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 GeoRedundancy Enabled

E85334-01

July 2017

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

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

Refer to Appendix 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.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures run to perform a software upgrade of Oracle Communications Policy Management Release 12.1.x/12.2.x to Release 12.3 when georedundancy is enabled.

- Upgrade of firmware may be required, but is not covered in this document.

Georedundancy as implemented in the MPE and the MRA uses the 2+1 server cluster scheme. The 2 refers to the current Active and Standby servers and the +1 refers to a third Spare server. The Spare server is added into the same cluster so that any server can assume the Active role if necessary. The Spare server is usually located in a separate geographical location in case the servers at the initial site become unavailable due to a site-wide failure. The Spare server, in most cases, would be unaffected by the same circumstances and would be able to continue to provide service as an Active server.

1.2 Acronyms

Acronym	Definition
BoD	Bandwidth on Demand - a type of component in a cable Policy Management solution
CMP	Configuration Management Platform
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
IPM	Initial Product Manufacture
LVM	Logical Volume Manager
MPE	Multimedia Policy Engine
MPE-LI	MPE for Lawful Intercept - a type of Multimedia Policy Engine
MPE-R	Routing MPE - a type of component in a cable Policy Management solution
MPE-S	Servicing MPE - a type of component in a cable Policy Management solution
MRA	Multiprotocol Routing Agent (also known as the Policy Front End or PFE)
OCS	Online Charging System
OOS	Out of Service
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rules Function—Oracle MPE
PM&C	Platform Management and Configuration
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment

1.3 Terminology

Term	Description
Primary Site (Site1)	Site where the MPE/MRA Server-A and Server-B are deployed.
Secondary Site (Site2)	Site where the MPE/MRA Server-C is deployed.
Spare Server or Server-C	Server that is ready to take over from the Active server if both the Active and Standby servers fail. It is generally in a different location than the Active and Standby servers.

1.4 Software Release Numbering

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

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to run 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 the operator 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 operator 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 operator intervention.

2.2 Upgrade Paths

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

This procedure applies to Active, Standby, and Spare servers. A group of servers is referred to as a cluster. The cluster types are CMP, MRA, MPE, and Mediation.

- For a CMP cluster, there are only 2 servers (Active and Standby) in a cluster and the cluster can be either a Primary or Secondary cluster.
- For a non-CMP cluster (MRA/MPE), there can be 3 servers (Active, Standby, and Spare).

A Policy Management deployment can consist of multiple clusters.

2.3.1 Required Cluster Upgrade Sequence

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

The following is the upgrade sequence, specific process are documented by an Oracle provided Maintenance Operation Procedure (MOP).

NOTE: TVOE, PM&C Server, and Firmware may be necessary prior to the Policy Management upgrade.

1. Upgrade PM&C Server at Site 1—Required if version is older than what is listed in Section 1.4.
2. Upgrade PM&C Server at Site 2—Required 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 CMP
5. Upgrade Secondary CMP (if applicable)
6. Site 1 Segment 1—Upgrade non-CMP clusters (see note below)
7. Site 2 Segment 1—Upgrade non-CMP clusters (see note below)
8. Site 1 Segment 2—Upgrade non-CMP clusters (see note below)
9. Site 2 Segment 2—Upgrade non-CMP clusters (see note below)

NOTE: Up to 16 non-CMP clusters can be upgraded in parallel.

2.3.2 Policy Management 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, the system that is running pre-12.3 release and release 12.3 mixed configuration would support the performance and capacity of pre-12.3 release. The mixed version Policy Management configuration would support pre-12.3 release 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 servers in both the previous release and release 12.3. In this mixed version configuration, release 12.3 CMP does not prevent an operator from configuring anything that you could configure in a previous release and all configuration items from the previous release are still available. However, the configuration changes during the upgrade of Policy Management system are discouraged and have limited support.

In the mixed version Policy Management configuration 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 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 servers is limited to parameters that are available in the previous version. Specifically, Network Elements can be added.

Table 1 Mixed-version configurations supported

Policy Management system components on	CMP R12.3	MRA R12.3	MPE R12.3
CMP 12.2.x, 12.1.x	Yes	No	No
MRA 12.2.x, 12.1.x	Yes	Yes	Yes
MPE 12.2.x, 12.1.x	Yes	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of the CMP and DR-CMP from the previous release 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, then the spare server, and then switching over from the active to the standby, and upgrading the new standby. The switchover of each non-CMP cluster has a small impact on traffic being processed at that cluster.

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 during or after upgrade.

2.6 TPD Version

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

In the case of an initial product manufacture (IPM) or clean install of a new server, the supported baseline TPD version 7.0.3 should be installed prior to upgrading to Policy Management release 12.3.

2.7 Server Hardware Platforms

The Policy Management release 12.3 software upgrade can be applied on any server that previously had Policy Management release 12.2.x, or 12.1.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 the `scp` or `ftp` command. 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

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

- Policy Management 12.3 software ISO files and TPD software ISO
- Policy Management 12.3 software Release Notes.
- TVOE, PM&C upgrade/installation documentation, software ISO files and TPD ISO (if applicable).
- HP Solutions Firmware Upgrade Pack 2.2.9 (or higher) documentation and ISO files (if applicable).

- The capability to remotely login to the target server as admusr.

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

- 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.
- User login IDs, passwords, IP addresses, and other administration information.
- VPN access to your network is required if that is the only method for remotely logging into the target servers. It must be also possible to access the Policy Management 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 User IDs and Passwords

You must confirm login information for key interfaces, and document the information using Table 2.

NOTES:

- It is assumed that the login information may be common across sites. If not, record the information for each site.
- 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 a permanent form.

Table 2 Login IDs, Passwords and release Information

Item	Value
CMP servers **NOTE:** Some older releases do not use admusr, instead use the default root Login using SSH.	GUI Administrator Login User/Password
	admusr password:
MPE/MRA 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 Management 12.3 software ISO image 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 previous upgrade pages. In the past it was up to the operator, with assistance from an MOP, to know the correct sequence of server selects and menu selections. The new Upgrade Manager takes a different approach. It determines the next course of action to either

- Begin/continue upgrading a cluster
- Begin/continue backing out a cluster.

IMPORTANT: There is a 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 not possible to select individual servers or to bulk select a group of servers. In fact, in order to perform any operation, it is necessary to select a cluster.

Another change is that certain operations are performed automatically on behalf of the operator. These operations are not presented to the operator as an option. However, the operator can see what has been done using the upgrade log.

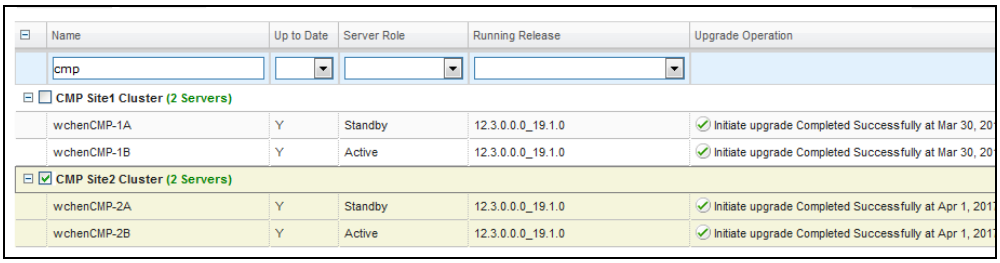


Figure 1 Sample display of the Upgrade Manager page

For the most part, the items in the display are self-explanatory. The following items are often used during the upgrade.

- **Start Rollback** and **Start Upgrade** buttons (upper left):

  If a cluster is selected and these buttons are disabled (grey), it means that there is not an appropriate action to take at this time. However, if a button is not disabled (white), 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. Only use the Upgrade Manager to perform upgrades unless the instructions direct otherwise.

- 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, it is expected that the servers raise alarms:

  The CMP raises alarms to indicate that it is initiating upgrade activity.

Servers reports 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.

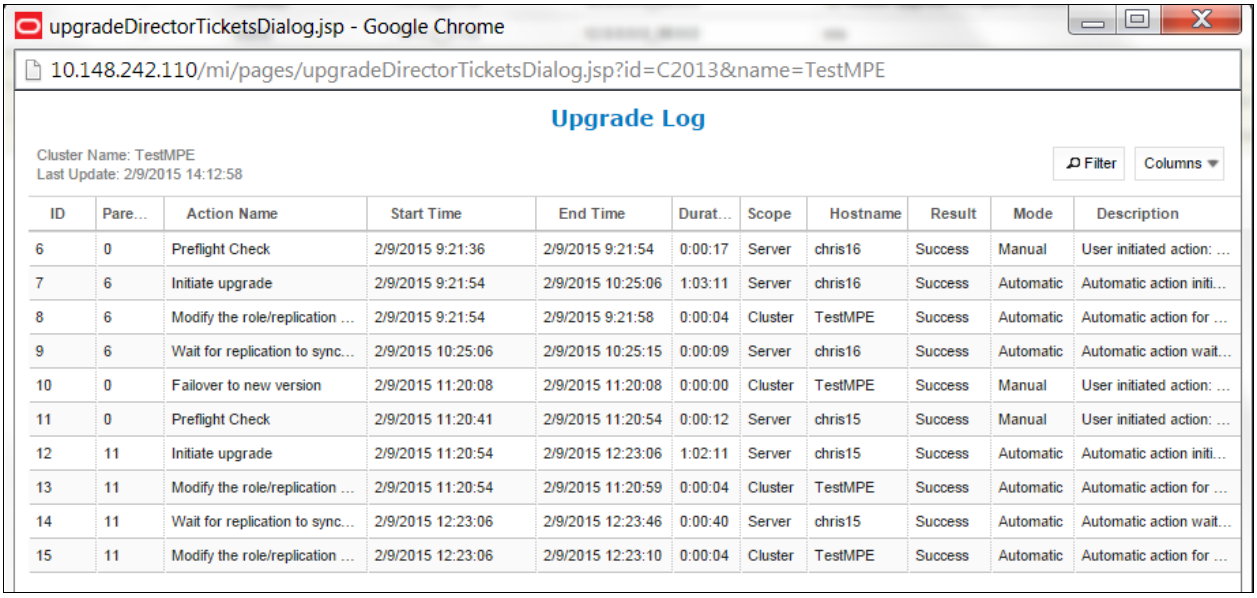
  N—Server is running old code and must be upgraded

  Y—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

Within the Upgrade Manager page, the operator can access the upgrade log. 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 is meant to track what the operator has done. This log is meant to capture the sequence of upgrade activity—whether it was initiated by an operator 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 using the **Upgrade** and **Backout** buttons. When the operator clicks one of these buttons, the Upgrade Director performs the next preferred action. However, there are times that the operator may want to take a slightly different—but still legal—procedure. For example, the Upgrade Director has a preferred order in which it upgrades a georedundant cluster. However, if the operator wanted to deviate from that default procedure—say to restrict upgrade to servers in a particular site—then they can use the optional actions menu. It is important to note that this menu is ONLY populated with legal/reasonable actions. Actions that are wrong or inconsistent are not displayed.

If the operator selects an optional action, they can go back to using the default/preferred 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 be either:

An upgrade to version *XXX*

To start a new upgrade, click on 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 file. This way, the CMP ISO file is always tied to the corresponding upgrade procedure.

When you select a new ISO file, you are telling the Upgrade Director to abandon the 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 hidden. However, there are conventions/operating principles that have visible effects.

3.1.5 Alarm Philosophy

During an upgrade, the Upgrade Manager asserts (that is, generates) and displays alarms. An upgrade typically triggers multiple minor, major, and critical alarms as servers are taken out of service, go into forced standby, or fail over. This is normal and to be expected. Figure 3 shows an example of an upgrade in progress asserting multiple transient alarms.

NOTE: Click on the active alarms summary, in the upper right corner of every CMP page, to display a list of current active alarms.

Name	Alarm Se...	Up to ...	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
wchenCMP-1A		N	Standby	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
wchenCMP-1B		N	Active	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
CMP Site2 Cluster (2 Servers)						
wchenCMP-2A		N	Standby	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
wchenCMP-2B		N	Active	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MPE1-s1 (3 Servers)						
MPE1-s1-b	Minor	N	Standby	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MPE1-s1-a	Minor	N	Active	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MPE1-s1-c	Minor	N	Spare	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MRA1-s1 (3 Servers)						
MRA1-s1-b	Minor	N	Active	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MRA1-s1-a	Minor	N	Spare	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout
MRA1-s1-c	Minor	N	Standby	12.3.0.0.0_23.1.0	12.2.1.0.0_6.1.0	Initiate backout

Figure 3 Upgrade in Progress Showing Transient Alarms

The Upgrade Manager clears alarms when appropriate, such as when server and cluster upgrades are complete. Table 3 lists transient alarms that the Upgrade Manager can assert during an upgrade.

Table 3 Transient Alarms Asserted During a Typical Upgrade

Alarm Number	Severity	Name
31227	Critical	HA availability status failed
31283	Critical	HA Server Offline / Lost Communication with server[2]
70001	Critical	QP_procmgr failed
70025	Critical	QP Slave database is a different version than the master
31233	Major	HA Path Down
70004	Major	QP Processes down for maintenance
31101	Minor	DB replication to slave failure
31106	Minor	DB merge to parent failure
31107	Minor	DB merge from child failure
31114	Minor	DB replication over SOAP has failed
31282	Minor	HA Management Fault
70500	Minor	System Mixed Version
70501	Minor	Cluster Mixed Version
70502	Minor	Cluster Replication Inhibited
70503	Minor	Server Forced Standby
70507	Minor	Upgrade in Progress

The Upgrade Manager also asserts an alarm if an unexpected error prevents it from continuing the upgrade. You should review all active alarms after each upgrade step to ensure that the alarms are expected. Alarms are described in the *Troubleshooting Guide*, Release 12.3, available at the Oracle Help Center.

3.1.6 General Upgrade Procedure

In general, the upgrade of a server goes through the following 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
2. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.
3. Preflight checks are VERY narrow. This prevents false positives for an otherwise valid upgrade.
4. The upgrade itself
5. Wait for replication to synchronize.

[2] The name of alarm 31283 changed in 12.1.2: Before 12.1.2, it was HA Server Offline, with 12.1.2 it became Lost Communication with Server. Depending on the original release and the upgrade progress, you might see the alarm with one or the other name.

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

3.1.6.1 Upgrade Order

With a two server cluster, there is only a single valid order:

1. Upgrade the standby
2. Failover
3. Upgrade the remaining server.

With georedundant clusters, there are many valid permutations. The default order that the Upgrade Director takes is:

1. Upgrade the standby server
2. Failover
3. Reapply the configuration

   NOTE: This requires you to navigate away from the Upgrade Manager page
4. Upgrade the spare server
5. Upgrade the remaining server in the primary site

3.1.6.2 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 promoted 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.

3.1.6.3 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, etc. In this sense, upgrade/backout should be fully reversible. However, you are not permitted to reverse direction if there is an ongoing action: You cannot kick off a backout of a server if another server in the cluster is being upgraded. You have to wait for the upgrade to finish.

3.1.6.4 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 must be in forced standby. This way, a simple failover does not cause a change in the version of code that is providing service.

NOTE: Forced standby is managed by the Upgrade Director and requires no action.

3.1.6.5 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 operator/support would investigate the original failure 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 exposed via the GUI.

4. UPGRADE PREPARATION

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

NOTE: If Veritas NetBackup is being used on the system, see the Maintenance Operation Procedure for pre and post upgrade steps.

Overview of steps:

Upgrade TVOE PM&C Server at Site1 (if applicable)

1. Upgrade TVOE PM&C Server at Site2 (if applicable)
2. Firmware (if applicable)
3. Upgrade Primary (Site1) CMP
4. Upgrade Secondary (Site2) CMP (if applicable)
5. Segment 1 Site1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
6. Segment 1 Site2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
7. Segment 2 Site1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
8. Segment 2 Site2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters

4.1 Prerequisites

The following procedure table verifies that all required prerequisite steps needed to be performed before the upgrade procedure begins.

TVOE, PM&C and Firmware might need to be upgraded prior to upgrade to Policy Management release 12.3.

Step	Procedure	Details
1. ☐	Verify all required materials are present	As listed in section 2.8 IntrRequired Materials and Remote Accessoduction.
2. ☐	Review Release Notes	Review Policy Management 12.3 Release Notes (E85334) for the following information: • Individual software components and versions included in target release. • New features included in target release.

Step	Procedure	Details
		• Issues (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: In release 12.3, only Mozilla Firefox and Google Chrome are fully supported.
---End of Procedure---		

4.2 TVOE and PM&C Server Upgrade

Policy Management release 12.3 requires PM&C Version 6.0.3 to support IPM of TPD 7.0.3 on c-Class servers.

PM&C can IPM TPD on a c-Class server if the server is introduced either for disaster recovery (DR) or when adding new servers to an enclosure (for example, capacity expansion).

See Appendix A to upgrade the 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 sequential steps:

Prerequisite: TVOE and PM&C Server upgraded. Firmware upgrade deployed if necessary.

1. Upgrade CMP clusters
2. Upgrade MPE/MRA clusters

Table 4 can be completed 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 procedure without backout procedure. Backout procedure time is typically the same as, or less than the upgrade procedure.

Table 4 Upgrade 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 Site1 and Site2 TVOE/PM&C	Site Names _____ and _____		3 hrs

Step	Procedure	Result	Engineer	Time
3. ☐	Upgrade Site1 and Site2 CMP clusters. Each cluster takes approximately 1 and ½ hours to complete	Site Names _____ and _____		3 hrs
4. ☐	Upgrade Site1 MPE/MRA clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site2 clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
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
---End of Procedure---				

4.5 Convert to Using Interval Statistics

Prior to Release 12.2, 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 became active or the operator manually reset the statistics. 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 not available. You must migrate to Interval statistics before upgrading to Release 12.3. Upon upgrade to R12.3, Oracle Communications Policy Management only uses Interval statistics and any Manual statistics not saved is lost.

Statistics affected by this change is reset to zero when migrating to Interval statistics. This affects both the information presented via the CMP GUI as well as 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 well in advance of the upgrade procedure:

Review your current configuration to determine which statistics method is currently being used by navigating to **GLOBAL CONFIGURATION → Global Configuration Settings → Stats Settings**.

If Manual is being used, change the Stats Reset Configuration parameter to Interval.

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

Use this procedure to determine the health and status of the servers to be upgraded and must be run 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 understood and resolved.***

Step	Procedure	Result
3. ☐	View KPI reports	Verify that the system is running within expected parameters. Export current KPIs into a file.

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

---End of Procedure---		

4.7 Deploy Policy Management Upgrade Software

Software should be deployed to each Policy Management server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This is typically done with utilities such as SCP, WGET or SFTP. Because of the large size of the software ISO file, sufficient time should be planned to accomplish this step. For Policy Management release 12.3, each ISO image size is about 1.0 Gigabytes.

4.7.1 Deploying Policy Management Upgrade Software to Servers

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

IMPORTANT: If the deployed image type (CMP, MPE, MRA, etc.) 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 be cleaned of all application software by an Install OS action using the PM&C GUI, and then the new application type installed.

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

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

NOTE: Not all Policy Management systems use a PM&C server. If that is the case, skip to the next section.

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

IMPORTANT: PM&C is not used for upgrade activities. The purpose of Use this procedure to be prepared for server recovery activities in case a server must be re-installed with software.

NOTES:

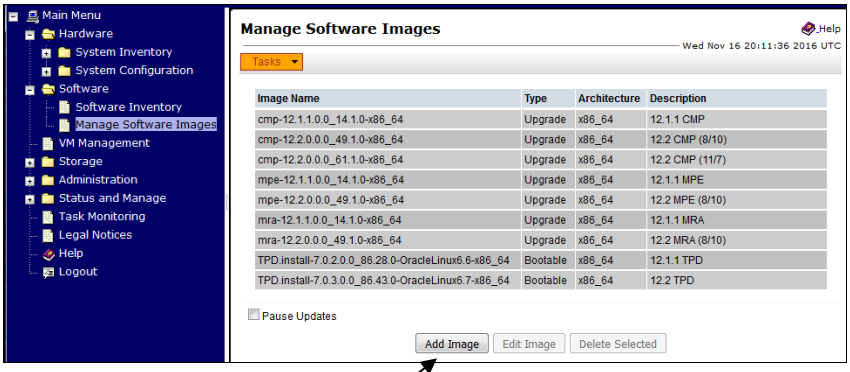
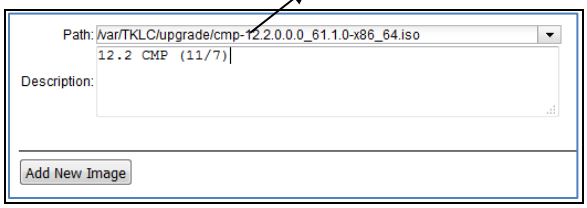
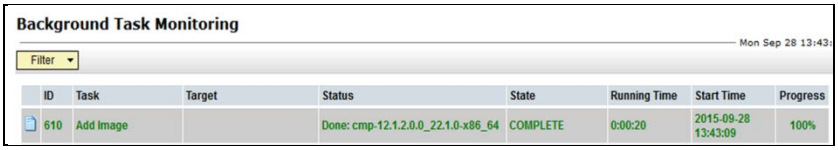
ISO file transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO file transfers to the target systems should be performed prior to and outside of the scheduled maintenance window. Schedule the required maintenance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

Because the ISO files are large, the procedure includes instructions to check the space available in the `/var/TKLC/upgrade` directory before copying the ISO files to the directory. After the Add Image action on the PM&C, the ISO files 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 that release 12.3 ISO files are not on the server	1. Log on to the PM&C Server GUI 2. Navigate to **Software → Manage Software Images**. 3. Confirm that the release 12.3 ISO files do not exist. If there are files, 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: If there are ISO files in the `/var/TKLC/upgrade` directory, you can remove the files to free up disk space or add the files to the PM&C repository.

3. ☐	Copy release 12.3 ISO files to the target directory in the PM&C server	1. Transfer all release 12.3 ISO files (CMP and non-CMP) into directory `/var/TKLC/upgrade` using one of the following methods: 2. SCP/WGET command in the following steps outline in this procedure **USB drive** **NOTE:** If the directory becomes full, you may have to use the scp command to transfer one ISO file at a time. Verify that the ISO file is in the directory before adding the next ISO file. You may also use the `/var/TKLC/smac/image/isoimages/home/smacftpusr` directory which has more available space.

Step	Procedure	Result
4. ☐	**PM&C GUI:** Adding the new release 12.3 ISO files	1. Navigate to **Software → Manage Software Images**. 2. Click **Add Image** to select the ISO files that were transferred to the PM&C server.   3. Click **OK**.
5. ☐	**PM&C GUI:** Verify that the ISO files were added successfully	Navigate to **Software → Manage Software Images**. The status of the image being added can be monitored using the Task Monitoring menu with the display as the following:  **NOTE:** The added ISO files are now stored in the `/var/TKLC/smac/image/repository` directory
---End of Procedure---		

4.7.3 Distribute Application ISO Image Files to Servers

This procedure applies to all server types. It assumes that the ISO image files is 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 and outside of the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

The distribution can be done in one of the following ways:

- Manual Distribution
- PM&C Distribution

4.7.3.1 Manual Distribution

Step	Procedure	Result
1. ☐	Transfer ISO files to Policy Management server.	1. Transfer release 12.3 ISO files (CMP and non-CMP) into the `/var/TKLC/upgrade` directory on the respective server using one of the following methods: - SCP/WGET command - USB drive 2. If the images are on a server in the same network, **`scp`** the files using the CLI, for example, for CMP: 3. Copy CMP software ISO file to ONE of the other CMP servers: `$sudo scp cmp-12.3.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/` 4. Repeat for one server of all clusters. **NOTE:** After copying the ISO to one of the respective servers, the ISO Maintenance is used to upload to the rest of the servers.
---End of Procedure---		

4.7.3.2 PM&C Distribution

The PM&C product is not used during Policy Management upgrade and backout procedures. However, if your topology is supported by PM&C servers, you should add the Policy Management ISO images to the PM&C image repository to support new installations and server field replacements.

Collect the following information and material beforehand:

- The URL of the PM&C server and the **`guiadmin`** password
- The Policy Management ISO files, loaded into the directory `/var/TKLC/upgrade` on the PM&C server

NOTE: You can instead add images from the following sources:

- Media mounted in the CD/DVD drive of the PM&C host
- USB media attached to the PM&C host
- External mounts (prefix the directory with `extfile://`)

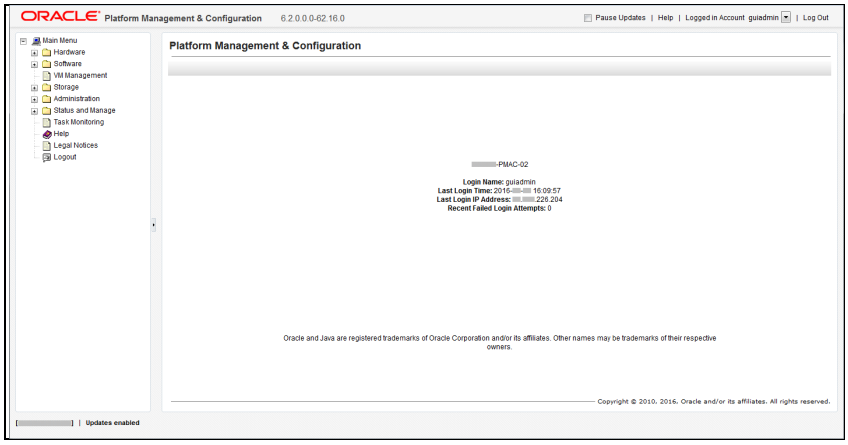
  These local search paths:

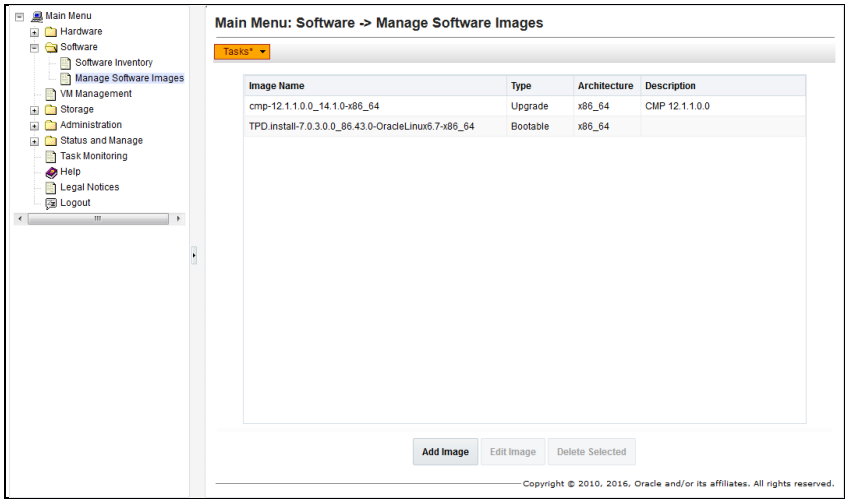
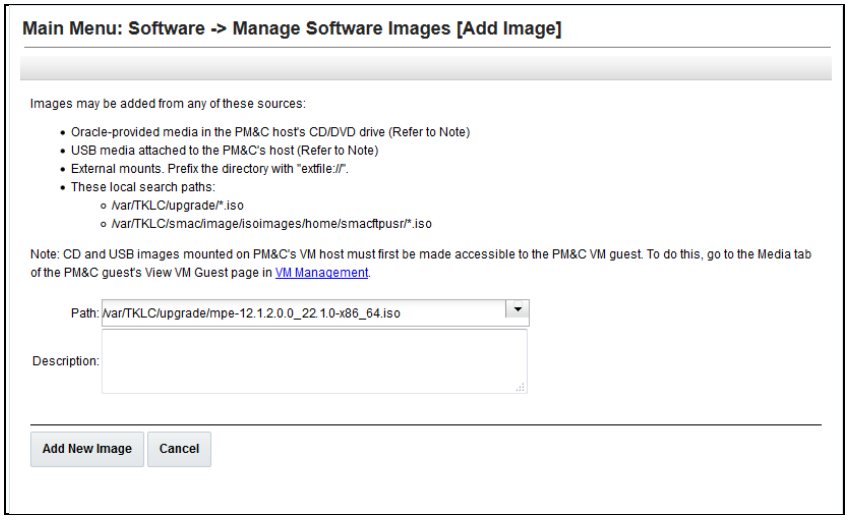
  `/var/TKLC/upgrade/`

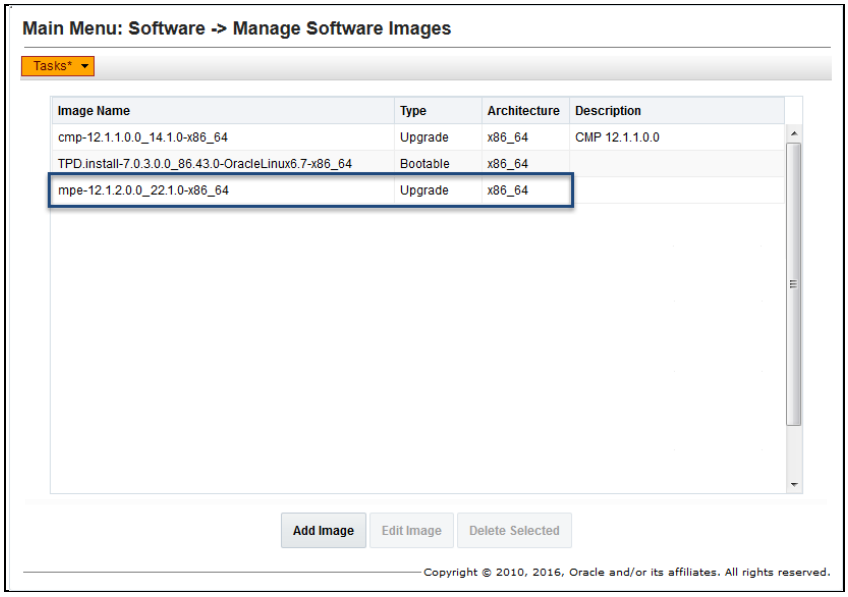
  `/var/TKLC/smac/image/isoimages/home/smacftpusr/`

NOTE: CD, DVD, and USB images mounted on the PM&C VM host must be made accessible to the PM&C VM guest. To do this, go to the Media tab of the PM&C View VM Guest page on the PM&C VM Management page.

This procedure assumes the ISO file is located in the `/var/TKLC/upgrade` directory on the PM&C server.

Step	Procedure	Result
1. ☐	Log in to PM&C	Open a browser, enter the URL of the PM&C server, and log in as guiadmin. The PM&C Main Menu opens. For example: 

Step	Procedure	Result
2. ☐	Select the ISO image	1. Navigate to **Main Menu → Software → Manage Software Images.** The **Manage Software Images** page opens. For example:  2. Click **Add Image** (at the bottom of the page).The Manage Software Images [Add Image] page opens. For example:  3. Select the ISO file from the **Path** list and click **Add New Image**. **Tip:** You can enter a description of the ISO file before adding it. You are prompted: Click **OK** to remove the image from `/var/TKLC/upgrade` directory after it is added to the repository. Click Cancel to leave it there.

Step	Procedure	Result
3. ☐	Move the ISO file to the repository	Click **OK** to move the file (or **Cancel** to copy it). The ISO file is loaded into the PM&C image repository in the background. **Tip:** You can click **Tasks** to check the progress of the task. When the upload is complete, the ISO file is in the list. For example: 

4. ☐	Verify that the image is not in the directory	Enter the following command:
		`$ sudo ls /var/TKLC/upgrade`
		`$`

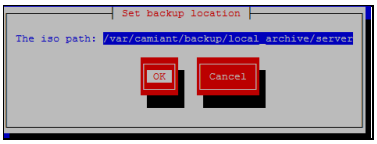
5. ☐	Load addition files	If you are loading multiple ISO files into the image repository, repeat steps 2–4 until all files are loaded.
6. ☐	Remove media	When you finish, remove the CD/DVD media or unmount the USB device.
---End of Procedure---		

4.7.4 Backups and Backup Locations

Perform the backups prior to the maintenance window period.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Step	Procedure	Result

1. ☐	**SSH CLI/iLO:** Access the server to be backed up
	
	NOTE: System backup is done on active CMP servers ONLY.
		IMPORTANT: Server backups (for each CMP and non-CMP server, active/standby/spare), 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
		4. Provide (or use the suggested) ISO backup filename in the default backup location path of:
		`/var/camiant/backup/local_archive/serverbackup/<filename>.iso`
		 
		
		5. Go back to the previous menu.
		Policy Configuration→Backup and Restore
		6. Select **System Backup**.
		7. Provide (or use the suggested) tarball backup filename in the default backup location path of:
		`/var/camiant/backup/local_archive/systembackup/<filename>.tar.gz`
		 

Step	Procedure	Result

2. ☐	**SSH CLI/iLO:** Verify the backup ISO file	If default location is accepted in the previous step, change to the following directory and verify the file. For example for an MPE server backup:
		`$ cd /var/camiant/backup/local_archive/serverbackup`
		`$ ls <hostname>-mpe-_12.3.x…x-serverbackup-<yyyy><mm><dd><hhmm>.iso`
		And for the system backup:
		`$ cd /var/camiant/backup/local_archive/systembackup`
		`$ ls <hostname>-cmp_12.3.x…x-systembackup-<yyyy><mm><dd><hhmm>.tar.gz`

3. ☐	Copy backup files.	1. Copy the files to remote server or local workstation/laptop.
		Example of a remote server copy.
		`$ sudo scp /var/camiant/backup/local_archive/systembackup/xx_tar.gz <remoteserver_ipaddress>:<destinationpath>`
		2. Remove the backup ISO file from the TPD Sever.
		`$sudo rm <backup_filename>.iso`

4. ☐	Identify backup location	3. Backup location is: _____ Instructions to access to backups are as follows: _____ _____ _____
---End of Procedure---		

4.7.5 Changing Non-Default root and admusr Passwords

4.7.5.1 Improve Password Security

The default password hash prior to Policy Management 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 causes issues during upgrade from pre-12.1.1to 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 is hashed with the strongest possible method, SHA512.

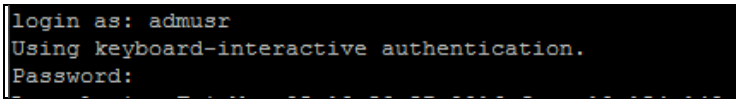
This procedure only addresses root and admusr passwords. Other users should also update their password to benefit from the new hashing. If they are not changed prior to the upgrade to 12.3, they is expired post upgrade.

IMPORTANT: The following procedure should be run prior to the upgrade to 12.3 only if the root or admusr passwords are non-default.

Order to perform the upgrade on an In-Service Policy Management system:

1. Standby CMPs
2. Active CMPs
3. Standby MPE/MRA
4. Spare MPE/MRA
5. Active MPE/MRA

Changing Non-Default root and admusr Passwords

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

Step	Procedure	Result

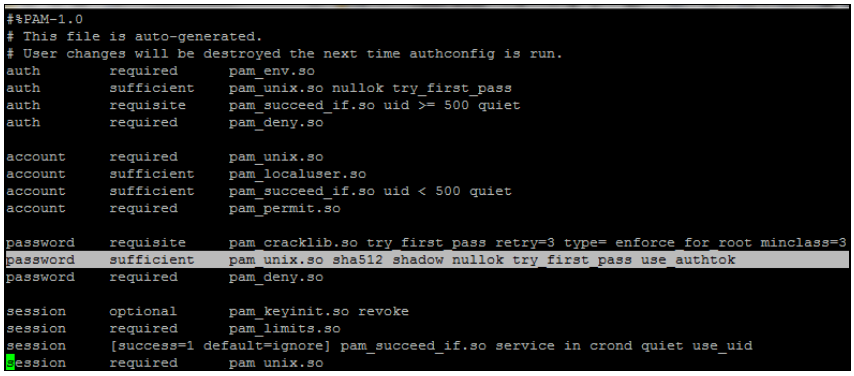
2. ☐	Check the password field of root and admusr	Issue the following:
		`#egrep '^(root|admusr)' /etc/shadow`
		EXAMPLE OUTPUT
		`root:$6$mErKrEsA$83n5G8dR3CgBJjMEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc.Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7:::`
		`admusr:$6$mUstAfa$gn2B8TsW1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825::::::`
		NOTES:
		• If the first two characters after the colon are $6, then this procedure is not needed on this server. Skip to the next section.
		• 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 3

3. ☐	Order to perform the change	Perform steps 4-15 on each server in the following order: 1. Standby CMP 2. Active CMP 3. Standby non-CMP servers 4. Spare non-CMP servers 5. Active non-CMP servers

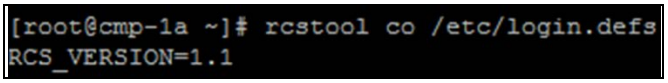
4. ☐	Login to the Server	1. Login as admusr and change to root using the following command:
		`$sudo su`
		`login as: admusr`
		`Using keyboard-interactive authentication.`
		`Password:`

5. ☐	Checkout revisions	Issue the following command:
		`#rcstool co /etc/pam.d/system-auth`
		`[root@cmp-1a ~]# rcstool co /etc/pam.d/system-auth`
		`RCS_VERSION=1.1`

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 md5 value to sha512
		- 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 configured:
		`#rcstool unco /etc/pam.d/system-auth`

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

9. ☐	Edit `login.defs` file	**Shadow password suite configuration**
		1. Open the `login.defs` file.
		`#vi /etc/login.defs`
		2. Change the encrypt method from `MD5` to `SHA12`.
		- Current Line:
		`ENCRYPT_METHOD MD5`
		- Modified Line:
		`ENCRYPT_METHOD SHA512`
		NOTE: The line to edit is near 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 was configured.
		`#rcstool unco /etc/login.defs`

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

12. ☐	Edit the `libuser.conf` file	Open the `libuser.conf` file and change the crypt style from `md5` to `sha12`
		`#vi /etc/libuser.conf`
		• Current Line:
		`crypt_style = md5`
		• Modified Line:
		`crypt_style = sha512`
		NOTE: The line to edit is close to the top of the file.
		After setting the password, the passwords are now successfully encrypted and are using SHA512 (the strongest hash algorithm).

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

14. ☐	Set the admusr and root passwords	• For root user:
		`#passwd root`
		• For admusr user:
		`#passwd admusr`
		NOTE: After setting the password, the passwords are now successfully encrypted and are using SHA512 (the strongest hash algorithm).

15. ☐	Verify	Logout of the current session and then login using the new password credentials.
---End of Procedure---		

5. UPGRADE CMP CLUSTERS (12.1.X TO 12.3)

Use this procedure to upgrade the Site1 CMP cluster, and if needed, upgrade the Site2 CMP cluster.

5.1 Upgrade CMP clusters Overview

The following is an overview of CMP cluster upgrade.

1. Upgrade Primary CMP cluster

   Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Primary Site 1

   a. Start upgrade

   b. Failover

   c. Log back into the CMP GUI

   d. Continue upgrade

2. Upgrade The Secondary CMP cluster

   Use the CMP GUI and select **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2.

   a. Start upgrade

   b. Failover

   c. Continue upgrade

It is assumed that the CMPs may be deployed as 2 Geo-Redundant clusters, identified as Site-1 and Site-2 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 Management system), and the other is as Secondary site (this site is ready to become Primary site, if needed).

CMP Sites Georedundant 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 Address _____

Server-A Status _____

Server-B Hostname _____

Server-B IP Address _____

Server-B Status _____

IMPORTANT:

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

1.2.1 Upgrade Primary CMP cluster

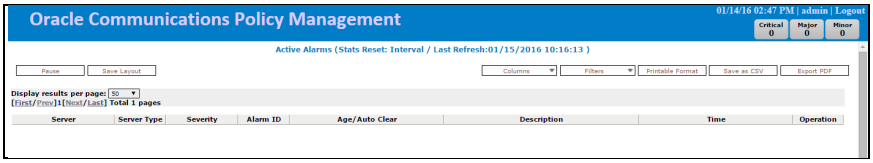
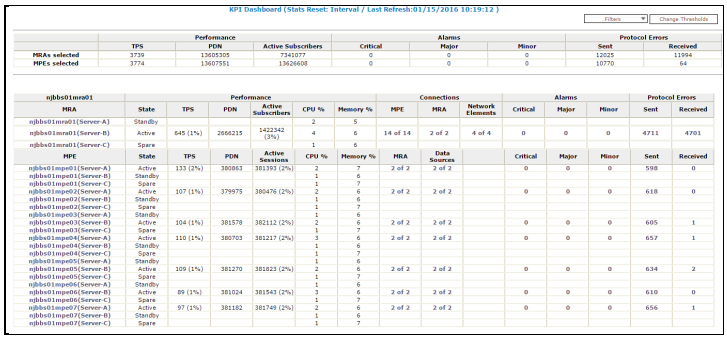
Use this procedure to upgrade a Primary CMP cluster.

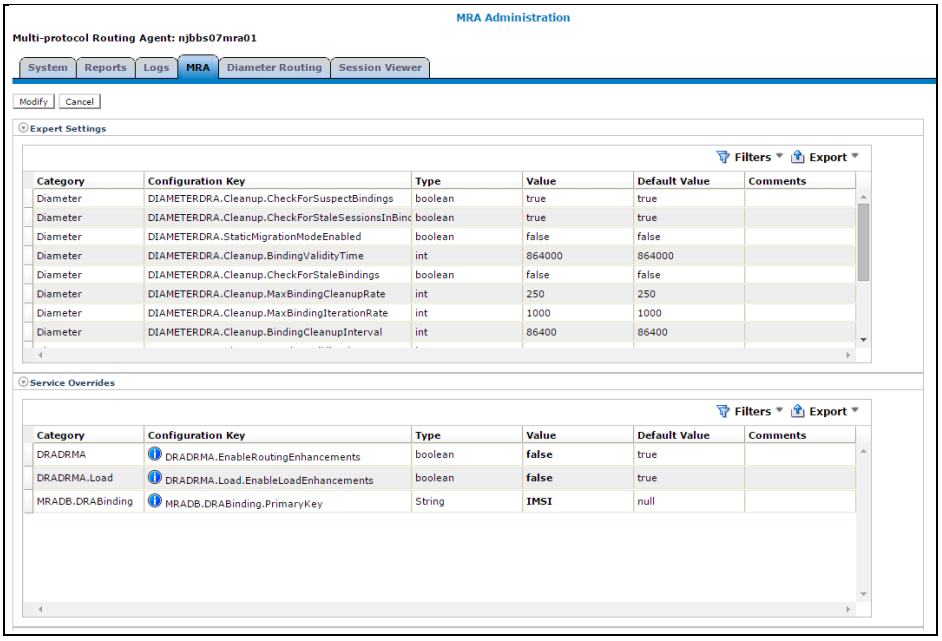
NOTES:

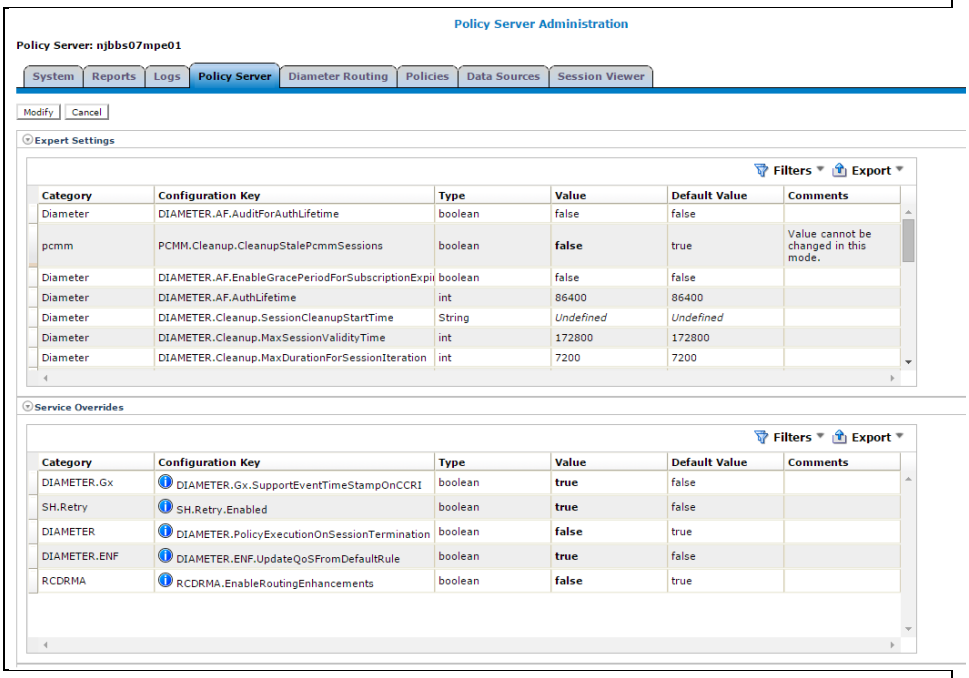
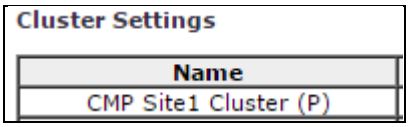
- This procedure must be performed in a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

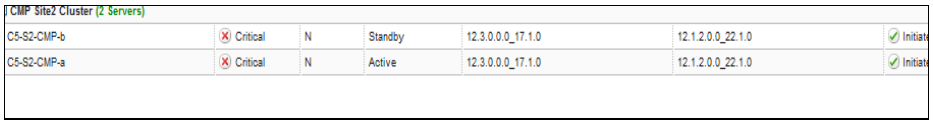
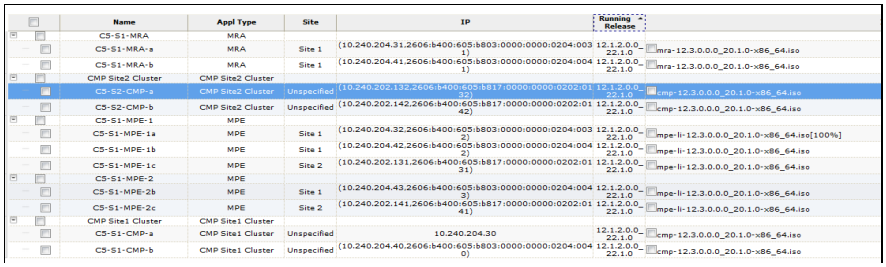
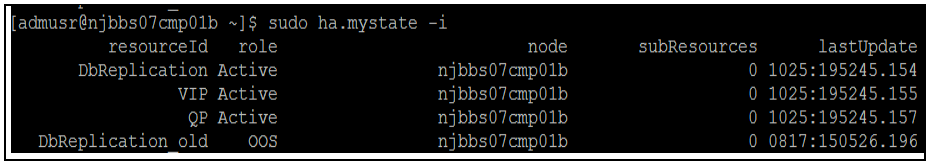
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 1: Upgrade Primary CMP cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify Alarm Status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Confirm that any existing alarm is understood and does not impact to the Upgrade procedure. 3. Capture the screen and save it into a file for reference. 
2. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates. 3. Capture the screen and save it into a file for reference. 

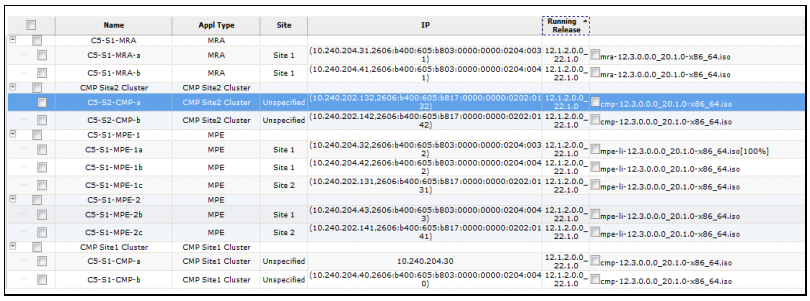
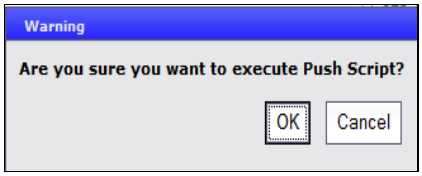
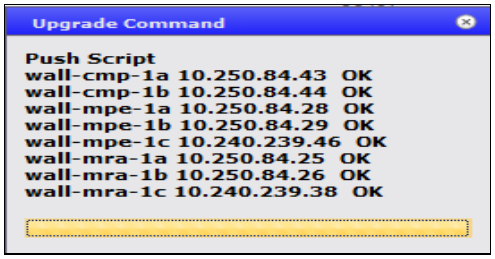
Step	Procedure	Details
3. ☐	**CMP GUI:** Capture MRA Advanced Settings	1. Capture screenshots of the advanced settings on the MRA prior to upgrading the CMP and save them into files for future reference check. 2. Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ MRA**. 3. Click **Advanced Settings**.  Alternatively, settings can be exported clicking **Export** on the right within each setting.

Step	Procedure	Details
4. ☐	**CMP GUI:** Capture MPE Advanced Settings	1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them into files for future reference check. 2. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ Policy Server** 3. Click **Advanced Settings**.  Alternatively, settings can be exported clicking **Export** on the right within each setting.
5. ☐	**CMP GUI:** Identify and Record the CMP cluster(s)	1. Navigate to **Platform Setting → Topology Settings → All Clusters**. 2. Note which cluster is the primary and which is the secondary. 3. Save a screenshot for future reference. The primary CMP is noted with a P 

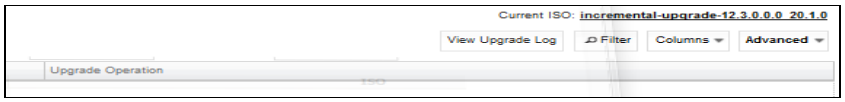
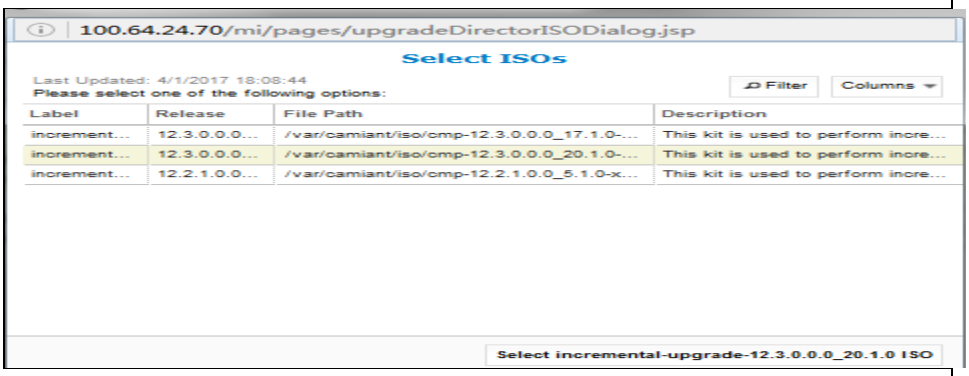
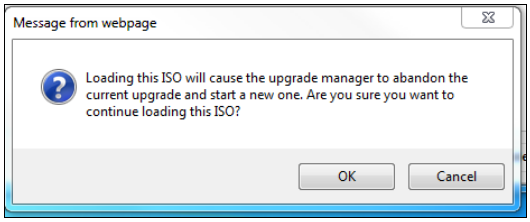
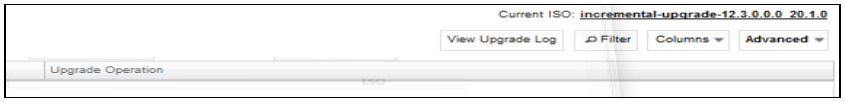
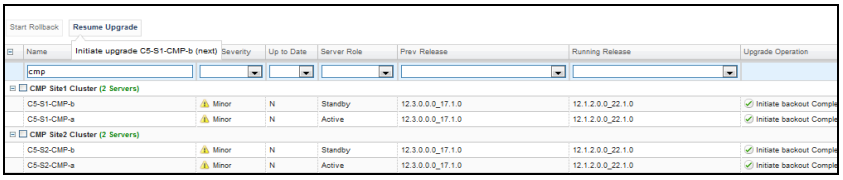
Step	Procedure	Details
6. ☐	**CMP GUI:** Verify Status of CMP clusters and ISO files are copied to each server	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that the CMP clusters have the following: - Server Role has Active/Standby status - Running Release is 12.1.x version  3. Navigate to **Upgrade → ISO Maintenance**. 4. Verify that Release 12.3.x ISO files copied to each of the servers (CMP/MRA/MPE/Mediation) 
7. ☐	**SSH Primary Active CMP:** SSH CLI Primary Active CMP and verify the Primary Active CMP Role	1. SSH into the Primary Active CMP with its VIP address. 2. Login as admusr. 3. Enter the password: <*provided password*>. 4. Run the **`sudo ha.mystate -i`** CLI command to confirm its role as Active. `$ sudo ha.mystate -i`  **NOTE:** DbReplication_old_OOS is a non-issue status event.

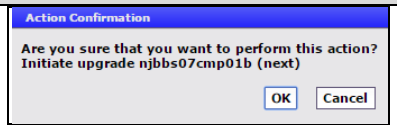
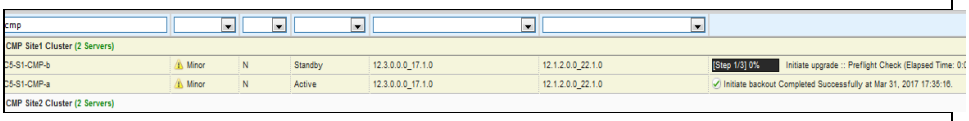
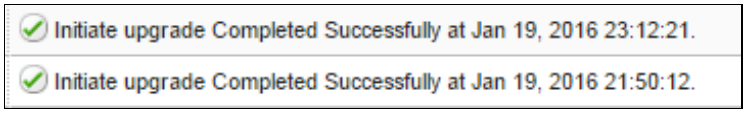
Step	Procedure	Details

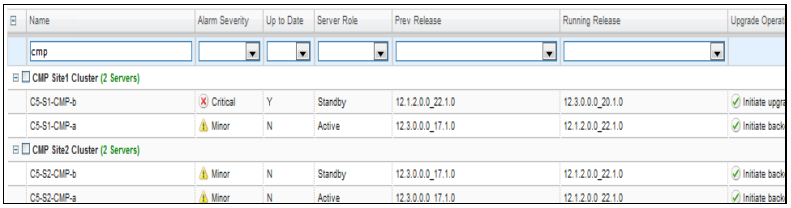
8. ☐	**SSH Primary Active CMP:** exchange keys	1. Exchange keys to all servers from the SITE 1 Active Primary CMP.
		2. Login as admusr.
		`$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.3.0.0_x.x.0-x86_64.iso /mnt/upgrade/`
		`$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		NOTE: If prompted, answer **Yes** to all questions.
		`$ sudo umount /mnt/upgrade`
		`$ sudo qpSSHKeyProv.pl --prov`
		• Required to enter the PASSWORD for admusr.
		• Ensure that the keys are exchanged successfully with all the server clusters.
		For example:
		`$ sudo qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:<admusr password>`
		`Connecting to admusr@njbbs07cmp01b ...`
		`Connecting to admusr@njbbs07cmp01a ...`
		`Connecting to admusr@txsls07mra01b ...`
		`Connecting to admusr@njbbs07mpe02a ...`
		`Connecting to admusr@txsls07mpe01b ...`
		`Connecting to admusr@njbbs07mra01a ...`
		`Connecting to admusr@njbbs07mpe02c ...`
		`Connecting to admusr@njbbs07mpe01c ...`
		`Connecting to admusr@txsls07mpe02a ...`
		`Connecting to admusr@txsls07mra01a ...`
		`:`
		`:`
		`[14/17] Provisioning SSH keys on njbbs07mra01c ...`
		`[15/17] Provisioning SSH keys on njbbs07mpe01b ...`
		`[16/17] Provisioning SSH keys on txsls07mpe02b ...`
		`[17/17] Provisioning SSH keys on njbbs07mra01b ...`
		`SSH keys are OK.`

Step	Procedure	Details
9. ☐	**CMP GUI:** Push the Release 12.3.x upgrade Scripts to all servers in the segment topology	1. Navigate to **Upgrade → ISO Maintenance**. 2. Select all the servers in the topology as shown.  3. Select **Operations → Push Scripts** operation. (It is safe to run the push script multiple times as needed) 4. Click OK to continue the operation.  5. Verify that Operation is successful with OK for each server.  **NOTE:** It may take up to couple minutes to complete

10. ☐	**Primary Active CMP:** SSH to primary active CMP and copy ISO to `/var/camiant/iso`	1. Logon to the primary active CMP as admusr.
		2. Copy the 12.3.x ISO to the `/var/camiant/iso` directory:
		`$ sudo cp /var/TKLC/upgrade/cmp-12.3.0.0_x.x.0-x86_64.iso /var/camiant/iso/`
		3. Verify:
		`$ ls /var/camiant/iso`

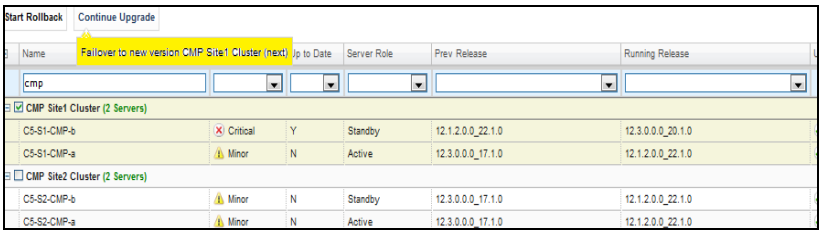
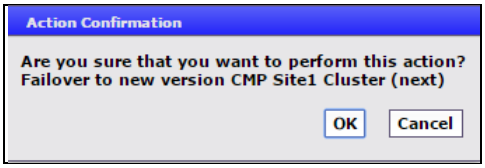
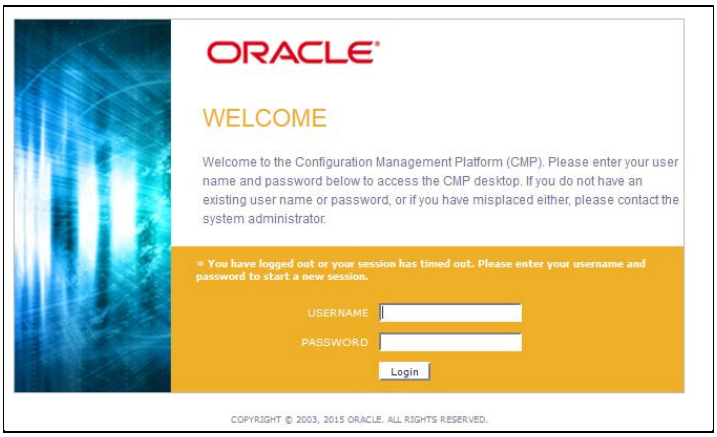
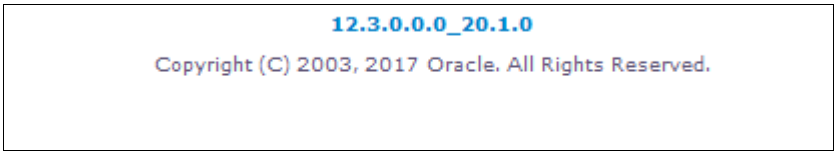
Step	Procedure	Details
11. ☐	**CMP GUI:** Select the new 12.3.x Upgrade release	1. Navigate to Upgrade → Upgrade Manager 2. Select the Current ISO.  This opens a dialog with a description of the ISO that was copied into `/var/camiant/iso`. 3. Highlight the available 12.3.x ISO 4. Click **Select incremental-upgrade-12.3.0.0.0_20.1.0 ISO** in the bottom right hand corner of the window  5. Click **OK**.  Within a few seconds, the Up to date column changes from Y (meaning up-to-date) or N (meaning needs upgrade).
12. ☐	**CMP GUI:** Upgrade Primary CMP cluster **NOTE:** This takes approximately 30 minutes to complete.	1. Navigate to Upgrade → Upgrade Manager. **NOTE:** Click **Filter** and enter `CMP` in the Name field to show only the CMP servers.  2. Select the Primary CMP Server Cluster 3. Click **Start Upgrade**.  4. Click **OK** to confirm and continue with the operation.

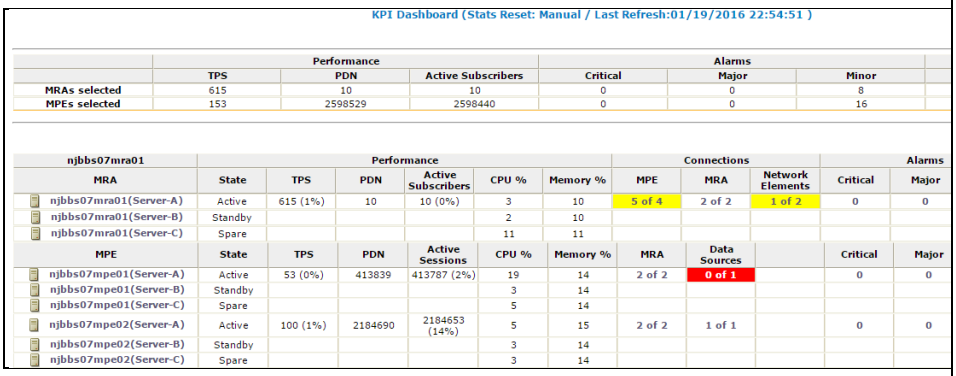
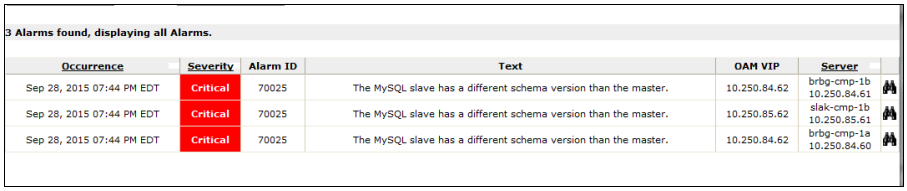
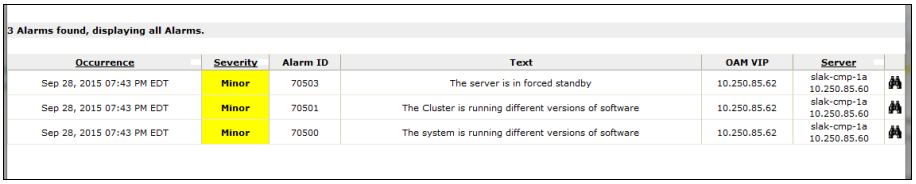
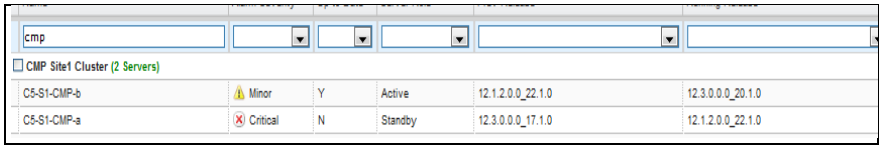
Step	Procedure	Details
		 The specific action taken is determined by the UM and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP cluster 5. In the Upgrade Operation column, the In Progress status along with the upgrade activities can be seen.  Upgrade Status changes to complete when done. During the Upgrade activities, the following alarms may be generated and are considered normal reporting events: **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault Upgrade is complete on the first CMP server in the cluster when the following message (completed successfully) displays in the Upgrade Operation column. 

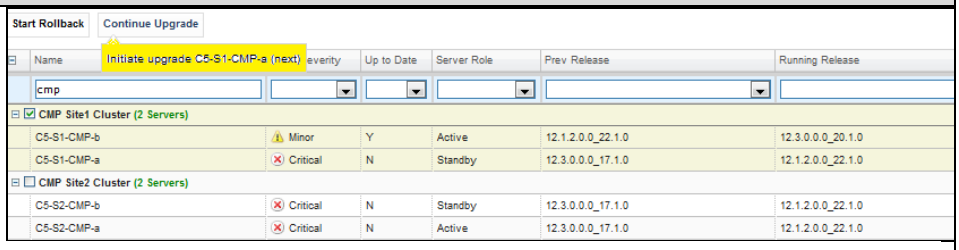
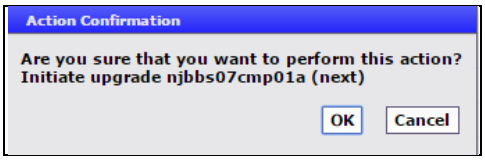
Step	Procedure	Details
13. ☐	**CMP GUI:** Verify the upgrade is successful	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the cluster. At this point, one server is on 12.3.x and the other server in the cluster is on 12.1. The Up To Date column shows Y for the 12.3.x server and N for the 12.1 server. 

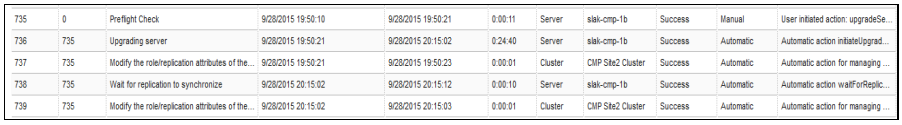
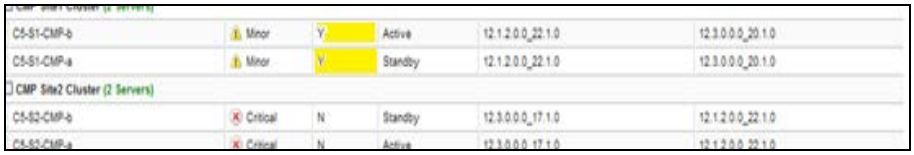
14. ☐	**CMP CLI:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the upgrade is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		To resolve this situation permanently, perform the following:
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change from primary=eth11 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

15. ☐	**CMP GUI:** Verify System Wide Reports – KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for a few refresh updates.

Step	Procedure	Details
16. ☐	**CMP GUI:** Continue upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server Cluster 3. Select **Continue Upgrade**. Notice the failover to new version message. **NOTE:** This causes a failover of the Primary CMP cluster  4. Click **OK** to confirm and continue with the operation.  The specific action takes about less minute to complete.
17. ☐	**CMP GUI:** Re-login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management Release 12.3.x CMP GUI Login page opens. The login and password credentials are the same as the pre-upgrade. 
18. ☐	**CMP GUI:** Verify new Policy Management release	1. Navigate to **Help→About**. 2. Verify the release displayed is 12.3.x 

Step	Procedure	Details
19. ☐	**CMP GUI:** Verify traffic	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs / MRAs. Observe it for few updates refresh.  KPI Dashboard (Stats Reset: Manual / Last Refresh:01/19/2016 22:54:51) Performance: TPS / PDN / Active Subscribers — Alarms: Critical / Major / Minor MRAs selected: 615 / 10 / 10 — 0 / 0 / 8 MPEs selected: 153 / 2598529 / 2598440 — 0 / 0 / 16 njbbs07mra01 — Performance: State / TPS / PDN / Active Subscribers / CPU % / Memory % — Connections: MPE / MRA / Network Elements — Alarms: Critical / Major njbbs07mra01(Server-A): Active / 615 (1%) / 10 / 10 (0%) / 3 / 10 — 5 of 4 / 2 of 2 / 1 of 2 — 0 / 0 njbbs07mra01(Server-B): Standby / 2 / 10 njbbs07mra01(Server-C): Spare / 11 / 11 MPE: State / TPS / PDN / Active Sessions / CPU % / Memory % / MRA / Data Sources / Critical / Major njbbs07mpe01(Server-A): Active / 53 (0%) / 413839 / 413787 (2%) / 19 / 14 / 2 of 2 / 0 of 1 / 0 / 0 njbbs07mpe01(Server-B): Standby / 3 / 14 njbbs07mpe01(Server-C): Spare / 5 / 14 njbbs07mpe02(Server-A): Active / 100 (1%) / 2184690 / 2184653 (14%) / 5 / 15 / 2 of 2 / 1 of 1 / 0 / 0 njbbs07mpe02(Server-B): Standby / 3 / 14 njbbs07mpe02(Server-C): Spare / 3 / 14
20. ☐	**CMP GUI:** Critical Alarms	Critical alarms 70025 is seen until the SQL Database matches the master (12.3.x). These alarms are expected and remain until all CMPs have been upgraded to the same version.  3 Alarms found, displaying all Alarms. Occurrence / Severity / Alarm ID / Text / OAM VIP / Server Sep 28, 2015 07:44 PM EDT / Critical / 70025 / The MySQL slave has a different schema version than the master. / 10.250.84.62 / brbg-cmp-1b 10.250.84.61 Sep 28, 2015 07:44 PM EDT / Critical / 70025 / The MySQL slave has a different schema version than the master. / 10.250.85.62 / slak-cmp-1b 10.250.85.61 Sep 28, 2015 07:44 PM EDT / Critical / 70025 / The MySQL slave has a different schema version than the master. / 10.250.84.62 / brbg-cmp-1a 10.250.84.60 Current Minor Alarms  3 Alarms found, displaying all Alarms. Occurrence / Severity / Alarm ID / Text / OAM VIP / Server Sep 28, 2015 07:43 PM EDT / Minor / 70503 / The server is in forced standby / 10.250.85.62 / slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT / Minor / 70501 / The Cluster is running different versions of software / 10.250.85.62 / slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT / Minor / 70500 / The system is running different versions of software / 10.250.85.62 / slak-cmp-1a 10.250.85.60 **NOTE:** The Upgrade Manager shows alarms as well.
21. ☐	**CMP GUI:** Verify the Policy Management Release 12.3.x CMP is Active	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that the: - Active server is on Running Release 12.3.x - Standby server is on the previous Release  cmp CMP Site1 Cluster (2 Servers) C5-S1-CMP-b / Minor / Y / Active / 12.1.2.0.0_22.1.0 / 12.3.0.0.0_20.1.0 C5-S1-CMP-a / Critical / N / Standby / 12.3.0.0.0_17.1.0 / 12.1.2.0.0_22.1.0 As noted, the Active CMP server is now on the Running Release of 12.3.x
22. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP cluster **NOTE:** This takes approximately 30 minutes to	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server Cluster. 3. Click **Continue Upgrade**. Notice the Initiate upgrade message.

Step	Procedure	Details
	complete.	 4. Click **OK** to continue the upgrade on the remaining server in the CMP cluster  **NOTE:** The remaining CMP server takes about 30 minutes to complete based on the size of My-SQL database. Server getting upgraded goes into OOS. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **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 **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault

Step	Procedure	Details
23. ☐	**CMP GUI:** Tracking the upgrade complete	1. Navigate to **Upgrade → Upgrade Manager**. The last step of the upgrade for the first CMP cluster is to wait for replication to complete. 2. Select the Upgraded CMP cluster. 3. Click **View Upgrade Log**. 
24. ☐	**CMP GUI:** Verify the status of the upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**.  Successful upgrade status shows both servers running the Release 12.3.x 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.
25. ☐	Proceed to next upgrade procedure	At this point, the Primary Site-1 is running Release 12.3.x • Secondary SITE is on R12.1.x. • Proceed to the next procedure to upgrade the secondary CMP cluster.
---End of Procedure---		

1.2.2 Upgrade Secondary CMP cluster

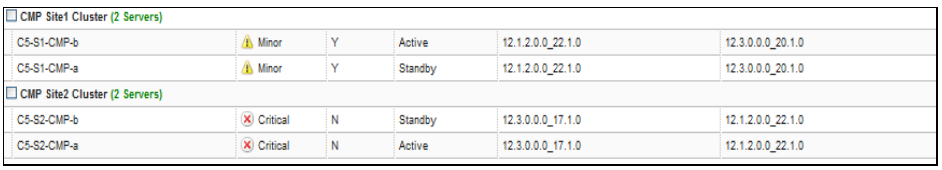
Use this procedure to upgrade Secondary CMP cluster.

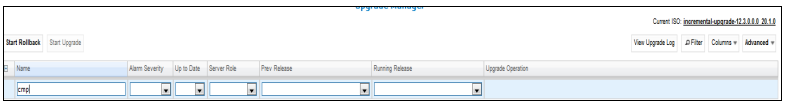
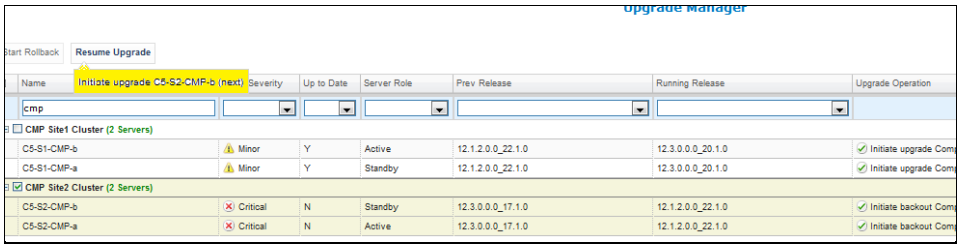
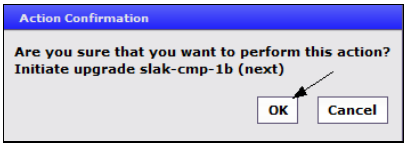
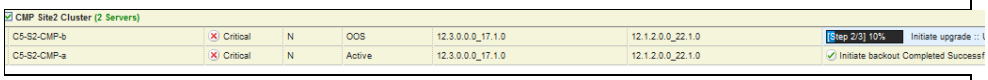
NOTES:

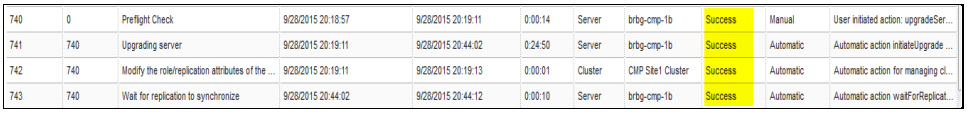
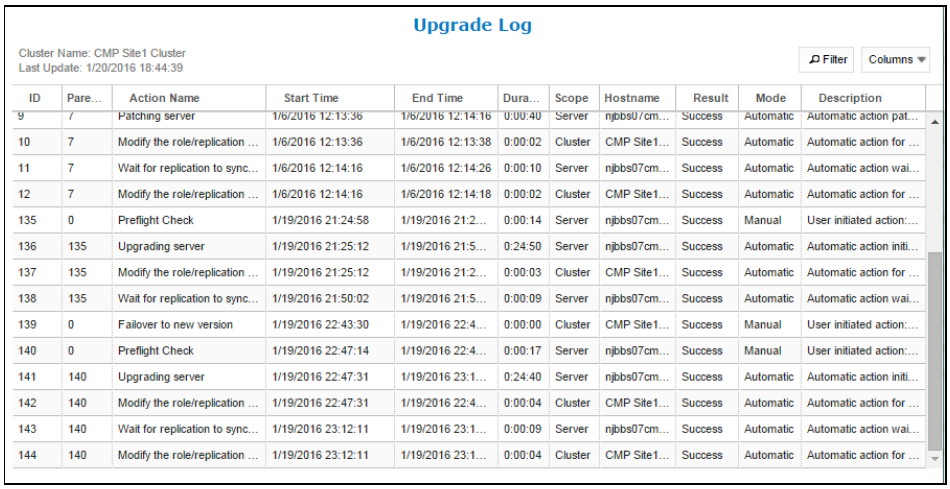
- This procedure must be performed in a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

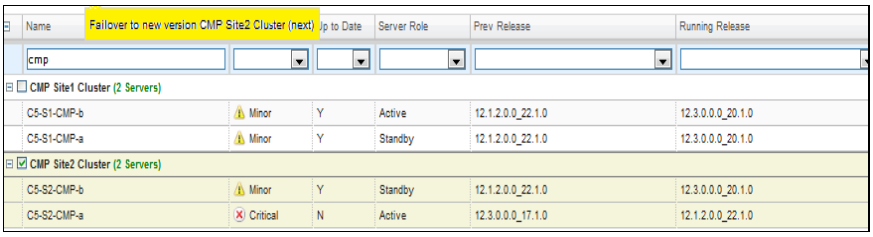
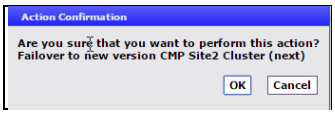
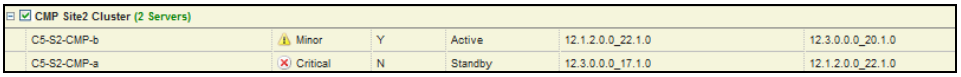
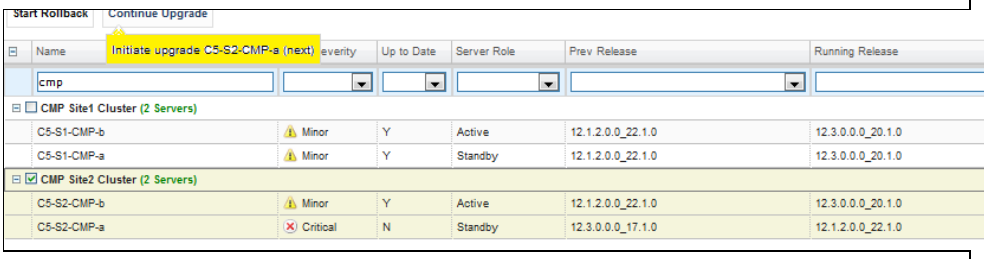
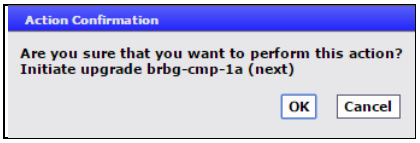
Procedure 2: Upgrade Secondary CMP cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify Status of CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Primary CMP is completely upgraded to 12.3.x. 3. Secondary CMP cluster is on 12.1.x. 

Step	Procedure	Details
2. ☐	**CMP GUI:** Upgrade the Secondary CMP cluster. **NOTE:** This takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. **NOTE:** Click **Filter** and enter `CMP` in the Name field to show the CMP servers only.  2. Select the Secondary CMP Server Cluster at Site-2 3. Select **Continue Upgrade**.  4. Click **OK** to confirm and continue with the operation.  The specific action taken is determined by the UM and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP cluster In the Upgrade Operation column, it displays the In Progress status along with the upgrade activities.  During the Upgrade activities, the following alarms may be generated and are considered normal reporting events: **<u>Expected Critical Alarms</u>** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **<u>Expected Major Alarms</u>** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **<u>Expected Minor Alarms</u>** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed

Step	Procedure	Details
		31106 DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault **LOG FILE from the GUI showing complete on the 1st server on the secondary site.** 
3. ☐	**CMP GUI:** Verify the upgrade is successful	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the partially upgraded cluster. 3. Select **View Upgrade LOG**. 

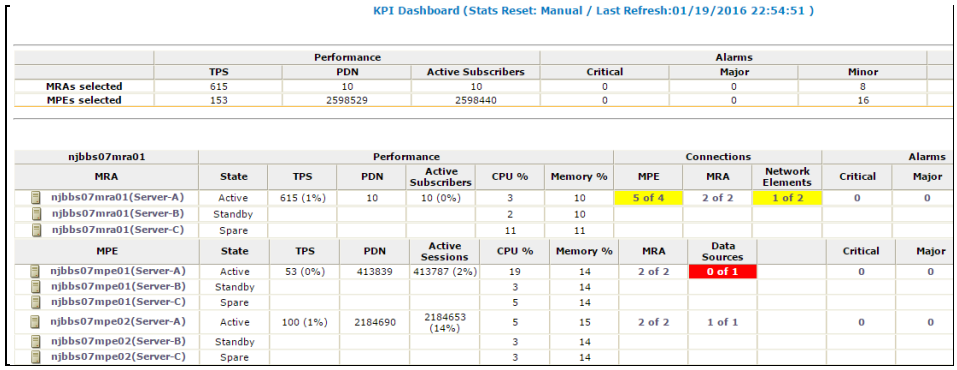
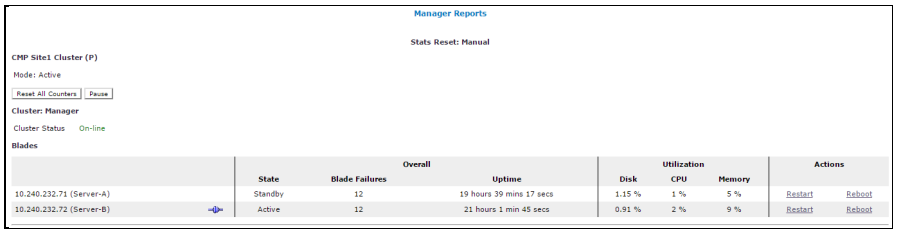
4. ☐	**CMP CLI:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the upgrade is successful, ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		To resolve this situation permanently, perform the following:
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change from primary=eth11 to primary=eth01.
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

Step	Procedure	Details
5. ☐	**CMP GUI:** Continue Upgrade of Secondary CMP cluster **NOTE:** This takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP Server Cluster at Site-2 3. Select **Continue Upgrade**. Notice the message indicating the failover to new version.  4. Click **OK** to confirm and continue with the operation  The action takes a minute to complete. Wait until the upgraded server is active, as shown below.  5. Select the Secondary CMP Server Cluster at Site-2 6. Select **Continue Upgrade**. When hovering over the **Continue Upgrade** button, the message displays the next action, which is upgrading the remaining CMP hostname.  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** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline

Step	Procedure	Details
		Expected Major Alarms **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **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 **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault
6. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	Navigate to **Upgrade → Upgrade Manager**. Successful upgrade status shows the Release 12.3.x in the Running Release column. Also, under Upgrade Operation column, it shows the Initiate Upgrade Completed Successfully message with the correct date and time.

7. ☐	**CMP CLI:** Verify eth01 is the primary device interface	This step only applies if the server has a condition in which after the upgrade is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following.
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01, and this step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change from primary=eth11 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

8. ☐	**CMP GUI:** Verify Alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarms** **70500** The system is running different versions of software

Step	Procedure	Details
9. ☐	**CMP GUI:** Verify System Wide Reports – KPI Dashboard Report	Navigate to **System Wide Reports → KPI Dashboard**.  KPI Dashboard (Stats Reset: Manual / Last Refresh:01/19/2016 22:54:51) Performance: TPS / PDN / Active Subscribers; Alarms: Critical / Major / Minor MRAs selected: 615 / 10 / 10 / 0 / 0 / 8 MPEs selected: 153 / 2598529 / 2598440 / 0 / 0 / 16 njbbs07mra01 — Performance: State / TPS / PDN / Active Subscribers / CPU % / Memory %; Connections: MPE / MRA / Network Elements; Alarms: Critical / Major njbbs07mra01(Server-A): Active / 615 (1%) / 10 / 10 (0%) / 3 / 10 / 5 of 4 / 2 of 2 / 1 of 2 / 0 / 0 njbbs07mra01(Server-B): Standby / 2 / 10 njbbs07mra01(Server-C): Spare / 11 / 11 MPE: State / TPS / PDN / Active Sessions / CPU % / Memory % / MRA / Data Sources / Critical / Major njbbs07mpe01(Server-A): Active / 53 (0%) / 413839 / 413787 (2%) / 19 / 14 / 2 of 2 / 0 of 1 / 0 / 0 njbbs07mpe01(Server-B): Standby / 3 / 14 njbbs07mpe01(Server-C): Spare / 5 / 14 njbbs07mpe02(Server-A): Active / 100 (1%) / 2184690 / 2184653 (14%) / 5 / 15 / 2 of 2 / 1 of 1 / 0 / 0 njbbs07mpe02(Server-B): Standby / 3 / 14 njbbs07mpe02(Server-C): Spare / 3 / 14 Verify that report shows all normal traffic processing for the MPEs/MRAs.
10. ☐	**CMP GUI:** Verify System Administration Reports	Navigate to **System Administration → Reports**.  Manager Reports Stats Reset: Manual CMP Site1 Cluster (P) Mode: Active Reset All Counters / Pause Cluster: Manager Cluster Status On-line Blades Overall: State / Blade Failures / Uptime; Utilization: Disk / CPU / Memory; Actions 10.240.232.71 (Server-A): Standby / 12 / 19 hours 39 mins 17 secs / 1.15 % / 1 % / 5 % / Restart / Reboot 10.240.232.72 (Server-B): Active / 12 / 21 hours 1 min 45 secs / 0.91 % / 2 % / 9 % / Restart / Reboot
11. ☐	**CMP GUI:** Verify Advanced settings on the MPE and MRA.	Compare the current advanced settings on the MRA and MPE with the captured screenshots saved prior to upgrading the CMP cluster.
12. ☐		• All CMP clusters Upgrade are complete and running Release 12.3.x. • ALL MRAs and MPEs are on Release 12.1.x • At this point, the OCPM system is running in mixed-version mode.
---End of Procedure---		

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

Use this procedure to upgrade the Site1 CMP cluster, and if needed, upgrade the Site2 CMP cluster in a single maintenance window.

6.1 Upgrade CMP clusters Overview

1. Upgrade Primary CMP cluster
2. Start upgrade
3. Failover
4. Log back into the CMP GUI
5. Continue upgrade
6. Upgrade Secondary CMP cluster
7. Start upgrade
8. Failover
9. 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 georedundant 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 Management 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 CMP sites to be upgraded, and verify which site is the Primary site and which site is the Secondary site:

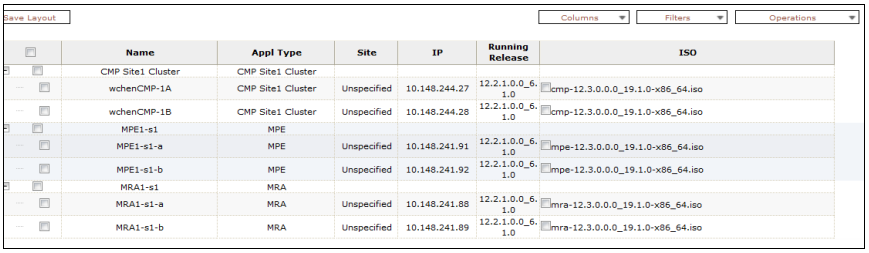
CMP Sites	Operator Site Name	Topology Site Designation (Site1 or Site2)	CMP Server-A	CMP Server-B
Primary Site			Server-A Hostname _____ Server-A IP Address _____ Server-A HA Status _____	Server-B Hostname _____ Server-B IP Address _____ Server-B HA Status _____
Secondary Site			Server-A Hostname _____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

IMPORTANT:

Site1 CMP MUST be upgraded to the new release before the Site2 CMP

CMP servers MUST be upgraded before the non-CMP clusters

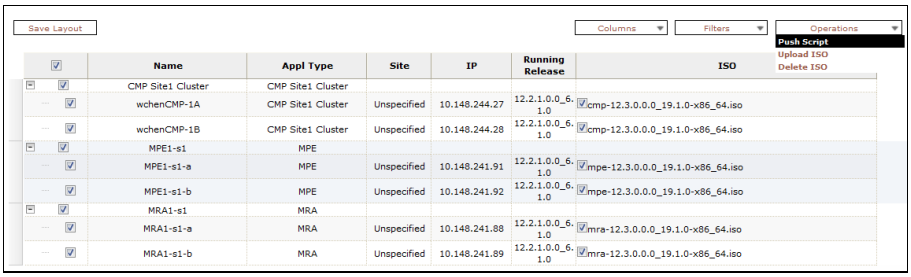
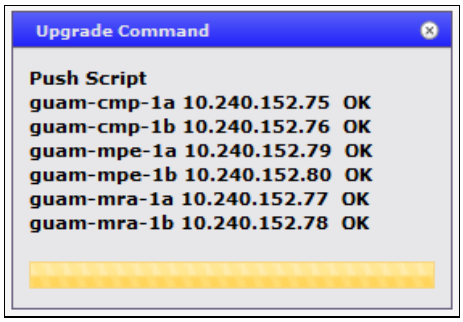
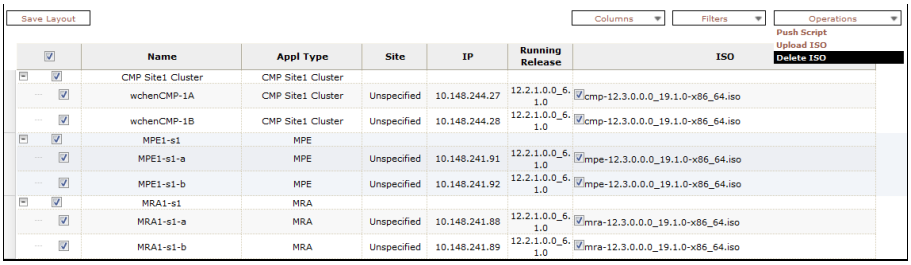
6.2 Upgrade Primary CMP cluster

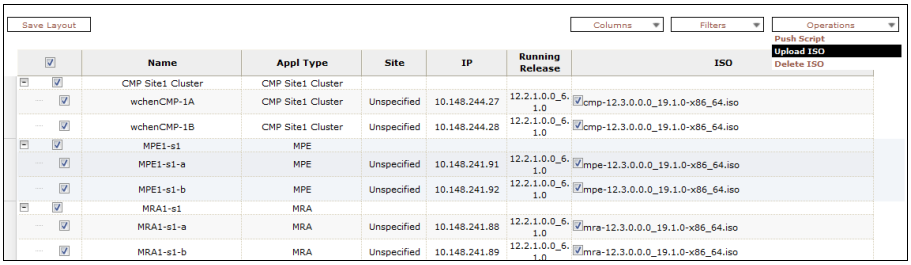
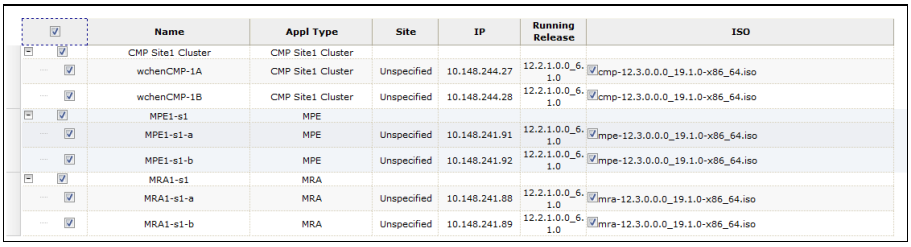
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **System Wide Reports → Alarms→Active Alarms**. 2. Confirm that any existing alarm is understood and is not an impact to the upgrade procedure. 3. Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and record the CMP cluster(s)	1. Navigate to **Platform Setting→Topology Settings → All Clusters**. **Cluster Settings** Name | Appl Type | Site Preference | OAM VIP | Server-A | Server-B | Server-C | Operation CMP Site1 Cluster (P) | CMP Site1 Cluster | N/A | 10.240.152.88/26 | 10.240.152.75 | 10.240.152.76 | N/A | View Demote CMP Site2 Cluster (S) | CMP Site2 Cluster | N/A | 10.240.152.89/26 | 10.240.152.98 | 10.240.152.99 | N/A | View Delete guam-mpe-1 | MPE | Normal | N/A (P) N/A (S) | 10.240.152.79 | 10.240.152.80 | 10.240.152.101 | View Delete guam-mra-1 | MRA | Normal | N/A (P) N/A (S) | 10.240.152.77 | 10.240.152.78 | 10.240.152.100 | View Delete 2. Note which cluster is the primary and which cluster 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 the status of the CMP clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm the CMP clusters have the following: - Active/Standby status - Running release 12.2.x 3. Navigate to **Upgrade → ISO Maintenance**. Release 12.3 ISO files copied to at least one of each server types (CMP/MRA/MPE)—Meaning, a copy of the MPE ISO file is on one of the MPE servers, an MRA ISO file is on one of the MRA servers and a copy of the CMP ISO file is on one CMP server

Step	Procedure	Result
4. ☐	**SSH CLI Primary Active CMP:** Exchange Keys	1. Exchange keys to all servers from the Site1 (Primary) Active CMP. Login as admusr and run the following command: `$sudo qpSSHKeyProv.pl --prov` 2. Enter the password for admusr. 3. Ensure that the keys are exchanged successfully with all the server clusters:

```
[admusr@guam-cmp-1a ~]$ sudo qpSSHKeyProv.pl -prov

The password of admusr in topology:
```

```
Connecting to admusr@guam-cmp-1a ...
Connecting to admusr@guam-mpe-1b ...
Connecting to admusr@guam-mra-1b ...
Connecting to admusr@guam-mpe-1a ...
Connecting to admusr@guam-cmp-1b ...
Connecting to admusr@guam-mra-1a ...

[1/6] Provisioning SSH keys on guam-cmp-1a ...

[2/6] Provisioning SSH keys on guam-mra-1b ...

[3/6] Provisioning SSH keys on guam-mpe-1b ...

[4/6] Provisioning SSH keys on guam-mpe-1a ...

[5/6] Provisioning SSH keys on guam-cmp-1b ...

[6/6] Provisioning SSH keys on guam-mra-1a ...


SSH keys are OK.
```

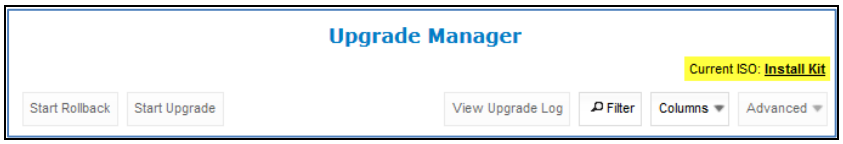
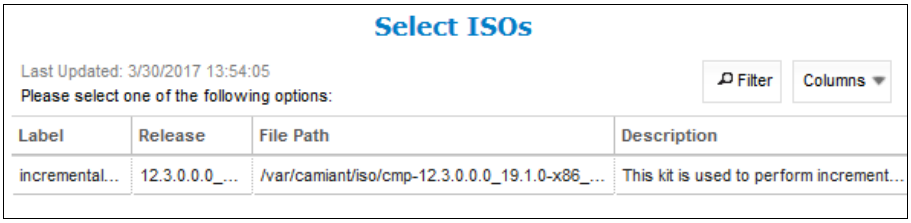
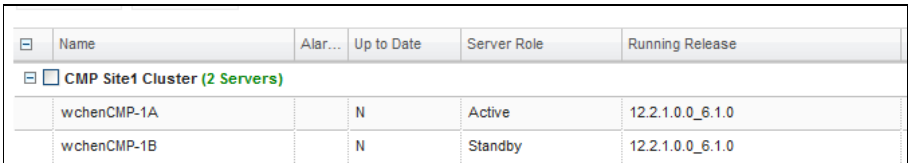
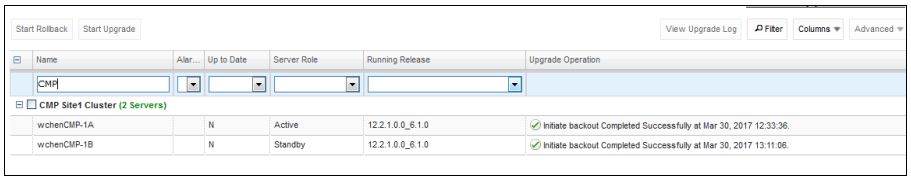
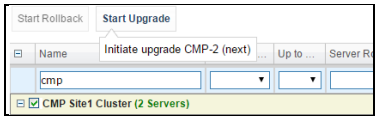
Step	Procedure	Result
5. ☐	**CMP GUI:** Push the Release 12.3 upgrade scripts to all servers	1. Navigate to **Upgrade → ISO Maintenance**. 2. Select all the servers in the topology as shown. 3. Select **Operations → Push Script** operation.  4. On the warning dialog, click **OK** to continue the operation. After a minute or so, a successful popup window similar to this should appear: 
6. ☐	**CMP GUI:** Access into Primary CMP Server—Remove old ISO files from servers.	1. Navigate to **Upgrade → ISO Maintenance**. 2. Select the servers that show old ISO files. 3. Select the server cluster. 4. Select **Operations → Delete ISO** to remove any older ISO files.  5. Click **OK** to continue and wait until seeing the successful deletion message 6. Wait until the ISO Maintenance page is refreshed and the ISO column does not show any old ISOs.

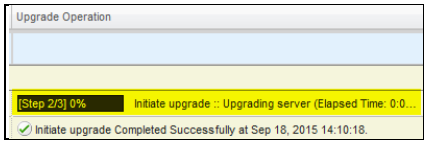
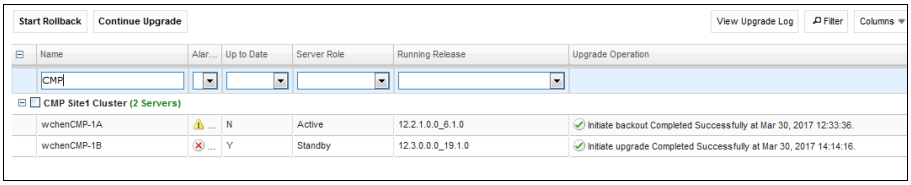
Step	Procedure	Result
7. ☐	**CMP GUI:** Distribute ISO files to CMP/MPE/MRA/ Mediation, servers NOTE: This step depends on the ISO file type. Distribute ISO files accordingly.	1. Navigate to **Upgrade → ISO Maintenance**. 2. Filter by server type (optional, but preferred step) 3. One application at a time, select one server type (CMP, MPE, etc.) to be upgraded. **NOTE:** The ISO files for each application type must be copied over to at least one server. See Distribute Application ISO Image Files to Servers. 4. Select **Operations → Upload ISO**.  5. 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/` <*server_type_iso_filename*> 6. Click **Add**. When completed, the ISO column is populated with the ISO filename and a notification of [100%] 7. Repeat for all cluster types.
8. ☐	**CMP GUI:** Verify ISO distribution to all the server	1. Navigate to **Upgrade → ISO Maintenance**. 2. Verify that the release 12.3 ISO file of the correct type is shown for each server. 3. When completed, the ISO column is populated with the ISO filename 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. 

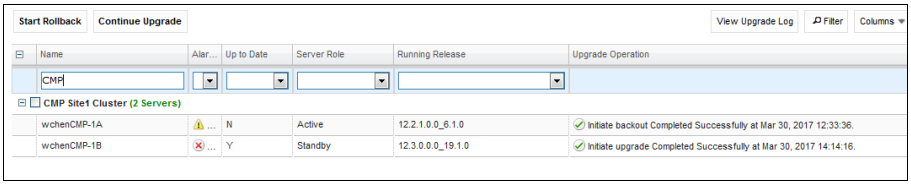
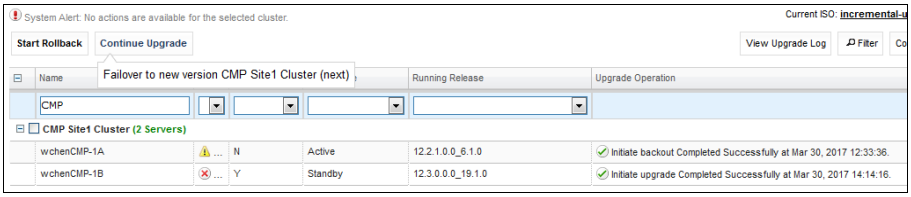
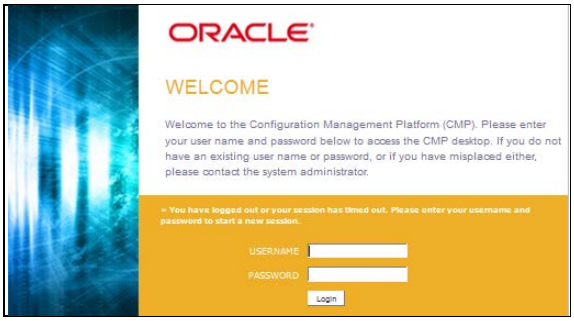
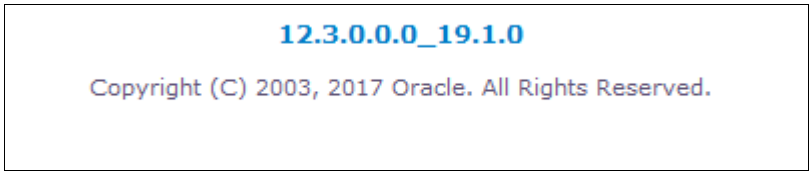
Name	Appl Type	Site	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster				
wchenCMP-1A	CMP Site1 Cluster	Unspecified	10.148.244.27	12.2.1.0.0_6.1.0	cmp-12.3.0.0.0_19.1.0-x86_64.iso
wchenCMP-1B	CMP Site1 Cluster	Unspecified	10.148.244.28	12.2.1.0.0_6.1.0	cmp-12.3.0.0.0_19.1.0-x86_64.iso
MPE1-s1	MPE				
MPE1-s1-a	MPE	Unspecified	10.148.241.91	12.2.1.0.0_6.1.0	mpe-12.3.0.0.0_19.1.0-x86_64.iso
MPE1-s1-b	MPE	Unspecified	10.148.241.92	12.2.1.0.0_6.1.0	mpe-12.3.0.0.0_19.1.0-x86_64.iso
MRA1-s1	MRA				
MRA1-s1-a	MRA	Unspecified	10.148.241.88	12.2.1.0.0_6.1.0	mra-12.3.0.0.0_19.1.0-x86_64.iso
MRA1-s1-b	MRA	Unspecified	10.148.241.89	12.2.1.0.0_6.1.0	mra-12.3.0.0.0_19.1.0-x86_64.iso

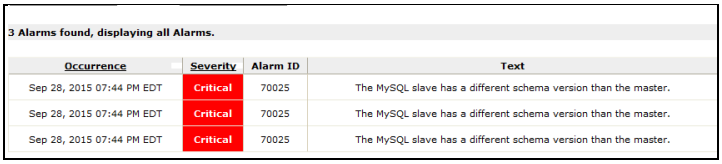
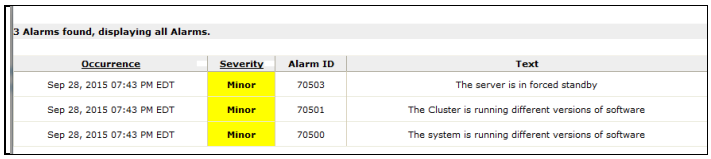
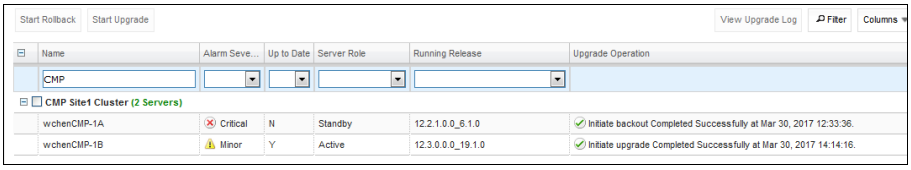
Step	Procedure	Result

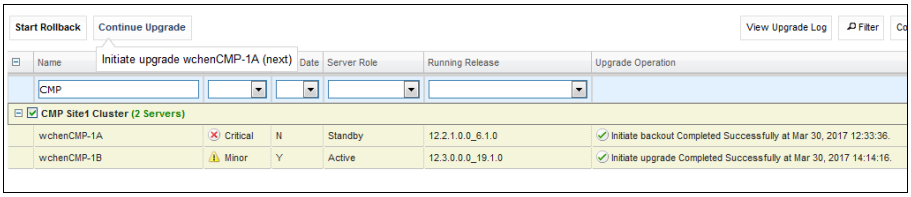
9. ☐	**Primary Active CMP:** SSH to primary active CMP and copy ISO file to `/var/camiant/iso` directory	1. Logon to the primary active CMP as admusr and copy the 12.3 ISO file to the `/var/camiant/iso` directory:
		`$sudo cp /var/TKLC/upgrade/cmp-12.3.x…x.iso /var/camiant/iso/`
		2. Verify the copy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

10. ☐	**CMP GUI:** Locate the new 12.3 upgrade manual	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the **Current ISO**. In this case it is labeled Install Kit.  A dialog box with a description of the ISO file that was copied into the `/var/camiant/iso` directory opens. 3. Highlight the ISO file and click **Select incremental-upgrade-12.2…** located in the bottom right-hand corner of the window.  4. When the confirmations message displays, click **OK**. Within a few seconds, the Up to Date column changes from Y (meaning up-to-date) or N (meaning needs upgrade). 
11. ☐	**CMP GUI:** Upgrade Primary CMP cluster **NOTE:** This takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. **NOTE:** Click **Filter** and enter `CMP` in the Name field to show the CMP servers only.  2. Select the Primary CMP Server cluster 3. Click **Start Upgrade**. 

Step	Procedure	Result
		4. Click **OK** to confirm and continue with the operation. This continues to upgrade the standby server only in the CMP cluster The Upgrade Operation column shows a progress bar along with the upgrade activities.  Upgrade Operation column indicates to completed when done. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** **31283** Lost Communication with server **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 standby server of the CMP cluster when the Initiate upgrade Completed successfully at… message displays in the Upgrade Operation column. 

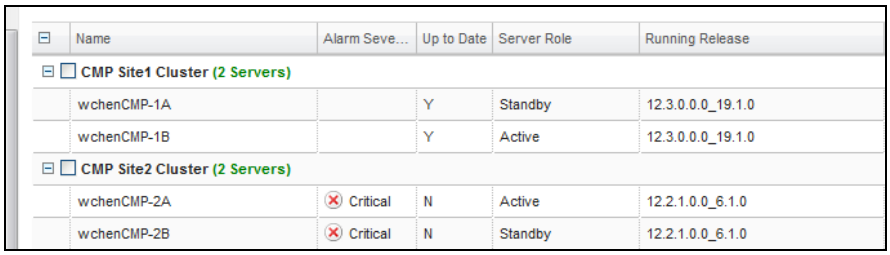
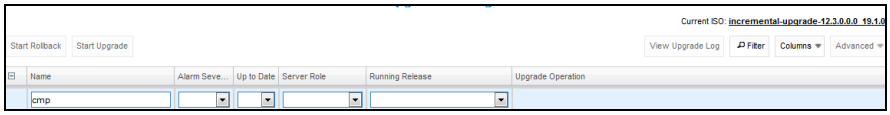
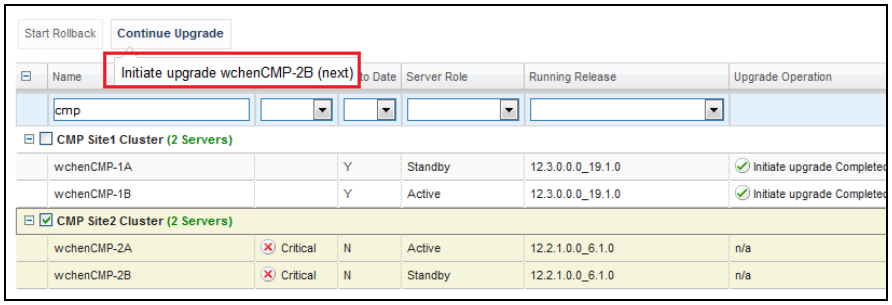
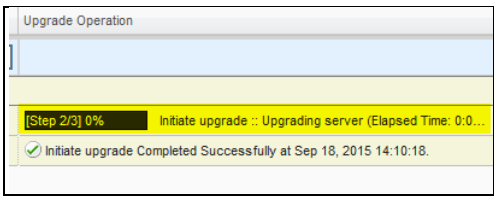
Step	Procedure	Result
12. ☐	**CMP GUI:** Verify that the upgrade is successful	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the cluster. 3. Verify the following information: - The standby server is on 12.3 - The other server in the cluster is on 12.2.x - The Up to Date column shows Y for the 12.3 server and N for the 12.2 server. 
13. ☐	**CMP GUI:** Continue to upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster. 3. Click **Continue Upgrad**e. Notice the Failover to new version CMP Site1 Cluster message.  4. Click **OK** to confirm and continue with the operation. The specific action takes a minute to complete.
14. ☐	**CMP GUI:** Login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management release 12.3 CMP GUI login page opens as shown—login and password credentials are the same as the pre-upgrade. 
15. ☐	**CMP GUI:** Verify new Policy Management release	Navigate to **Help→About**. Verify the release displayed is 12.3. 

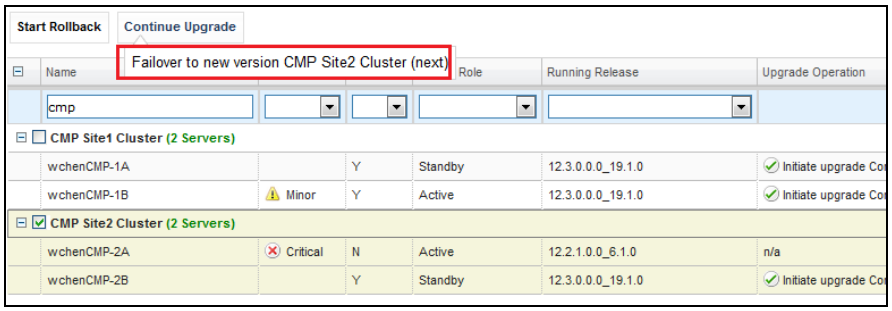
Step	Procedure	Result
16. ☐	**CMP GUI:** Critical alarms	Critical alarm 70025, QP Slave database is a different version than the master, is seen until the SQL Database matches the master (12.3). This alarm is expected and remains until all CMP servers are upgraded to the same version. **Current Critical Alarms** **70025** QP Slave database is a different version than the master:  3 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. **Current Minor Alarms** **70503** Server Forced Standby **70500** System Mixed Version **70501** Cluster Mixed Version  3 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text Sep 28, 2015 07:43 PM EDT | Minor | 70503 | The server is in forced standby Sep 28, 2015 07:43 PM EDT | Minor | 70501 | The Cluster is running different versions of software Sep 28, 2015 07:43 PM EDT | Minor | 70500 | The system is running different versions of software **NOTE:** The Upgrade Manager shows alarms as well.
17. ☐	**CMP GUI:** Verify the Policy Management release 12.3 CMP is Active	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify the following - Active server is running release12.3 - Standby server is on the previous release  Start Rollback | Start Upgrade | View Upgrade Log | Filter | Columns Name | Alarm Seve... | Up to Date | Server Role | Running Release | Upgrade Operation CMP CMP Site1 Cluster (2 Servers) wchenCMP-1A | Critical | N | Standby | 12.2.1.0.0_6.1.0 | Initiate backout Completed Successfully at Mar 30, 2017 12:33:36. wchenCMP-1B | Minor | Y | Active | 12.3.0.0.0_19.1.0 | Initiate upgrade Completed Successfully at Mar 30, 2017 14:14:16.

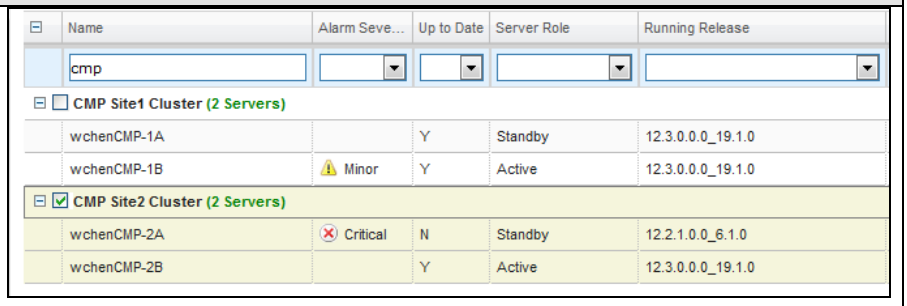
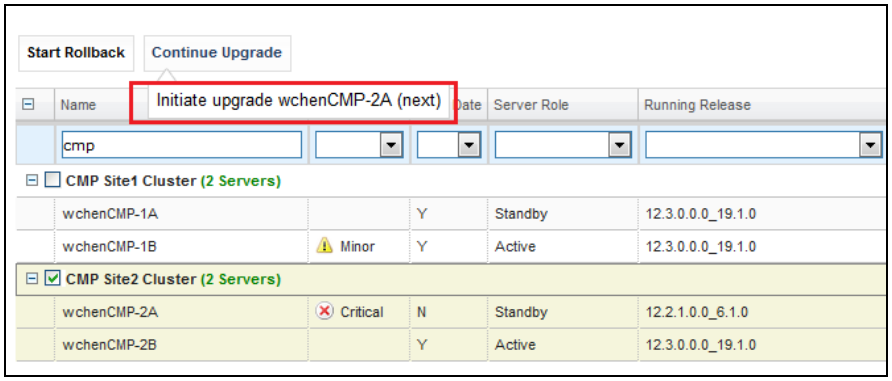
Step	Procedure	Result
18. ☐	**CMP GUI:** Complete the upgrade of the Primary CMP cluster **NOTE:** Remaining CMP server takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster 3. Click **Continue Upgrade**. Notice the Initiate upgrade <*standbyserver*> (next) message when hovering over the button.  4. Click **OK** to continue the upgrade on the remaining server in the CMP cluster **NOTE:** The server that is being upgraded goes into an OOS state. **Expected Critical Alarms** **31227** HA availability status failed **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** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault

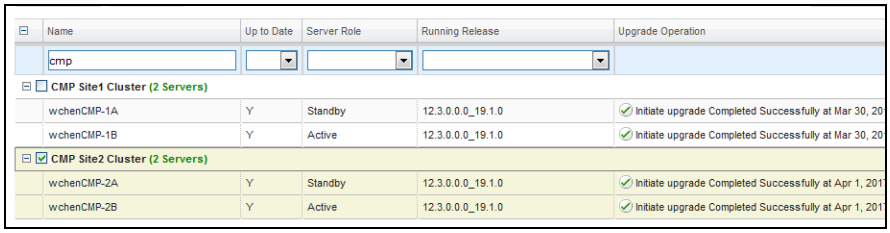
Step	Procedure	Result
19. ☐	**CMP GUI:** Tracking the upgrade complete	Navigate to **Upgrade → Upgrade Manager**. The last step of the upgrade for the first CMP cluster is to wait for replication to complete. With the CMP cluster selected, click **View Upgrade Log** to open a window where you can verify that synchronization has taken place: **Upgrade Log** Cluster Name: CMP Site1 Cluster Last Update: 11/10/2016 9:01:00 ID | Parent ID | Action Name | Duration | Scope | Hostname | Result | Mode 1 | 0 | Preflight Check | 0:00:15 | Server | guam-cmp-1b | Success | Manual 2 | 1 | Upgrading server | 0:22:00 | Server | guam-cmp-1b | Success | Automatic 3 | 1 | Modify the role/replication attributes of the server | 0:00:01 | Cluster | CMP Site1 Cluster | Success | Automatic 4 | 1 | Wait for replication to synchronize | 0:00:09 | Server | guam-cmp-1b | Success | Automatic 5 | 0 | Failover to new version | 0:00:00 | Cluster | CMP Site1 Cluster | Success | Manual 6 | 0 | Preflight Check | 0:00:15 | Server | guam-cmp-1a | Success | Manual 7 | 6 | Upgrading server | 0:21:50 | Server | guam-cmp-1a | Success | Automatic 8 | 6 | Modify the role/replication attributes of the server | 0:00:01 | Cluster | CMP Site1 Cluster | Success | Automatic 9 | 6 | Wait for replication to synchronize | 0:00:29 | Server | guam-cmp-1a | Success | Automatic 10 | 6 | Modify the role/replication attributes of the server | 0:00:01 | Cluster | CMP Site1 Cluster | Success | Automatic
20. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**. Name | Alarm Seve... | Up to Date | Server Role | Running Release | Upgrade Operation CMP Site1 Cluster (2 Servers) wchenCMP-1A | | Y | Standby | 12.3.0.0.0_19.1.0 | Initiate upgrade Completed Successfully at Mar 30, 2017 14:43:54. wchenCMP-1B | Minor | Y | Active | 12.3.0.0.0_19.1.0 | Initiate upgrade Completed Successfully at Mar 30, 2017 14:14:16. Successful upgrade status shows the following for both servers in the Primary CMP cluster: • 12.3 in the Running Release column for both servers • A Y in the Up to Date column • Active or Standby state for both servers in the Primary CMP cluster.
21. ☐	Proceed to next upgrade procedure	Verify the following information: • Primary Site1 is running release 12.3 • Secondary Site is on release 12.2.x • Proceed to the next procedure to upgrade the secondary CMP cluster.
---End of Procedure---		

6.3 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 **NOTE:** This takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. **NOTE:** Click **Filter** and enter CMP in the Name field to see only the CMP servers.  2. Select the Secondary CMP Server cluster at Site2 3. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade <*site2_standbyserver*> (next).  4. Click **OK** to confirm and continue with the operation. This continues to upgrade the standby server only in the CMP cluster The Upgrade Operation column shows a progress bar along with the upgrade activities.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events:

Step	Procedure	Result
		Expected Critical alarm **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** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault Upgrade is complete on the standby server of the Site2 CMP cluster when the Initiate upgrade Completed successfully at… message displays in the Upgrade Operation column. 
3. ☐	**CMP GUI:** Failover of the 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 CMP Site2 Cluster message  4. Click **OK** to confirm and continue with the operation. The failover takes about a minute to complete. Wait until the upgraded server is active, running 12.2 as shown below.

Step	Procedure	Result
		
4. ☐	**CMP GUI:** Continue upgrade of the Secondary CMP cluster	1. Select the Secondary CMP Server cluster at Site2 2. Click **Continue Upgrade**. When hovering over the button, the message displays the next action, which is upgrading the remaining CMP in standby, still running 12.2.x.  3. 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 alarm** **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** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault

Step	Procedure	Result
5. ☐	**CMP GUI:** Verify that the upgrade completed successfully.	Navigate to **Upgrade → Upgrade Manager**. Successful upgrade status shows release 12.3 in the Running Release column and the Upgrade Operation. The Upgrade Operation column shows: • Initiate Upgrade Completed Successfully at.. message • the correct date and time. 
6. ☐	**CMP GUI:** Verify alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarms** **70500** System Mixed Version
7. ☐	Procedure is complete.	Verify the following information: • All CMP clusters upgrades are complete and running release 12.3 • All MRA and MPE clusters are running release 12.2.x The Policy Management system is running in mixed-version mode.
---End of Procedure---		

7. UPGRADE NON-CMP CLUSTERS (MPE, MRA, MEDIATION)

The following procedures upgrades a site/segment containing one or more MPE, MRA, Mediation clusters.

NOTE: Different cluster types can be upgraded at the same time. For example, 2 MPEs and 2 MRAs can be upgraded in parallel.

7.1 Upgrade Preparation

Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	Use the supported browser to login as the admin user or as a user with administrative privileges.
2. ☐	**CMP GUI:** Verify current Upgrade Manager status and software release 12.3 ISO files	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that all CMP clusters have both Active, Standby status. 3. Verify that all MPE and MRA clusters have an Active, Standby, and Spare server. 4. Verify that Policy Management release 12.3 ISO files are available for all MPE, and MRA clusters. One ISO per server 5. Verify that the CMP cluster is upgraded successfully and running Policy Management release 12.3
---End of Procedure---		

7.2 Upgrade MRA and MPE Servers

Use this procedure to upgrade one or more clusters (MPE and/or MRA).

This procedure is applicable for a 12.1.x or 12.2.x upgrade to 12.3.

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

The upgrade procedure is essentially the same for an MRA cluster and an MPE cluster.

Select and start upgrade on the standby server

Failover

Re-apply configuration

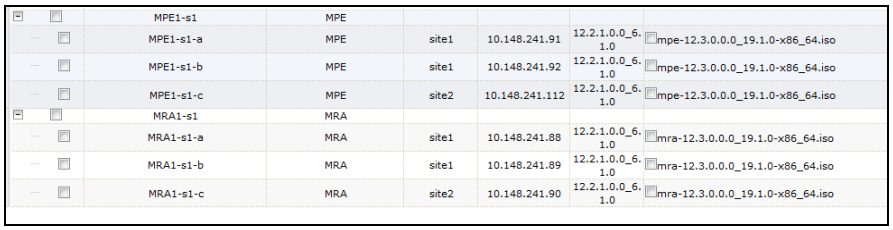
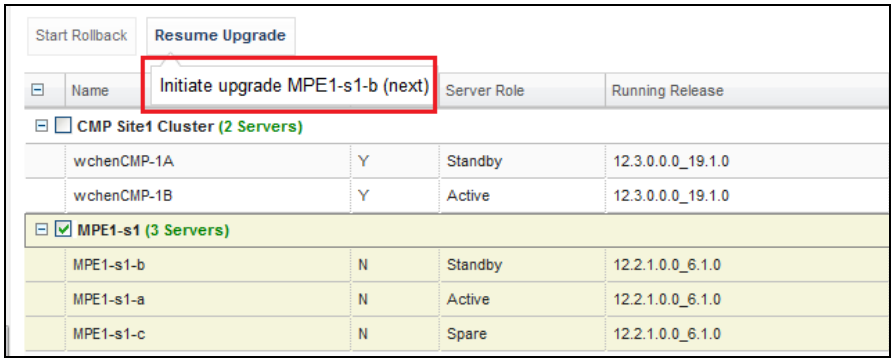
Continue to upgrade the spare server

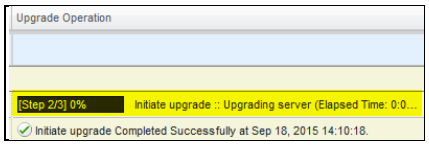
Continue upgrade on remaining server

(MPE only) Re-apply configuration one MPE cluster at a time

NOTES:

- All CMP clusters must be upgraded to Policy Management release 12.3 prior to performing the following procedures.
- Four (4) clusters (8 for 12.1.x) can be running the upgrade at one time.
- 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 MPE/MRA servers to be upgraded	Perform the following: 1. Check for current active alarms 2. Reset MPE/MRA counters to make a baseline - For the MPE: **Policy Server → Configuration →** <*server_name*> **→ Reports → Reset Counters** - For the MRA: **MRA → Configuration →** <*server_name*> **→ Reports → Reset Counters** 3. Go to the KPI Dashboard and capture a screenshot. **System Wide Reports → KPI Dashboard**
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify information for the MRA/MPE servers: - Current release 12.1.x, or 12.2.x installed - Active/Standby/Spare status - ISO version to be deployed is 12.3 (verify the current ISO files are 12.3 by going to **Upgrade → ISO Maintenance**)  MPE1-s1 MPE MPE1-s1-a MPE site1 10.148.241.91 12.2.1.0.0_6.1.0 mpe-12.3.0.0.0_19.1.0-x86_64.iso MPE1-s1-b MPE site1 10.148.241.92 12.2.1.0.0_6.1.0 mpe-12.3.0.0.0_19.1.0-x86_64.iso MPE1-s1-c MPE site2 10.148.241.112 12.2.1.0.0_6.1.0 mpe-12.3.0.0.0_19.1.0-x86_64.iso MRA1-s1 MRA MRA1-s1-a MRA site1 10.148.241.88 12.2.1.0.0_6.1.0 mra-12.3.0.0.0_19.1.0-x86_64.iso MRA1-s1-b MRA site1 10.148.241.89 12.2.1.0.0_6.1.0 mra-12.3.0.0.0_19.1.0-x86_64.iso MRA1-s1-c MRA site2 10.148.241.90 12.2.1.0.0_6.1.0 mra-12.3.0.0.0_19.1.0-x86_64.iso
3. ☐	**CMP GUI:** Upgrade clusters **NOTE:** The upgrade of a single server takes approximately 40 minutes to complete.	**NOTE:** Start the upgrade on ONE cluster. Wait until the cluster shows OOS, and then continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running upgrade at any time. 3. Navigate to **Upgrade → Upgrade Manager**. 4. Select the cluster to be upgraded, it can be an MRA or MPE 5. Click **Continue Upgrade**.  Start Rollback Resume Upgrade Initiate upgrade MPE1-s1-b (next) Name Server Role Running Release CMP Site1 Cluster (2 Servers) wchenCMP-1A Y Standby 12.3.0.0.0_19.1.0 wchenCMP-1B Y Active 12.3.0.0.0_19.1.0 MPE1-s1 (3 Servers) MPE1-s1-b N Standby 12.2.1.0.0_6.1.0 MPE1-s1-a N Active 12.2.1.0.0_6.1.0 MPE1-s1-c N Spare 12.2.1.0.0_6.1.0 6. Click **OK** to confirm and continue with the operation. It begins to upgrade the standby server of that cluster. Wait until the cluster reports OOS before selecting the next cluster

Step	Procedure	Result
		Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **70001** QP_procmgr failed **31227** HA availability status failed **Expected Major Alarm** **31233** High availability path loss of connectivity **70004** QP Processes down for maintenance Severity / Alarm ID / Text Major / 31233 / High availability path loss of connectivity Severity / Alarm ID / Text Major / 70004 / The QP processes have been brought down for maintenance. **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault **78001** Rsync Failed Severity / Alarm ID / Text Minor / 31107 / DB merging from a child Source Node has failed Minor / 31107 / DB merging from a child Source Node has failed Minor / 31107 / DB merging from a child Source Node has failed Minor / 31107 / DB merging from a child Source Node has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 31114 / DB Replication of configuration data via SOAP has failed Minor / 70501 / The Cluster is running different versions of software Minor / 70503 / The server is in forced standby Minor / 70507 / An upgrade/backout action on a server is in progress

Step	Procedure	Result

Severity	Alarm ID	Text
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31101	DB replication to a slave DB has failed

Upgrade is complete on the first server in the cluster when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to Standby state when the upgrade completes.

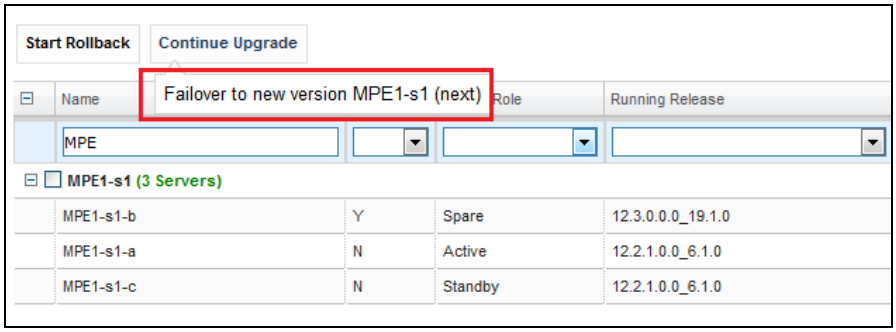
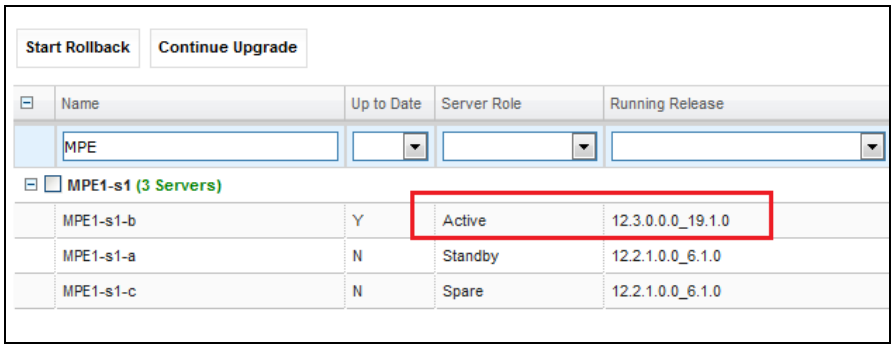
MPE1-s1 (3 Servers)			
MPE1-s1-b	Y	Spare	12.3.0.0.0_19.1.0
MPE1-s1-a	N	Active	12.2.1.0.0_6.1.0
MPE1-s1-c	N	Standby	12.2.1.0.0_6.1.0

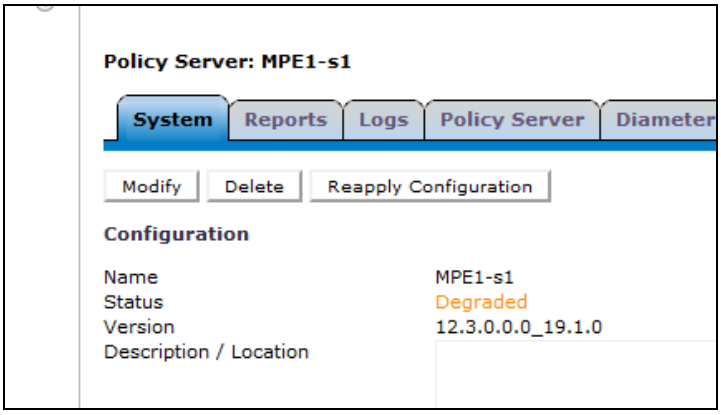
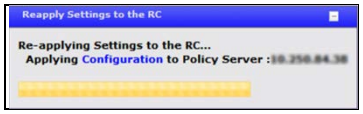
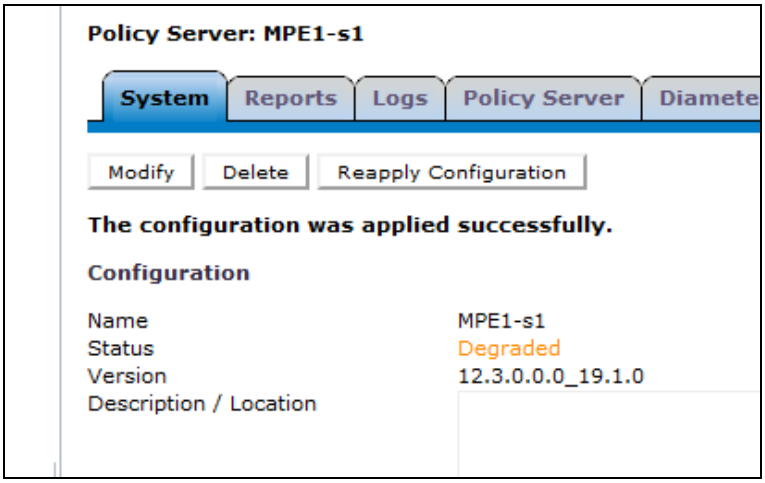
During the upgrade activities, the following alarms may be generated and are considered normal reporting events.

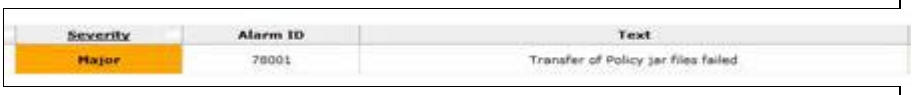
Alarm 31224—HA configuration error (major) is raised noting that there is a configuration error. This clears a few minutes after the upgrade completes on the first server. The following minor alarms may be present:

Expected Minor Alarms

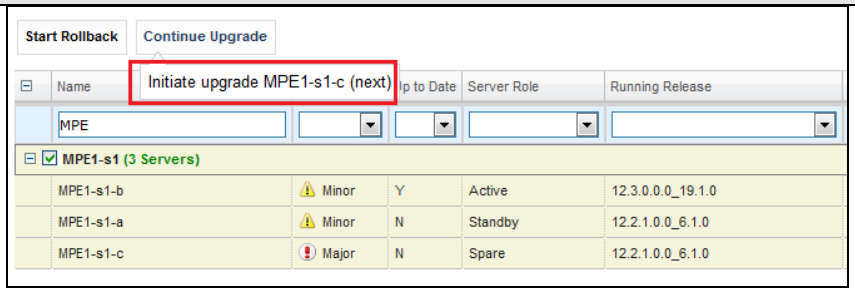
78001 Rsync Failed
70500 System Mixed Version
70501 Cluster Mixed Version
70503 Server Forced Standby

Step	Procedure	Result
4. ☐	**CMP GUI:** Continue to upgrade the 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.	Fail over ONE cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster being upgraded (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 starts to failover the cluster. Wait until failover completes before failing over the next cluster, This takes a minute or two to complete. Verify the 12.3 server is now active. The process is complete when there is an active/standby at site 1 and spare at site 2. 

Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the upgrade successfully.	• For MPE: **PolicyServer → Configuration →** <*mpe_cluster name*> **→ System** • For MRA: **MRA → Configuration →** <*mra_cluster name*> **→ System** The selected cluster shows status Degraded as it has different releases for the Active and Standby servers. It may display Config mismatch as well. This is expected. 1. Click **Reapply Configuration**.  **NOTE:** A progress bar displays for the MPE reapply configuration only. The MRA reapply configuration does not display the progress bar.  2. Note the version is successfully changed to the upgraded release 12.3. **NOTE:** The status shows Degraded because the servers are still in different releases. 

Step	Procedure	Result
6. ☐	**CMP GUI:** Current alarms	During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** None **Expected Major Alarm** **78001** Rsync Failed  **Expected Minor Alarms** **70503** Server Forced Standby **70502** Cluster Replication Inhibited **70500** System Mixed Version **70501** Cluster Mixed Version **71402** Connectivity Lost **31101** Database replication to slave failure
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	1. Navigate to Upgrade Manager → System Maintenance. - If traffic is active, go to step 9. - If traffic does not become active within 90 seconds: 2. Select the Partially upgraded cluster, and select **Operations → Rollback**. The pre-12.2 MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	• For MPE: **Policy Server → Configuration → <***mpe_cluster name***> → System** • For MRA: **MRA → Configuration → <***mra_cluster name***> → System** 1. Click Reapply Configuration 2. 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.
9. ☐	**CMP GUI:** Continue upgrade of the MRA/MPE clusters. Next operation is initiate upgrade on the Spare server	Continue the upgrade on ONE cluster, when the server goes into OOS, continue with the next cluster and so on. **NOTE:** Up to 4 clusters (8 for 12.1.x) can be running the upgrade process at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for a cluster. - Select one cluster at a time - Can be an either an MRA or MPE cluster 3. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade… on the spare server

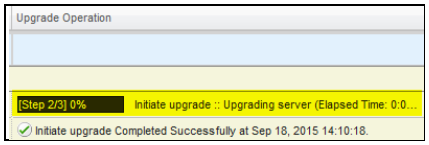
Step	Procedure	Result



4. Click **OK** to confirm and continue with the operation.

Wait until the cluster reports OOS before selecting the next cluster

Follow the progress in the Upgrade Operation column.



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

Expected Critical Alarms

31283 HA Server Offline / Lost Communication with server
31227 HA availability status failed
70001 QP_procmgr failed

Expected Major Alarm

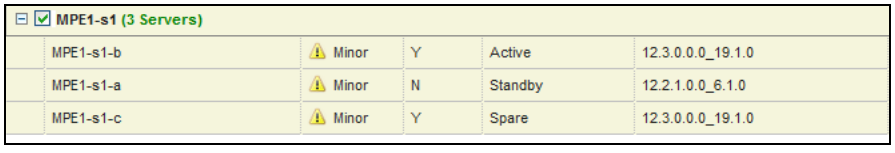
70004 QP Processes down for maintenance

Expected Minor Alarms

70503 Server Forced Standby
70507 Upgrade In Progress
70500 System Mixed Version
70501 Cluster Mixed Version
70502 Cluster Replication Inhibited

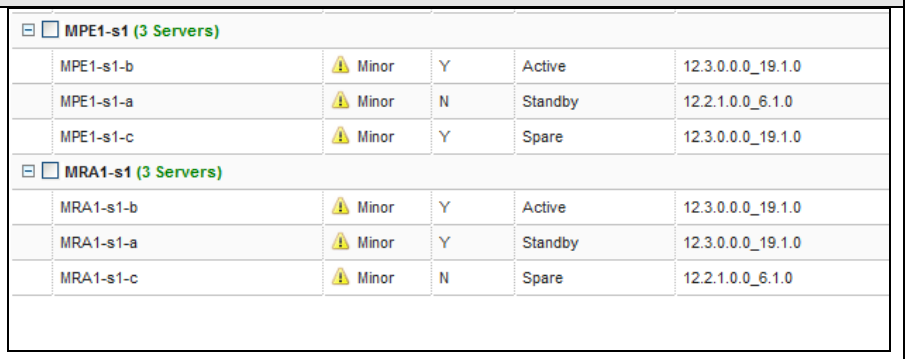
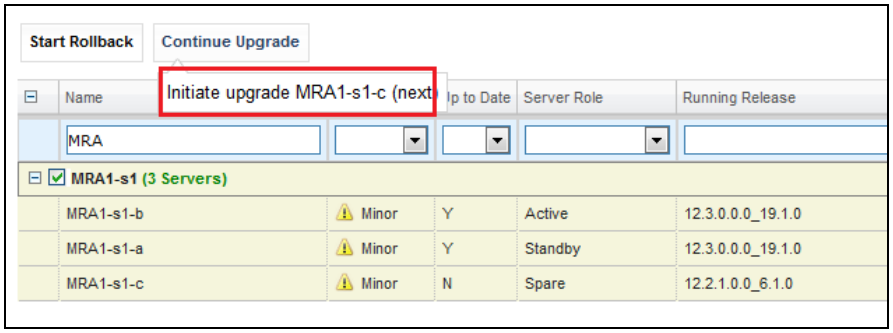
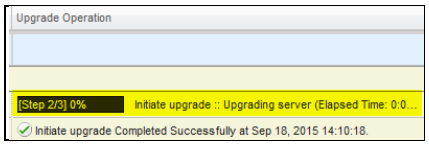
Upgrade is complete on the spare server in the georedundant cluster when:

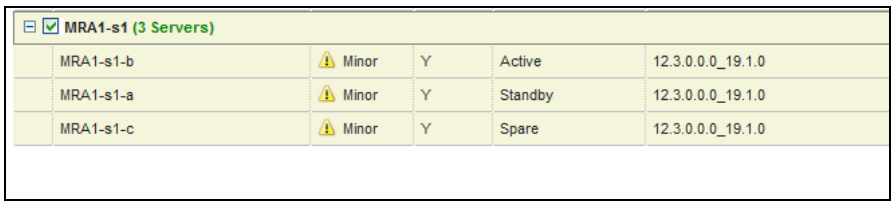
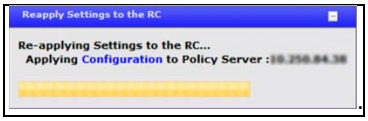
- The Initiate upgrade Completed Successfully… message shows in the Upgrade Operation column.

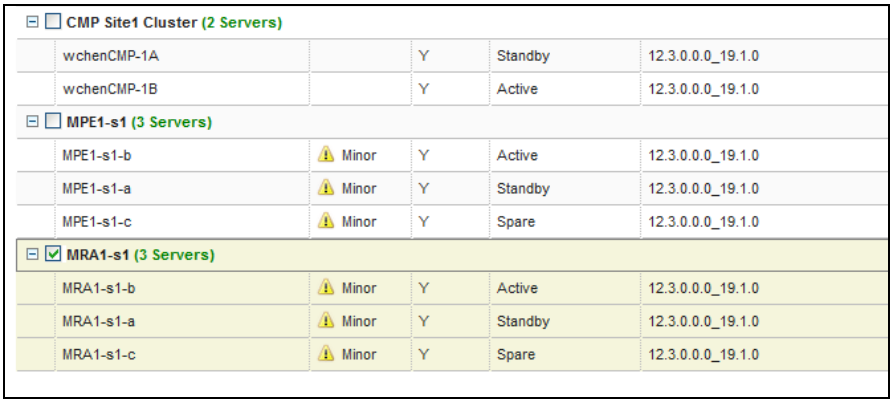


- The server goes back to the Spare state.
- The Up to Date column shows a Y (YES).

The Active and Spare servers are on release 12.3 and the current Standby is on the previous release

Step	Procedure	Result
		
10. ☐	**CMP GUI:** Continue to upgrade the MRA/MPE clusters. Next operation is Initiate upgrade on the standby server	Continue the upgrade on ONE cluster, when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running the upgrade at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for a cluster: - Select one cluster at a time - Can be an either an MRA or MPE cluster 3. Click **Continue Upgrade**. When hovering over the button, the message indicates the next action, which is to initiate the upgrade of the standby server.  4. Click **OK** to confirm and continue with the operation. It begins the final server upgrade of the cluster Wait until the cluster reports OOS before selecting the next cluster Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events—these is cleared after the MPE cluster is completely upgraded. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server

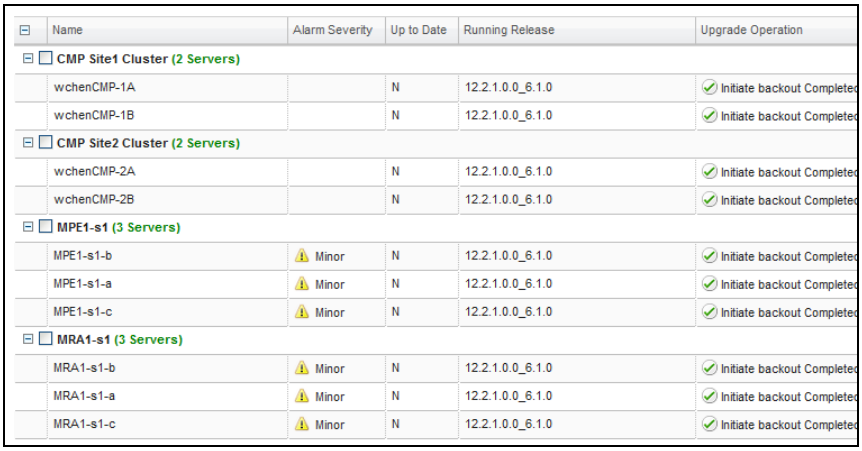
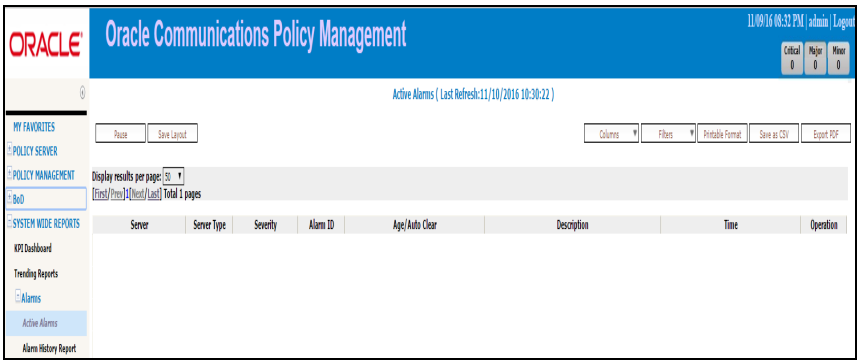
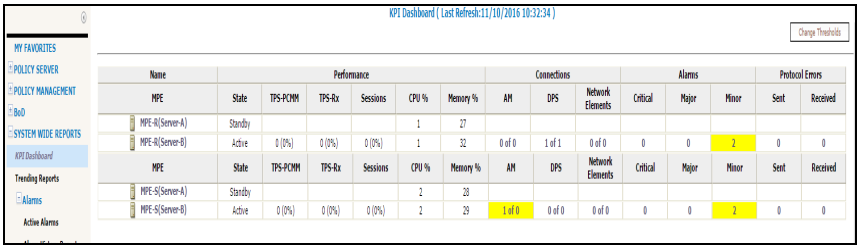
Step	Procedure	Result
		31227 HA availability status failed **70001** QP_procmgr failed **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31102** Database replication from master failure **31113** DB replication manually disabled Upgrade is complete on the third server in the georedundant cluster when: • The completed successfully message shows in the Upgrade Operation column. • The server goes back to the Standby state. • The Up to Date column shows a Y (YES)  MRA1-s1 (3 Servers) MRA1-s1-b Minor Y Active 12.3.0.0.0_19.1.0 MRA1-s1-a Minor Y Standby 12.3.0.0.0_19.1.0 MRA1-s1-c Minor Y Spare 12.3.0.0.0_19.1.0 All servers are now running release 12.3
11. ☐	**CMP GUI: (MPE only)** Reapply configuration on the fully upgraded MPE clusters.	**For MPE only** 1. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** 2. Click **Reapply Configuration**. **NOTE:** A progress bar displays for the MPE reapply configuration.  Reapply Settings to the RC Re-applying Settings to the RC... Applying Configuration to Policy Server :
12. ☐	Repeat steps 1–14 for the next MPE or MRA clusters	Proceed with next cluster(s)

Step	Procedure	Result
13. ☐	Upgrade Completed	At this point all servers have been upgraded. 
---End of Procedure---		

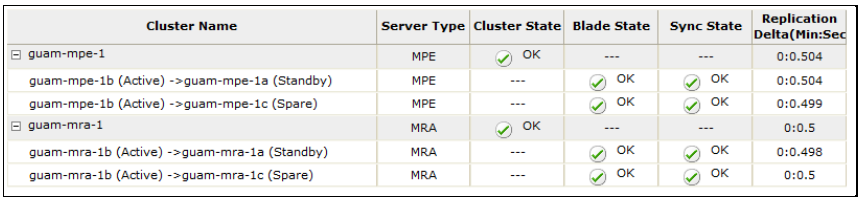
☐ **CMP Site1 Cluster** (2 Servers)				
wchenCMP-1A		Y	Standby	12.3.0.0.0_19.1.0
wchenCMP-1B		Y	Active	12.3.0.0.0_19.1.0
☐ **MPE1-s1** (3 Servers)				
MPE1-s1-b	Minor	Y	Active	12.3.0.0.0_19.1.0
MPE1-s1-a	Minor	Y	Standby	12.3.0.0.0_19.1.0
MPE1-s1-c	Minor	Y	Spare	12.3.0.0.0_19.1.0
☑ **MRA1-s1** (3 Servers)				
MRA1-s1-b	Minor	Y	Active	12.3.0.0.0_19.1.0
MRA1-s1-a	Minor	Y	Standby	12.3.0.0.0_19.1.0
MRA1-s1-c	Minor	Y	Spare	12.3.0.0.0_19.1.0

8. POST UPGRADE HEALTH CHECK FOR WIRELESS SYSTEMS

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 CMP/MRA/MPE clusters.	1. Navigate to **Upgrade → Upgrade Manager**. 2. 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. Make sure everything looks normal. 

<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)

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 colspan="3">---End of Procedure---</td></tr>
</table>

9. BACKOUT (ROLLBACK) 12.1.X/12.2.X WIRELESS MODE

Use this procedure if an issue is found during the upgrade, as well as post-upgrade which impacts network performance.

The Policy Management system is backed out to the previous release.

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

9.1 Backout Sequence

The backout sequence order is the reverse of the upgrade order. The following is the overall backout sequence:

1. Back out the non-CMP clusters (from both Site1 and Site2, if applicable)
2. Back out the Secondary CMP cluster (if applicable)
3. Back out the Primary CMP cluster

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

NOTE: In the case of a non-CMP clusters, the upgrade/backout is NOT complete until the operator performs a Reapply Configuration from the CMP. The MRA/MPE can still operate, but may not be fully functional.

9.2 Pre-requisites

No new policies or features have been configured or run on the upgraded release.

The CMP cluster cannot backout if other non-CMP Policy Management servers are still on the upgraded release.

9.3 Backout of Fully Upgraded Cluster

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

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

Expected pre-conditions:

1. The primary active CMP is on release 12.3
2. The cluster servers to be backed out are on release 12.1.x/12.2.x

9.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, MPE) is in georedundant mode with active, standby and spare 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, each cluster must start the backout procedure one at a time, staggering by about 1 minute each.

9.3.1.1 Overview on Backout/Rollback MRA/MPE cluster

The following sequence preserves the cluster as a georedundant MRA/MPE cluster.

1. Back out of the standby server
2. Back out of the spare server
3. Fail over
4. Reapply the configuration
5. Back out of the new standby server

9.3.1.2 Backout Secondary CMP (if applicable)

NOTE: At this time, all MPEs and MRAs must be backed out to the previous release.

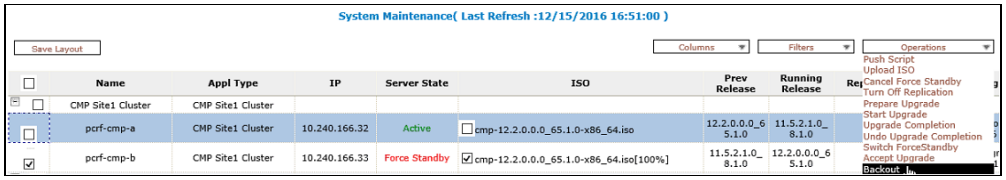
Use the CMP GUI (Upgrade Manager) to backout the Secondary CMP cluster

9.3.1.3 Backout Primary CMP (12.2.x)

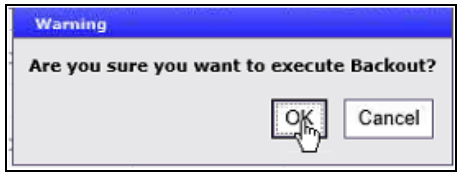
NOTE: At this time, all of the MPE/MRA clusters must be backed out, the Secondary CMP must also be backed out.

1. Use the CMP GUI (Upgrade Manager) to backout the Primary standby CMP cluster
2. Select the CMP cluster and click **Rollback** on the top left, would initiate backout on Standby CMP

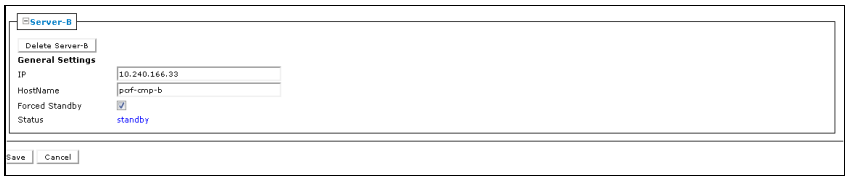
3. Continue Rollback, which would failover to older version CMP cluster.
4. Log back in to the Primary CMP VIP.
5. Use the 12.1.x/12.2.x System Maintenance to complete backout of the Primary CMP cluster.



6. Click **OK** to run backout.



7. After rollback of CMP cluster, manually remove Forced Standby.



8. If needed, go to **Policy Server→ Configuration → Policy Server** and click **Reapply Configuration**.

9.3.1.4 Backout Primary CMP (12.3.x)

Use the CMP GUI (Upgrade Manager) to backout the CMP cluster, the steps are the same as 9.3.1.3.

9.3.2 Back-out Partially Upgraded MPE/MRA Cluster

Use this procedure to back-out a partially upgraded MPE/MRA Cluster.

Expected Pre-conditions:

1. Primary Active CMP is on Release 12.3.x
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 12.3.x
4. Other servers of target cluster are on Release 12.1.x

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45 minutes per Blade.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

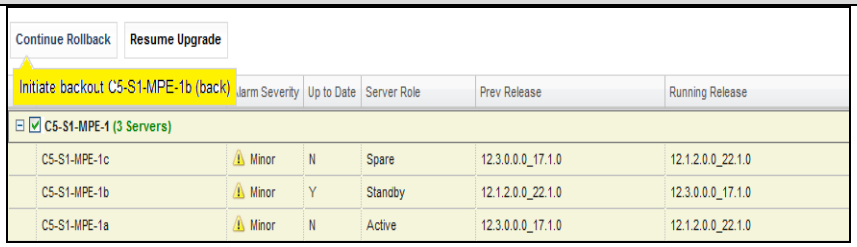
Procedure 3: Back-out Partially Upgraded MPE/MRA Cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of affected Clusters	Navigate to **Upgrade → Upgrade Manager**. Confirm status of the cluster to be backed out: • Primary Active CMP is on Release 12.3.x • Target Cluster has 2 servers on Release 12.1.x, and 1 server on Release 12.3.x • Active server is on 12.1.x

2. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

3. ☐	**CMP GUI:** Verify the status of affected Clusters **NOTE:** This takes approximately30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the partially upgraded cluster to back-out. 3. Select the cluster (one cluster at a time) (can be an MRA or MPE) 4. Click Start Rollback. When hovering over the button, it indicates the server to get backed out.

Step	Procedure	Details



5. Click **OK** to confirm and continue with the operation. It begins to back-out.

Follow the progress status in the Upgrade Operation column.

During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.

Expected Critical Alarms

70001 The qp_procmgr process has failed
31227 The high availability status is failed due to raised alarms
70028 Signaling bonded interface is down
31283 High availability server is offline

Expected Major Alarms

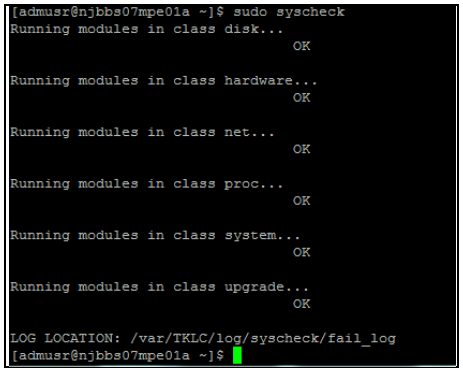
70004 The QP processes have been brought down for maintenance
31236 High availability TCP link is down
31233 High availability path loss of connectivity

Expected Minor Alarms

70503 The server is in forced standby
70507 An upgrade/backout action on a server is in progress
70501 The Cluster is running different versions of software
31101 DB replication to a slave DB has failed
31102 DB replication from a master DB has failed
31282 The HA manager (cmha) is impaired by a s/w fault
31232 High availability server has not received a message
31284 High availability remote subscriber has not received a heartbeat
31107 DB merging from a child Source Node has failed
31114 DB Replication of configuration data via SOAP has failed
31104 DB Replication latency has exceeded thresholds
78001 Transfer of Policy jar files failed
70500 The system is running difference versions of software
31100 The DB replication process is impaired by a s/w fault

Back-out of the server is complete when the following message (Initiate Back-out Completed Successfully)

Step	Procedure	Details

4. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to back-out server and verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		3. If the permissions are not as listed above then perform the following; otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		4. Verify:
		`$ ls -l /`
		5. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

5. ☐	**MPE/MRA CLI:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth02.
		5. Change from primary=eth02 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

---End of Procedure---		

9.3.3 Back-out Fully Upgraded MPE/MRA Cluster

Use this procedure to back-out fully upgraded MPE/MRA Clusters.

Prior to performing this procedure, Oracle recommends consulting the Technical Services team to discuss the next appropriate course of actions.

This procedure is used to back-out a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster is on Release 12.1.x (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

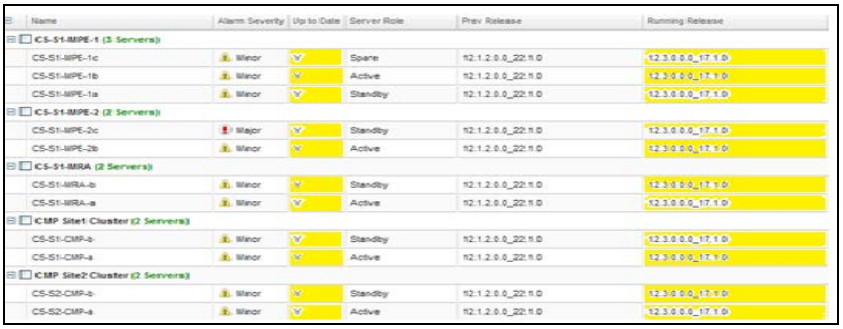
1. Primary Active CMP is on Release 12.3.x
2. Cluster is of MPE or MRA
3. Servers of target cluster are on Release 12.3.x in either in Active, Standby, Force Standby or Spare role

NOTES:

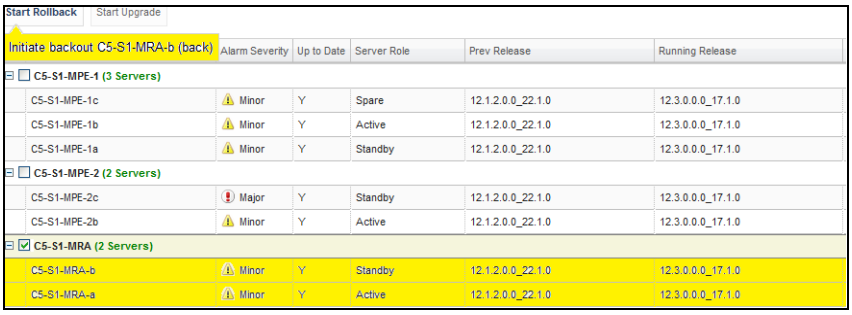
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

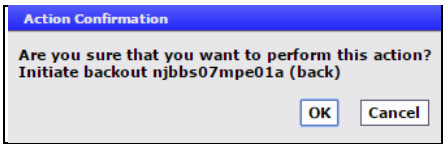
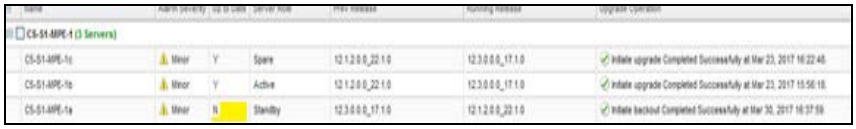
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

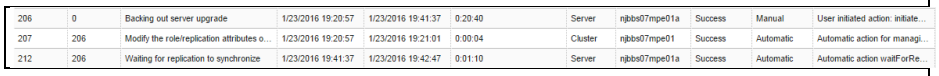
Procedure 4: Back-out Fully Upgraded MPE/MRA Cluster

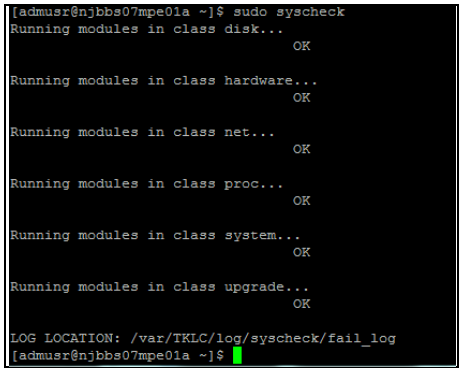
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of affected Clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster is backed out: - Primary Active CMP is on Release 12.3.x - MPE/MRA is on Release 12.3.x Up to Date column shows Y for all servers **EXAMPLE:** 

2. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby and Spare servers to be backed out as admusr.
		2. **NOTE:** Currently Active server is checked after the failover later on in this procedure.
		`$ ls -lh /var/log/messages`
		ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

3. ☐	**CMP GUI:** Initiate Back-out **NOTE:** Each back-out of one blade server completes in approximately30 minutes. **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster (one cluster at a time, can be an MRA, MPE, or Mediation cluster). 3. Click **Start Rollback**. When hovering over the button, it indicates the server to be backed out. In this case it is the current standby server. 

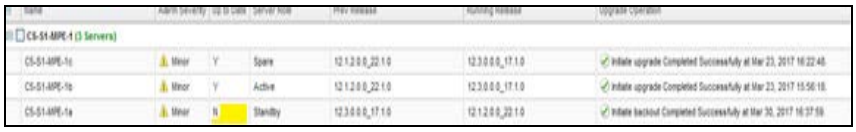
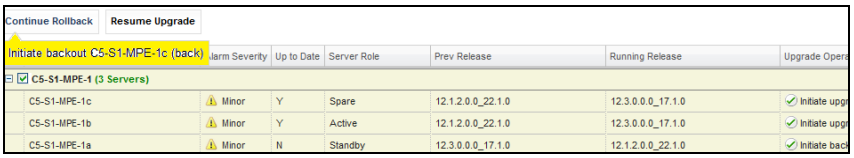
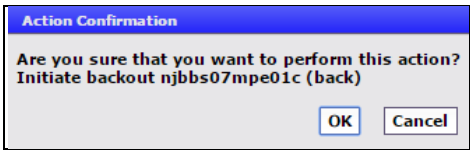
Step	Procedure	Details
		4. Click **OK** to confirm and continue with the operation. It begins to back-out.  Follow the progress status in the Upgrade Operation column. At this point, the server backing out goes into OOS state Wait until the server goes to an OOS state before selecting the next cluster to back-out. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server shows running release of 12.1.x/12.2.x and return to standby with an N in the Up To Date column. 
4. ☐	**CMP GUI:** Verify the back-out is	1. Select the partially backed out cluster

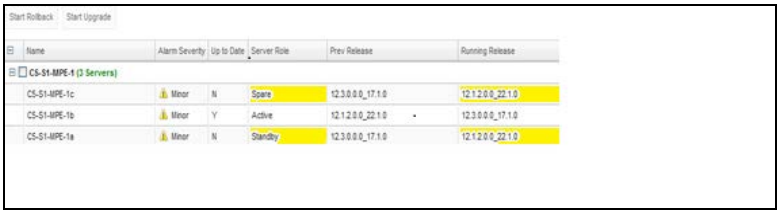
Step	Procedure	Details
	successful	2. Select the View Upgrade LOG  3. Check upgrade logs for the remainder of partially backed out clusters.

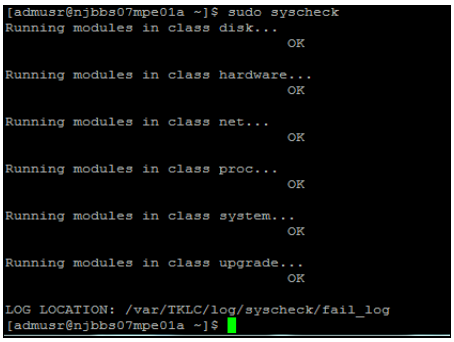
5. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Standby server and verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		3. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		4. Verify:
		`$ ls -l /`
		5. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

6. ☐	**MPE/MRA CLI:** Verify eth01 is primary device interface	This step only applies if the backed-out Standby server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth02.
		5. Change from primary=eth02 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

7. ☐	Confirm MPE/MRA server status	Ensure that the Active/Spare are on 12.3.x and the standby server shows running release of 12.1.x 
8. ☐	**CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is Initiate Back-out on spare server **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time. **NOTE:** This takes approximately 30 minutes to complete.	1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it indicates to initiate Back-out  3. Click **OK** to confirm and continue with the operation.  Wait until the server goes to an OOS state before selecting the next cluster. Follow the progress status in the Server Role column. The Server shows OOS in the server role until the back-out completes. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms**

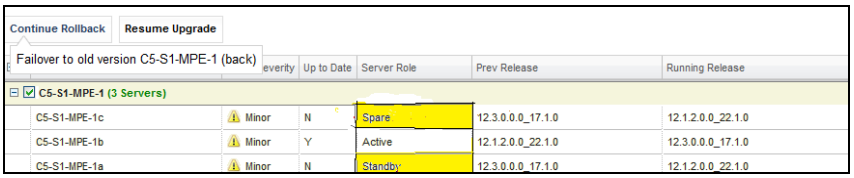
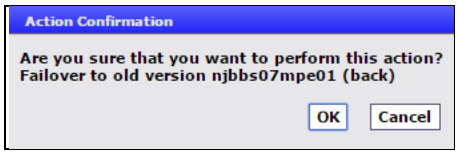
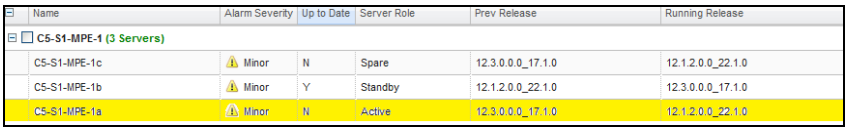
Step	Procedure	Details
		70001 The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to running release of 12.1.x 

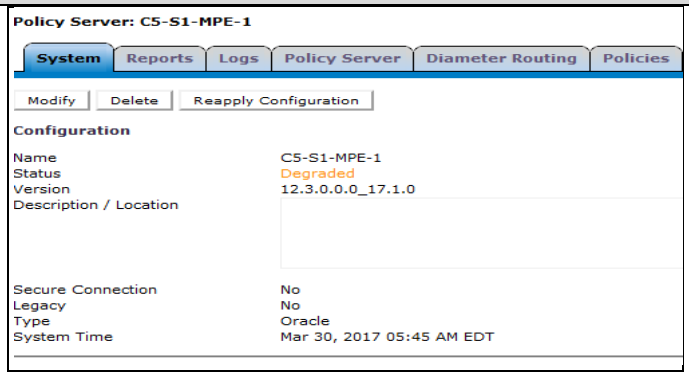
9. ☐	**MPE/MRA SSH:**
	Verify **`syscheck`** and `/tmp` directory permission
		1. Login to the backed-out Spare server as admusr.
		2. Verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`

Step	Procedure	Details

		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

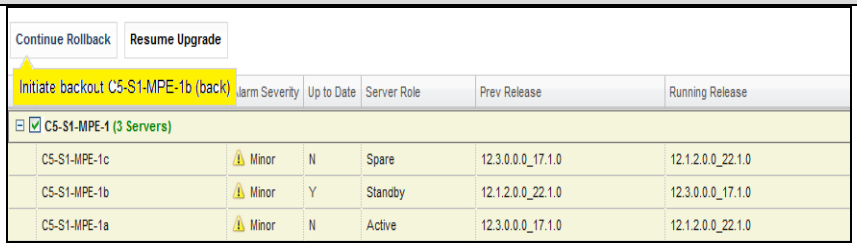
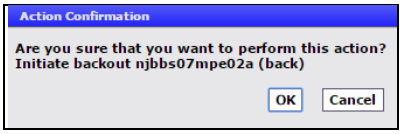
10. ☐	**MPE/MRA CLI:** Verify eth01 is primary device interface	This step only applies if the backed-out Spare server has a condition in which after the back-out is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		To resolve this situation permanently, perform the following:
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth02.
		5. Change from primary=eth02 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

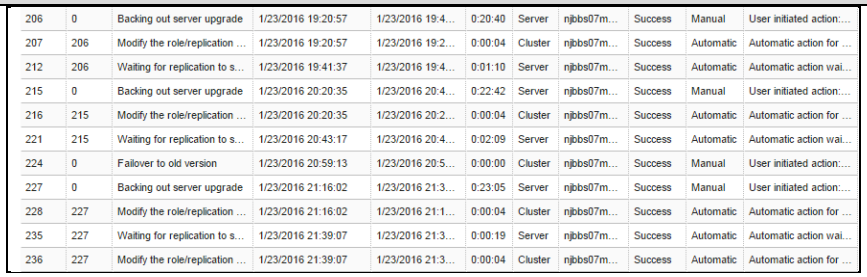
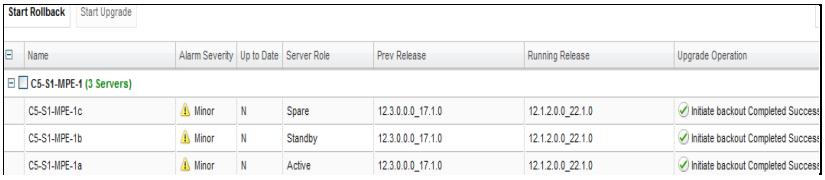
Step	Procedure	Details
11. ☐	**CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is failover to the 12.1.x server. **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.	Current state of the cluster must be as follows. • Active Server is on Release 12.1.x • Standby Server is on Previous release • Spare Server is on Previous release 1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it informs you to failover to old version, which is 12.1.x  3. Click OK to confirm and continue with the operation. It begins to failover.  Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **Expected Major Alarms** **74603** The number of failed MPE primary cluster reaches the threshold **Expected Minor Alarms** **70503** The server is in forced standby **31102** DB replication from a master DB has failed **71402** Diameter Connectivity Lost **31101** DB replication to a slave DB has failed **78001** Transfer of Policy jar files failed State of the cluster looks like the following when the failover completes. 
12. ☐	**CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully	• MPE Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** • MRA: Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ System** The selected Cluster status is Degraded as expected as shown:

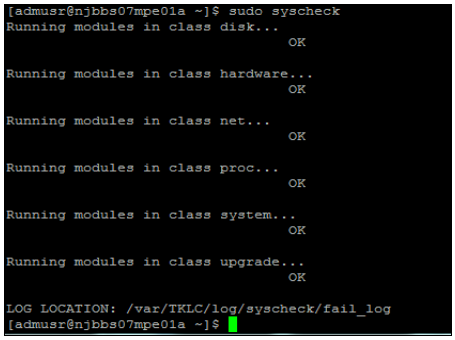
Step	Procedure	Details
		 Click **Reapply Configuration**. Note the Version is successfully changed to the upgraded Release 12.1.x **NOTE:** The status be Degraded which is a normal reporting event as the servers are in different status. **MPE:** 

13. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

14. ☐	**CMP GUI:** Complete Back-out of cluster(s) **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.	1. Select the cluster (one cluster at a time) (can be an MRA, MPE, or Mediation) 2. Click **Continue Rollback**. When hovering over the button, it indicates the back-out server.

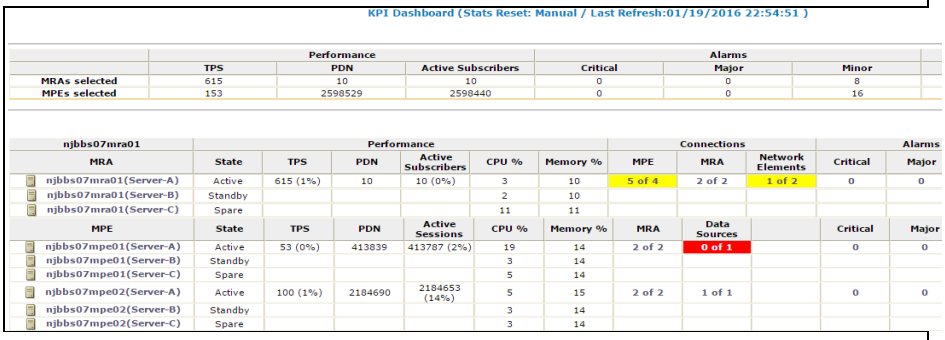
Step	Procedure	Details
	NOTE: Each back-out of a one blade server completes in approximately 30 minutes	 3. Click **OK** to confirm and continue with the operation. It begins to back-out.  Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. Verify in Upgrade Log that that back-out was successful:

Step	Procedure	Details
		 All of the servers is on Release 12.1.x at this point and show active/standby/spare 

15. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Standby server as admusr.
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

16. ☐	**MPE/MRA CLI:** Verify eth01 is primary device interface	This step only applies if the backed-out Standby server has a condition in which after the back-out is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth02.
		5. Change from primary=eth02 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

17. ☐	**CMP GUI:** Verify that backed out cluster is processing traffic normally.	Verify Cluster is processing traffic normally: Navigate to **System Wide Reports → KPI Dashboard**.  KPI Dashboard (Stats Reset: Manual / Last Refresh:01/19/2016 22:54:51) Performance: TPS / PDN / Active Subscribers; Alarms: Critical / Major / Minor MRAs selected: 615 / 10 / 10 / 0 / 0 / 8 MPEs selected: 153 / 2598529 / 2598440 / 0 / 0 / 16 njbbs07mra01 — Performance: State / TPS / PDN / Active Subscribers / CPU % / Memory % — Connections: MPE / MRA / Network Elements — Alarms: Critical / Major njbbs07mra01(Server-A): Active / 615 (1%) / 10 / 10 (0%) / 3 / 10 / 5 of 4 / 2 of 2 / 1 of 2 / 0 / 0 njbbs07mra01(Server-B): Standby / 2 / 10 njbbs07mra01(Server-C): Spare / 11 / 11 MPE: State / TPS / PDN / Active Sessions / CPU % / Memory % / MRA / Data Sources — Alarms: Critical / Major njbbs07mpe01(Server-A): Active / 53 (0%) / 413839 / 413787 (2%) / 19 / 14 / 2 of 2 / 0 of 1 / 0 / 0 njbbs07mpe01(Server-B): Standby / 3 / 14 njbbs07mpe01(Server-C): Spare / 5 / 14 njbbs07mpe02(Server-A): Active / 100 (1%) / 2184690 / 2184653 (14%) / 5 / 15 / 2 of 2 / 1 of 1 / 0 / 0 njbbs07mpe02(Server-B): Standby / 3 / 14 njbbs07mpe02(Server-C): Spare / 3 / 14
18. ☐	**CMP GUI:** Verify alarms	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Verify that there are not any unexpected active alarms present. **NOTE:** Some Alarms take appoximately 30 minutes to 1 hour to auto clear. ***NOTE: After the backout of the clusters, if Critical Alarm 31283 (High availability server is offline) does not clear, then REP route might be missing from the backed-out server. Therefore Routes need to be verified and added. In this case, proceed to next step, otherwise, skip to step 20.***

19. ☐	**MPE/MRA SSH:** Verify routes	1. Login into MPE/MRA server as admusr
		2. Copy routes_output.txt from /home/admusr to /tmp
		`$ sudo cp routes_output.txt /tmp`
		`$ cd /tmp`
		`$ ls`
		`routes_output.txt`

Step	Procedure	Details

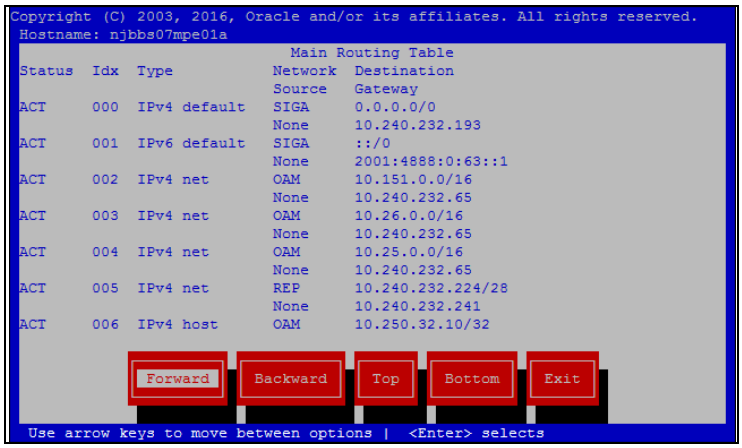
WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.

3. Run the platcfg utility:

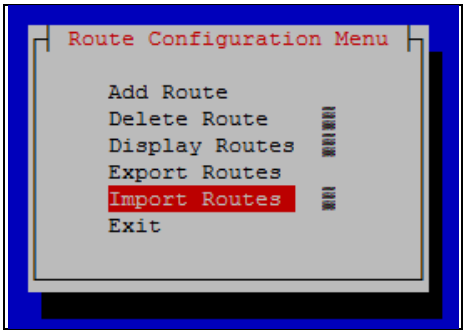
```
$ sudo su - platcfg
```

4. Navigate to **Policy Configuration → Routing Config → Display Routes**.
5. Verify that all routes are present.
6. Click **Forward** to view all the routes.

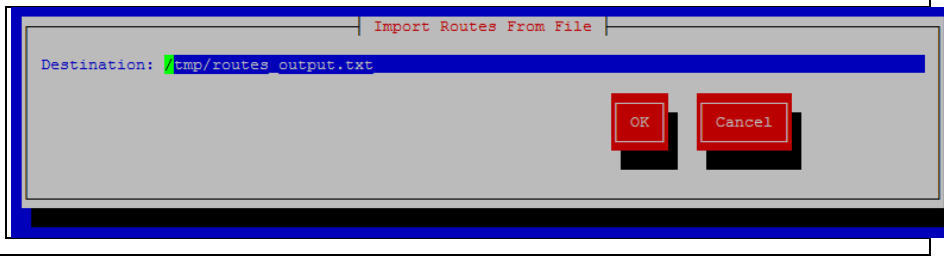
Example:

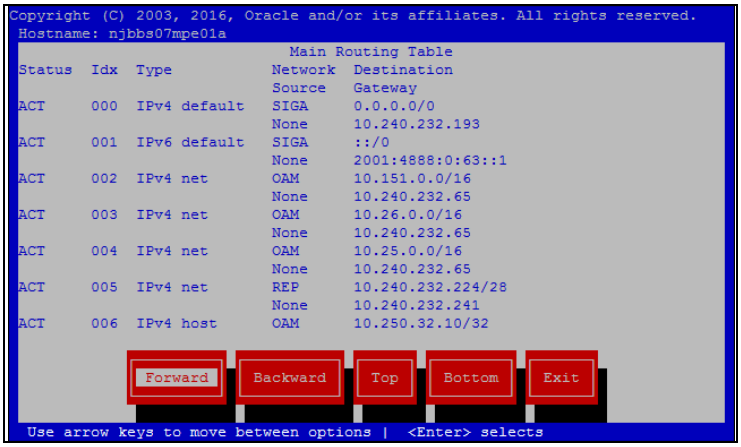


7. If any of the routes are missing then perform the following otherwise skip to step 20
8. Navigate back to **Route Configuration Menu** and select **Import Routes**.



9. Click **OK**.



Step	Procedure	Details
		Routes is imported from `/tmp/routes_output.txt` file and **Route Configuration Menu** is displayed again. 10. Select **Display Routes**. 11. Verify that all routes are present. 12. Click **Forward** to view all the routes. **Example:**  13. Exit the platcfg utility **WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.**
20. ☐	Repeat for other clusters as needed	Repeat this procedure for remainder of MPE/MRA servers, if not fully backed out yet.
21. ☐	Perform **`syscheck`** and verify that alarms are clear.	Another **`syscheck`** on all the back-out servers can be performed to ensure all modules are still operationally OK before progressing to the next procedure. 1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Verify that there are not any unexpected active alarms present. **NOTE:** Some Alarms take appoximately 30 minutes to 1 hour to auto clear.
---End of Procedure---		

9.3.4 Back-out Fully Upgraded Secondary CMP cluster

Use this procedure to back-out a fully upgraded Secondary CMP cluster.

Expected Pre-conditions:

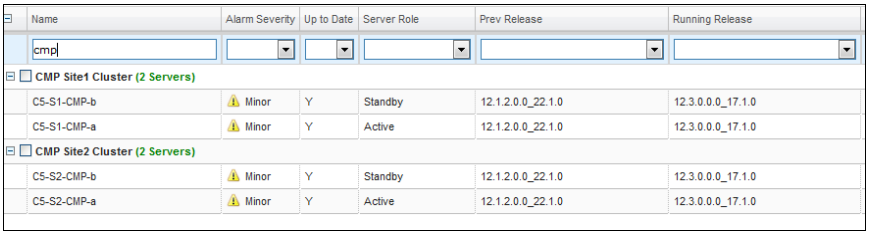
1. Primary Active CMP is on Release 12.3.x
2. Secondary CMP cluster is on Release 12.3.x
3. All MPE/MRA Clusters are on Release 12.1.x/12.2.x

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

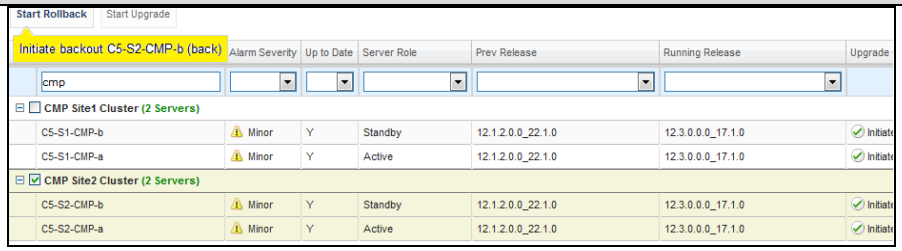
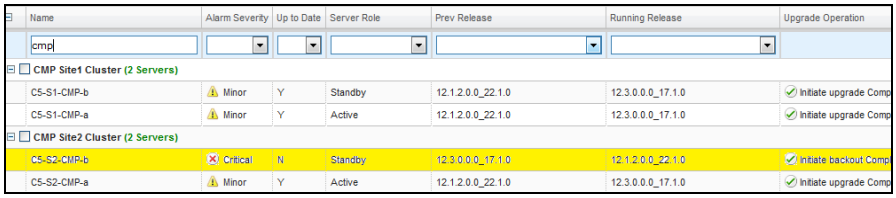
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 5: Back-out Fully Upgraded Secondary CMP cluster

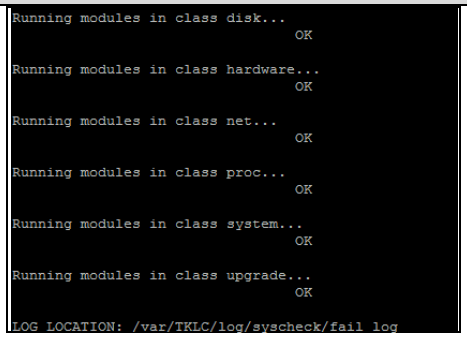
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 12.3.x - Secondary CMP cluster is on Release 12.3.x - Up to Date column shows Y for all servers 3. Click **Filter** and enter `cmp` in the **Name** field. **Example:** 

2. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

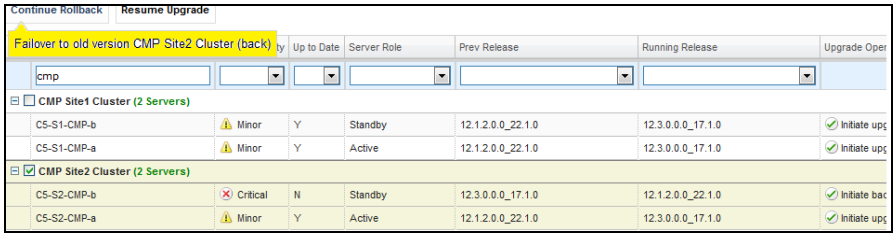
3. ☐	**CMP GUI:** Back-out clusters **NOTE:** Each back-out of one server takes about 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP cluster 3. Click **Start Rollback**. When hovering over the button, it indicates the back-out server.

Step	Procedure	Details
		 4. Click **OK** to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to standby state and show running release of 12.1.x 
4. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server and verify that there are not any failures in **`syscheck`**: `$ sudo syscheck`

Step	Procedure	Details

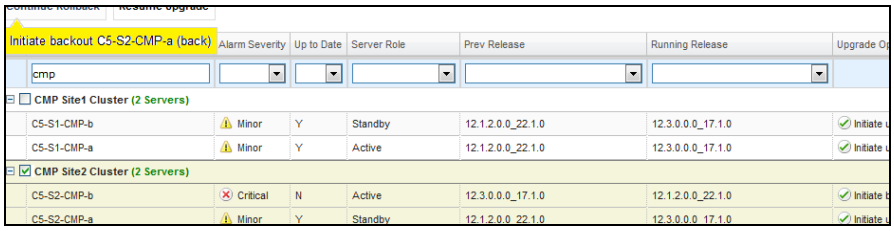
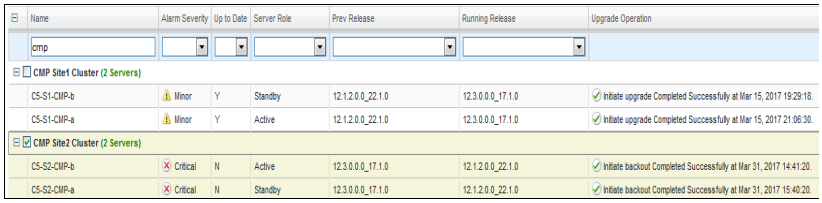
		
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following:
		`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`
		3. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		4. Verify:
		`$ ls -l /`
		5. Perform **`syscheck`** again:
		`$ sudo syscheck`

5. ☐	**CMP SSH:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		To resolve this situation permanently, perform the following:
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If the CMP is the active server, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change from primary=eth11 to primary=eth01
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

Step	Procedure	Details
6. ☐	**CMP GUI:** Continue the back-out. Next operation is failover.	1. Select Secondary CMP cluster. 2. Navigate to **Upgrade → Upgrade Manager**. 3. Select the Secondary CMP cluster 4. Click **Continue Rollback**. When hovering over the button, it informs you to failover.  5. Click **OK** to confirm and continue with the operation. It begins to failover. Follow the progress status in the Server Role column. Wait for the server to show standby. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **74604** Policy cluster is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software

Step	Procedure	Details

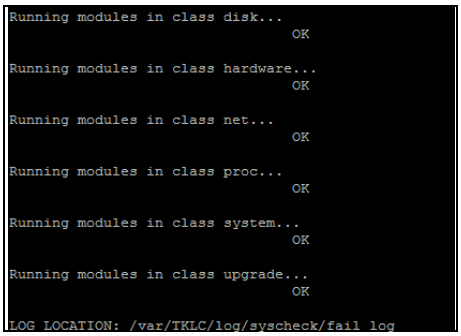
7. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

8. ☐	**CMP GUI:** Continue the backed-out. Next operation is Initiate Back-out **NOTE:** Each back-out of one server takes about 30 minutes to complete.	4. Navigate to **Upgrade → Upgrade Manager**. 5. Select the Secondary CMP cluster. 6. Click **Continue Rollback**. When hovering over the button, it informs you to rollback.  7. Click **OK** to confirm and continue with the operation. It begins to failover. Follow the progress status in the Server Role column. Wait until the server to back-out comes to Standby state before continuing. Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column.  **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master

Step	Procedure	Details
		Expected Minor Alarms **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software 8. Verify in Upgrade Log that that back-out was successful: All Secondary CMP servers is on Release 12.1.x at this point and show active/standby

206	0	Backing out server upgrade	1/23/2016 19:20:57	1/23/2016 19:4…	0:20:40	Server	njbbs07m…	Success	Manual	User initiated action:…
207	206	Modify the role/replication …	1/23/2016 19:20:57	1/23/2016 19:2…	0:00:04	Cluster	njbbs07m…	Success	Automatic	Automatic action for …
212	206	Waiting for replication to s…	1/23/2016 19:41:37	1/23/2016 19:4…	0:01:10	Server	njbbs07m…	Success	Automatic	Automatic action wai…
215	0	Backing out server upgrade	1/23/2016 20:20:35	1/23/2016 20:4…	0:22:42	Server	njbbs07m…	Success	Manual	User initiated action:…
216	215	Modify the role/replication …	1/23/2016 20:20:35	1/23/2016 20:2…	0:00:04	Cluster	njbbs07m…	Success	Automatic	Automatic action for …
221	215	Waiting for replication to s…	1/23/2016 20:43:17	1/23/2016 20:4…	0:02:09	Server	njbbs07m…	Success	Automatic	Automatic action wai…
224	0	Failover to old version	1/23/2016 20:59:13	1/23/2016 20:5…	0:00:00	Cluster	njbbs07m…	Success	Manual	User initiated action:…
227	0	Backing out server upgrade	1/23/2016 21:16:02	1/23/2016 21:3…	0:23:05	Server	njbbs07m…	Success	Manual	User initiated action:…
228	227	Modify the role/replication …	1/23/2016 21:16:02	1/23/2016 21:1…	0:00:04	Cluster	njbbs07m…	Success	Automatic	Automatic action for …
235	227	Waiting for replication to s…	1/23/2016 21:39:07	1/23/2016 21:3…	0:00:19	Server	njbbs07m…	Success	Automatic	Automatic action wai…
236	227	Modify the role/replication …	1/23/2016 21:39:07	1/23/2016 21:3…	0:00:04	Cluster	njbbs07m…	Success	Automatic	Automatic action for …

Step	Procedure	Details

9. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr.
		2. Verify that there are not any failures in **`syscheck`**.
		`$ sudo syscheck`
		 
		
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

10. ☐	**CMP SSH:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change from primary=eth11 to primary=eth01.
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

---End of Procedure---		

9.3.5 Back-out Fully Upgraded Primary CMP cluster

Use this procedure to back-out a fully upgraded Primary CMP cluster.

Expected Pre-conditions:

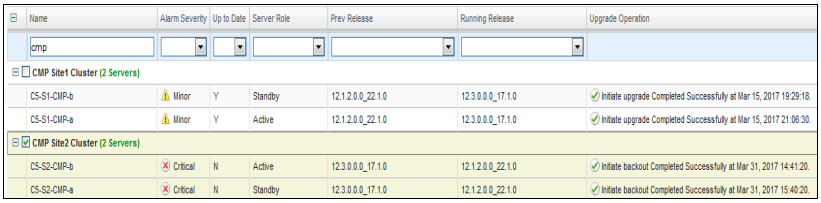
1. Primary Active CMP cluster is on Release 12.3.x
2. Secondary CMP, MPE and MRA Clusters are on Release 12.1.x

NOTES:

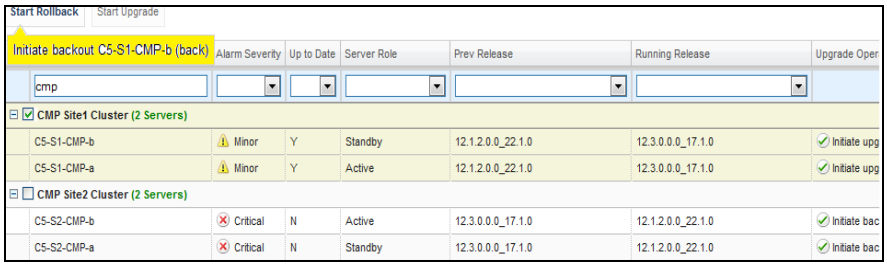
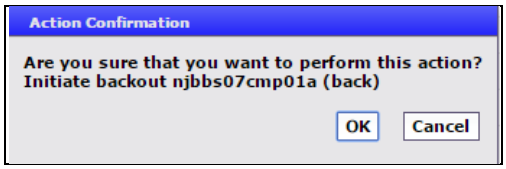
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

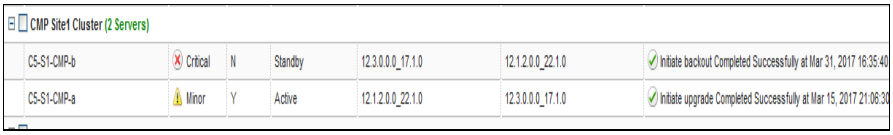
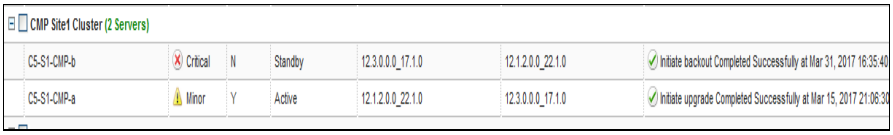
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 6: Back-out Fully Upgraded Primary CMP cluster

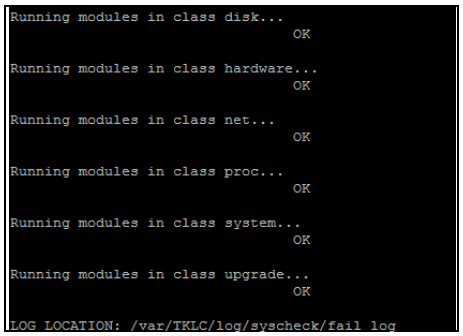
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP clusters	7. Navigate to **Upgrade → Upgrade Manager** 8. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 12.3.x - Secondary CMP, MPE and MRA Clusters are on Release 12.1.x - Up to Date column shows Y for all servers in Primary CMP cluster - Click Filter and enter cmp in the Name field. **Example:** 

2. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

3. ☐	**CMP GUI:** Back-out standby server of Primary CMP cluster **NOTE:** Back-out of one server takes about 30 minutes to complete.	1. Select the Primary CMP cluster 2. Click **Start Rollback**. When hovering over the button, it indicates the server to back out.  3. Click **OK** to confirm and continue with the operation. It begins to back-out.  Server goes into an OOS server Role

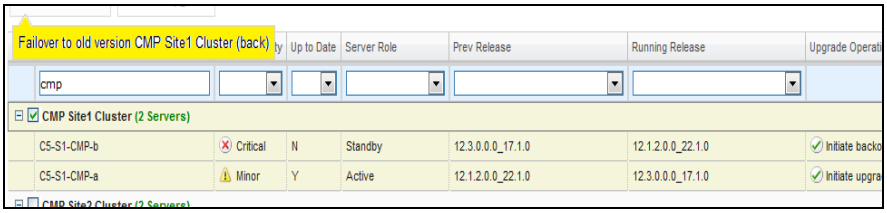
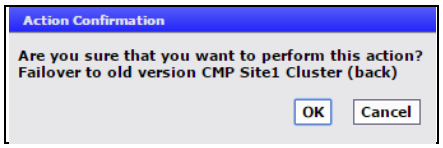
Step	Procedure	Details
		Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.  **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the initiate Back-out completed successfully message displays in the Upgrade Operation column. The server goes back to standby state and show running release of 12.1.x 

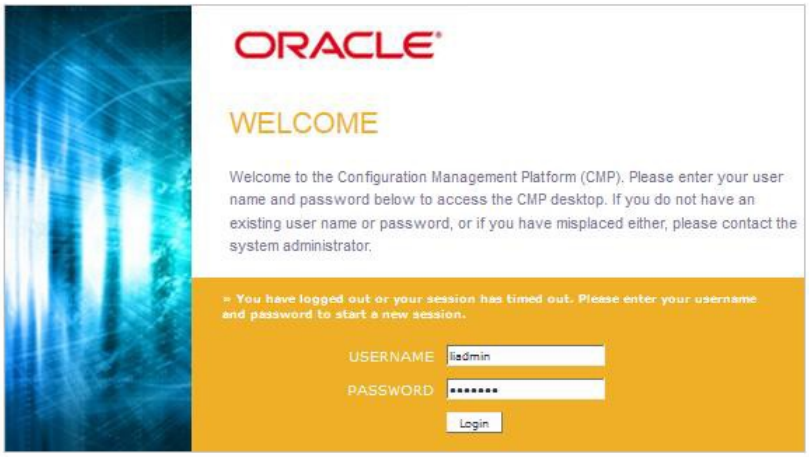
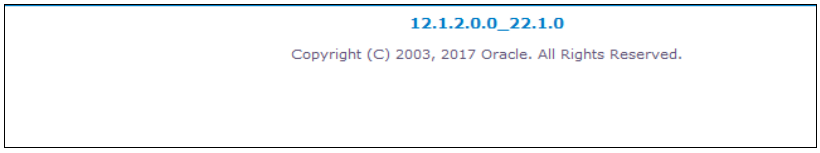
Step	Procedure	Details

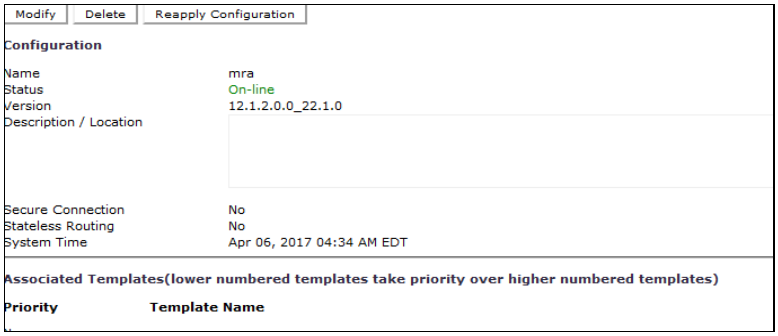
4. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr.
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

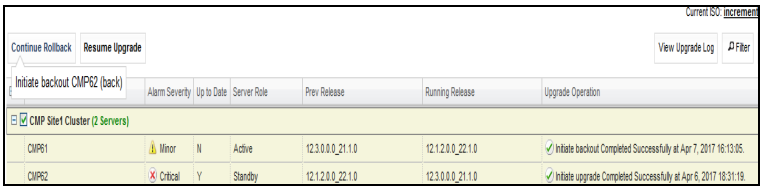
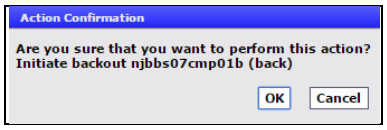
5. ☐	**CMP SSH:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. Login as admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change primary=eth11 to primary=eth01.
		6. Save and exit (for example, vi uses ESC :wq!).
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

6. ☐	**CMP GUI:** Continue the back-out. Next operation is failover.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster. 3. Click **Continue Rollback**. When hovering over the button, it informs you to failover.  4. Click **OK** to confirm and continue with the operation. It begins to failover. The failover takes couple of minutes.  After a minute, you are required to log back in.

Step	Procedure	Details
7. ☐	**CMP GUI:** Log back into the Primary CMP VIP	After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP. 
8. ☐	CMP GUI: Verify previous Policy Management Release	1. Navigate to **Help → About**. 2. Verify the release displayed is 12.1.x.x 

Step	Procedure	Details
9. ☐	**CMP GUI:** If a Config Mismatch is observed on MPE or MRA	**MPE:** Navigate to **Policy → Configuration →** <*mpe_cluster name*> **→ System** **MRA:** Navigate to **MRA → Configuration →** <*MRA Cluster*> **→ System**  Click **Reapply Configuration**. Config Mismatch is resolves: 

10. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of /var/log/messages is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

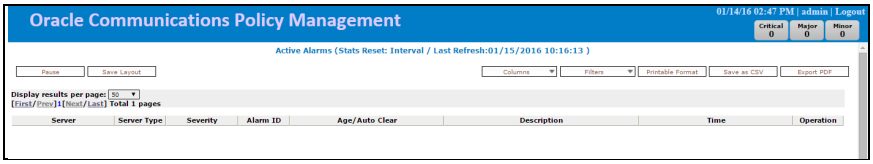
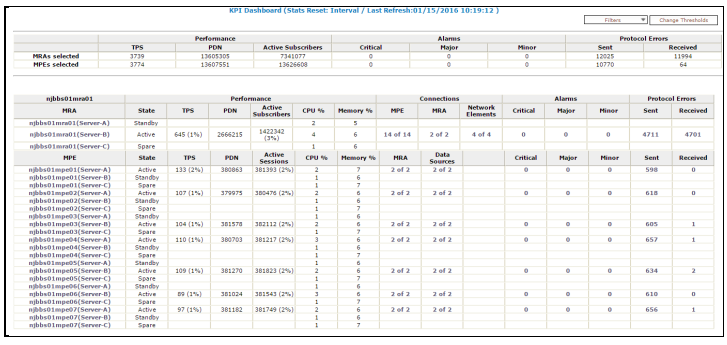
Step	Procedure	Details
11. ☐	**CMP GUI:** Continue the back-out of the Primary CMP cluster **NOTE:** Back-out of one server takes about 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster. 3. Click Continue Rollback. When hovering over the button, it indicates the server to get backed out. At this point it is the remaining standby server.  4. Click OK to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role  Follow the progress status In the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to standby state and show the previous release.

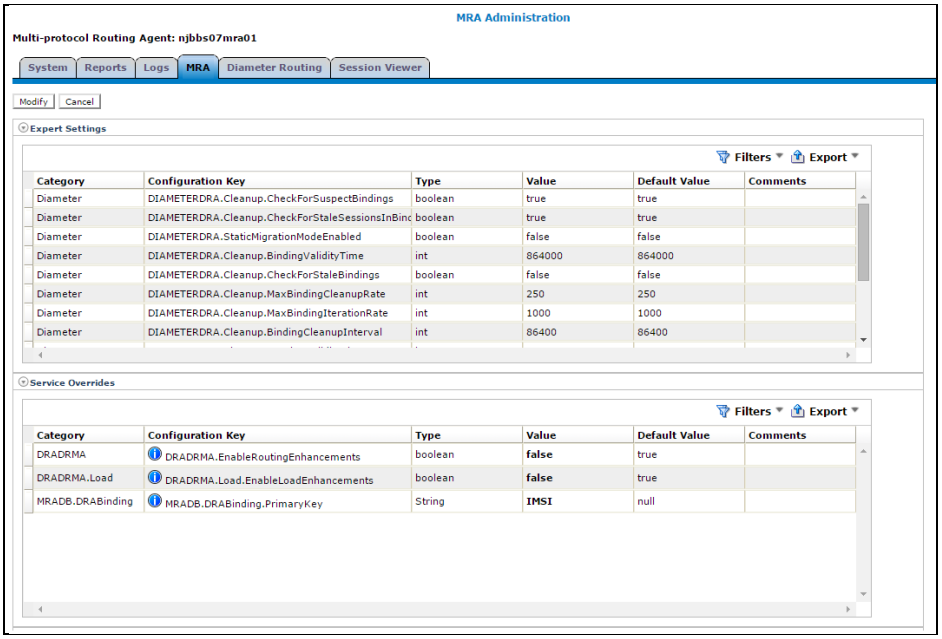
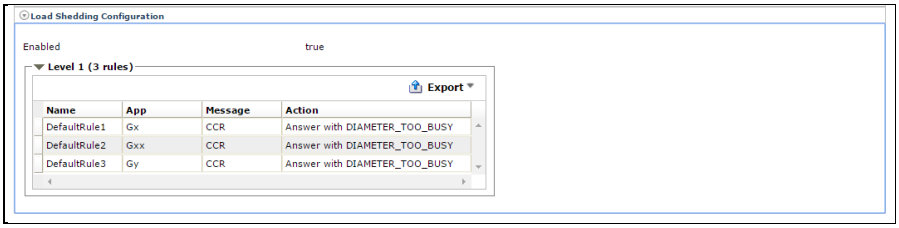
Step	Procedure	Details
		Start Rollback Start Upgrade Name / Alarm Severity / Up to Date / Server Role / Prev Release / Running Release CMP Site1 Cluster (2 Servers) CMP61 — N — Active — 12.3.0.0.0_21.1.0 — 12.1.2.0.0_22.1.0 CMP62 — N — Standby — 12.3.0.0.0_21.1.0 — 12.1.2.0.0_22.1.0 Verify in Upgrade Log that that back-out was successful: 206 / 0 / Backing out server upgrade / 1/23/2016 19:20:57 / 1/23/2016 19:4… / 0:20:40 / Server / njbbs07m… / Success / Manual / User initiated action:… 207 / 206 / Modify the role/replication … / 1/23/2016 19:20:57 / 1/23/2016 19:2… / 0:00:04 / Cluster / njbbs07m… / Success / Automatic / Automatic action for … 212 / 206 / Waiting for replication to s… / 1/23/2016 19:41:37 / 1/23/2016 19:4… / 0:01:10 / Server / njbbs07m… / Success / Automatic / Automatic action wai… 215 / 0 / Backing out server upgrade / 1/23/2016 20:20:35 / 1/23/2016 20:4… / 0:22:42 / Server / njbbs07m… / Success / Manual / User initiated action:… 216 / 215 / Modify the role/replication … / 1/23/2016 20:20:35 / 1/23/2016 20:2… / 0:00:04 / Cluster / njbbs07m… / Success / Automatic / Automatic action for … 221 / 215 / Waiting for replication to s… / 1/23/2016 20:43:17 / 1/23/2016 20:4… / 0:02:09 / Server / njbbs07m… / Success / Automatic / Automatic action wai… 224 / 0 / Failover to old version / 1/23/2016 20:59:13 / 1/23/2016 20:5… / 0:00:00 / Cluster / njbbs07m… / Success / Manual / User initiated action:… 227 / 0 / Backing out server upgrade / 1/23/2016 21:16:02 / 1/23/2016 21:3… / 0:23:05 / Server / njbbs07m… / Success / Manual / User initiated action:… 228 / 227 / Modify the role/replication … / 1/23/2016 21:16:02 / 1/23/2016 21:1… / 0:00:04 / Cluster / njbbs07m… / Success / Automatic / Automatic action for … 235 / 227 / Waiting for replication to s… / 1/23/2016 21:39:07 / 1/23/2016 21:3… / 0:00:19 / Server / njbbs07m… / Success / Automatic / Automatic action wai… 236 / 227 / Modify the role/replication … / 1/23/2016 21:39:07 / 1/23/2016 21:3… / 0:00:04 / Cluster / njbbs07m… / Success / Automatic / Automatic action for … All Primary CMP servers is on Release 12.1.x at this point and show active/standby

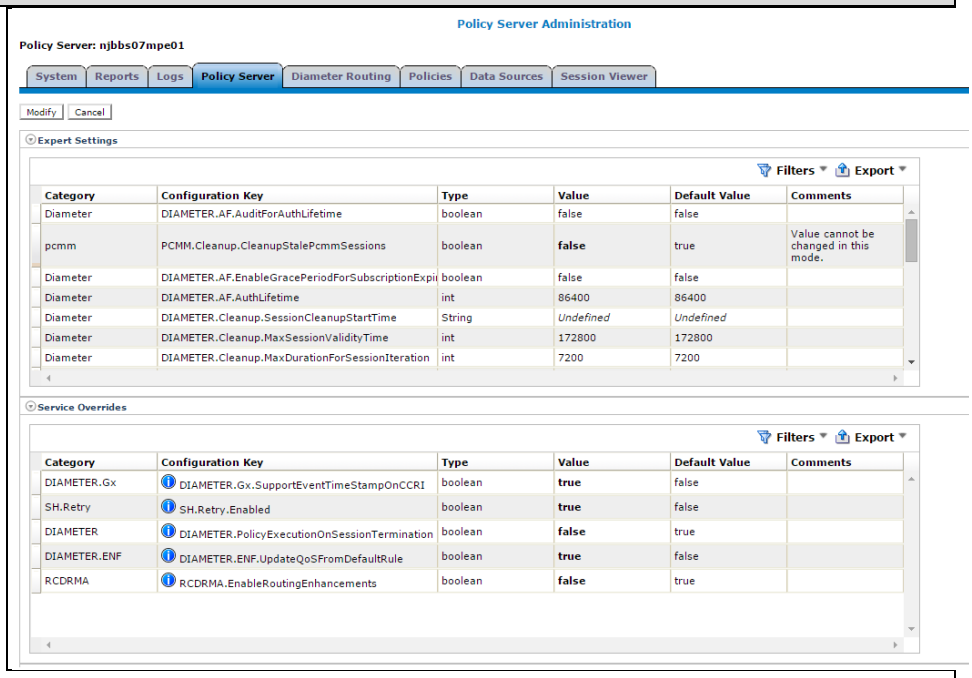
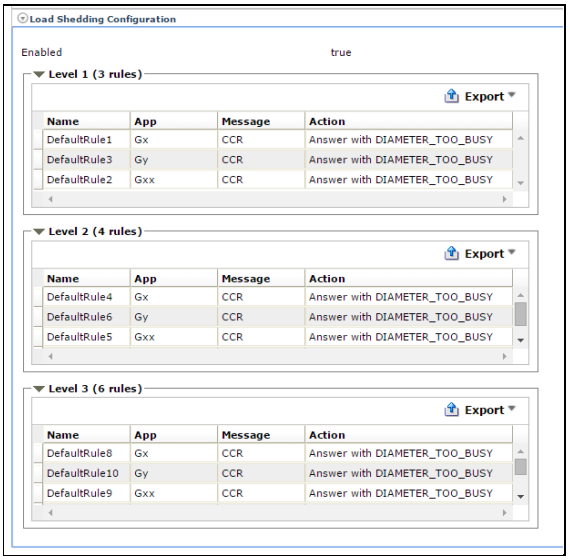
12. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		Running modules in class disk... OK
		Running modules in class hardware... OK
		Running modules in class net... OK
		Running modules in class proc... OK
		Running modules in class system... OK
		Running modules in class upgrade... OK
		LOG LOCATION: /var/TKLC/log/syscheck/fail_log
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details

13. ☐	**CMP SSH:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following:
		
		1. As admusr, run the following:
		`$ sudo cat /proc/net/bonding/bond0`
		2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.
		3. If this blade is the active blade, change it to standby before performing the following operations.
		`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`
		4. Find eth11.
		5. Change primary=eth11 to primary=eth01.
		6. Save and exit (for example, vi uses ESC :wq!)
		`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`
		`$ sudo reboot`

14. ☐	**CMP GUI:** Verify Alarm Status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Confirm that any existing alarm is understood. 
15. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Confirm that all Connections and Traffic status are as expected. Observe it for a few screen refresh updates. 

Step	Procedure	Details
16. ☐	**CMP GUI:** Verify Advanced Settings on the MRA	1. Capture screenshots of the advanced settings on the MRA and compare it with prior to upgrade screen captures. 2. Verify that there are not any differences. 3. Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ MRA**. 4. Click **Advanced**.  
17. ☐	**CMP GUI:** Verify Advanced Settings on the MPE	1. Capture screenshots of the advanced settings on the MPE and compare it with prior to upgrade screen captures. 2. Verify that there are not any difference 3. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ Policy Server**. 4. Click **Advanced**.

Step	Procedure	Details
		  Alternately, settings can be exported clicking **Export** on the right within each setting.
---End of Procedure---		

A.1 TVOE and PM&C Server Upgrade

Use this procedure to add the TVOE software image to the TVOE host.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Adding TVOE software image to TVOE host

Step	Procedure	Details

1. ☐	**TVOE Host:** Verify there is enough space on the server for TVOE software image	Log in to the TVOE host and run the following to verify there is sufficient space:
		`$ df -h /var/TKLC/upgrade/`
		The system returns output similar to the following to indicate the disk usage of where the TVOE software image should reside.
		`Filesystem Size Used Avail Use% Mounted on`
		`/dev/mapper/vgroot-plat_var_tklc`
		`4.0G 848M 3.0G 23% /var/TKLC`
		If the Avail column is smaller than the size of the TVOE software image, contact Oracle Support for information about how to proceed.

2. ☐	Add TVOE software image to TVOE host	Place a copy of the TVOE software image into the /var/TKLC/upgrade/ directory on the TVOE host by utilizing scp or USB media.
		• SCP from PC using Linux
		From the command line of a Linux system, use the following command to copy the backup ISO image to the TVOE host:
		`$ scp <path_to_image> <user>@<TVOE_ip>:/var/TKLC/upgrade/`
		Where:
		<*path_to_image*> is the path to the TVOE ISO image local to the Customer PC
		<*TVOE_ip*> is the TVOE IP address
		<*user*> should be admusr for TVOE releases 2.5 or newer.
		• SCP from PC using Windows
		Use WinSCP to copy the TVOE ISO image to the TVOE host.
		• USB Media
		a. Attach the USB media to the TVOE host.
		b. Login on the TVOE host and run the following to list ISOs on the USB media:
		`$ sudo ls /media/*/*.iso`
		`/media/usb/TVOE-3.0.3.x.x_86.4.0-x86_64.iso`
		c. Replacing <*PATH_TO_TVOE_ISO*> with the output of the command above, copy the ISO to the `/var/TKLC/upgrade` directory using the **cp** command:
		`$ sudo cp <PATH_TO_TVOE_ISO> /var/TKLC/upgrade/`
		d. Unmount the USB media:
		`$ sudo umount /media/usb`

---End of Procedure---		

A.2 TVOE Upgrade

Use this procedure to upgrade the PM&C Server to 6.0.3 and the TVOE host to 3.0.3

NOTE: The TVOE upgrade procedure can run either during the same maintenance window as PM&C upgrade or in a separate maintenance window.

NOTE: If PM&C TVOE host cannot be upgraded at this time then PM&C upgrade must not be attempted.

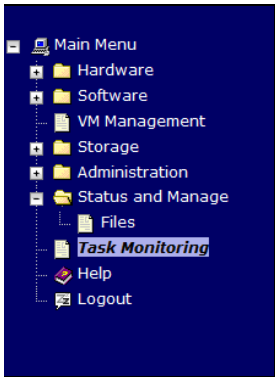
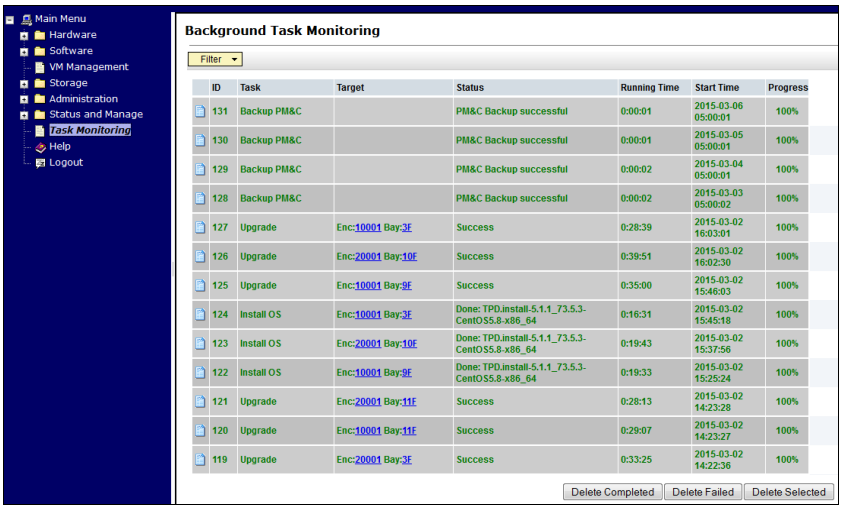
- TVOE Pre-Upgrade Validation
- Pre-Upgrade Backup
- Add TVOE Software Image to TVOE HOST
- Add PM&C Upgrade Software to PM&C Server
- Stand Alone TVOE Host Upgrade
- TVOE Post-Upgrade Validation
- PM&C upgrade
- Stand Alone TVOE Upgrade Accept
- PM&C Upgrade Accept

NOTE: It is recommended NOT to accept TVOE upgrade until after PM&C upgrade has been accepted for the following reasons:

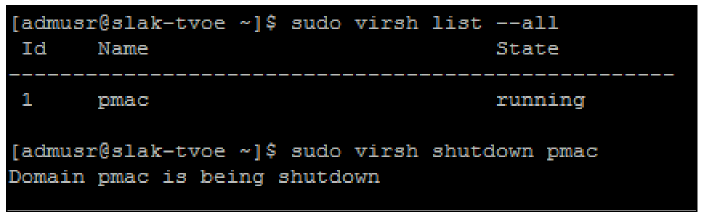
- If you are upgrading from PM&C 5.5, this release cannot be deployed on an upgraded TVOE 3.0.3 system.
- If an issue occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade has to be rejected to allow PM&C 5.5 to be re-deployed.

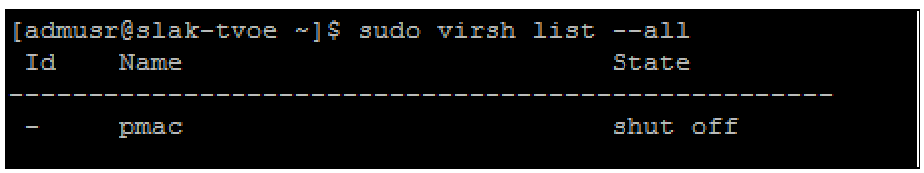
A reject cannot be performed after an upgrade has been accepted.

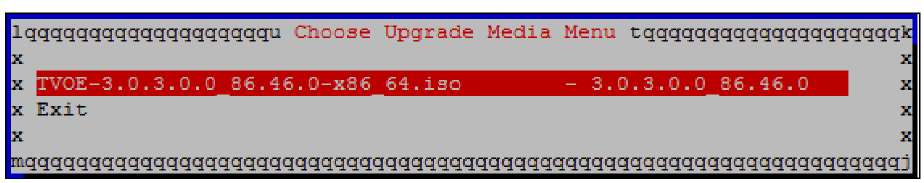
Step	Procedure	Details
1. ☐		**NOTE:** Upgrade of TVOE host shuts down all guest OS (including PM&C) during the upgrade. Still, prior to upgrading the TVOE host, ensure the PM&C server is gracefully shut down.

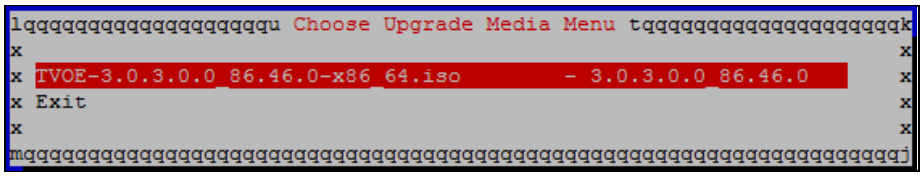
Step	Procedure	Details
2. ☐	Check any in-progress task(s) on PM&C	1. On a supported web browser, log in to PM&C GUI as pmacadmin 2. Navigate to PM&C GUI background tasks page: **Main Menu → Task Monitoring**  3. Verify all tasks are complete indicated by green 100% progress **NOTE:** If any task shows in-progress (blue or red) then wait for the task to complete prior to continuing the next step. 

Step		Procedure	Details

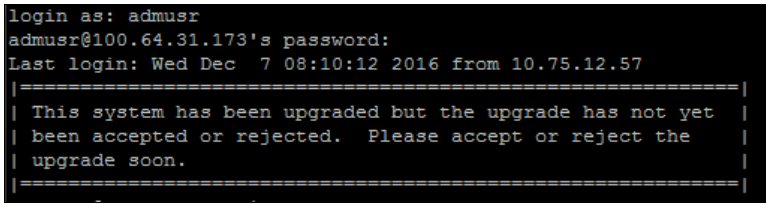
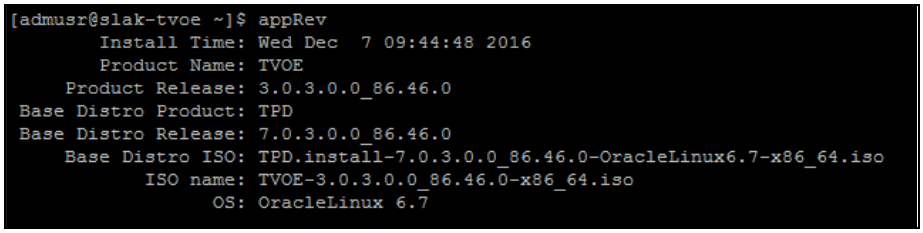
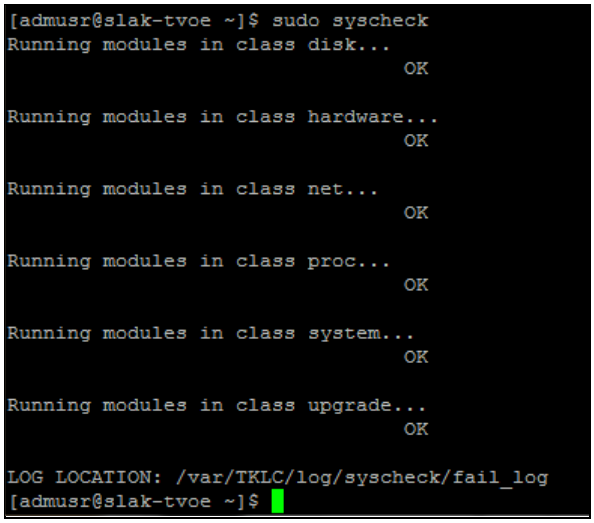
3.	☐	Shutdown PM&C	**NOTE:** Assuming all tasks are completed (previous step) it is safe to shut down PM&C
			1. Log on to the TVOE host as admusr.
			2. Obtain the name of the PM&C guest by running the following command:
			`$ sudo virsh list --all`
			`Id Name State`
			`--------------------------------------------`
			`1 <pmac_name> running`
			3. Stop the PM&C process by using the following command:
			`$ sudo virsh shutdown <pmac_name>`
			 
			NOTE: It is imperative to log in to the TVOE host instead of using SSH to the PM&C guest. The upgrade might fail otherwise.

4.	☐	Verify PM&C guest is shut down	1. Login to the TVOE host as admusr. 2. Verify that the PM&C is shut down with the following command: `[admusr@tvoe approximately]# sudo virsh list --all`  **NOTE:** This should show PM&C guest state as shut off.

5.	☐	Validate media	1. Logged on to the TVOE host as admusr.
			2. Run the platcfg utility.
			`$ sudo su - platcfg`
			3. Navigate to **Maintenance → Upgrade → Validate Media**.
			4. Select the new TVOE ISO
			 
			5. Press **Enter** to validate the ISO file
			The TVOE ISO image is validated with an expected result of:
			`The media validation is complete, the result is: PASS`
			If the image validation fails, this procedure should be stopped. The ISO image should be copied again to the TVOE host and this procedure should be re-started from the beginning.

Step	Procedure	Details
6. ☐	Start TVOE upgrade **NOTE:** The upgrade process takes 15 minutes	1. Press **Enter** to return to platcfg and then press Exit to go back to the Upgrade menu. Do not quit platcfg. 2. Select: **Maintenance → Upgrade → Initiate Upgrade.** 3. Select the new TVOE ISO filename  4. Press **Enter** to initiate the upgrade. **NOTE:** TVOE host is rebooted at the end of the upgrade process (around 15 minutes) and returns to the login prompt. At this point the upgrade is complete.

Step	Procedure	Details

7. ☐	Verify the Upgrade status	1. Log in to TVOE as admusr
		 
		
		2. Verify the upgraded TVOE revision by running the following command:
		`$appRev`
		You get an output similar to this:
		 
		
		3. Run the **`verifyUpgrade`**:
		`$sudo verifyUpgrade`
		No output is expected from this command. Any output displays potential issues.
		4. Run **`syscheck`**:
		`$sudo syscheck`
		 

8. ☐		**NOTE:** It is recommended not to accept TVOE upgrade until after PM&C upgrade has been accepted for the following reasons: • Some older PM&C releases cannot be deployed on upgraded TVOE 3.0.3 system. • If issues occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade has to be rejected to allow older PM&C to be re-deployed. • A reject cannot be performed after an upgrade has been accepted.
---End of Procedure---		

A.3 PM&C Upgrade

Use this procedure to perform software upgrade of the PM&C.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

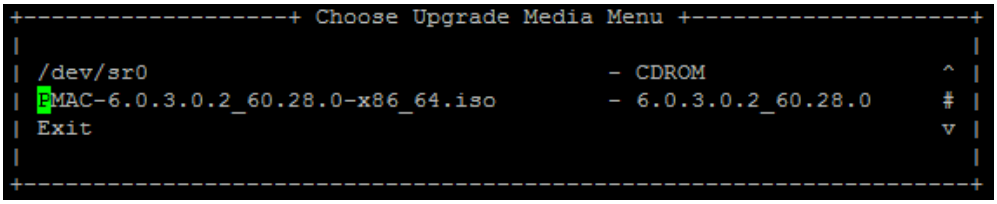
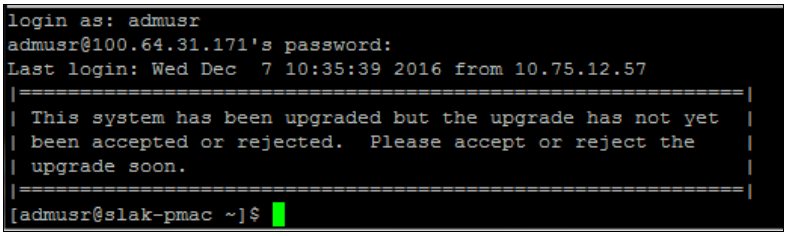
Step	Procedure	Details

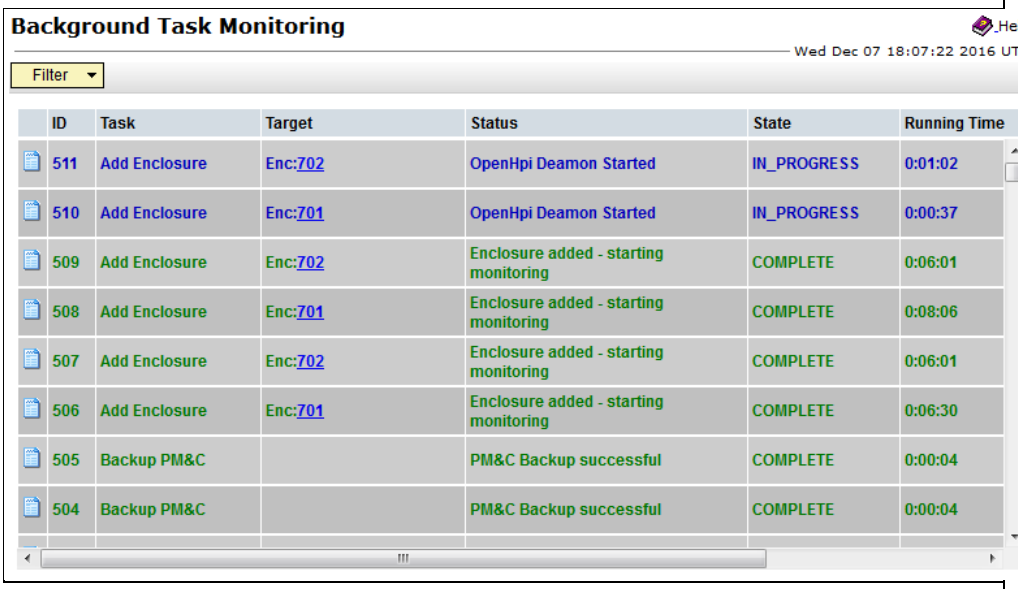
1. ☐	Start the PM&C guest	1. If not logged in to the TVOE host as admusr, log in.
		2. Start the PM&C guest if not started:
		3. Query the list of guests to check whether the PM&C guest is in running state.
		`$ sudo virsh list --all`
		`Id Name State`
		`----------`
		`1 <pmac_name> running`
		- If it is running, skip to the next step.
		- If it is not running, issue the following command.
		`$ sudo virsh start <pmac_name>`
		`Domain <pmac_name> started`

2. ☐	Close any active browser sessions to PM&C	If any open browsers are connected to PM&C, close them before proceeding

3. ☐	Login to the TVOE host as root	1. From the TVOE host CLI, issue the following command to log on to the PM&C guest as admusr:
		`$sudo virsh console <pmac_name>`
		NOTE: You may have to press **Enter** twice
		2. Verify the correct ISO file is located in the `/var/TKLC/upgrade` directory of the PM&C guest. If not, copy the PM&C ISO to `/var/TKLC/upgrade` on the PM&C guest.
		3. Verify by issuing the following command:
		`# ls -lth /var/TKLC/upgrade`

4. ☐	Run upgrade from PM&C Server	From PM&C guest as admusr (accessed via the TVOE virsh console in the previous step), run the platcfg utility: `# sudo su – platcfg`

Step	Procedure	Details
5. ☐	In the platcfg utility, select **Initiate Upgrade** to start the upgrade process	1. Open the platcfg utility and navigate to **Maintenance → Upgrade → Initiate Upgrade**. 2. Select **Initiate Upgrade** to start the upgrade process Wait for the Choose Upgrade Media Menu to open before proceeding to the next step  3. Select the new PM&C 6.0.3 target ISO filename and press **Enter** to start the upgrade process - The upgrade begins and after 20 minutes, the connection is lost as it reboots. - Do not take any action on the PM&C until the server reboots. The reboot takes approximately 5 minutes. - After you log back into PM&C, you see something similar to this: 

Step	Procedure	Details
6. ☐	**PM&C GUI:** Verify the upgrade after 30 minutes	1. Open a browser and type in the IP address of the PM&C server 2. Login as pmacadmin 3. Verify the release at the top of the page.  4. Navigate to the task manager and verify all tasks are complete. DO NOT proceed with the next step until all tasks are completed. Tasks still in progress: 
---End of Procedure---		

9.4 Verify PM&C Upgrade

Use this procedure to verify the success of the PM&C upgrade and perform other required post upgrade steps

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Step	Procedure	Details

7. ☐	Access PM&C guest console	1. Log on to TVOE host SSH as admusr.
		2. Verify that the PM&C console is running by issuing the following command:
		`$ sudo virsh list`
		`[admusr@brbg-tvoe-host ~]$ sudo virsh list`
		` Id  Name  State`
		`----------`
		` 1  brbgpmac  running`
		3. Log on to PM&C guest console by issuing the following command from the TVOE console:
		`$ sudo virsh console <pmac_name>`
		4. Remember to press **Enter** twice.
		NOTE: If you connected from the TVOE console, the guest session to PM&C is broken with CTRL+]

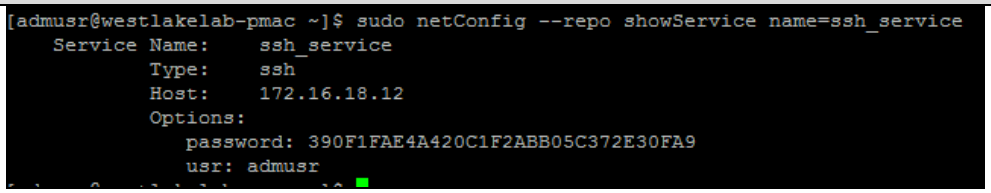
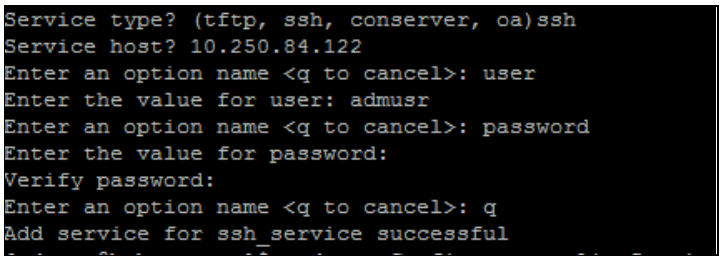
8. ☐	Verify the date/timestamp	Logged in to the PM&C console, run the following command
		`$ ls -l /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@slak-pmac ~]$ ls -l /var/TKLC/log/upgrade/upgrade.log`
		`-rw-rw-r-- 1 platcfg root 127103 Dec  7 11:51 /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@slak-pmac ~]$`
		And verify that the date and timestamps up the upgrade align with the actual time of the upgrade.

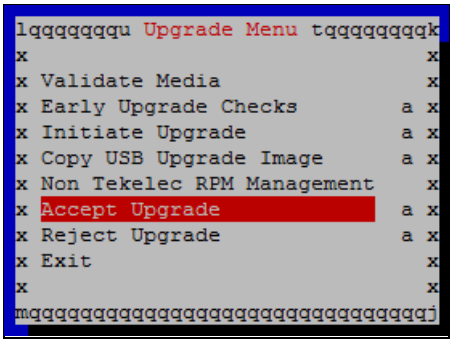
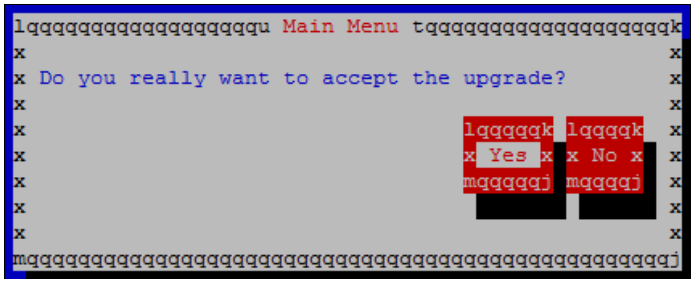
9. ☐	Verify that the release version has been updated	Run the following command and verify the release
		`$ appRev`
		`[admusr@slak-pmac ~]$ appRev`
		`  Install Time: Wed Dec  7 11:50:31 2016`
		`  Product Name: PMAC`
		`  Product Release: 6.0.3.0.2_60.28.0`
		`  Base Distro Product: TPD`
		`  Base Distro Release: 7.0.3.0.0_86.45.0`
		`  Base Distro ISO: TPD.install-7.0.3.0.0_86.45.0-OracleLinux6.7-x86_64.iso`
		`  ISO name: PMAC-6.0.3.0.2_60.28.0-x86_64.iso`
		`  OS: OracleLinux 6.7`

10. ☐	Verify successful completion through the upgrade log	Run the following commands on PM&C
		`$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@brbgpmac ~]$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`
		`1419272892::UPGRADE IS COMPLETE`
		`$sudo verifyUpgrade`
		NOTE: This command could take over a minute to complete. No output is expected, only the prompt should return. If there are messages, contact Oracle support.

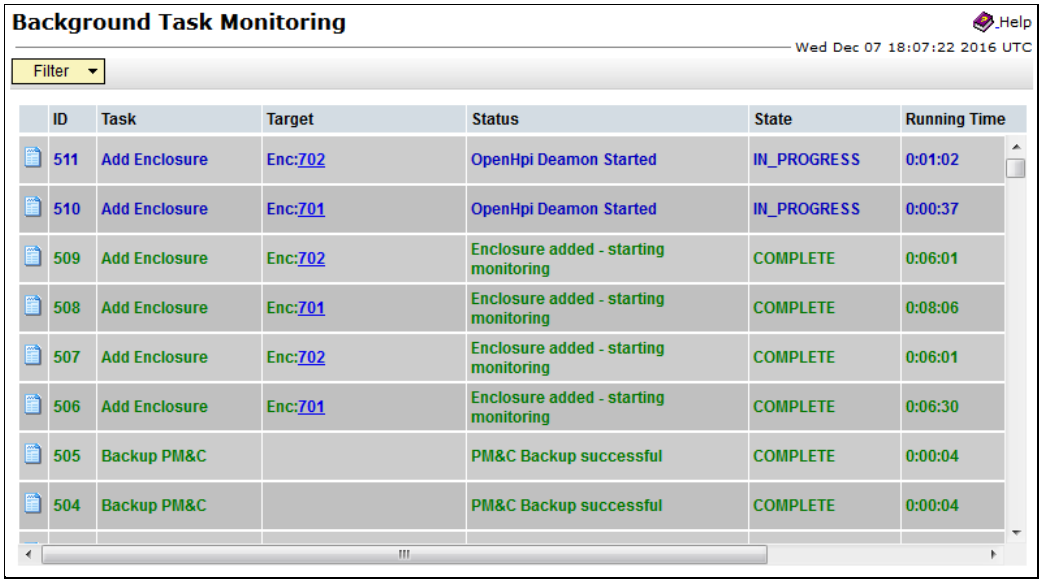
11. ☐	Run syscheck	Run syscheck and verify everything is OK. `$ sudo syscheck`
12. ☐	**PM&C SSH CLI:** Recreate the ssh_service with admusr	1. Verify that the ssh service exists with admusr credentials by running the following command: `$ sudo netConfig --repo showService name=ssh_service`

Step	Procedure	Details

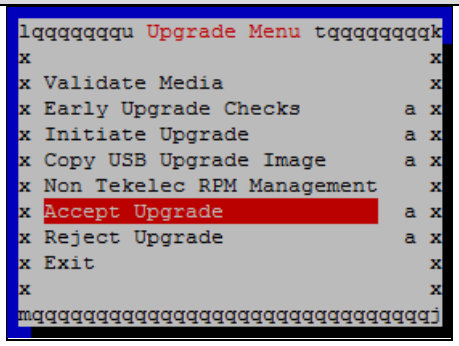
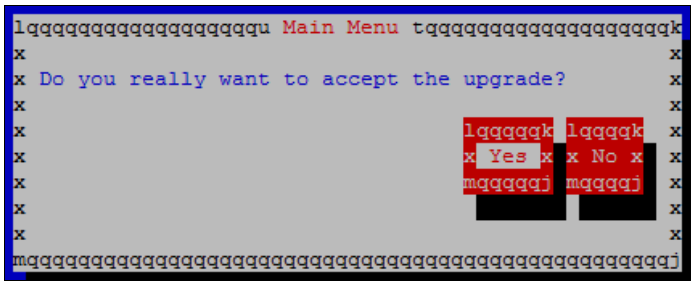
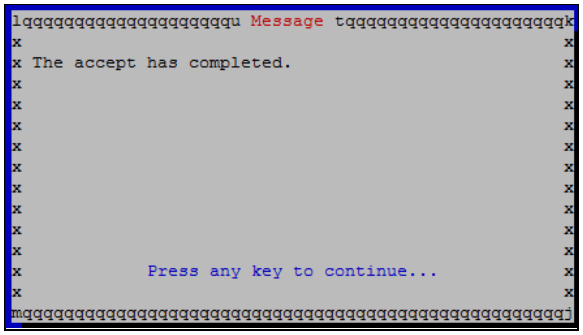
	credentials on PM&C guest console if it does not exist	
		- If the results are similar to the above, that is, the Options section includes:
		▪ usr: admusr
		▪ An encrypted password.
		Skip to the next step.
		- If the results do not include the usr: admusr option or if the service does not exist, continue with this step:
		2. Delete the ssh_service if it exists
		`$ sudo netConfig --repo deleteService name=ssh_service`
		3. Answer YES to the message if prompted.
		4. Recreate ssh_service with admusr.
		`$ sudo netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <pmac_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: admusr`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: Duk******`
		`Verify Password : Duk******`
		`Enter an option name(q to cancel): q`
		Example output
		 
		5. Ensure the information entered is correct by running the following command and compare the output with the configuration in the last step.
		`$ sudo netConfig --repo showService name=ssh_service`
		Example output
		 

Step	Procedure	Details
13. ☐		If ALL health checks passed, accept PM&C server and TVOE upgrades. If health checks do not pass or a backout is needed, skip to Appendix B to reject/backout the upgrade in entirety. This includes both the PM&C server and the TVOE host.
14. ☐	Accept the upgrade for PM&C **NOTE:** Accept takes approximately 5 minutes	1. Close any open PM&C GUI browsers **NOTE:** After accepting the upgrade, you are not able to roll back to the previous release. 2. Login to PM&C guest console 3. Run the platcfg utility. `$ sudo su - platcfg` 4. Navigate to **Maintenance → Upgrade → Accept Upgrade**.  5. Select **Accept Upgrade** and press **Enter**.  6. Click **Yes** to start accept upgrade process. If a message shows up prompting to hit any key to continue, DO NOT hit any key, the server reboots on its own. The connection is lost while the PM&C reboots (approximately 5 minutes).

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>15. ☐</td><td>Health Checks</td><td>
1. Run the syscheck command.
<pre>$sudo syscheck</pre>
2. Open a browser and launch the PM&C GUI.
3. Verify the release at the top of the page.


4. Navigate to Task Manager and monitor as tasks complete. DO NOT continue to the next step until all tasks are complete. It may take more than 5 minutes to complete.


</td></tr>
<tr><td>16. ☐</td><td>Accept the upgrade for TVOE</td><td>
NOTE: It is recommended not to accept the TVOE upgrade until after the PM&C upgrade has been accepted for the following reasons:
• Some older PM&C releases cannot be deployed on upgraded TVOE 3.0.3 system.
• If issues occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade has to be rejected to allow older PM&C to be re-deployed.
• A reject cannot be performed after an upgrade has been accepted.
NOTE: Once the upgrade is accepted, you are not be able to roll back to the previous release.
1. Login as admusr to TVOE host CLI and run the platcfg utility:
<pre>$ sudo su - platcfg</pre>
2. Navigate to Maintenance → Upgrade → Accept Upgrade.
</td></tr>
</table>

Step	Procedure	Details
		 3. Select **Accept Upgrade** and press **Enter**.  4. Click **Yes** to start accept upgrade process. **NOTE:** A session is launched when accepting the upgrade, press **q** to close the window and return to platcfg.  5. Click **Exit** or press **F12** until exiting platcfg. The upgrade process is now complete.
---End of Procedure---		

A.1 TVOE and PM&C Server Backout

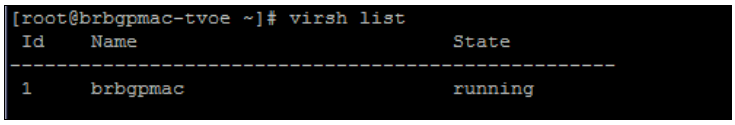
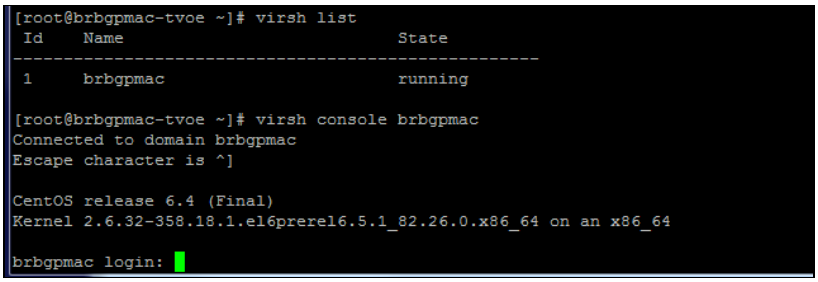
Use this procedure to backout/reject the PM&C server upgrade.

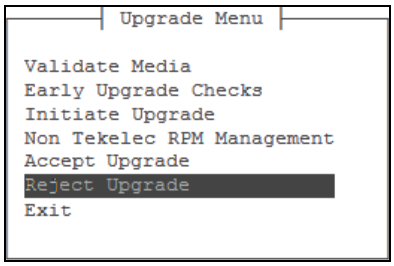
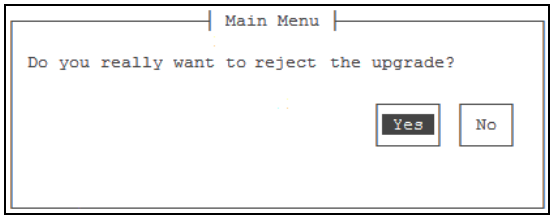
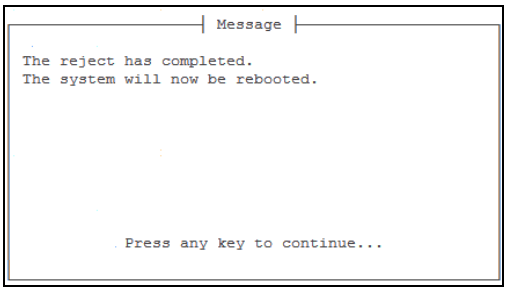
NOTE: A reject cannot be performed after an upgrade has been accepted.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Step	Procedure	Details
1. ☐	Close any active browser sessions of PM&C	Close any open browsers connected to PM&C before proceeding.

Step	Procedure	Details

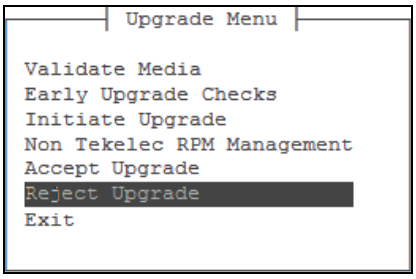
2. ☐	If necessary, access PM&C guest console	1. Log on to TVOE host as admusr.
		2. Verify PM&C console is running by issuing the following command
		`$sudo virsh list`
		 
		3. Log on to PM&C guest console by issuing the following command
		`$sudo virsh console <pmac_name>`
		 
		4. Log on to PM&C as admusr if needed – may not require a login.
		`Last login: Wed Jun 6 08:39:14 on ttyS0`
		`|============================================================|`
		`| This system has been upgraded but the upgrade has not yet |`
		`| been accepted or rejected. Please accept or reject the |`
		`| upgrade soon. |`
		`|============================================================|`
		`[admusr@pmac approximately]$`
		NOTE: To break the guest session to go back to TVOE host, press CTRL+]

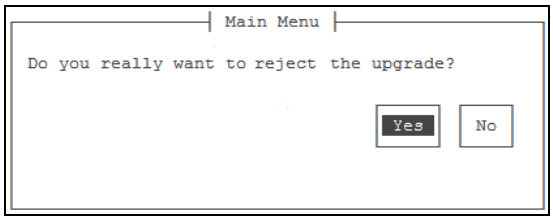
Step	Procedure	Details
3. ☐	Run platcfg utility on the PM&C Server	1. At the prompt, run: `$sudo su - platcfg` 2. Navigate to **Maintenance → Upgrade**  3. Select **Reject Upgrade** and press **Enter** to start the reject process. 4. The following window opens, click **Yes** to begin the backout.  **NOTE:** 5 minutes into the backout, a reboot completes the backout, the system reboots automatically.
4. ☐	Backout requires reboot	The following image is only for illustrative purposes **NOTE:** DO NOT press any key when the window prompts, the system reboots on its own.  **NOTE:** From this point on, it takes approximately 20 minutes to complete the backout.
5. ☐	Wait for PM&C login prompt	After the successful completion of backout, you are returned to a login prompt. Login as admusr.

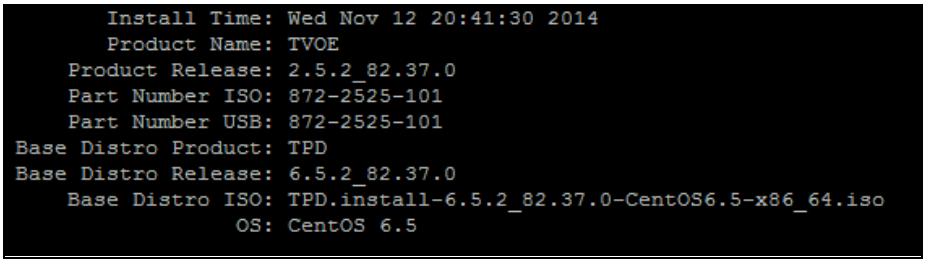
Step	Procedure	Details

6. ☐	Verify backout completed	Run the following command to verify source PM&C release :
		`[admusr@pmac approximately]# appRev`
		`Install Time: Thu Nov 13 10:04:56 2014`
		`Product Name: PMAC`
		`Product Release: 5.5.2_55.20.0`
		`Part Number ISO: 872-2586-102`
		`Part Number USB: 872-2586-102`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.5.2_82.37.0`
		`Base Distro ISO: TPD.install-6.5.2_82.37.0-CentOS6.5-x86_64.iso`
		`OS: CentOS 6.5`
		If the correct Product Release is not displayed, contact Oracle Customer Service and do not proceed until instructed by an Oracle Customer Care representative.

7. ☐	TVOE iLo SSH	1. As Administrator on the TVOE iLO – log in through the iLO and run the following command to check the logical drives that is used for the backout.
		2. Login as admusr to the TVOE console
		`$sudo /sbin/lvs -o lv_name,snap_percent @upgrade`
		Typical output:
		`LV snap %`
		`plat_root_snap 27.52`
		`plat_usr_snap 7.70`
		`plat_var_snap 5.08`
		`plat_var_tklc_snap 19.14`
		NOTE: Anything below 50% is OK.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>8. ☐</td><td>TVOE Server iLO:
manually backout upgrade</td><td>1. At the prompt run:
<pre>$sudo su - platcfg</pre>2. Navigate to Maintenance → Upgrade.
 

3. Select Reject Upgrade and press Enter to start the reject process.
4. The following window opens, click Yes to begin the backout.
 

The system undergoes a backout. As part of the process the system reboots several times.
After completing the final reboot the login prompt is presented. Some of the final startup output along with an example of the login prompt is shown below:
5. Login as admusr.
<pre>CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.16.0.x86_64 on an x86_64
hostname1342210584 login:</pre></td></tr>
<tr><td>1.</td><td>TVOE Server iLO:
check server health.</td><td>1. Log in and run the following:
<pre># appRev</pre> 
</td></tr>
<tr><td>9. ☐</td><td>TVOE Server iLO:
check server health</td><td>Run the following command to check the health of the server:
<pre># sudo alarmMgr --alarmStatus</pre>If any output is produced, an alarm is present on the system. Contact Oracle for information about how to proceed.</td></tr>
<tr><td>10. ☐</td><td>Clear browser cache</td><td>Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary.</td></tr>
</table>

Step	Procedure	Details
11. ☐	**PM&C GUI**	Login to the PM&C GUI to verify the old PM&C version
---End of Procedure---		

APPENDIX A. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE AND HOTLINES

Access to the Oracle Customer Support site is restricted to current Oracle customers only. This section describes how to log into the Oracle Customer Support site and link to Oracle Support Hotlines

1. Log into the Oracle Customer Support site at https://support.oracle.com
2. Refer Oracle Support Hotlines http://www.oracle.com/us/support/contact/index.html and http://www.oracle.com/us/corporate/acquisitions/tekelec/support/index.html