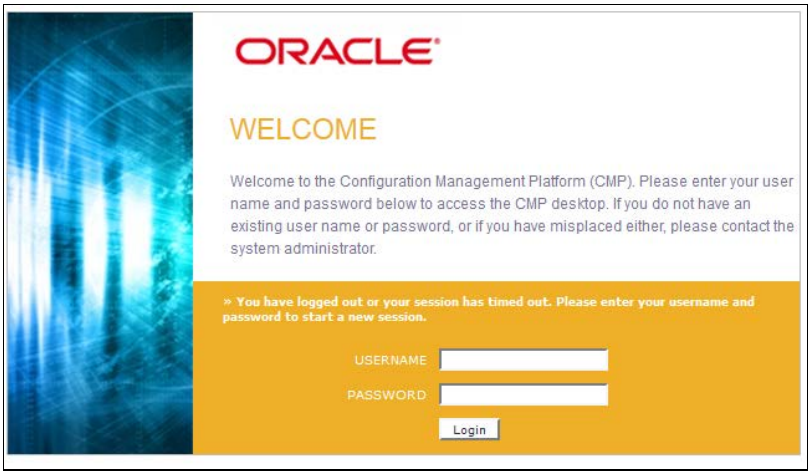
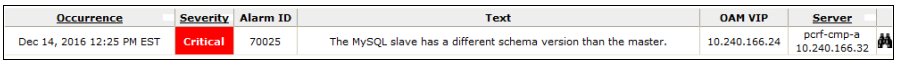
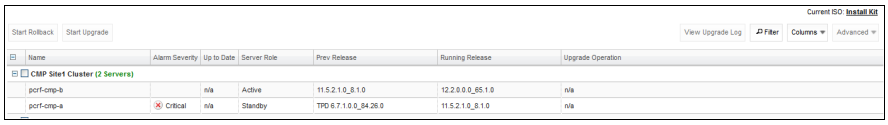
Step	Procedure	Result
8. ☐	**CMP GUI**: Set Force-Standby mode on the Standby CMP - Primary cluster	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Select the Standby CMP Server at Primary Site 3. Select **Operations → Force Standby**.  4. Click **OK** to confirm and continue with the operation.  5. Confirm the step completes successfully:  The Standby CMP server state is changed to Force Standby. 
9. ☐	**CMP GUI:** Upgrade the Force-Standby CMP server at the primary site **NOTE:** This takes approximately 40 minutes to complete.	1. Navigate to **Upgrade Manager → System Maintenance.** 2. Select the Force-Standby CMP Server at the Primary Site. 3. Select **Operation → Start Upgrade**.  4. Click **OK** to continue with the operation.  5. Monitor the upgrade status activities from the Upgrade Status column.  The Upgraded Status column shows the In Progress status along with the upgrade activities which typically takes approximately 40 minutes to complete. During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical Alarm</u>**

Step	Procedure	Result
		31283 High availability server is offline  **Expected Major Alarms** **31233** HA Path Down **70004** The QP processes have been brought down for maintenance. **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master    **Expected Minor Alarms** **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB replication to slave DB has failed Wait until the upgrade was completed message displays in the Upgrade Status column.  **Note:** If there is other status message appeared other than the Upgrade complete message, stop here and contact Oracle Technical Services to troubleshoot and determine if a rollback should be performed.
10. ☐	**CMP GUI:** Verify Upgrade Completion is successful	Navigate to **Upgrade Manager → System Maintenance**. Successful upgrade status shows Release 12.3 in the Running Release column and the Upgrade Status column.  **NOTE:** Expect that the server state role is shown as Force Standby, same as prior to the upgrade. A Sync Broken indicator ( ) means that the data replication between the two servers of the cluster is not synced yet. This may take up to 45 minutes depending on the database size. Do not continue if there is a Sync Broken indicator on the server that was upgraded.

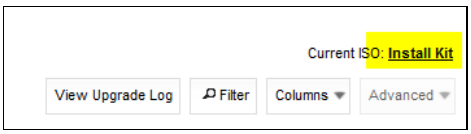
Step	Procedure	Result

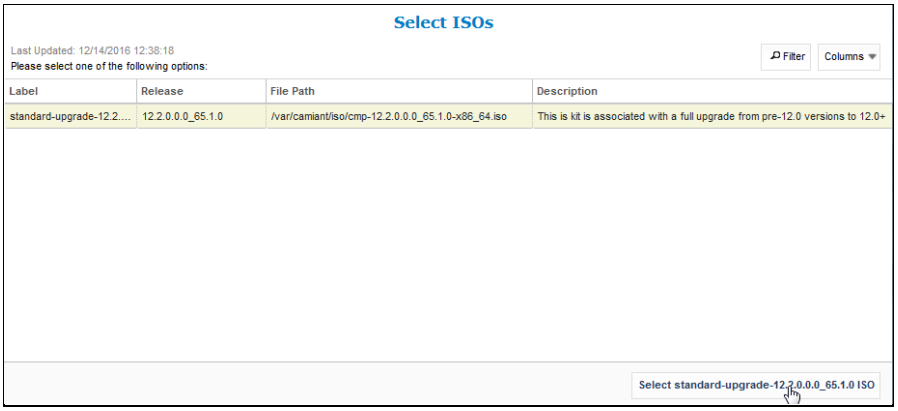
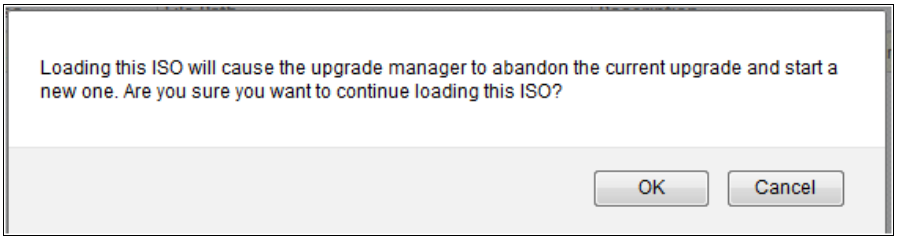
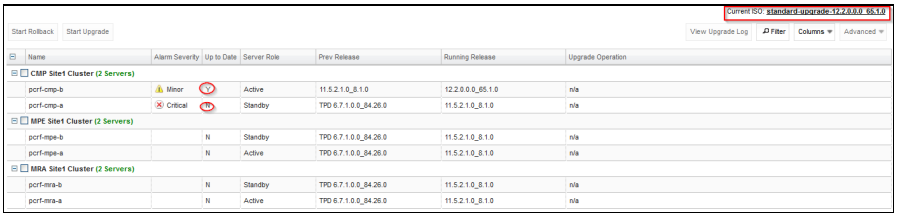
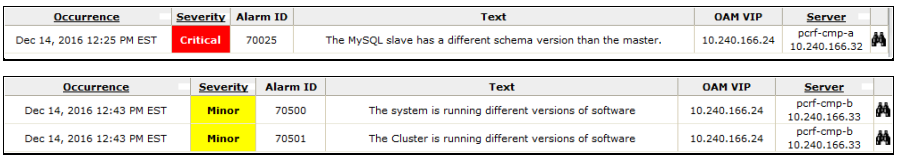
11. ☐	**Upgraded server SSH:** Verify upgrade log file	SSH to upgraded server and check the upgrade log file to validate it completed successfully:
		`[admusr@pcrf-cmp-b ~]$ cd /var/TKLC/log/upgrade/`
		`[admusr@pcrf-cmp-b upgrade]$ tail upgrade.log`
		`1481734697::Updating platform revision file...`
		`1481734697::RCS_VERSION=1.2`
		`1481734697::Upgrade returned success!`
		`1481734698::Creating RC script to set alarm on next boot`
		`1481734698::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus'`
		`1481734698::Cleaning up chroot environment...`
		`1481734698::`
		`1481734996:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute`
		`1481735041:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm`
		`1481735041:: /etc/rc4.d/S99TKLCupgradeStatus -`
		`[admusr@pcrf-cmp-b upgrade]$`

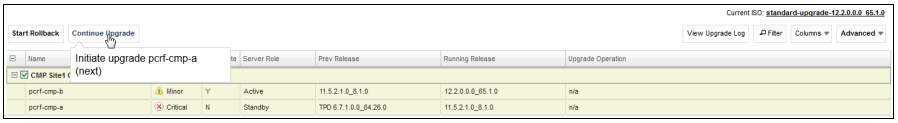
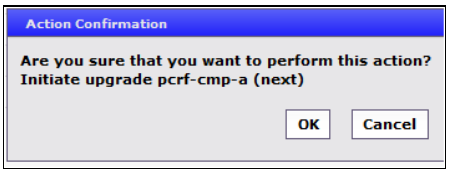
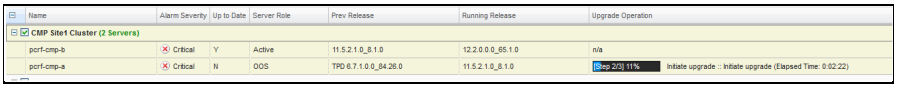
12. ☐	**CMP GUI:** Verify alarms	Navigate to **System Wide Reports → Active Alarms**. The following is an expected alarm (ID: 70025).  The alarm be clears after everything on the cluster is upgraded to the same release.
13. ☐	**CMP GUI:** Switch the upgraded Release 12.3 CMP server to Active	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Select the CMP cluster to be switched–primary cluster only. 3. Select **Operations→ Switch ForceStandby**.  4. Click **OK** to continue with the operation and a successful message appears.  **NOTE:** At this point, the current CMP GUI browser connection is lost–if it is the primary CMP cluster, need to re-login as illustrated in the next step. 5. Close the browser and re-open.

Step	Procedure	Result
14. ☐	**CMP GUI:** Relogin to the CMP server VIP	1. Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Release 12.3 CMP GUI Login displays. 2. Login and password credentials are the same as before the upgrade. 
15. ☐	**CMP GUI:** Verify the Policy Release	1. Navigate to **Help→About**. 2. Verify the release number is displayed as 12.3.
16. ☐	**CMP GUI:** Critical alarms	Critical alarm 70025 displays until the SQL Database matches the master (12.3) and minor alarm 31101. These alarms are expected and remain until all CMP servers are upgraded to the same version.  **NOTE:** The Upgrade Manager shows the same alarms.
17. ☐	**CMP GUI:** Verify the Policy Release 12.2 CMP is active	Navigate to **Upgrade→Upgrade Manager**.  As noted, the Active CMP server is now on the Running Release of 12.3.

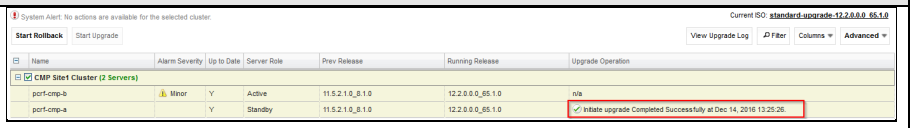
18. ☐	**Primary Active CMP**: ssh to primary active CMP and copy iso to `/var/camiant/iso` directory.	1. Logon to the primary active CMP as admusr and copy the 12.3 ISO file to the `/var/camiant/iso` directory:
		`$sudo cp /var/TKLC/upgrade/cmp-12.3.x…x.iso /var/camiant/iso/`
		2. Verify the copy by using the following command:
		`$ ls /var/camiant/iso/`

19. ☐	**CMP GUI:** Locate the 12.3 Upgrade Manual	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Current ISO–in this case it is labeled install kit. 

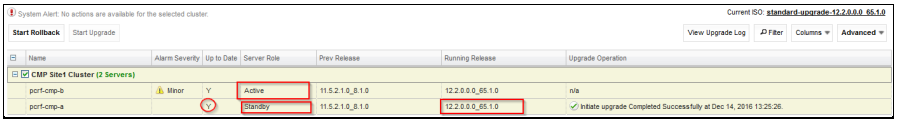
Step	Procedure	Result
		A dialog box with a description of the ISO that was just copied into `/var/camiant/iso`. 3. Highlight the available ISO and click the button on the bottom right hand corner of the pop-up window  4. Click **OK** on the confirmation dialog.  Within a few seconds, the Up to date column transition from n/a to Y (meaning up-to-date) or N (meaning needs upgrade). Also, the Install Kit now displays the selected CMP ISO file 
20. ☐	**CMP GUI:** Alarms introduced with Release 12.3	The following minor alarms, along with the already active critical alarms, are now active. 

Step	Procedure	Result
21. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP cluster **NOTE**: Remaining CMP server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary Site 1 CMP cluster **Continue Upgrade** becomes available. 3. Click **Continue Upgrade**.  4. Click **OK** to continue the upgrade on the remaining server in the CMP cluster  During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical Alarms** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarms** **31233** HA Path Down **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **NOTE**: Remaining CMP server takes approximately 40 minutes to complete.
22. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**. Notice the upgrade operation column displays the steps of the upgrade process:  At end of the upgrade process, upgrade operation column should display successful upgrade completion message for the upgraded CMP server as follows:

Step	Procedure	Result



- Successful upgrade status shows that both servers are running the Release 12.2 in the Running Release column.-
- A Y in the Up to Date column
- Active/standby state for both servers in the Primary CMP Cluster.



During the upgrade activities, the following alarms may be generated and are considered normal reporting events.

Expected Critical Alarms

31283 High availability server is offline
70001 QP_procmgr failed
70025 The MYSQL Slave has a different scheme version than the master

Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 04, 2017 04:42 PM EST	Critical	31283	High availability server is offline	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 12:46 PM EST	Critical	70025	The MySQL slave has a different schema version than the master.	10.240.166.60	ohio-cmp-b 10.240.166.29
Jan 04, 2017 12:46 PM EST	Critical	70025	The MySQL slave has a different schema version than the master.	10.240.166.60	ohio-cmp-a 10.240.166.28

Expected Major Alarms

31233 High Availability path loss of connectivity
70004 QP Processes down for maintenance

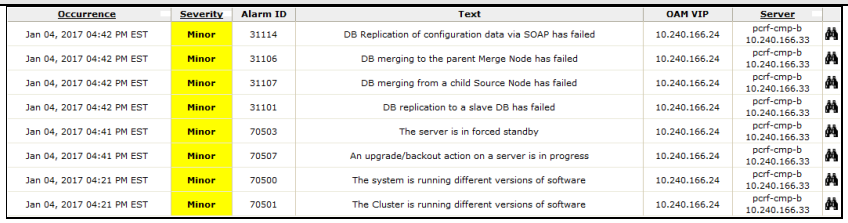
Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 04, 2017 04:41 PM EST	Major	70004	The QP processes have been brought down for maintenance.	10.240.166.24	pcrf-cmp-a 10.240.166.32

Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 04, 2017 05:07 PM EST	Major	70022	The MySQL slave failed synchronizing with the master	10.240.166.24	pcrf-cmp-a 10.240.166.32
Jan 04, 2017 05:07 PM EST	Major	70021	The MySQL slave is not connected to the master	10.240.166.24	pcrf-cmp-a 10.240.166.32

Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 04, 2017 05:41 PM EST	Major	31233	High availability path loss of connectivity	10.240.166.60	ohio-cmp-a 10.240.166.28

Expected Minor Alarms

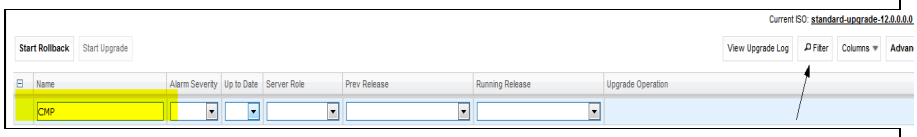
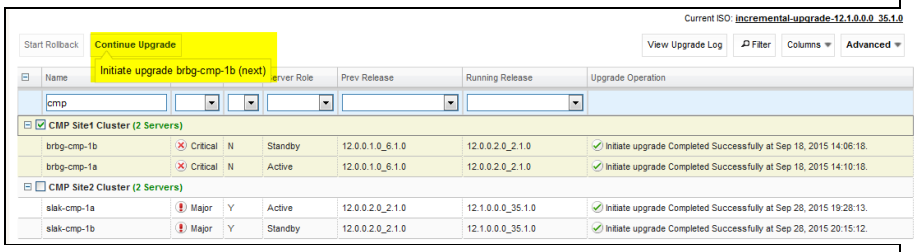
31114 DB Replication over SOAP has failed
31106 DB Merge To Parent Failure
31107 DB Merge From Child Failure
31101 DB Replication To Slave Failure
70503 Upgrade Director Server Forced Standby
70507 An Upgrade/Backout action on a server is in progress
70500 Upgrade Director System Mixed Version
70501 Upgrade Director Cluster Mixed Version

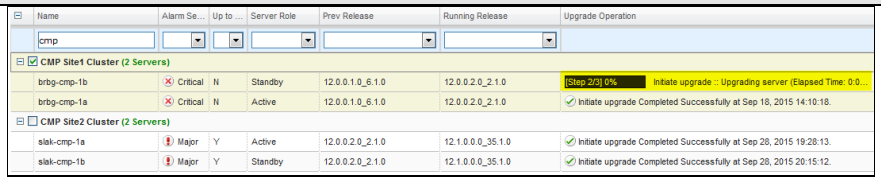
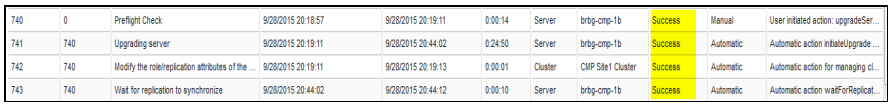
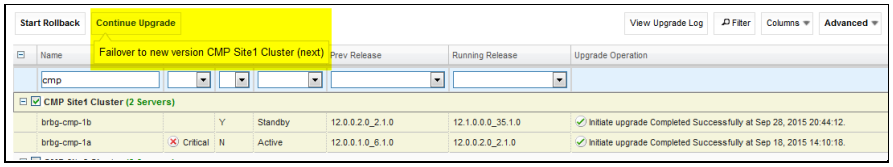
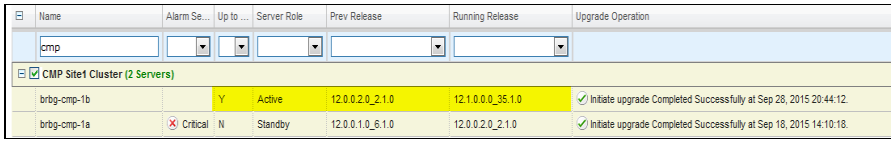
Step	Procedure	Result
		

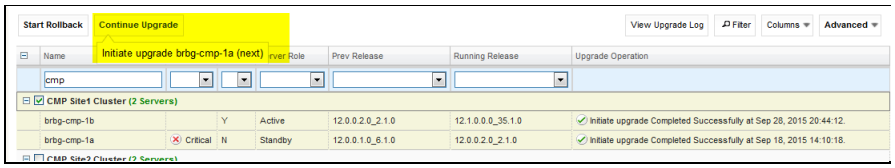
Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 04, 2017 04:42 PM EST	Minor	31114	DB Replication of configuration data via SOAP has failed	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:42 PM EST	Minor	31106	DB merging to the parent Merge Node has failed	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:42 PM EST	Minor	31107	DB merging from a child Source Node has failed	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:42 PM EST	Minor	31101	DB replication to a slave DB has failed	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:41 PM EST	Minor	70503	The server is in forced standby	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:41 PM EST	Minor	70507	An upgrade/backout action on a server is in progress	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:21 PM EST	Minor	70500	The system is running different versions of software	10.240.166.24	pcrf-cmp-b 10.240.166.33
Jan 04, 2017 04:21 PM EST	Minor	70501	The Cluster is running different versions of software	10.240.166.24	pcrf-cmp-b 10.240.166.33

23. ☐	Proceed to next upgrade procedure	• At this point, the Primary Site1 is running Release 12.3. • Secondary SITE, if applicable, is on R12.2.x. • All C Level Nodes are on Release 12.2.x. • Go to the next procedure if there is a DR CMP to upgrade. If not, skip to *Post Upgrade Health Check*.
THIS PROCEDURE HAS BEEN COMPLETED		

7.3.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP cluster	Navigate to **Upgrade → Upgrade Manager**. • Primary CMP is completely upgraded to 12.3 • Secondary CMP cluster is on 12.2.x
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. **NOTE:** The Filter button can be used to show only the CMP servers. Type in CMP under NAME.  2. Select the Secondary CMP Server cluster at Site2 3. Click **Start Upgrade**.  4. Click **OK** to confirm and continue with the operation. The specific action taken is determined by the Upgrade Manager and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP cluster **NOTE:** This takes approximately 30 minutes to complete. The Upgraded Status column displays the In Progress status along with the upgrade activities.

Step	Procedure	Result
		 During the Upgrade activities, the following alarms may be generated and considered normal reporting events. **Expected Critical Alarms** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarms** **70004** QP Processes down for maintenance **Expected Minor Database replication Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **LOG FILE from the GUI showing complete on the 1st server on the secondary site.** 
3. ☐	**CMP GUI**: Continue Upgrade Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP Server cluster at Site2 3. Click **Continue Upgrade**. Notice the Failover to new version message.  4. Click **OK** to confirm and continue with the operation. The specific action takes a minute to complete. Wait until the upgraded server is active, as shown below. 

Step	Procedure	Result
		5. Select the Secondary CMP Server cluster at Site2 6. Click **Continue Upgrade**. When hovering over the button, the message displays the next action, which is upgrading the remaining CMP.  7. Click **OK** to confirm and continue with the operation, During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical Alarms** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Database Replication Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault
4. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	Navigate to **Upgrade → Upgrade Manager**. Successful upgrade status shows Release 12.3 in the Running Release column and the Upgrade Status column.
5. ☐	**CMP GUI:** Verify alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarm** **70500** System in Mixed version

8. UPGRADE CMP CLUSTERS (12.2.X TO 12.3)

CMPs may be deployed as 2 georedundant clusters, identified as Site1 and Site2 on the CMP GUI. When deployed as such, one site is designated as the Primary Site (the site that manages the Policy system), and the other is designated as the Secondary Site (this site is ready to take over in case the primary site fails).

This procedure upgrades the Site1 (Primary) CMP cluster first, then upgrade the Site2 (Secondary) CMP cluster, both in a single maintenance window.

If the system is deployed with only one CMP, then evidently the upgrade of a Site2 (Secondary) CMP is not necessary.

8.1 Upgrade CMP Clusters Overview

8.2 Upgrade the Primary CMP cluster

1. Upgrade CMP Site1
    a. Start upgrade on the standby server
    b. Failover
    c. Continue upgrade with the remaining Site1 CMP server

8.3 Upgrade the Secondary CMP cluster

1. Upgrade CMP Site2
    a. Start upgrade on the standby server
    b. Failover
    c. Continue upgrade with the remaining Site2 CMP server

This procedure should not be service affecting, but it is recommended to perform this in a maintenance window.

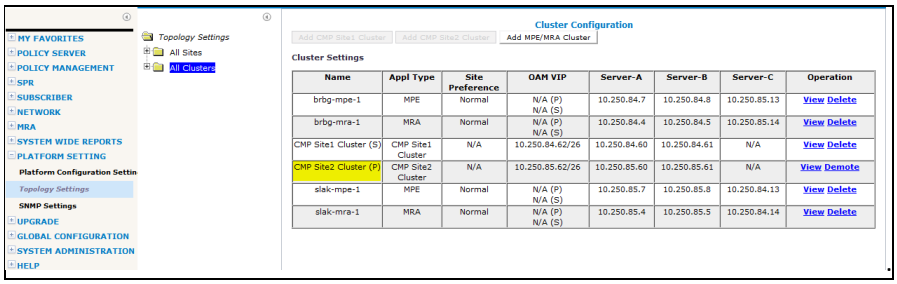
Identify the CMP sites to be upgraded here, and verify which site is Primary and which one is Secondary:

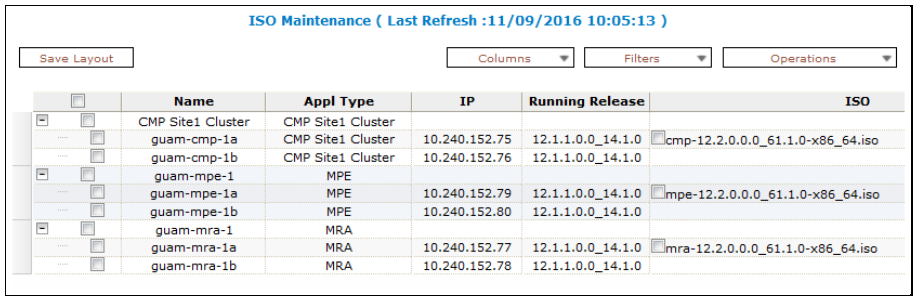
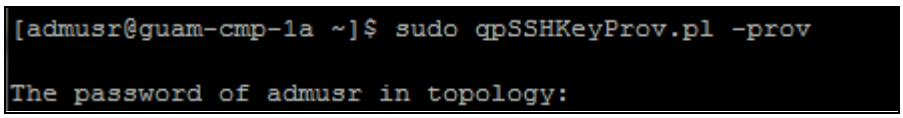
CMP Sites	Operator Site Name	Topology Site Designation (Site1 or Site2)	CMP Server-A	CMP Server-B
Primary Site			Server-A Hostname _____ Server-A IP Address _____ Server-A HA Status _____	Server-B Hostname _____ Server-B IP Address _____ Server-B HA Status _____
Secondary Site			Server-A Hostname _____ Server-A IP Address _____ Server-A HA Status _____	Server-B Hostname _____ Server-B IP Address _____ Server-B HA Status _____

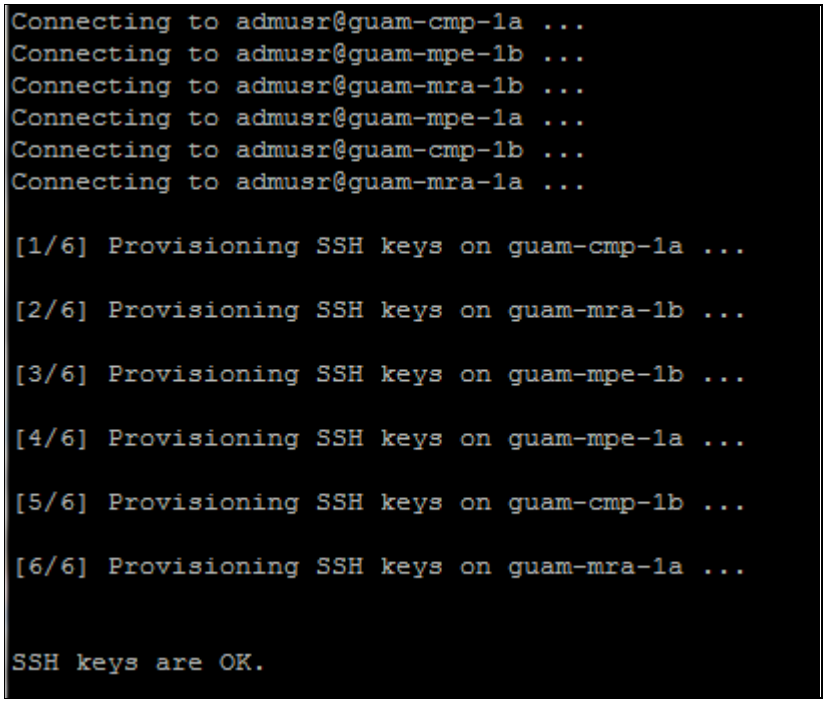
IMPORTANT:

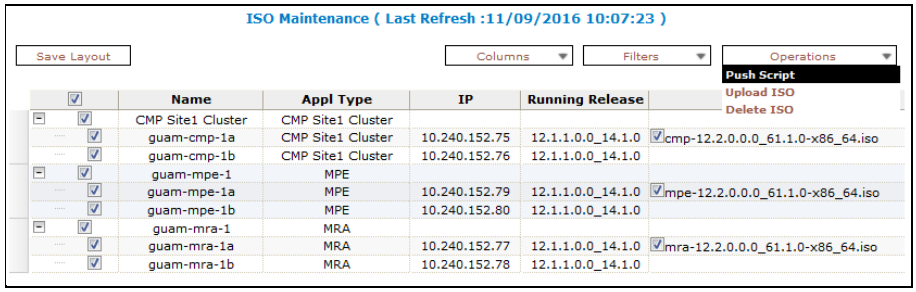
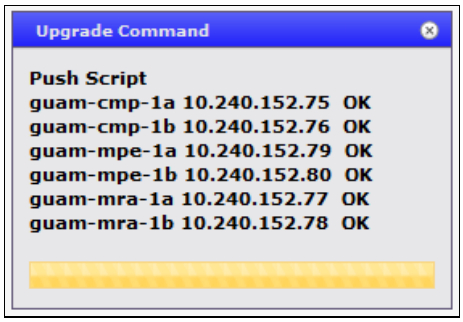
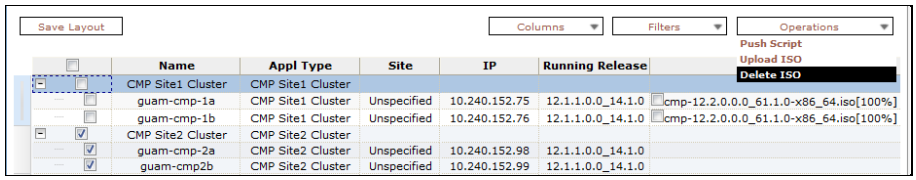
- The Primary CMP site must be upgraded to the new release before the Secondary CMP Site
- CMP servers must be upgraded before non-CMP servers

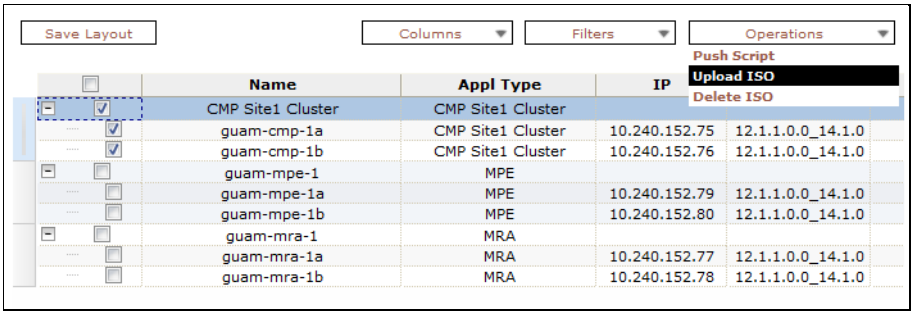
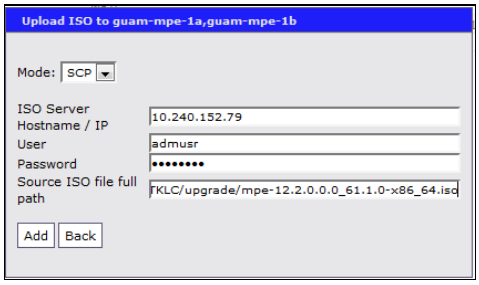
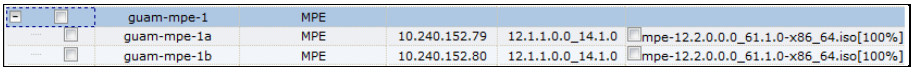
8.3.1 Upgrade Primary CMP cluster

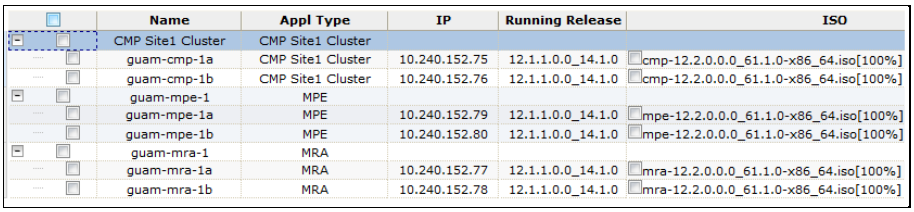
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Confirm that any existing alarm has no impact to the upgrade procedure. 3. Capture a screenshot and save it into a file for reference.
2. ☐	**CMP GUI:** Identify and Record the CMP clusters	1. Navigate to Platform Setting → Topology Settings. 2. Note which cluster is the primary and which one is the secondary.  The Primary CMP is noted with (P). The Secondary CMP with (S).

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>3. ☐</td><td>CMP GUI: Verify Status of CMP cluster s</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Confirm the CMP clusters are:
- In Active/Standby status
- Running release 12.2.x software
3. Navigate to Upgrade → ISO Maintenance.
4. Ensure Release 12.3 ISO files have been copied to at least one of each corresponding server types (CMP, MPE, MRA, and so on.)
 
</td></tr>
<tr><td>4. ☐</td><td>SSH CLI Primary Active CMP:
Exchange Keys</td><td>1. Exchange keys to all servers from the Site1 (Primary) Active CMP. Login as admusr user and run the following command:
<code>$sudo qpSSHKeyProv.pl --prov</code>
 

2. Enter the password for admusr user.
3. Ensure that the keys are exchanged successfully with all the server clusters:
 
</td></tr>
</table>

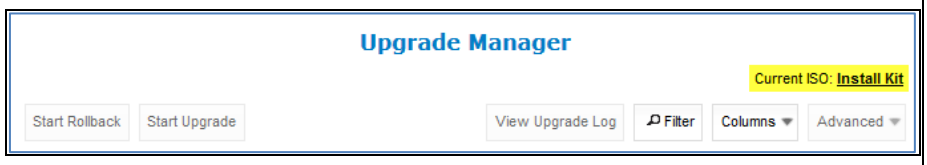
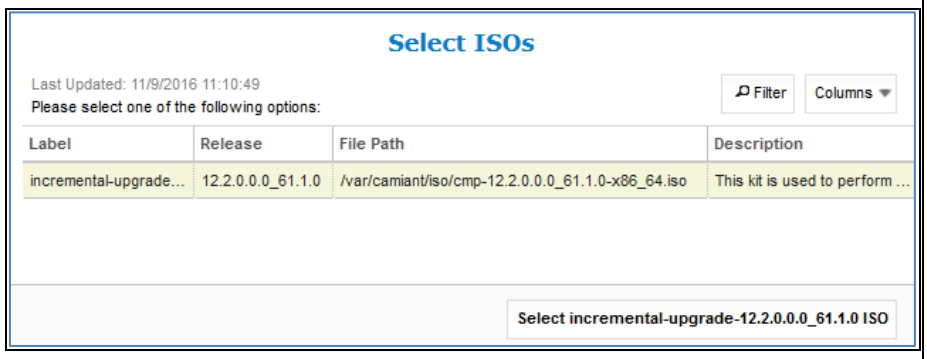
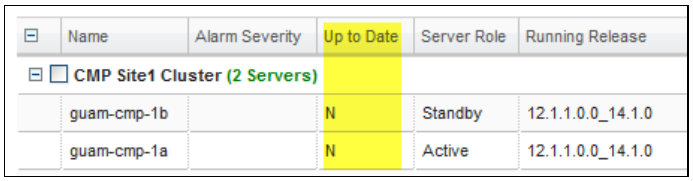
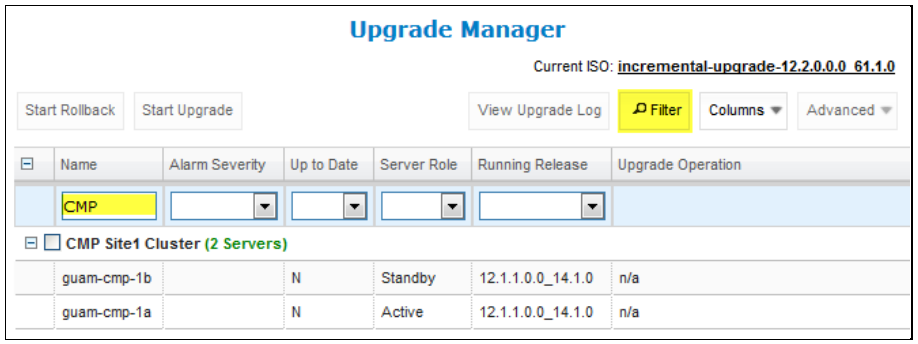
Step	Procedure	Result
5. ☐	**CMP GUI**: Push the Release 12.3 upgrade scripts to all servers	1. Navigate to U**pgrade → ISO Maintenance**. 2. Select all the servers in the topology as shown. 3. Select **Operations → Push Script**.  4. On the Push Script warning window, click **OK** to continue the operation. After approximately a minute, a successful message similar to this displays: 
6. ☐	**CMP GUI Access** into Primary CMP Server–Remove old ISO files from servers, if any.	1. Navigate to Upgrade → ISO Maintenance. 2. Select the server(s) that show any old ISOs. 3. Select **Operations → Delete ISO** to remove any older ISOs.  4. Click **OK** to continue and wait until the successful deletion message displays. 5. Wait until the ISO Maintenance page refreshes and the ISO column does not show any old ISO files.

Step	Procedure	Result
7. ☐	**CMP GUI:** Distribute ISOs to CMP/MPE/MRA/ Mediation servers **NOTE:** This step depends on the ISO type. Distribute ISOs accordingly.	1. Navigate to Upgrade → ISO Maintenance. 2. Filter by server type (optional but preferred step) 3. One application at a time, check one server type (MPE/MRA/CMP/Mediation) for upgrade. 4. Select **Operations → Upload ISO**.  5. Enter the configuration information: Mode = SCP 6. ISO Server Hostname / IP = <*IP address where the ISOs are located*> User = admusr Password = <*admusr password of the server*> Source ISO Full Path = /var/TKLC/upgrade/<*server type iso filename*>  7. Click **Add.** When completed, the ISO column is populated with the ISO and a notification of [100%]  8. Repeat for all cluster types

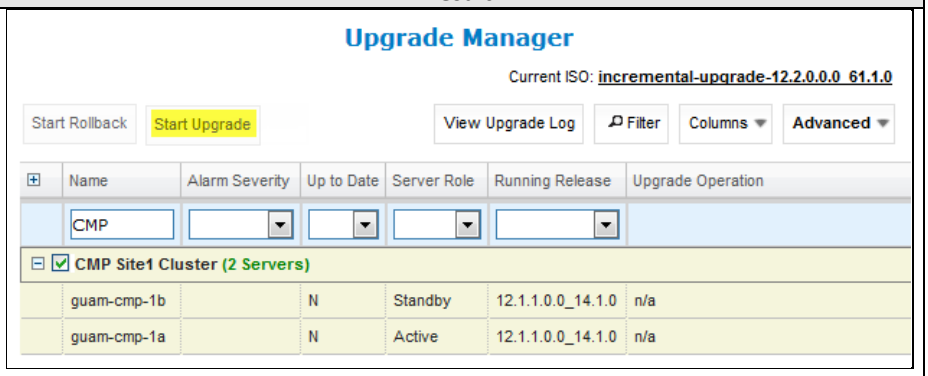
Step	Procedure	Result
8. ☐	**CMP GUI:** Verify ISO distribution to all the Servers	1. Navigate to **Upgrade → ISO Maintenance**. 2. Verify that the Release 12.3 ISO file of the correct type is shown for each server. When completed, the ISO column is populated with the ISO and a notification of [100%]  **NOTE**: For those servers where the ISO file was copied from the local machine, there is not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management feature.

9. ☐	**Primary Active CMP:** ssh to primary active CMP and copy ISO to /var/camiant/iso	1. Logon to the primary active CMP as admusr and copy the 12.3 ISO to the directory `/var/camiant/iso`
		`$ sudo cp -p /var/TKLC/upgrade/cmp-12.3.<…>.iso /var/camiant/iso/`
		2. Verify the file was successfully copied:
		`$ ls /var/camiant/iso/`

Name	Appl Type	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster			
guam-cmp-1a	CMP Site1 Cluster	10.240.152.75	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-cmp-1b	CMP Site1 Cluster	10.240.152.76	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1	MPE			
guam-mpe-1a	MPE	10.240.152.79	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1b	MPE	10.240.152.80	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1	MRA			
guam-mra-1a	MRA	10.240.152.77	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1b	MRA	10.240.152.78	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]

Step	Procedure	Result
10. ☐	**CMP GUI:** Locate the 12.3 Upgrade ISO	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the current ISO, in this case it is labeled Install kit.  A dialog box opens with a description of the ISO that was copied into `/var/camiant/iso` displays. 3. Highlight the available ISO file and click **Select incremental-upgrade-12.3…** on the bottom of the window:  4. On the confirmation window, click OK. Within a few seconds, the Up to Date column transitions from Y (meaning up-to-date) to N (meaning needs upgrade). 
11. ☐	**CMP GUI**: Upgrade Primary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter cmp in the Name field.  3. Select the Primary CMP cluster 4. Click **Start Upgrade**.

Step	Procedure	Result



5. Click **OK** to confirm and continue the operation.

   The first action upgrades the standby server in the CMP cluster.

   NOTE: This takes approximately 30 minutes to complete.

The Upgrade Operation column shows a progress bar along with the upgrade activities.

During the upgrade activities, the server being updated changes to OOS (Out of Service) and the following alarms may be generated. They are considered normal reporting events:

Expected Critical Alarms

31283 HA Server Offline
31227 HA Availability Status Failed
70025 QP Slave Database is a Different Version than the Master
70001 QP_procmgr failed

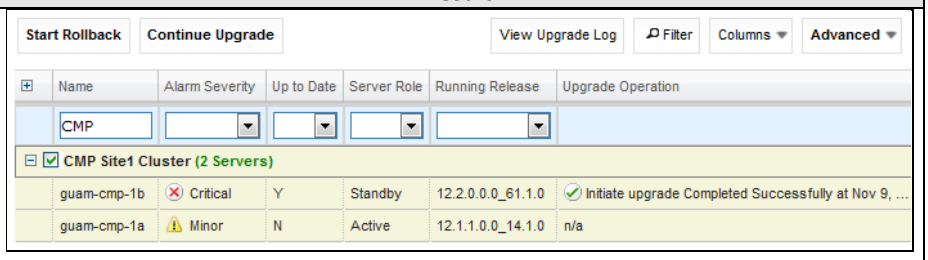
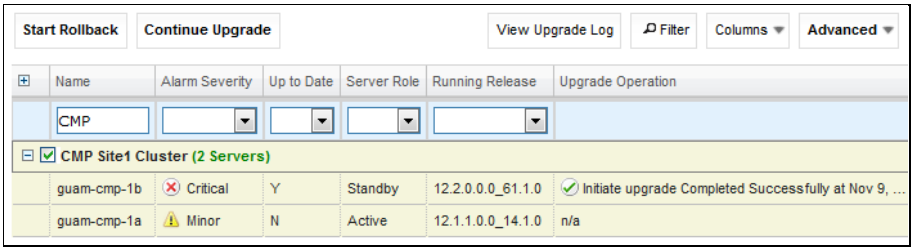
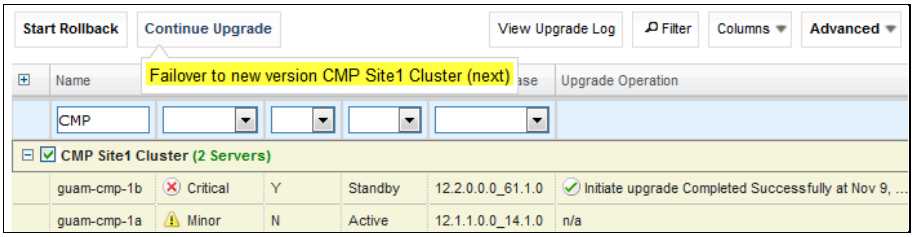
Expected Major Alarm

70004 QP Processes Down for Maintenance.

Expected Minor Database Replication Alarms

70503 Server Forced Standby
70507 Upgrade In Progress
70500 System Mixed Version
70501 Cluster Mixed Version
31106 Database merge to parent failure
31107 Database merge from child failure
31101 Database replication to slave failure
31114 DB replication over SOAP has failed
31282 HA Management Fault

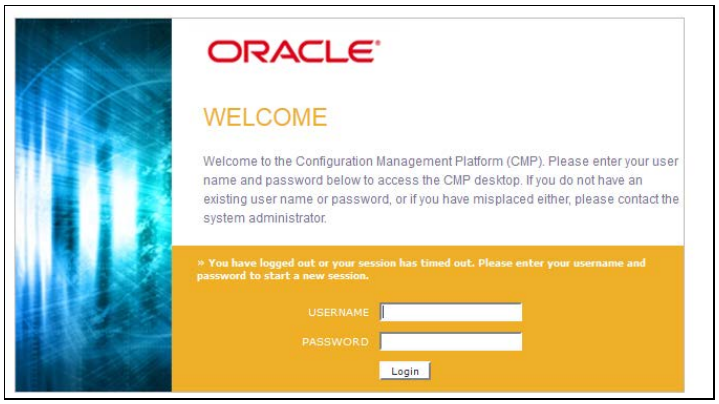
Upgrade is complete on the first server in the cluster when the successful message displays in the Upgrade Operation column.

Step	Procedure	Result
		
12. ☐	**CMP GUI:** Verify the upgrade is successful	Navigate to **Upgrade → Upgrade Manager**. View the cluster. At this point, the standby server is on 12.3 and the other server in the cluster is on 12.1.x. The Up To Date column shows Y for the 12.3 server and N for the 12.1.x server.  The critical alarm 70025 is active as well as the minor alarms 70500 and 70501.
13. ☐	**CMP GUI**: Continue upgrade on CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that the Primary CMP cluster is selected. 3. Click **Continue Upgrade**. Notice the Failover to new version message.  4. Click **OK** to confirm and continue with the operation. The specific action takes approximately a minute to complete.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>14. ☐</td><td>CMP GUI: Re-login to the CMP VIP</td><td>1. Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address.

The Policy Release 12.3 CMP GUI login form opens.

2. Login and password credentials are the same as the credentials prior to the-upgrade.

 
</td></tr>
<tr><td>15. ☐</td><td>CMP GUI: Verify the Policy release</td><td>1. Navigate to HELP→About.

2. Verify the release displayed is 12.3</td></tr>
<tr><td>16. ☐</td><td>CMP GUI: Critical alarms</td><td>Critical alarm 70025 and the minor alarms 70503, 70501, 70500 are listed.

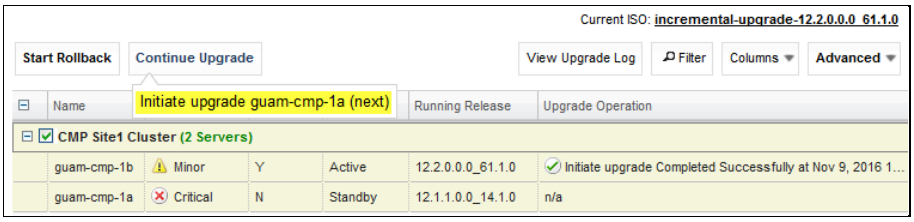
These alarms are expected and remain until all CMP clusterss have been upgraded to the same version.

Current Major Alarm
<table>
<tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th><th>OAM VIP</th><th>Server</th></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td><td>10.240.152.88</td><td>guam-cmp-1a 10.240.152.75</td></tr>
</table>
Current Minor Alarms
<table>
<tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th><th>OAM VIP</th><th>Server</th></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70503</td><td>The server is in forced standby</td><td>10.240.152.88</td><td>guam-cmp-1b 10.240.152.76</td></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70501</td><td>The Cluster is running different versions of software</td><td>10.240.152.88</td><td>guam-cmp-1b 10.240.152.76</td></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70500</td><td>The system is running different versions of software</td><td>10.240.152.88</td><td>guam-cmp-1b 10.240.152.76</td></tr>
</table></td></tr>
<tr><td>17. ☐</td><td>CMP GUI: Verify the Policy Release 12.3 CMP is Active</td><td>1. Navigate to Upgrade → Upgrade Manager.

2. Verify the following:

- The Active server is running release 12.3
- The Standby server is running the previous release

<table>
<tr><th></th><th>Name</th><th>Alarm Severity</th><th>Up to Date</th><th>Server Role</th><th>Running Release</th><th>Upgrade Operation</th></tr>
<tr><td colspan="7">CMP Site1 Cluster (2 Servers)</td></tr>
<tr><td></td><td>guam-cmp-1b</td><td>Minor</td><td>Y</td><td>Active</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at Nov 9, 2...</td></tr>
<tr><td></td><td>guam-cmp-1a</td><td>Critical</td><td>N</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>n/a</td></tr>
</table></td></tr>
</table>

Step	Procedure	Result
18. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster 3. Click **Continue Upgrade** button. Notice the Initiate upgrade <*standbyserver*> (next) message  4. Click **OK** on the pop-up to continue the upgrade on the remaining server in the CMP cluster **NOTE:** Remaining CMP server takes approximately 30 minutes to complete. **NOTE:** When the server is upgraded, the server goes into the OOS state. **Expected Critical Alarms** **31227** HA availability status failed **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>19. ☐</td><td>CMP GUI: Tracking the upgrade complete</td><td>1. Navigate to Upgrade → Upgrade Manager.

The last step in the upgrade for the first CMP cluster is to wait for replication to complete.

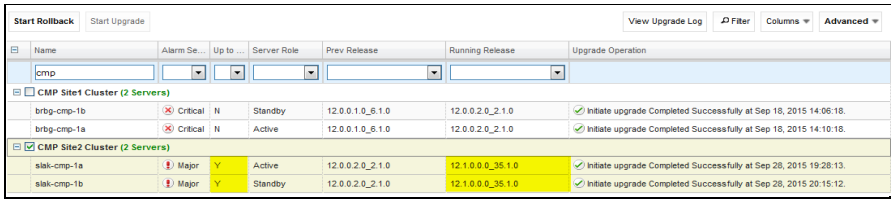
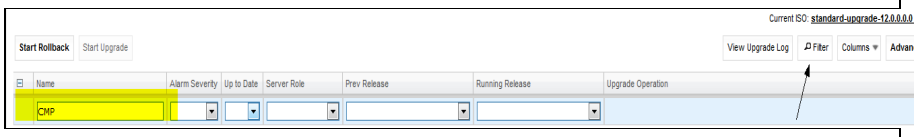
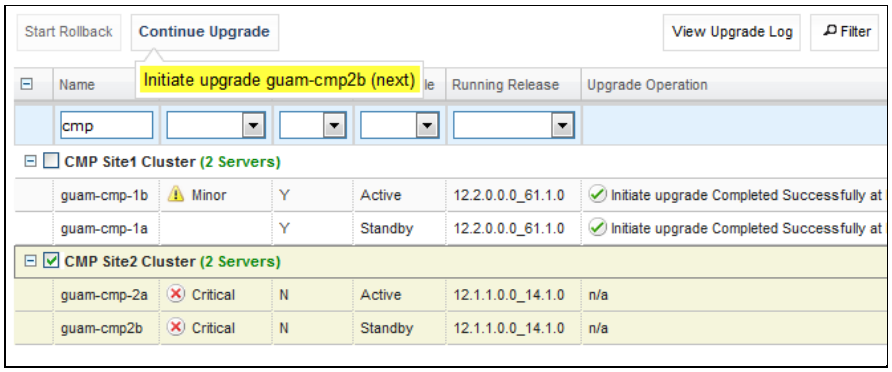
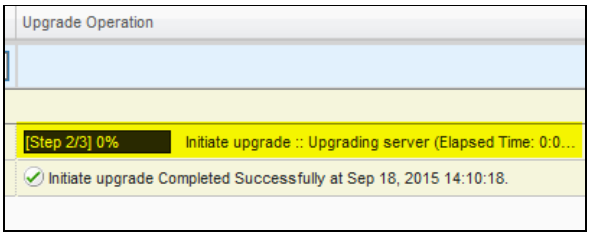
2. With the CMP cluster selected, click View Upgrade Log.

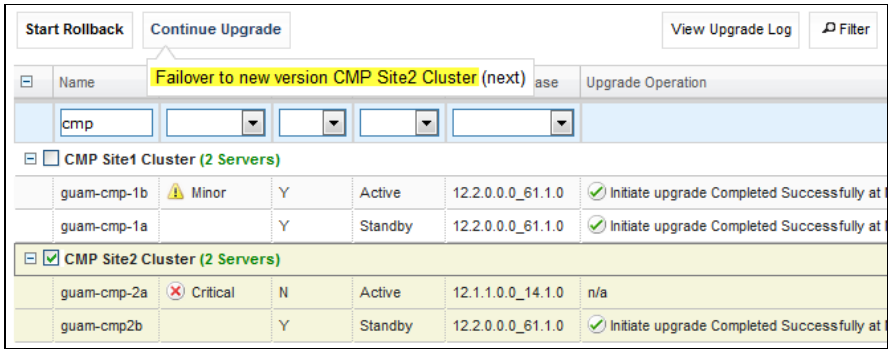
A window opens where you can verify that synchronization has taken place.

Upgrade Log
Cluster Name: CMP Site1 Cluster
Last Update: 11/10/2016 9:01:00
<table><tr><th>ID</th><th>Parent ID</th><th>Action Name</th><th>Duration</th><th>Scope</th><th>Hostname</th><th>Result</th><th>Mode</th></tr><tr><td>1</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Manual</td></tr><tr><td>2</td><td>1</td><td>Upgrading server</td><td>0:22:00</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>3</td><td>1</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>4</td><td>1</td><td>Wait for replication to synchronize</td><td>0:00:09</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>5</td><td>0</td><td>Failover to new version</td><td>0:00:00</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Manual</td></tr><tr><td>6</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Manual</td></tr><tr><td>7</td><td>6</td><td>Upgrading server</td><td>0:21:50</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>8</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>9</td><td>6</td><td>Wait for replication to synchronize</td><td>0:00:29</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>10</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr></table></td></tr>
<tr><td>20. ☐</td><td>CMP GUI: Verify the status of the upgraded CMP server.</td><td>Navigate to Upgrade → Upgrade Manager.

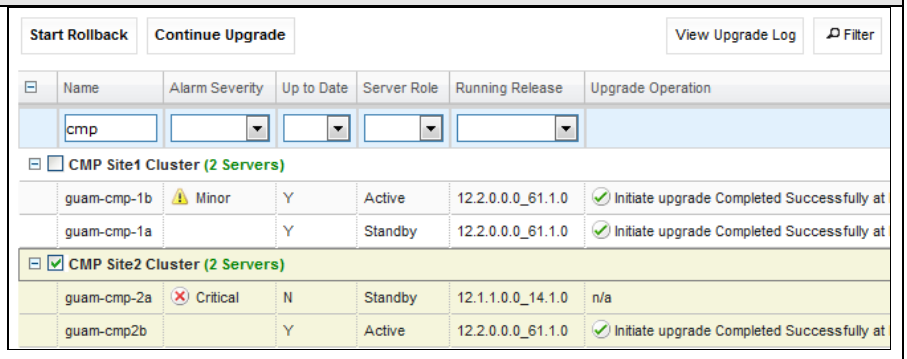
<table><tr><th></th><th>Name</th><th>Alarm Severity</th><th>Up to Date</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr><tr><td colspan="8">CMP Site1 Cluster (2 Servers)</td></tr><tr><td></td><td>guam-cmp-1b</td><td>Minor</td><td>Y</td><td>Active</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr><tr><td></td><td>guam-cmp-1a</td><td></td><td>Y</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr></table>
• Successful upgrade status shows both servers running the Release 12.3 in the Running Release column and Y for both servers in the Up To Date column
• Active/standby state for both servers in the Primary CMP cluster.</td></tr>
<tr><td>21. ☐</td><td>Proceed to next upgrade procedure</td><td>• At this point, the primary site is running Release 12.3.
• The Secondary site, if it exists, is on release 12.2.x.
• Proceed to the next procedure to upgrade the secondary CMP cluster.</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED</td></tr>
</table>

8.3.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP cluster	Navigate to **Upgrade → Upgrade Manager**. • Primary CMP is completely upgraded to 12.3 • Secondary CMP cluster is on 12.2.x 
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter CMP in the Name field.  3. Select the Secondary CMP cluster at Site2 4. Click **Continue Upgrade**.  5. Click **OK** to confirm and continue with the operation. This continues the upgrade of the standby server only in the CMP cluster **NOTE:** This takes approximately 30 minutes to complete. The Upgrade Operation column displays the In Progress status along with the upgrade activities.  During the Upgrade activities, the following alarms may be generated and considered normal reporting events.

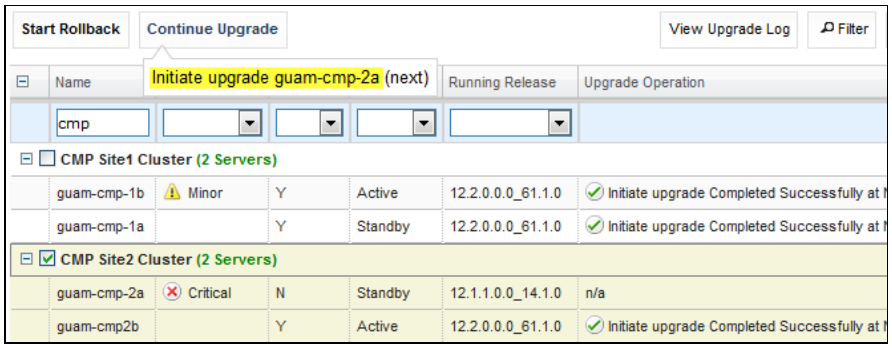
Step	Procedure	Result
		Expected Critical Alarms **31283** Lost Communication with server **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault
3. ☐	**CMP GUI**: Continue Upgrade Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP Server cluster at Site2 3. Click **Continue Upgrade**. When hovering over the button, the message displays the next action, which is to failover to new version CMP Site2 cluster.  4. Click **OK** to confirm and continue with the operation. 5. The specific action takes a minute to complete. Wait until the upgraded server is active, running 12.3.

Step	Procedure	Result



6. Click the checkbox for the Secondary CMP Server cluster at Site2

7. Click **Continue Upgrade**. When hovering over the button, the message displays the next action, which is upgrading the remaining CMP in standby, running 12.1.x



8. Click **OK** to confirm and continue with the operation,

During the Upgrade activities, the following alarms may be generated and considered normal reporting events.

Expected Critical Alarms

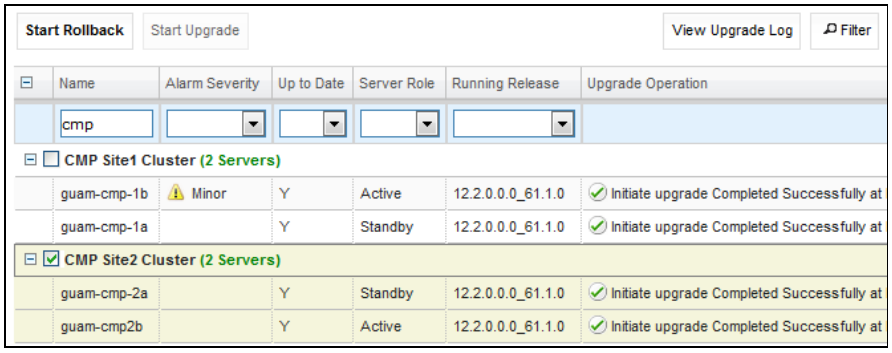
31283 Lost Communication with server
70001 QP_procmgr failed
70025 QP Slave database is a different version than the master

Expected Major Alarm

70004 QP Processes down for maintenance

Expected Minor Alarms

70503 Upgrade Director Server Forced Standby
70507 Upgrade Director In Progress
70500 Upgrade Director System Mixed Version
70501 Upgrade Director Cluster Mixed Version
31114 DB Replication over SOAP has failed
31106 DB Merge To Parent Failure
31107 DB Merge From Child Failure
31101 DB Replication To Slave Failure
31282 HA management fault

Step	Procedure	Result
4. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	Navigate to **Upgrade → Upgrade Manager**. • Successful upgrade status shows Release 12.3 in the Running Release column. • The Upgrade Operation column shows the Inititiate Upgrade Completed Successfully at… message 
5. ☐	**CMP GUI:** Verify alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarm** **70500** System Mixed Version
6. ☐	Procedure is complete.	• All CMP clusters upgrade are complete and running Release 12.3. • ALL MRAs and MPEs are on Release 12.2.x At this point, the Policy Management system is running in mixed-version mode.
THIS PROCEDURE HAS BEEN COMPLETED		

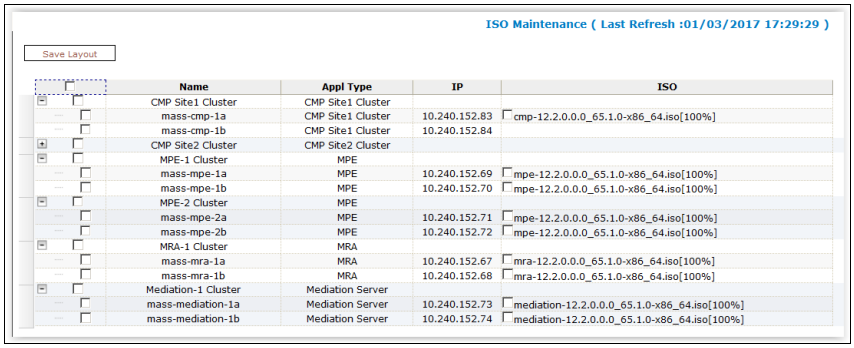
9. UPGRADE NON-CMP CLUSTERS (12.2.X TO 12.3)

The following procedures upgrade a site/segment containing one or more non-CMP clusters such as MPEs, MRAs and Mediations .They are applicable for Release 12.2.x upgrade to Release 12.3.0.

NOTE: An upgrade of up to 4 clusters can be performed in parallel.

9.1 Site/Segment Upgrade Preparation

9.1.1 Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into Primary site CMP	Use the supported browser to login as administrative user or as a user with administrator privileges.
2. ☐	**CMP GUI:** Verify Current Upgrade Manager status and Software Release 12.3 ISO files	1. Navigate to **Upgrade → Upgrade Manager**. - Verify that all CMP clusters have both Active, and Standby status. - Verify that all MPE, MRA, and Mediation clusters have both Active and Standby status. 2. Navigate to **Upgrade → ISO Maintenance**. - Verify that Policy release 12.3 ISO files are available for all clusters. One ISO per server type as shown in the example below 
THIS PROCEDURE HAS BEEN COMPLETED		

ISO Maintenance (Last Refresh :01/03/2017 17:29:29)

Save Layout

Name	Appl Type	IP	ISO
CMP Site1 Cluster	CMP Site1 Cluster		
mass-cmp-1a	CMP Site1 Cluster	10.240.152.83	cmp-12.2.0.0.0_65.1.0-x86_64.iso[100%]
mass-cmp-1b	CMP Site1 Cluster	10.240.152.84	
CMP Site2 Cluster	CMP Site2 Cluster		
MPE-1 Cluster	MPE		
mass-mpe-1a	MPE	10.240.152.69	mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
mass-mpe-1b	MPE	10.240.152.70	mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
MPE-2 Cluster	MPE		
mass-mpe-2a	MPE	10.240.152.71	mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
mass-mpe-2b	MPE	10.240.152.72	mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
MRA-1 Cluster	MRA		
mass-mra-1a	MRA	10.240.152.67	mra-12.2.0.0.0_65.1.0-x86_64.iso[100%]
mass-mra-1b	MRA	10.240.152.68	mra-12.2.0.0.0_65.1.0-x86_64.iso[100%]
Mediation-1 Cluster	Mediation Server		
mass-mediation-1a	Mediation Server	10.240.152.73	mediation-12.2.0.0.0_65.1.0-x86_64.iso[100%]
mass-mediation-1b	Mediation Server	10.240.152.74	mediation-12.2.0.0.0_65.1.0-x86_64.iso[100%]

9.2 Upgrade Non-CMP Clusters

At this point, all CMP clusters should have been upgraded successfully to release 12.3 before executing the following procedure.

This procedure upgrades one or more non-CMP clusters at a site/segment. The general upgrade sequence is based of Section 2.3.

The following sequence of server types to be upgraded for the system.

1. Upgrade MPE clusters
2. Upgrade MRA clusters
3. Upgrade Mediation clusters

This procedure is generally applicable for those server types and steps to be repeated for every server type.

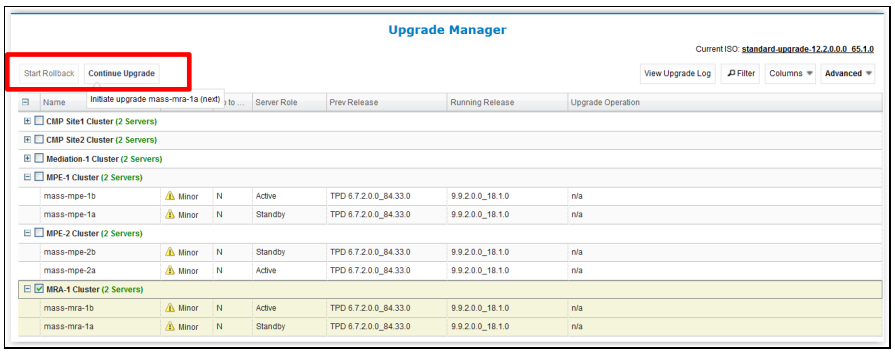
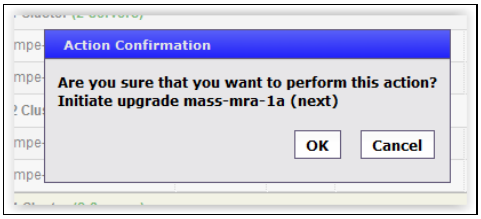
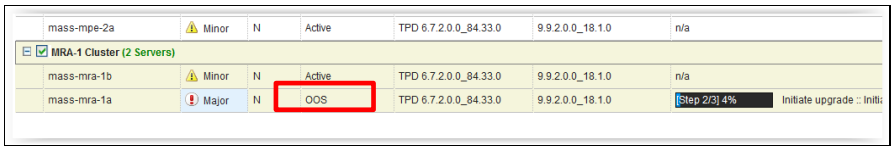
This section can be replicated for each site/segment to be upgraded, allowing the upgrade engineer to add cluster and site specific information.

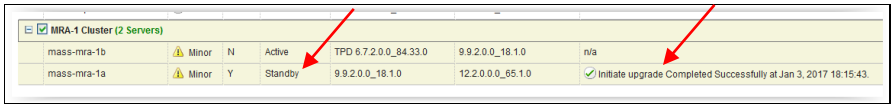
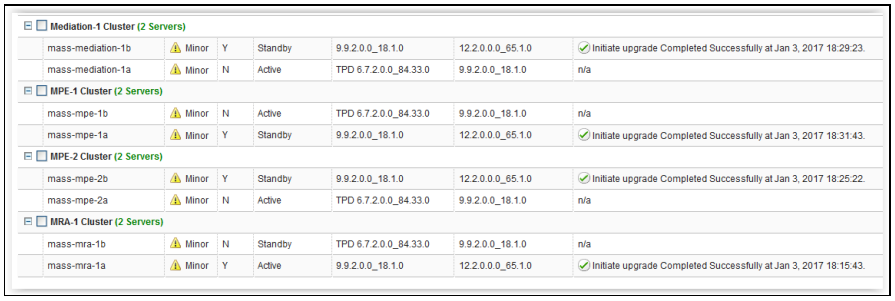
The upgrade procedure is essentially the same for any non-CMP cluster.

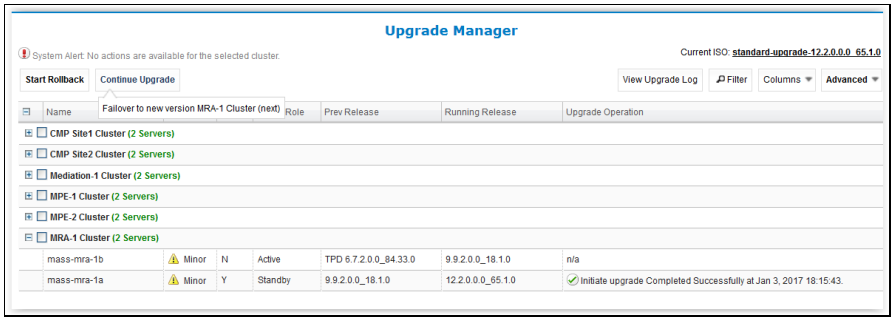
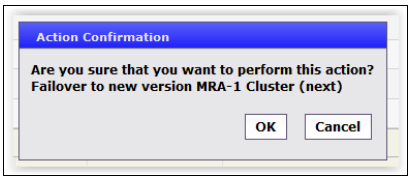
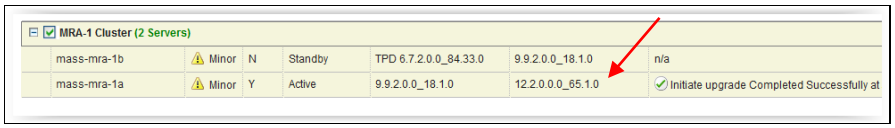
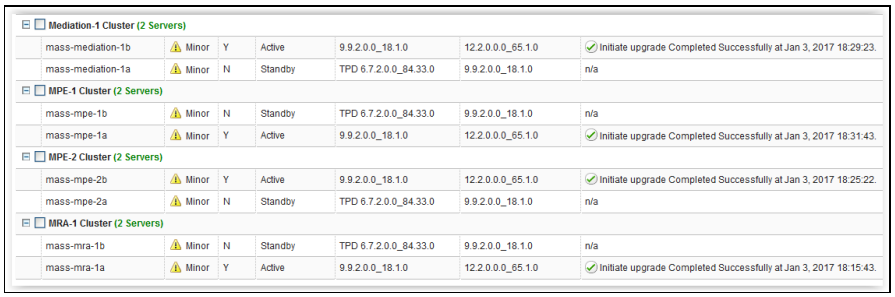
NOTES:

- The default sequence performed by the Upgrade Manager to upgrade a two-server cluster is of the following.
  a. Select and start upgrade on Standby server
  b. Failover one cluster at a time
  c. Re-apply configuration one cluster at a time
  d. Continue upgrade on remaining server
  e. Perform second Re-apply configuration on MPE cluster ONLY.
- Only one cluster can be selected for an upgrade activity, the bulk selection of clusters is not supported in release 12.3.

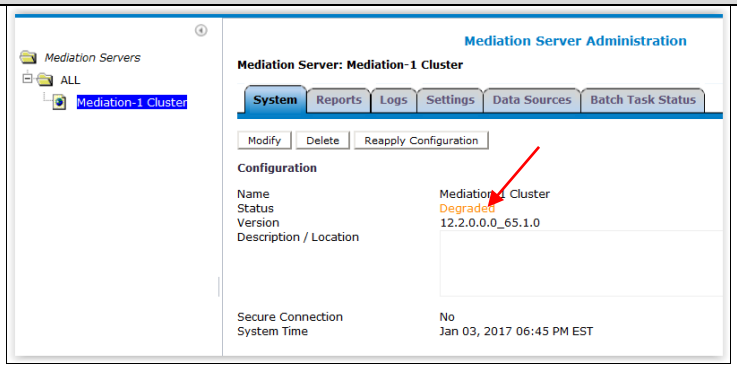
Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the servers to be upgraded	1. Perform the following: a. Check for any known active alarms. b. Reset server counters to make a baseline • For the MPE: **Policy Server→Configuration→Reports → Reset Counters** • For the MRA: **MRA→Configuration→Reports → Reset Counters** • For the Mediation: **Mediation → Configuration → Reports → Reset Counters** 2. Check the KPI Dashboard. 3. Capture screenshots to save for the counter statistics for comparison purposes if unexpected performance issues occur during the upgrade.
2. ☐	**CMP GUI**: Upgrade clusters **NOTE:** Start the	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select a cluster (one cluster at a time) which can be an MRA/MPE/Mediation cluster.

Step	Procedure	Result
	upgrade one cluster at a time and wait for the server being upgraded shows OOS status, then continue with the next cluster and so on. Up to 4 clusters can be performed in parallel. **NOTE:** Each server takes approximately 35 minutes to complete.	3. Click **Continue Upgrade** to initiate the upgrade procedure on the selected cluster.  4. Click **OK** to confirm and continue with the operation. It begins to upgrade the Standby server of that cluster.  5. Wait until the Standby server reports OOS before selecting the next cluster.  Follow the progress status bars in the Upgrade Operation column. It takes approximately 35 minutes to complete. During the upgrade activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster are completely upgraded. **Expected Critical Alarms** **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70001** The qp_procmgr process has failed. **Expected Major Alarms** **31233** High availability path loss of connectivity **70004** The QP processes have been brought down for maintenance. **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed

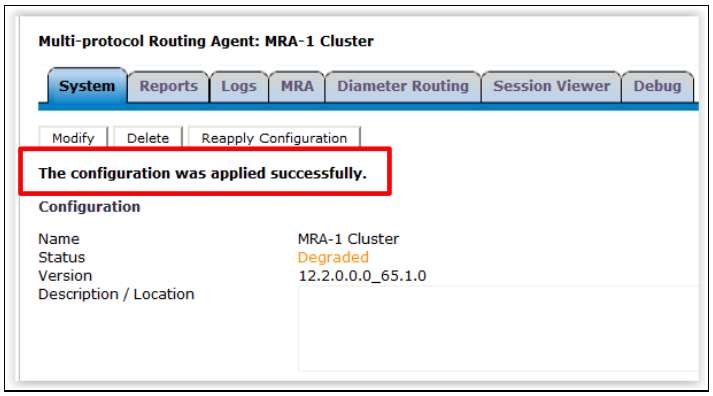
Step	Procedure	Result
		31106 DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed **NOTE:** Each server backout takes approximately 35 minutes to complete. Some minor alarms remained as expected to be auto-cleared but no functional impact. • The server status reverts to standby when the Upgrade is completed which can be verified by the successful message shown in the Upgrade Operation column. The server is now running release 12.3.  • Perform similar check on the status for the remaining clusters as illustrated in the example below–this should be done before proceeding to the next step 

Step	Procedure	Result
3. ☐	**CMP GUI**: Continue Upgrade MRA/MPE/ Mediation clusters with a failover Operation applied to the clusters **NOTE:** Up to 4 clusters can be performed in parallel.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Continue Upgrade** to perform the failover operation on the selected cluster.  3. Click **OK** to confirm and continue with the failover operation for the selected cluster.  4. Wait until failover operation completed and the server running release 12.3 is now Active as shown.  5. Perform the similar failover operation to the remaining clusters before proceeding to the next step. 
4. ☐	**CMP GUI:** Perform reapply configuration on the MPE/MRA/ Mediation clusters after successfully failed over.	• For MPE: Policy Server → Configuration → <*MPE cluster*> → System tab • For MRA: MRA → Configuration→ <*MRA cluster*> → System tab • For Mediation: Mediation → Configuration → < *Mediation cluster* > → System tab The selected cluster has the status Degraded status as shown in the Mediation cluster example below.

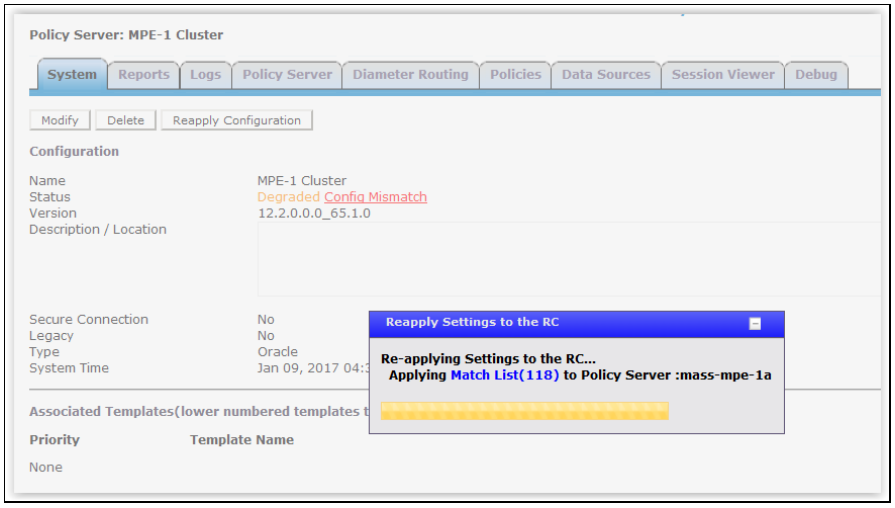
Step	Procedure	Result



1. Click **Reapply Configuration** and wait until the successful message displays as shown.

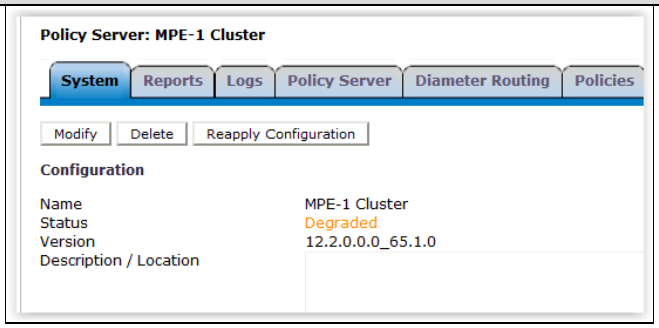


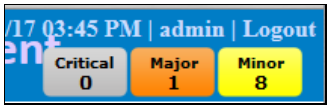
NOTE: The following progress banner ONLY displays for the MPE cluster after the reapply configuration is being performed, but NOT for the MRA and Mediation. This behavior is as expected.



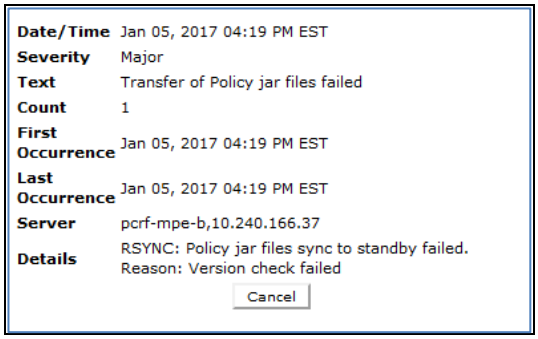
2. Verify that the Version is successfully changed to the upgraded Release 12.3.

   The selected cluster shows Degraded status.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td> 

3. Repeat this step for the remaining backed out clusters before proceeding to the next step.</td></tr>
<tr><td>5. ☐</td><td>CMP GUI: Major alarm 78001</td><td>During the upgrade activities, major alarm 78001 in particular may be generated. And even though it is a normal event, the alarm does not clear by itself. Before continuing verify that the alarm is cleared.
1. Click Major in the upper right part to display the alarms:
 

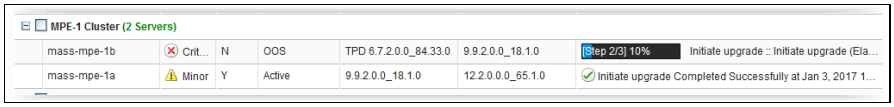
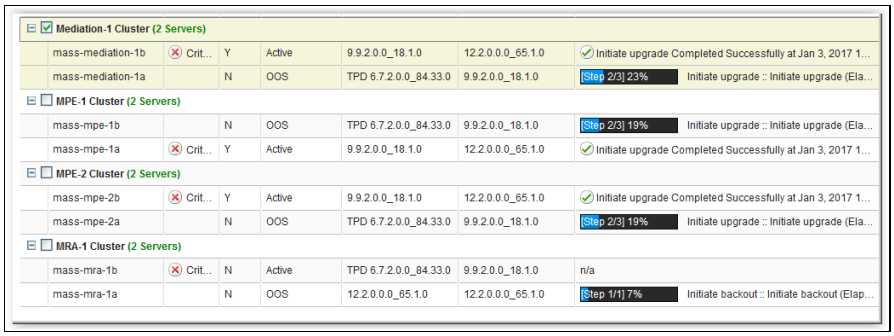
2. Click the binoculars icon on the right to display details for the 78001 major alarm.
 

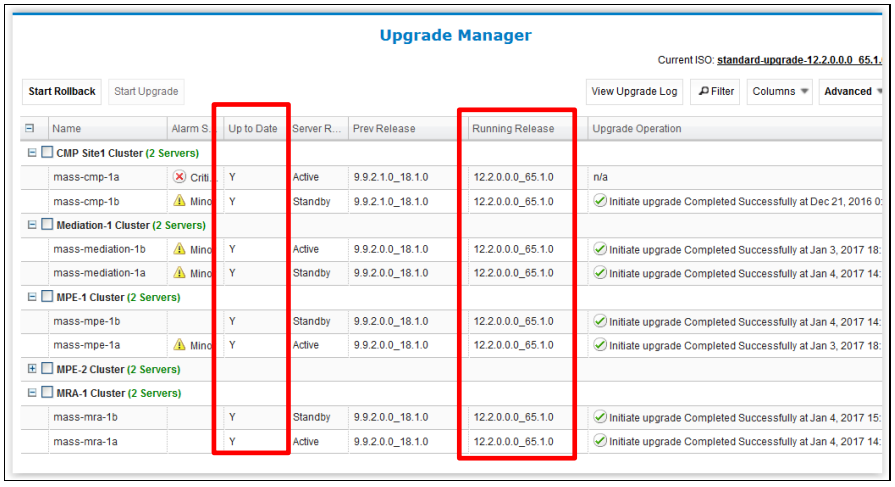
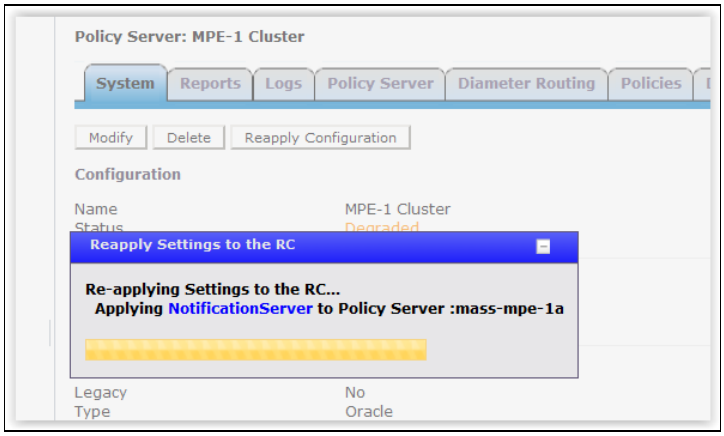
The last line of the details that the reason for the major alarm is that the version check failed.
 

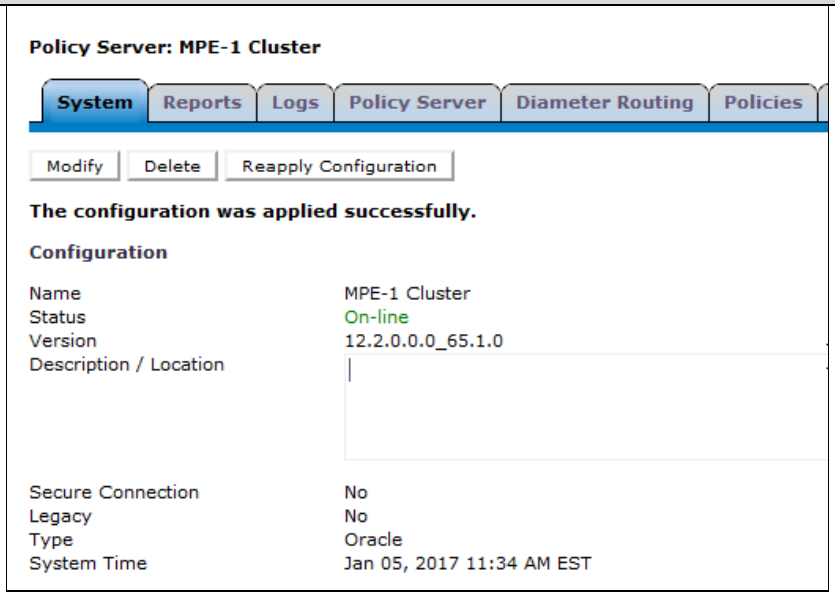
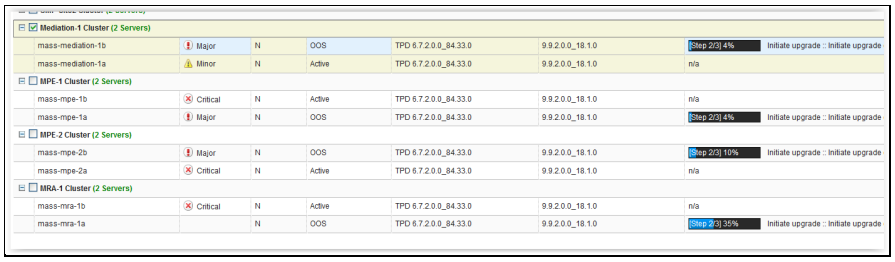
- If you see a different reason, stop and contact My Oracle Support.
- If you see that the version check failed, continue here.

3. Navigate to System Wide Reports > Alarms > Active Alarms and select the 78001 major alarm
 

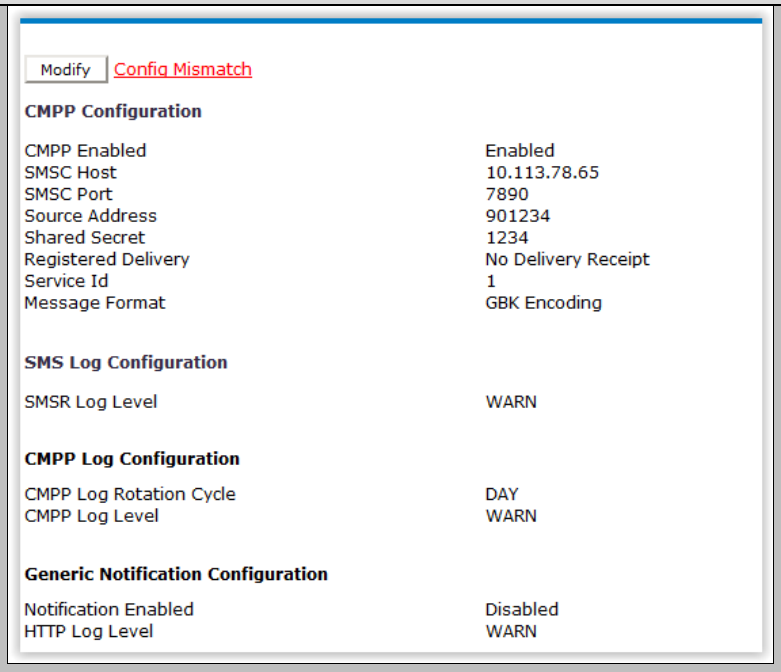
4. Click the trash can icon on the right to clear this alarm.</td></tr>
<tr><td>6. ☐</td><td>CMP GUI: Continue Upgrade on Standby MRA/MPE/Mediation servers</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Select the cluster (one cluster at a time) which can be an MRA/MPE/Mediation.</td></tr>
</table>

Step	Procedure	Result
	NOTE: Start the upgrade one cluster at a time and wait until the server being performed shows OOS status, then continue with the next cluster and so on. Up to 4 clusters can be performed in parallel. **NOTE:** Each server takes approximately 35 minutes to complete.	3. Click **Continue Upgrade** to initiate the upgrade procedure on the selected cluster. 4. Click **OK** to confirm and continue with the operation. The upgrade begins on the Standby server of that cluster.  5. Wait until the Standby server reports OOS before selecting the next cluster 6. As shown in the example below showing four clusters upgrade in parallel.  Follow the progress status bars in the Upgrade Operation column. It takes approximately 35 minutes to complete. During the upgrade activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster are completely upgraded. **Expected Critical Alarms** **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70001** The qp_procmgr process has failed. **Expected Major Alarms** **31233** High availability path loss of connectivity **70004** The QP processes have been brought down for maintenance. **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed **NOTE:** Each server backout takes approximately 35 minutes to complete. Some minor alarms remained as expected to be auto-cleared but no functional impact. • The server status reverts to standby when the Upgrade is completed which can be verified by the successful message displaying in the Upgrade

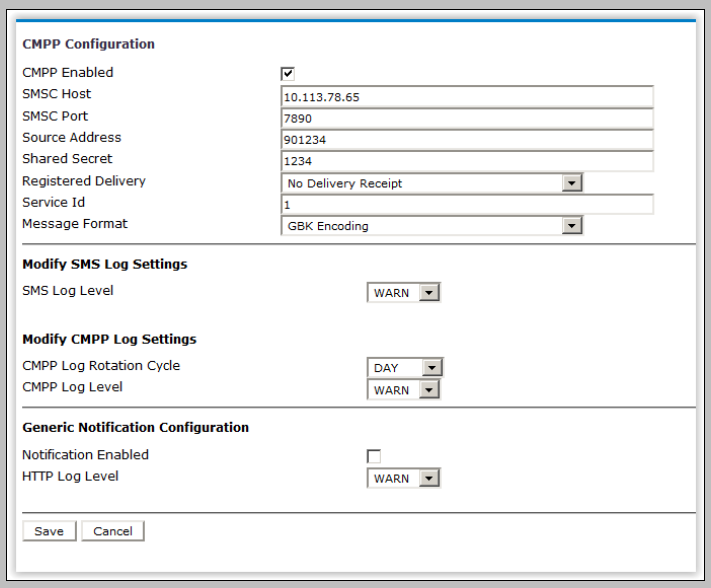
Step	Procedure	Result
		Operation column. • All the upgraded clusters should now be Running Release 12.3 with the Up to Date column showing Y for every cluster.  **NOTE:** The subsequent instruction ONLY applicable to all upgraded MPE clusters with second Reapply configuration, otherwise skip to the next Step. 7. Navigate to **Policy Server → Configuration →** < *MPE cluster*> **→ System**. 8. The selected MPE cluster has the status shown as Degraded status. 9. Click **Reapply Configuration** and wait for the successfully message displays as shown.  10. Verify that the status is showing On-line and the Version is showing the Release 12.3.0.0.0_65.1.0 as shown.

Step	Procedure	Result
		 11. Apply the same above instructions of performing this second Reapply Configuration to the rests of upgraded MPE clusters. 12. After it is complete, proceed to the next Step.
7. ☐	**REPEAT** Steps 1 through 6 for next batch of MPE/MRA /Mediation clusters	As shown in the example below showing four clusters upgrade in parallel .  Proceed with the next batch of four clusters until all Policy sites/segments have been upgraded to release 12.3.
8. ☐	**<Wireless-C Mode> CMP GUI:** Modify/save SMSR configuration	1. Navigate to **System Administration → SMS Relay → Modify**. Initial access into this configuration upon upgrade to release 12.3, the screen configuration shows Config Mismatch.

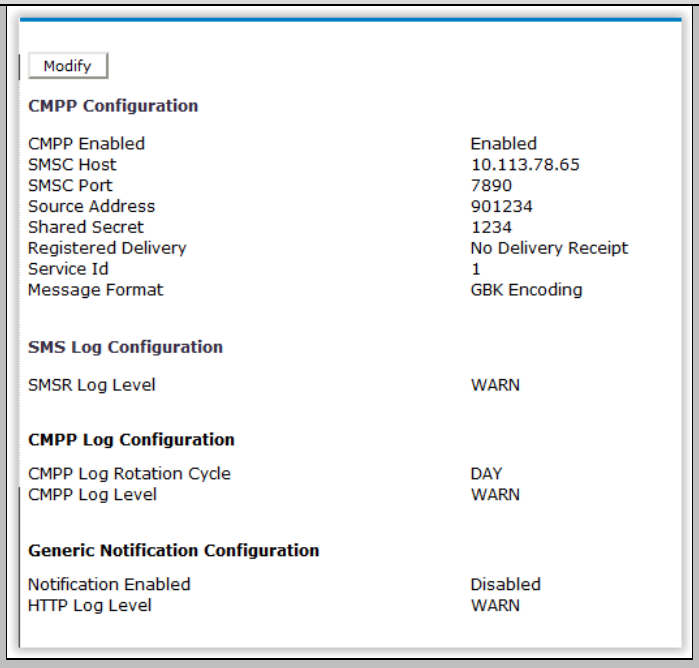
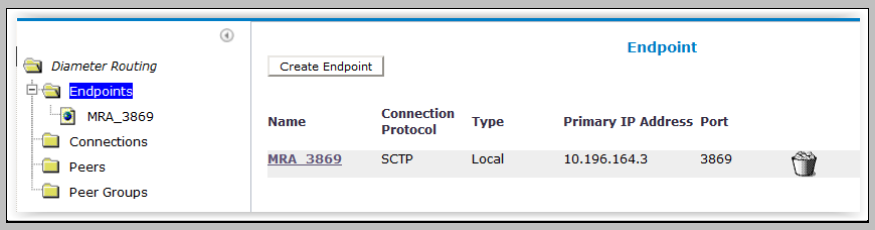
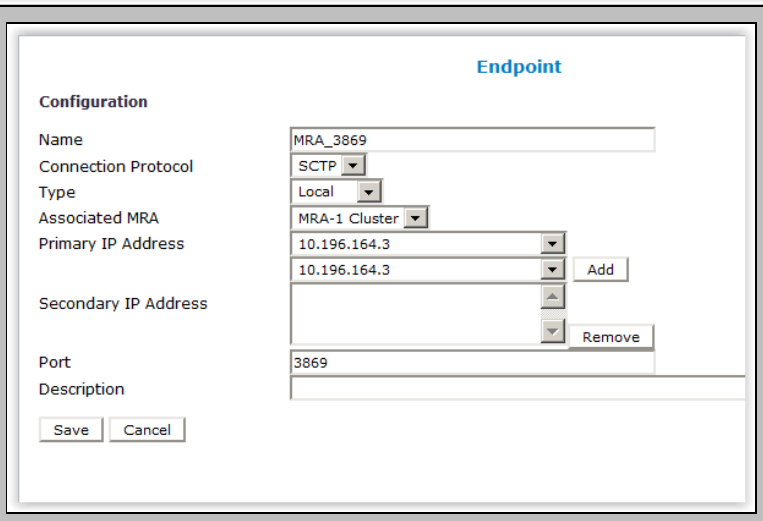
Step	Procedure	Result

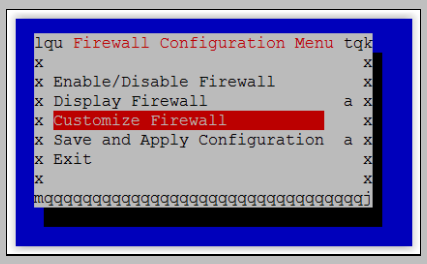
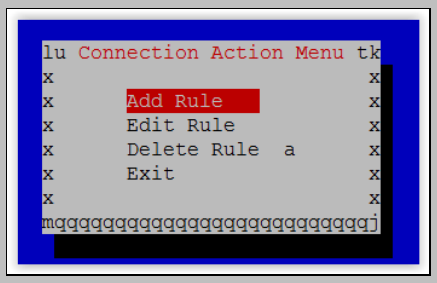
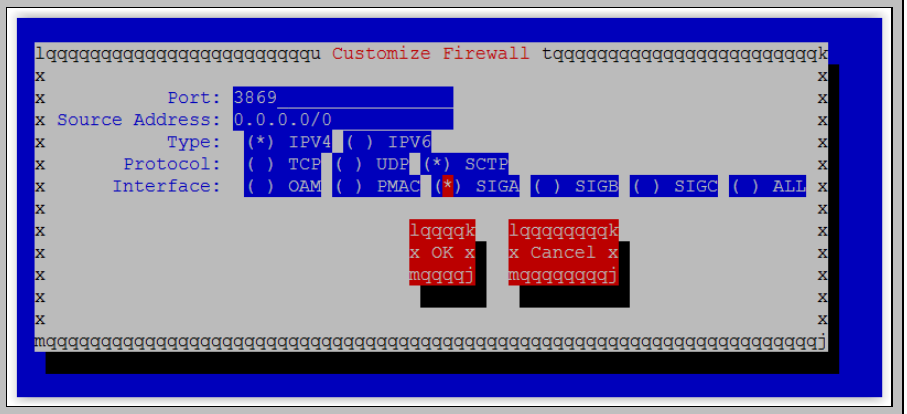
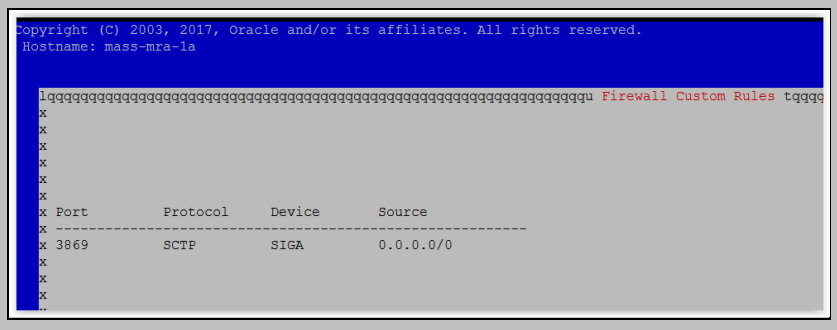


2. Click **Modify** to view the SMSR configuration–DO NOT change any of the configuration if it has been working in the past.

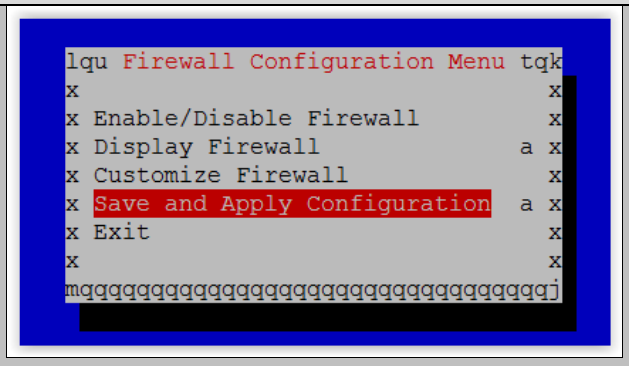


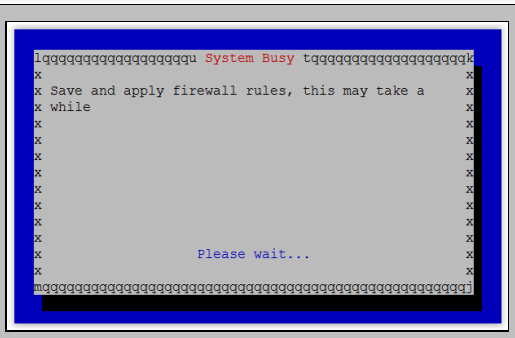
3. Click **Save** to re-save the configuration and continue as shown.

Step	Procedure	Result
		 **NOTE:** The Config Mismatch message is no longer there with the saved configuration.
9. ☐	**<Wireless-C Mode> Checking and Adding** MRA Firewall rules for Diameter Routing with SCTP Port: 3869	1. **CMP GUI:** Navigate to **MRA → Diameter Routing → Endpoints.**   2. Login into Active MRA server and run the platcfg utility to access the Firewall configuration as shown. `# su-platcfg`

Step	Procedure	Result
		3. Navigate to **Policy Configuration → Firewall**.  4. Select **Customize Firewall** and click **Edit** to add the following rules .  5. Define the Firewall Rule as in the example below  6. Click **OK** to save and continue. 7. Verify that the added Customed Firewall Rule is as shown.  8. Select **Save and Apply Configuration** as shown.

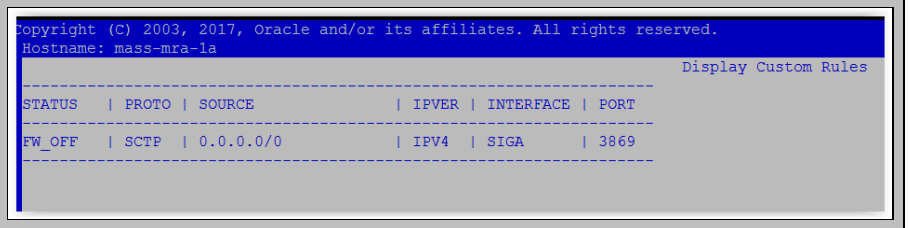
Step	Procedure	Result





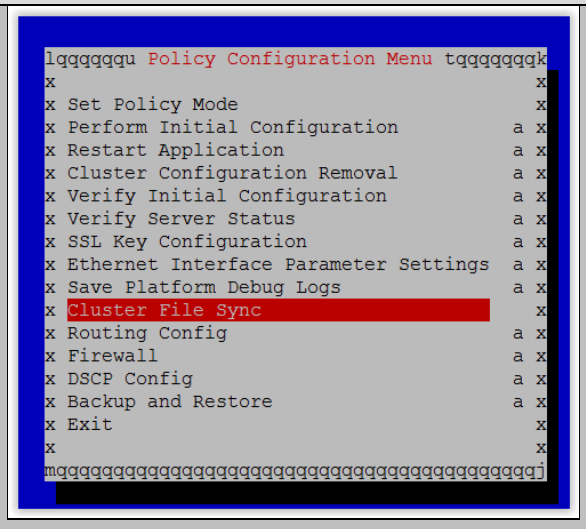
9. Validate the applied customed firewall rule with the menu option as shown.

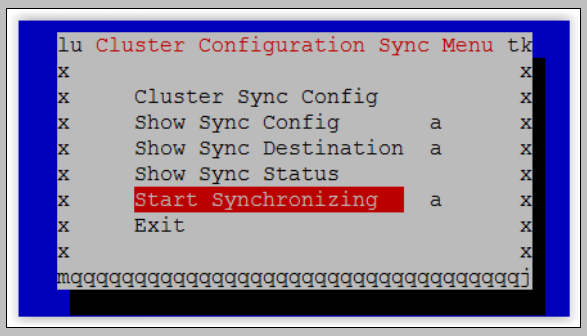
10. Select **Display Custom Rules** to view the rule.



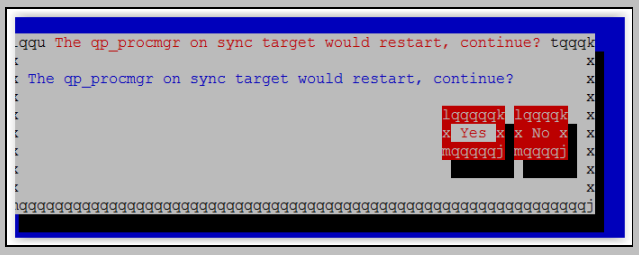
11. Return to the Cluster File Sync menu and select **Start Synchronizing** to synch the added Firewall Rule to the mated MRA server.

Step	Procedure	Result

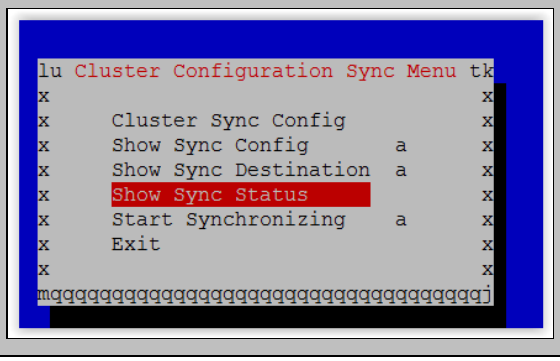


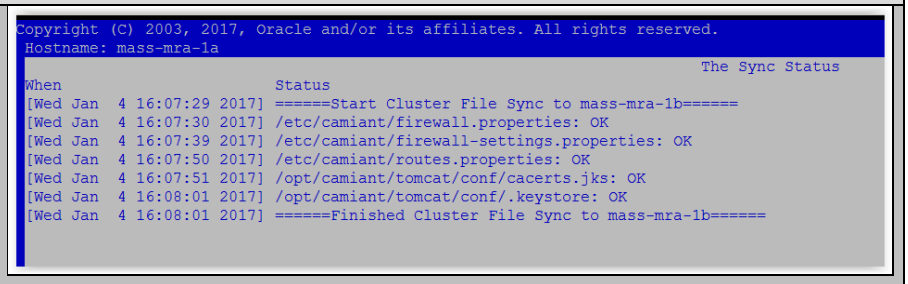


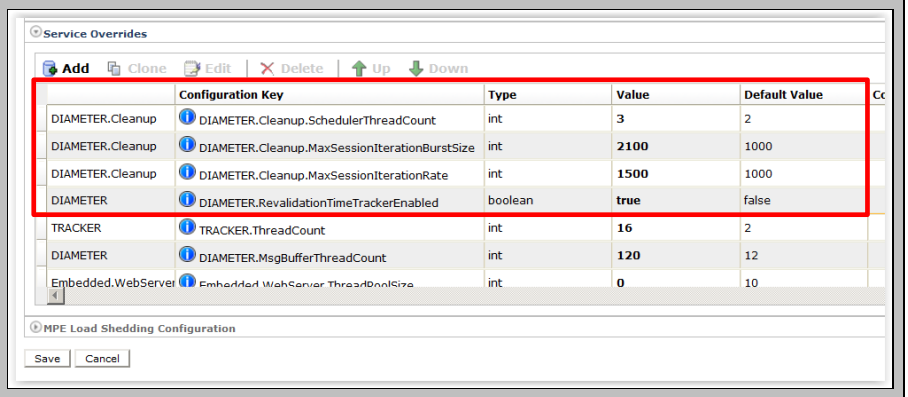
12. Click **Yes** to continue and there are activity messages displayed during the synchronization process as expected.



13. Validate that the synchronization is successful by selecting **Show Sync Status**. Ensure that the related Firewall.properties showing OK message.



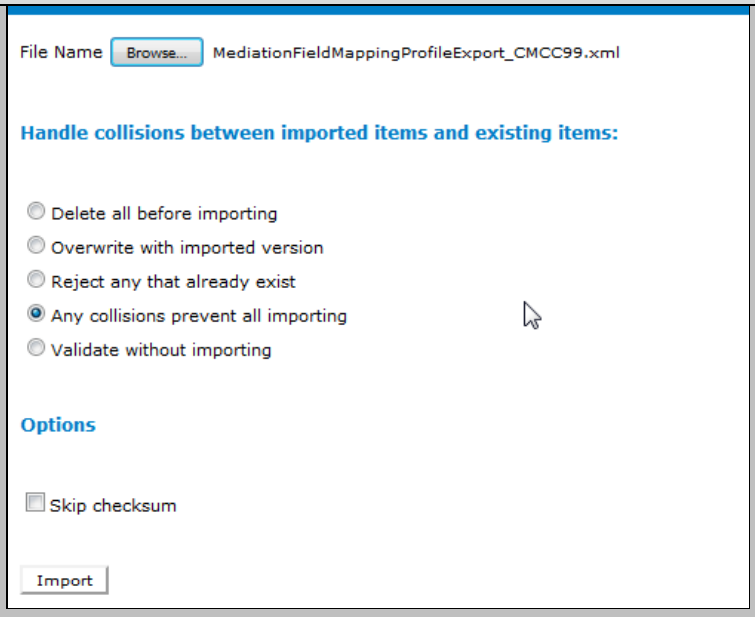
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>


14. Exit the platcfg utility and return to the shell prompt.
</td></tr>
<tr><td>10. ☐</td><td>< Wireless-C Mode> CMP GUI: MPE Service Override configuration for Stale Sessions Handling</td><td>
1. Navigate to Policy Server → All → < MPE cluster > → Policy Server → Advanced → Service Overrides → Add.
2. Add the following Configuration Parameters in the Service Overrides sections and click Save to continue as shown .
DIAMETER.Cleanup.SchedulerThreadCount = 3
DIAMETER.Cleanup.MaxSessionIterationBurstSize = 2100
DIAMETER.Cleanup.MaxSessionIterationRate = 1500
DIAMETER.RevalidationTimeTrackerEnabled = true


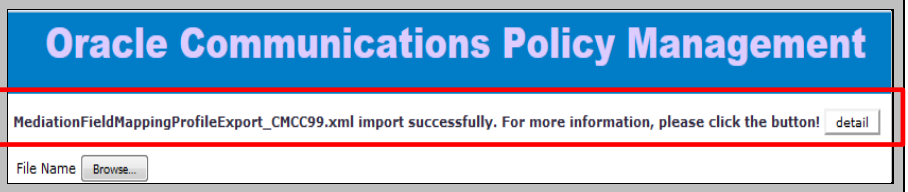
</td></tr>
<tr><td>11. ☐</td><td><Wireless-C Mode> Re-importing the Mediation Server Field Mapping profile</td><td>
1. Login to the active Mediation server.
2. Perform secured copy (SCP)/upload of the Field Mapping profile configuration file to the local PC where the CMP GUI browser is launched -
<code># scp -p /opt/camiant/mediation/cfg/MediationFieldMappingProfileExport_CMCC99.xml <Active CMP IP address>:/opt/camiant/mediation/cfg</code>
3. Logout of the Mediation server.
4. Login to the CMP GUI using a supported browser.
5. Browse for the Mediation Field Mapping profile file on the local PC directory where it was previously uploaded to.


6. Click Import on the Field Mapping file as shown below:
CMP GUI: System Administration → Import/Export → Import
</td></tr>
</table>

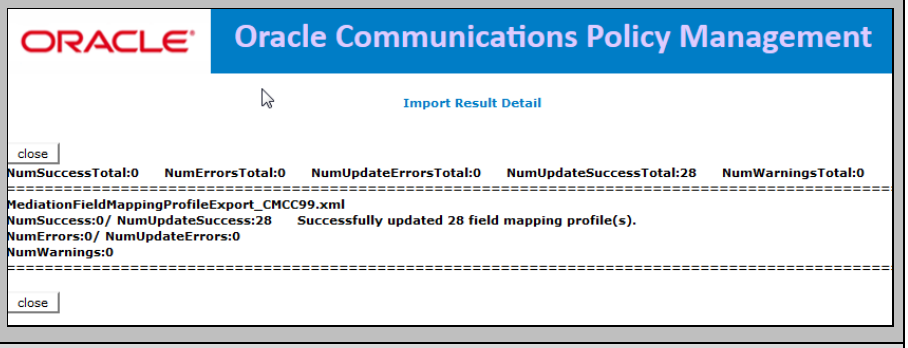
Step	Procedure	Result



7. Click **OK** to proceed with the import.
8. After it is imported, it shows the following message on top of the CMP GUI screen as shown.



9. Click **detail** to validate that the import is successful with NumUpdateErrorsTotal and NumWarningsTotal are both zero.
10. When you finish, click **close** to close the window.



THIS PROCEDURE HAS BEEN COMPLETED

10. UPGRADE NON-CMP CLUSTERS (MPE, MRA) 12.2.X/12.3.X WIRELESS MODE

These procedures upgrade a site/segment containing one or more non-CMP clusters such as MPE, MRA.

NOTES:

- An upgrade of up to 4 clusters can be running at the same time.
- Different types of non-CMP clusters can be upgraded at the same time. 2 MPEs and 2 MRAs, for example, can be upgraded in parallel.

10.1 Site/Segment Upgrade Preparation

10.1.1 Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	Use the supported browser to login as administrative or as a user with administrator privileges.
2. ☐	**CMP GUI:** Verify current Upgrade Manager status and Software Release 12.3 ISO files	1. Navigate to **Upgrade → Upgrade Manager**. - Verify that all CMP clusters have both Active and Standby status. - Verify that all MPE and MRA clusters have both Active and Standby status. - Verify that the CMP cluster is upgraded successfully and running Policy Release 12.3 2. Navigate to **Upgrade -> ISO Maintenance**. - Verify that Policy release 12.3 ISO files are available for all clusters. One ISO per server
THIS PROCEDURE HAS BEEN COMPLETED		

10.2 Upgrade Non-CMP Clusters

This procedure upgrades one or more non-CMP clusters at a site/segment.

This procedure is applicable for an 12.2.x upgrade to 12.3

This section can be replicated for each site/segment to be upgraded, to allow the upgrade engineer to add cluster and site specific information.

The upgrade procedure is essentially the same for any non-CMP cluster.

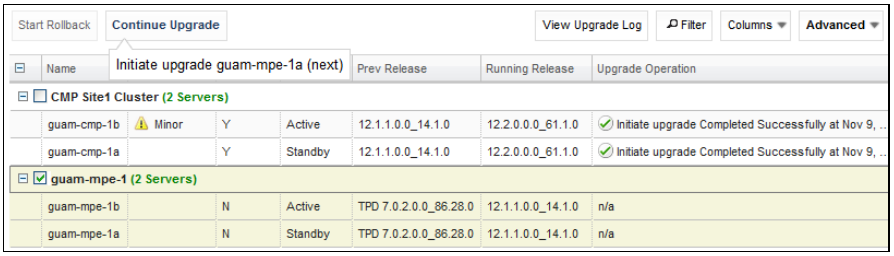
1. Select and start upgrade on the Standby server
2. Failover
3. Re-apply configuration
4. Continue upgrade on remaining server
5. Re-apply configuration

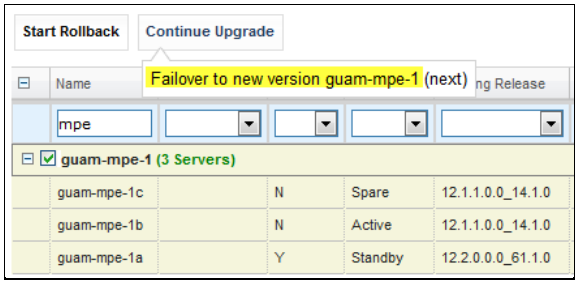
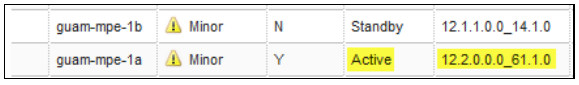
NOTES:

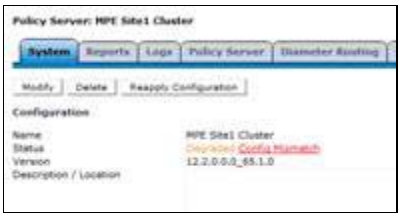
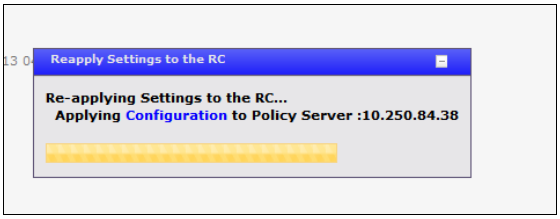
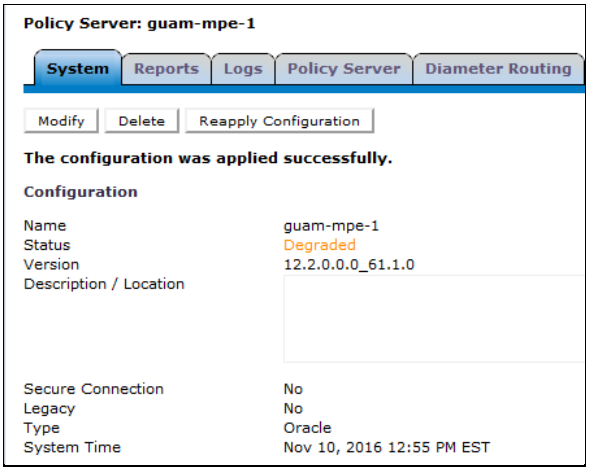
- All CMP clusters must have been upgraded to Policy release 12.3 before executing the following procedures.
- The maximum clusters to be running the upgrade at one time is 4, except for release 12.2.x where 8 clusters can be upgraded in parallel.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 12.3

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the servers to be upgraded	Perform the following: • Check for current active alarms • Reset server counters to make a baseline For the MPE: **Policy Server→Configuration→Reports → Reset Counters** For the **MRA: MRA→Configuration→Reports → Reset Counters** • Check KPI Dashboard (capture and save screenshot to a file)
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	1. Navigate to **Upgrade →Upgrade Manager**. 2. Verify information for the MRAs/MPEs: - Current Release 12.1.x or 12.2.x installed - Running with Active/Standby status 3. Navigate to **Upgrade → ISO Maintenance**. - Verify the ISO version to be deployed is 12.3

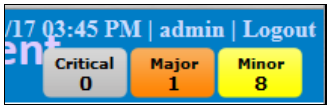
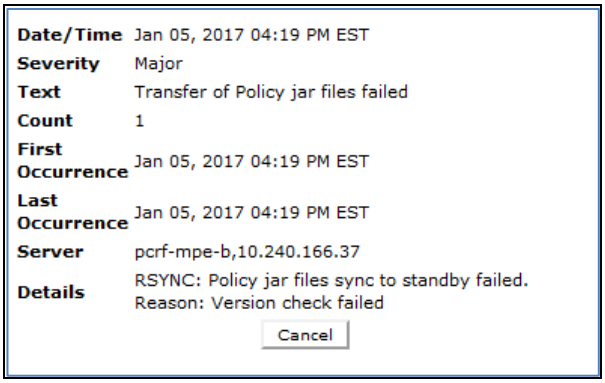
Name	Appl Type	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster			
guam-cmp-1a	CMP Site1 Cluster	10.240.152.75	12.2.0.0.0_61.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-cmp-1b	CMP Site1 Cluster	10.240.152.76	12.2.0.0.0_61.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1	MPE			
guam-mpe-1a	MPE	10.240.152.79	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1b	MPE	10.240.152.80	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1	MRA			
guam-mra-1a	MRA	10.240.152.77	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1b	MRA	10.240.152.78	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]

Step	Procedure	Result
3. ☐	**CMP GUI**: Upgrade clusters **NOTE:** Each upgrade of one blade server takes approximately 35 minutes to complete.	Start the upgrade on ONE cluster. Wait until the cluster shows OOS, then continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running upgrade at any one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster (one cluster at a time.) It can be an MRA or an MPE. 3. Click **Continue Upgrade**.  4. Click **OK** to confirm and continue with the operation. The upgrade of the standby server for the cluster begins. Wait until the standby server reports OOS before selecting the next cluster Follow the progress status in the Upgrade Operation column. During the upgrade activities, the following alarms may be generated and considered normal reporting events–these are cleared after the clusters are completely upgraded. **Expected Critical Alarms** **31283** High availability server is offline **70001** QP_procmgr failed **31227** High availability status failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31102** DB replication from a master DB has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **78001** RSYNC Failed Upgrade is complete on the first server of the cluster when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to the standby state when the upgrade completes.

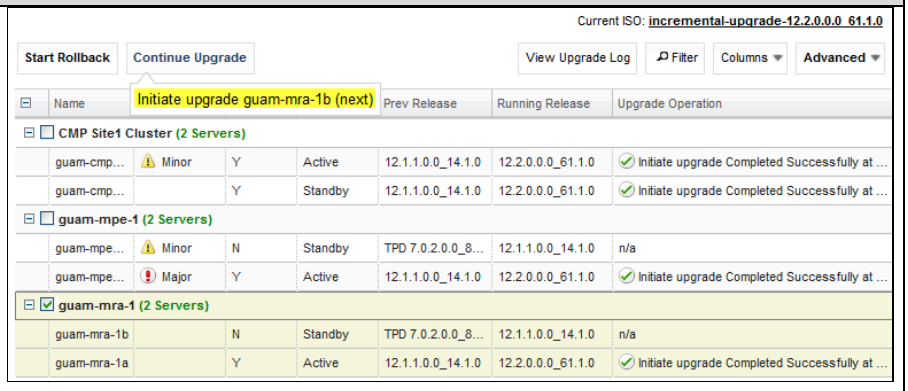
Step	Procedure	Result
		guam-mpe-1b | N | Active | 12.1.1.0.0_14.1.0 | Initiate backout Completed Successfully at guam-mpe-1a | Y | Standby | 12.2.0.0.0_61.1.0 | Initiate upgrade Completed Successfully at A number of different alarms may be raised at this point: **Expected Minor Alarms** **78001** RSYNC Failed **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **70503** The server is in forced standby
4. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Next Operation is a failover **NOTE:** 4 clusters (8 for 12.1.x) can be running the upgrade process at one time.	Failover ONE cluster at a time. Wait for a minute, before moving on to the next cluster. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster (one cluster at a time). It can be an MRA or MPE. 3. Click **Continue Upgrade**. When hovering over the button, it says Failover to new version.  4. Click **OK** to confirm and continue with the operation. It begins to failover the cluster. Wait until failover completes, that is, the server running 12.3 is now Active, before failing over the next cluster. 

Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on the MPE/MRA cluster that failed over successfully.	• For MPE: **Policy Server → Configuration →** <*MPE cluster*> **→ System** • For MRA: **MRA→Configuration→**<*MRA cluster*>**→System** The selected cluster has the status of Degraded and shows the old release version. Config mismatch may also be displayed. 1. Click **Reapply Configuration**.  **NOTE:** A progress banner appears for the MPE reapply configuration and NOT the MRA reapply configuration  2. Verify that the Version changed to Release 12.3 3. The cluster shows the Degraded status: 

Step	Procedure	Result
6. ☐	**CMP GUI**: Current alarms	Some of the alarms below may appear: **Expected Critical Alarm** None **Expected Major Alarm** **78001** Rsync Failed **Expected Minor Alarms** **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **70503** The server is in forced standby **71402** Diameter Connectivity Lost **31101** DB Replication To Slave Failure **31113** DB Replication Manually Disabled
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	Navigate to **Upgrade Manager → System Maintenance** • If traffic is active, go to step 9. • If traffic does not become active within 90 seconds: a. Select the checkbox for the partially upgraded cluster. b. Select **Operations → Rollback**. The pre-12.3 MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	1. **Policy Server → Configuration →** *<mpe_cluster name>* **→ System** tab or **MRA → Configuration →** *<mra_cluster name>* **→ System** tab 2. Click **Reapply Configuration** • Verify that the version is changed back to 12.1.x or 12.2.x, and the action report success. • If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.

Step	Procedure	Result
9. ☐	**CMP GUI:** Major alarm 78001	During the upgrade activities, major alarm 78001 in particular may be generated. And even though it is a normal event, the alarm does not clear by itself. Before continuing verify that the alarm is cleared. 1. Click **Major** in the upper right part to display the alarms:  2. Click the binoculars icon on the right to display details for the 78001 major alarm.  You should see in the last line of the details that the reason for the major alarm is that the version check failed.  - If you see a different reason, stop and contact My Oracle Support. - If you see the version check failed message, continue here. 3. Navigate to **System Wide Reports > Alarms > Active Alarms** and select the 78001 major alarm  4. Click the trash can icon on the right to clear this alarm.
10. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Upgrade on the Standby server	Continue the upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters may be running upgrade at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select a cluster (one cluster at a time), it can be an MRA or an MPE. 3. Click **Continue Upgrade**. When hovering over the button, it says Initiate upgrade… on the standby server

Step	Procedure	Result



4. Click **OK** to confirm and continue with the operation.The final server upgrade of the cluster begins.

If you plan to perform the upgrade for several clusters in parallel (up to 4), wait until the server being upgraded changes to OOS before moving on to the next cluster

Follow the progress status in the Upgrade Operation column.

During the upgrade activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely upgraded.

Expected Critical Alarms

31283 High availability server is offline
31227 High availability Status Failed
70001 QP_procmgr failed

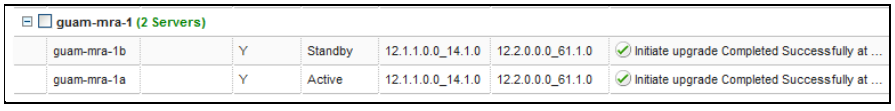
Expected Major Alarm

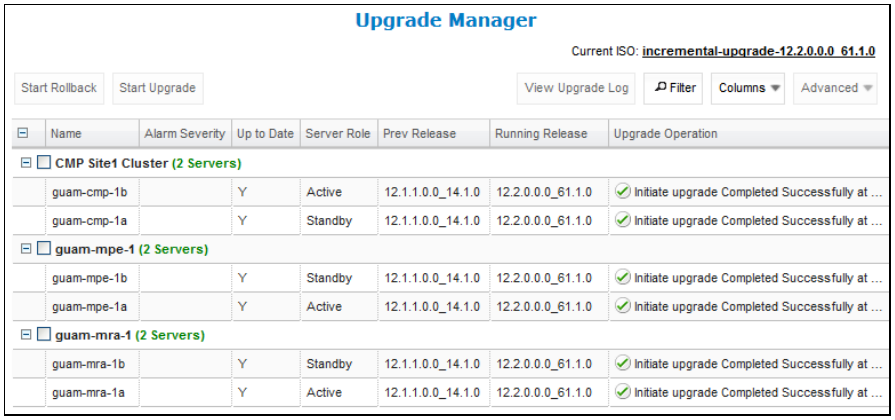
70004 QP Processes down for maintenance

Expected Minor Alarms

70503 Upgrade Director Server Forced Standby
70507 Upgrade Director In Progress
70500 Upgrade Director System Mixed Version
70501 Upgrade Director Cluster Mixed Version
70502 Upgrade Director Cluster Replication Inhibited
31114 DB Replication over SOAP has failed
31106 DB Merge To Parent Failure
31107 DB Merge From Child Failure
31101 DB Replication To Slave Failure
31102 DB Replication from Master Failure
31113 DB Replication manually Disabled

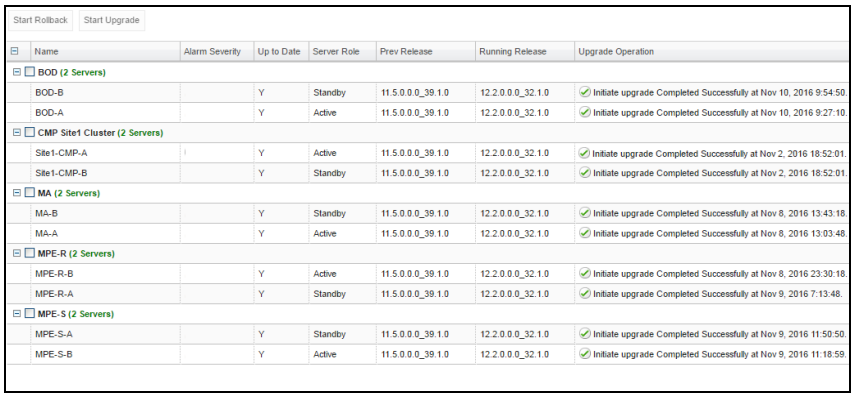
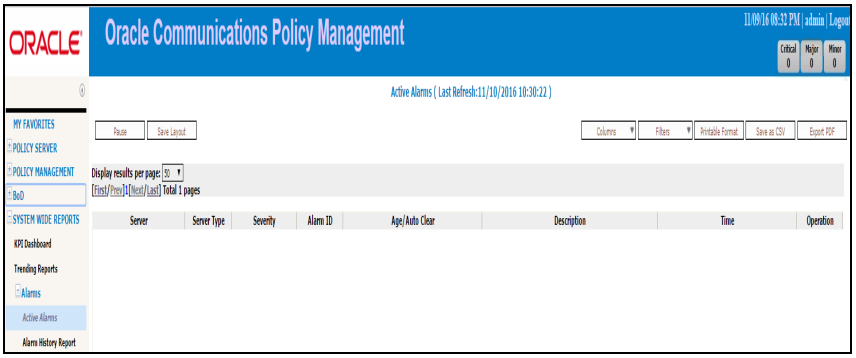
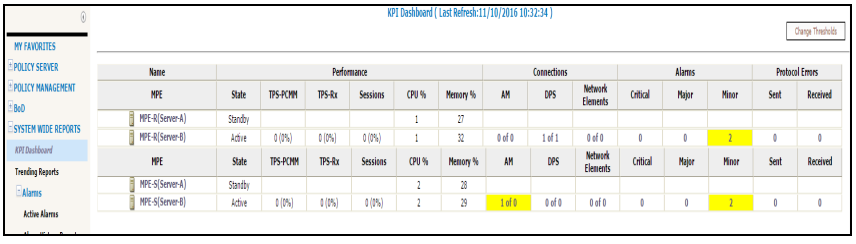
Upgrade is complete when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to Standby state and the Up to Date column shows a Y (YES)



Step	Procedure	Result
11. ☐	REPEAT the above Steps 1 through 10 for next MPE/MRA cluster	Proceed with the next cluster until all clusters have been upgraded. 
THIS PROCEDURE HAS BEEN COMPLETED		

11. POST UPGRADE HEALTH CHECK

NOTE: This section is used when the entire topology is running release 12.3

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the upgrade is successful on all clusters.	**Upgrade → Upgrade Manager** View the Up to Date, Running Release, and Upgrade Operation columns and verify they read Y, 12.3...., and Initiate upgrade completed successfully at… respectively, for all servers in all clusters. 
2. ☐	**CMP GUI:** View current alarms	1. Navigate to **System Wide Reports→Alarms→Active Alarms** 2. Verify that all alarms due to the upgrade have been cleared. 
3. ☐	**CMP GUI**: View current KPIs	1. Navigate to **System Wide Reports→KPI Dashbord** 2. Verify that the counter stats are incrementing properly. 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>4. ☐</td><td>CMP GUI: Replication stats</td><td>Navigate to System Wide Reports→Others→MPE/MRA Rep Stats (for a wireless system)

Verify all clusters and servers are in OK state.

Wireless:

<table>
<tr><th>Cluster Name</th><th>Server Type</th><th>Cluster State</th><th>Blade State</th><th>Sync State</th><th>Replication Delta(Min:Sec</th></tr>
<tr><td>⊟ guam-mpe-1</td><td>MPE</td><td>OK</td><td>---</td><td>---</td><td>0:0.504</td></tr>
<tr><td>guam-mpe-1b (Active) ->guam-mpe-1a (Standby)</td><td>MPE</td><td>---</td><td>OK</td><td>OK</td><td>0:0.504</td></tr>
<tr><td>guam-mpe-1b (Active) ->guam-mpe-1c (Spare)</td><td>MPE</td><td>---</td><td>OK</td><td>OK</td><td>0:0.499</td></tr>
<tr><td>⊟ guam-mra-1</td><td>MRA</td><td>OK</td><td>---</td><td>---</td><td>0:0.5</td></tr>
<tr><td>guam-mra-1b (Active) ->guam-mra-1a (Standby)</td><td>MRA</td><td>---</td><td>OK</td><td>OK</td><td>0:0.498</td></tr>
<tr><td>guam-mra-1b (Active) ->guam-mra-1c (Spare)</td><td>MRA</td><td>---</td><td>OK</td><td>OK</td><td>0:0.5</td></tr>
</table>
</td></tr>
<tr><td>5. ☐</td><td>Verify System Health</td><td>Use the command sudo syscheck on every server. Verify that each class test returns OK. For example:

<pre>$ sudo syscheck
Running modules in class disk... OK
Running modules in class hardware... OK
Running modules in class net... OK
Running modules in class proc... OK
Running modules in class system...OK</pre>
LOG LOCATION: <code>/var/TKLC/log/syscheck/fail_log</code></td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED</td></tr>
</table>

12. BACKOUT (ROLLBACK) 12.2.X WIRELESS OR 12.3.X

This procedure is performed if an issue is found during the upgrade, or during the post-upgrade if somethings impacts network performance.

The Policy system is backed out to the previous release.

Oracle strongly recommends consulting My Oracle Support before initiating the backout procedure. Oracle Support determines the appropriate course of recovery options.

12.1 Backout Sequence

The Backout sequence order is the reverse of the Upgrade order as in the following sequence:

1. Backout MRA/MPE
2. Backout the Secondary CMP cluster (if applicable)
3. Backout the Primary CMP cluster.

During a backout, it is important to control what version of the software is currently active. This control needs to be maintained even if there are unexpected failures.

NOTE: In the case of an MPE/MRA, the upgrade/backout is NOT complete until you perform a Reapply Configuration from the CMP. The MRA/MPE can operate, but may not be fully functional.

12.2 Pre-requisites

1. No new policies or features have been configured or performed on the upgraded release.
2. The CMP cluster cannot be backed out if other Policy servers (MPEs, MRAs) are on the upgraded release.

12.3 Backout of Fully Upgraded Cluster

Prior to executing this procedure, Oracle recommends first consulting My Oracle Support to discuss the next appropriate course of actions.

This procedure is used to backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster are on pre-12.3 release with Active/Standby status.

Expected pre-conditions:

- The primary active CMP is on release 12.3.
- The cluster servers to be backed out are all on release 12.3.
- One server of target cluster is on Release 12.3 in Active role.
- One server of target cluster is on Release 12.3 in either Standby or Force Standby.

12.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, MPE) are in non-georedundant mode with active and standby servers. CMP clusters may be in Site1 or Site2.

NOTE: It is possible, and desirable, to backout multiple clusters in parallel. However, in order to do this, you must select one cluster at a time, staggering by approximately 1 minute each.

12.3.1.1 Overview on Backout/Rollback MRA/MPE

1. Back out of the standby server
2. Fail over
3. Back out of the new standby server

12.3.1.2 Backout Secondary CMP (if applicable):

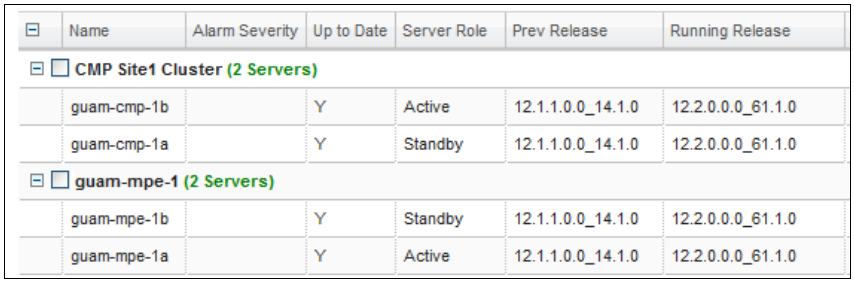
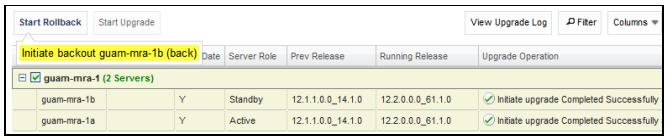
NOTE: At this time, all MPE and MRA servers must already be backed out.

1. Use the CMP Upgrade Manager to backout the Secondary CMP cluster

12.3.1.3 Backout the Primary CMP:

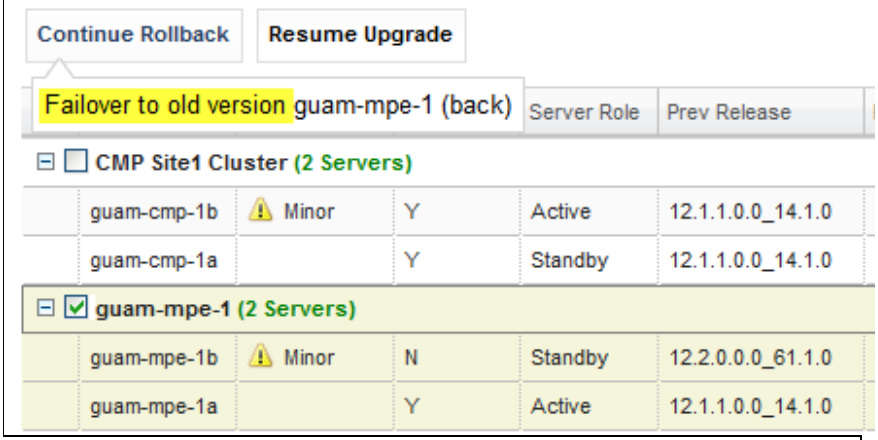
1. Use the CMP Upgrade Manager to backout the CMP cluster

12.3.2 Backout Fully Upgraded MPE/MRA Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	1. Navigate to Upgrade → Upgrade Manager. 2. Confirm status of the cluster to be backed out - Primary CMP is on Release 12.3 - All Standby servers are on Release 12.3 - Up to Date column shows Y for all servers **EXAMPLE:** 
2. ☐	**CMP GUI**: Rollback standby MPE/MRA clusters **NOTE:** Each backout of a blade server is completed within approximately 40 minutes time. **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the MPE/MRA/Mediation cluster to be backed out 3. Click **Start Rollback**. When hovering over the button, it informs you of the server to get backed out, in this case it is the current standby server.  4. Click **OK** to confirm and continue with the operation. It begins to backout the server. 5. Follow the progress status in the Upgrade Operation column. 6. At this point, the server backing out goes into the OOS state 7. Wait until the server goes into an OOS state before selecting the next cluster to backout.

Step	Procedure	Result
		During the backout activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarms** **78001** Rsync Failed **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault Backout of the server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. The backed out server shows that it is running the previous release and returns to standby with an N in the Up to Date column.
3. ☐	**CMP GUI**: Continue the backout of the MRA/MPE clusters. Next operation is « failover» to the server in the previous release. **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	1. Select the cluster to backout. Current state of the cluster needs to be as follows: - Active server on 12.3 Release - Standby server on pre-12.3 Release Some minor alarms (for example, 70501 Cluster running different versions of software) are normal at this point. 2. Navigate to **Upgrade → Upgrade Manager**. 3. Select the cluster 4. Click **Continue Rollback**. When hovering over the button, it informs you that the next step is to fail over to the old version

Step	Procedure	Result



5. Click **OK** to confirm and continue with the operation. The failover begins.

Wait until the server fails over before selecting the next cluster. This takes a minute or two.

Expected Critical Alarms

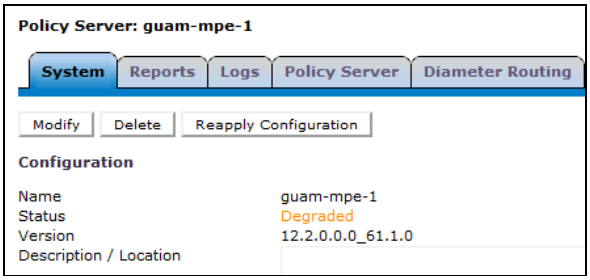
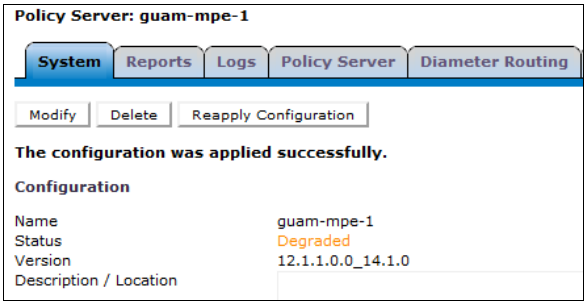
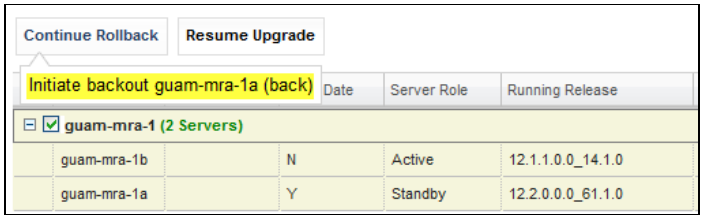
31283 High availability server is offline
31227 High availability Status Failed
70001 QP_procmgr failed

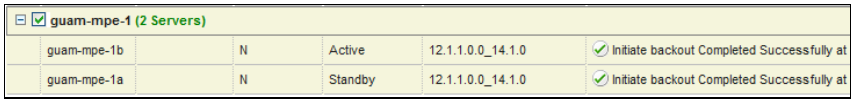
Expected Major Alarms

70004 QP Processes down for maintenance
31233 HA Path Down
31126 Audit Blocked

Expected Minor Alarms

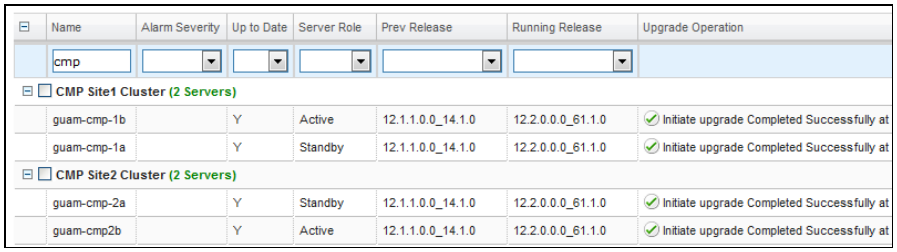
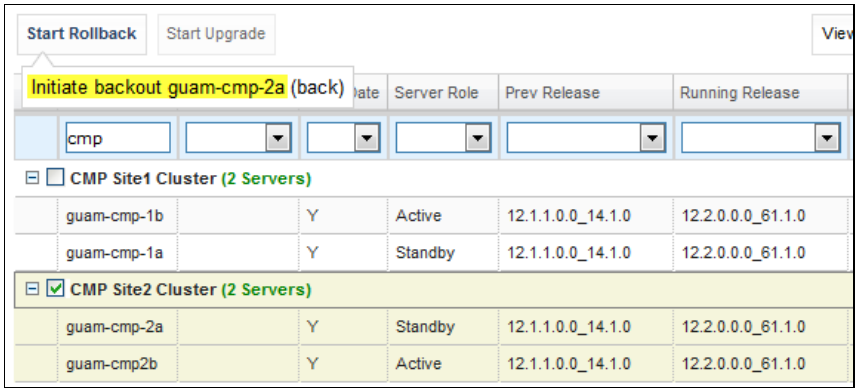
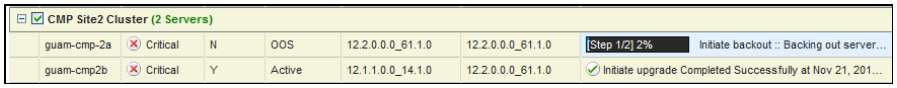
70503 Upgrade Director Server Forced Standby
70507 Upgrade Director In Progress
70500 Upgrade Director System Mixed Version
70501 Upgrade Director Cluster Mixed Version
78001 RSYNC Failed
70502 Upgrade Director Cluster Replication Inhibited
31114 DB Replication over SOAP has failed
31106 DB Merge To Parent Failure
31107 DB Merge From Child Failure
31101 DB Replication To Slave Failure
31102 DB Replication from Master Failure
31113 DB Replication manually Disabled
31282 HA Management Fault

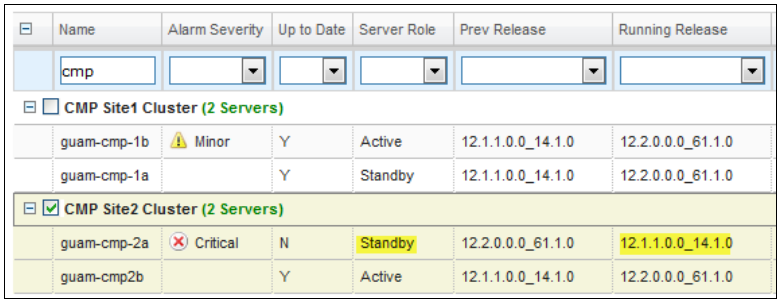
Step	Procedure	Result
4. ☐	**CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the failover successfully.	• For MPE: **Policy Server → Configuration → <MPE cluster> → System**. • For MRA: **MRA→Configuration→<MRA cluster>→System**. The selected cluster has the status as Degraded and running version as 12.3.  1. Click **Reapply Configuration**. The MPE opens a dialog box that shows the progress of the reapply, the MRA does not show anything. 2. Note the Version is successfully changed to the previous release, for example 12.3.  **NOTE:** The status shows Degraded. This is a normal reporting event as the servers are in different status.
5. ☐	**CMP GUI**: Complete backout of cluster(s) **NOTE:** Each backout of a blade server is completed within approximately 35 minutes time. **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	1. Select the partially backed out cluster 2. Navigate to **Upgrade → Upgrade Manager**. 3. Select the the cluster 4. Click **Continue Rollback**. When hovering over the button, it informs you of the standy server running 12.3to be backed out.  5. Click **OK** to confirm and continue with the operation. Follow the progress status in the Upgrade Operation column. During the backout activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely backed out.

Step	Procedure	Result
		Expected Critical Alarms **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault Backout of the server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. Both servers in this cluster are on a pre-12.3 release at this point and show active/standby. 
6. ☐		Repeat this procedure for the remainder of the MPE/MRA servers, if necessary.
THIS PROCEDURE HAS BEEN COMPLETED		

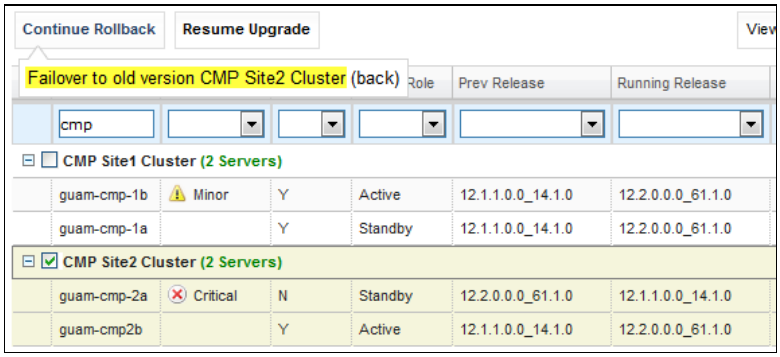
12.3.3 Backout Fully Upgraded Secondary CMP Cluster

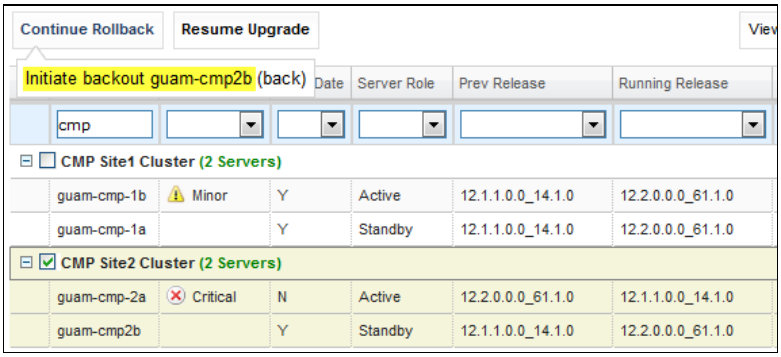
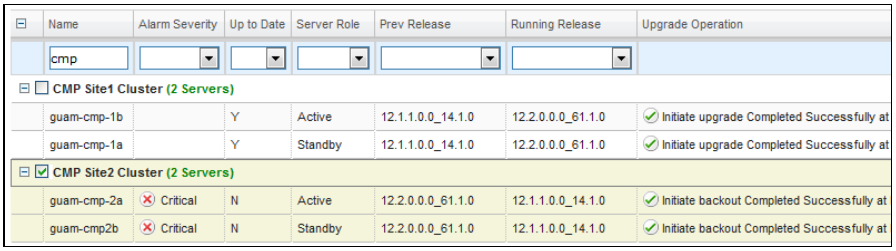
NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site1 cluster.

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP cluster s	1. Navigate to **Upgrade Manager → System Maintenance**. 2. Click **Filter** and enter `cmp`. 3. Confirm status of the cluster to be backed out: - Primary CMP is on Release 12.3 - All other non-CMP clusters are on a pre-12.3 release - Up to Date column shows Y for all servers **EXAMPLE:** 
2. ☐	**CMP GUI**: backout secondary cmp cluster NOTE: Each backout of one server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager.** 2. Select the secondary CMP cluster. 3. Click **Start Rollback**. When hovering over the button, it informs you that the standby server to be backed out.  4. Click **OK** to confirm and continue with the operation. The backout begins and the server go into the OOS server role. Follow the progress status in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely backed out.

Step	Procedure	Result
		Expected Critical Alarms **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **70025** The MySQL slave has a different schema version than the master. **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault
		Backout of the server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. The server goes back to the standby state and shows the previous release 

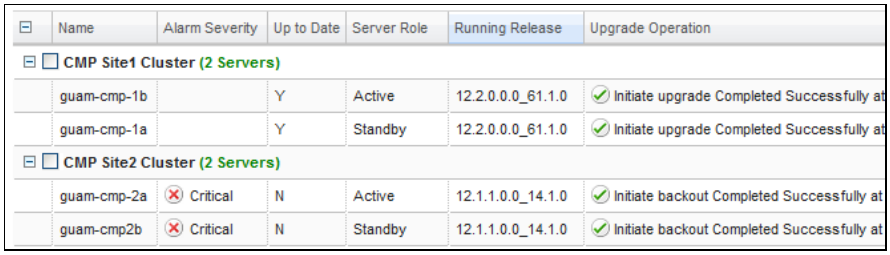
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release
cmp					
CMP Site1 Cluster (2 Servers)					
guam-cmp-1b	Minor	Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-cmp-1a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
CMP Site2 Cluster (2 Servers)					
guam-cmp-2a	Critical	N	Standby	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0
guam-cmp2b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0

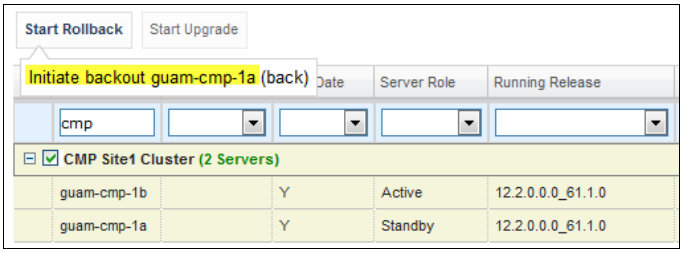
Step	Procedure	Result
3. ☐	**CMP GUI**: Continue the backout. Next Operation is failover	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP cluster. 3. Click **Continue Rollback**. When hovering over the button, it informs you that it is going to failover the cluster to the previous version.  4. Click **OK** to confirm and continue with the operation. The failover begins. 5. Wait until the previous release becomes active before continuing **Expected Critical Alarm** **70025** QP Slave database is a different version than the master **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70500** Upgrade Director System Mixed Version

Step	Procedure	Result
4. ☐	**CMP GUI**: Continue the backout. Next Operation is initiate backout	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of the server it is going to back out.  4. Click **OK** to confirm and continue with the operation. Follow the progress status in the Upgrade Operation column. **Expected Critical Alarm** **70025** QP Slave database is a different version than the master **Expected Minor Alarm** **70500** Upgrade Director System Mixed Version The procedure ends when both Secondary CMP servers are in the previous release. 
THIS PROCEDURE HAS BEEN COMPLETED		

12.3.4 Backout Fully Upgraded Primary CMP Cluster

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1. ☐</td><td>CMP GUI: Verify the status of the CMP clusters</td><td>3. Navigate to Upgrade Manager → System Maintenance.
4. Confirm status of the Primary CMP cluster:
- Primary CMP cluster is on Release 12.3
- Secondary CMP cluster (if present) is already on pre-12.3 Release
- Up to Date column shows Y for all servers in Primary CMP cluster
EXAMPLE:
 
</td></tr>
<tr><td>2. ☐</td><td>CMP GUI: backout standby Primary CMP cluster

NOTE: backout of one server takes approximately 40 minutes to complete.</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Click Filter and enter <code>cmp</code> to display CMP clusters only.
3. Select the Primary CMP cluster.
4. Click Start Rollback. When hovering over the button, it informs you that the standby server is going to be backed out.
 

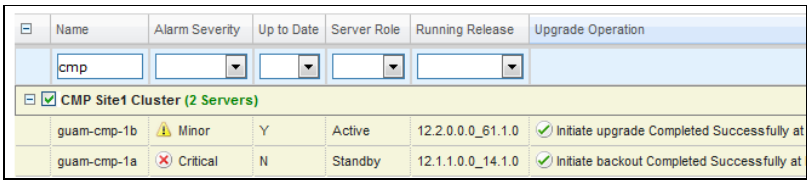
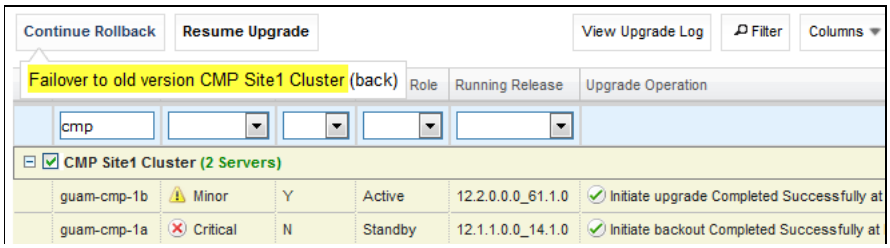
5. Click OK to confirm and continue with the operation.The backout begins and the server goes into the OOS Server Role

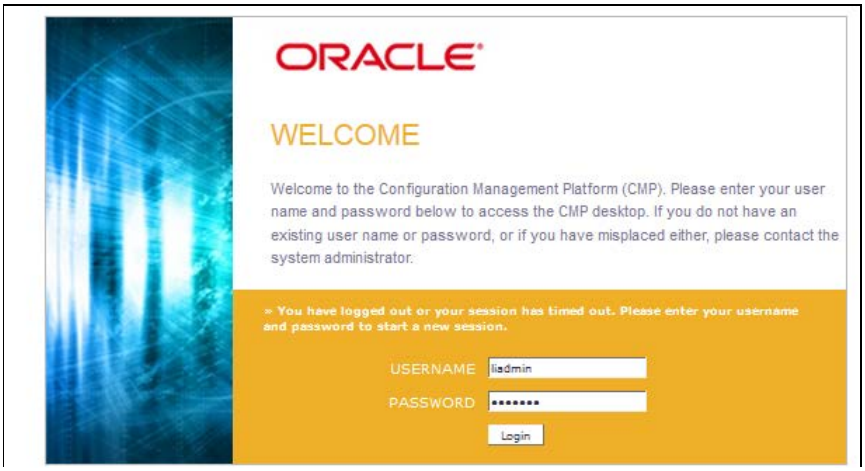
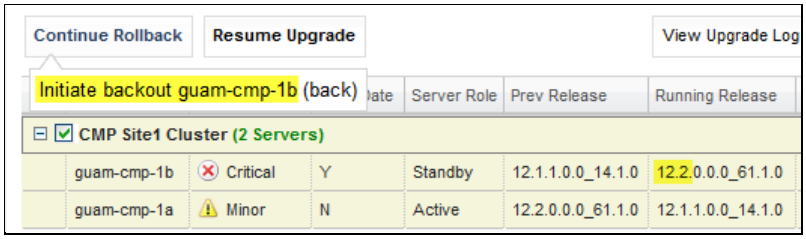
Follow the progress status in the Upgrade Operation column.

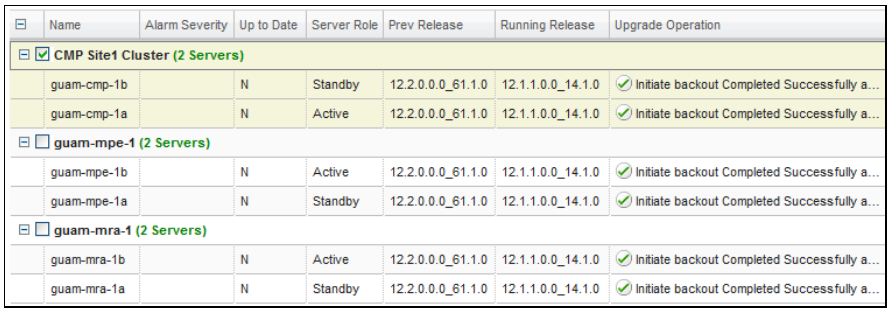
During the backout activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely backed out.

<u>Expected Critical Alarms</u>

31283 High availability server is offline
31227 High availability Status Failed
70001 QP_procmgr failed
31236 HA Link Down</td></tr>
</table>

Step	Procedure	Result
		Expected Major Alarm **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **31114** DB Replication over SOAP has failed 31106 DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited
3. ☐		Backout of the server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. The server goes back to the standby state and shows the previous release. 
4. ☐	**CMP GUI**: Continue the backout. Next operation is failover.	1. Select the Primary CMP cluster. 2. Navigate to Upgrade → Upgrade Manager 3. Click the checkbox for the Primary CMP cluster 4. Click **Continue Rollback** button. When hovering over the button, it informs you that the next action is to fail over to the old CMP version.  5. Click **OK** to confirm and continue with the operation.The failover begins. Failover takes a couple minutes.

Step	Procedure	Result
5. ☐	**CMP GUI**: Log back in to the Primary CMP VIP	After failover, you must log back in to the CMP GUI using the Primary CMP VIP. 
6. ☐	**CMP GUI:** Verify release	Navigate to **Help→About**. Verify the proper pre-12.3 release number is displayed
7. ☐	**CMP GUI**: Continue the backout of the Primary CMP cluster **NOTE:** backout of one server takes approximately 40 minutes to complete.	1. Select Primary CMP cluster to complete the backout. 3. Navigate to **Upgrade → Upgrade Manager**. 4. Select the checkbox for the Primary CMP cluster 5. Click **Continue Rollback**. When hovering over the button, it informs you that the standby server running 12.3 is being backed out  6. Click **OK** to confirm and continue with the operation. The backout begins. The server goes into an OOS server role. 7. Follow the progress status in the Upgrade Operation column. During the backout activities, the following alarms may be generated and considered normal reporting events–these are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** 70503 Upgrade Director Server Forced Standby

Step	Procedure	Result
		70507 Upgrade Director In Progress 70500 Upgrade Director System Mixed Version 70501 Upgrade Director Cluster Mixed Version 78001 RSYNC Failed 70502 Upgrade Director Cluster Replication Inhibited 31114 DB Replication over SOAP has failed 31106 DB Merge To Parent Failure 31107 DB Merge From Child Failure 31101 DB Replication To Slave Failure 31102 DB Replication from Master Failure 31113 DB Replication manually Disabled Backout of the server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. The server goes back to standby state and shows the previous release:  All backout-related alarms should also be cleared.
THIS PROCEDURE HAS BEEN COMPLETED		

Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
guam-cmp-1b		N	Standby	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…
guam-cmp-1a		N	Active	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…
guam-mpe-1 (2 Servers)						
guam-mpe-1b		N	Active	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…
guam-mpe-1a		N	Standby	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…
guam-mra-1 (2 Servers)						
guam-mra-1b		N	Active	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…
guam-mra-1a		N	Standby	12.2.0.0.0_61.1.0	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully a…