Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management 12.1.x or 12.2.x to 12.3 Cloud Upgrade Procedure, Georedundancy Enabled

E85338-01

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.

Oracle Communications Oracle Communications Policy Management 11.5.x/12.1.x to 12. 2 Upgrade Procedure Georedundancy Enabled

TABLE OF CONTENTS

List of Figures

List of Tables

1. INTRODUCTION

1.1 Purpose and Scope

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

- Upgrade of firmware is 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, is unaffected by the same circumstances and is able to continue to provide service as an Active server.

1.2 Acronyms

Acronym	Definition
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
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 Virtual Operating Environment
UE	User Equipment

1.3 Terminology

Term	Definition
Primary Site (Site1)	Site where the MPE/MRA/Mediation Server-A and Server-B are deployed.
Secondary Site (Site2)	Site where the MPE/MRA/MA/Mediation 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.
Segment	A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster can be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.

1.4 Software Release Numbering

- 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 perform Policy Management release 12.3 software upgrades.

2.1 Upgrade Status Values

Status	Condition
OK	All servers are up-to-date and no alarms are present.
Info	No alarms are present, but a condition (such as out-of-date) is present that 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:

1. Policy Management 12.2.x to 12.3
2. Policy Management 12.1.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 or MA:

- For a CMP cluster, there are only 2 servers (Active and Standby) in a cluster and the cluster is either a Primary or Secondary cluster.
- For a non-CMP cluster (MRA/MPE/Mediation), 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 Server software upgrades are performed on a cluster by cluster basis at the local and remote sites within the same maintenance window.

Software Upgrade Procedure
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—Needed if version is older than what is listed in Section 1.4
2. Upgrade PM&C Server at Site 2—Needed if version is older than what is listed in Section 1.4
3. Firmware upgrade—If needed (not covered in this document)
4. Upgrade Primary 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 4 non-CMP clusters can be upgraded in parallel.

2.3.2 Policy Release Mixed-Version Operation and Limitation

The general expectation is that a system that is running in a mixed version configuration should support features, and perform at a level of the previous version. Thus, 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 the customer and Oracle before deployment to verify that these policies indeed do not use new conditions or actions.
- The support for configuration of MPE/MRA/MA 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	MA R12.3
CMP 12.2.x	Yes	No	No	No
MRA 12.2.x	Yes	Yes	Yes	N/A
MPE 12.2.x	Yes	Yes	Yes	Yes
MA 12.2.x	Yes	N/A	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 once 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.

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 perform an upgrade:

1. Policy 12.3 software ISO files and TPD software ISO
2. Policy 12.3 software Release Notes.
3. TVOE, PM&C upgrade/installation documentation, software ISO files and TPD ISO (if applicable).

4. HP Solutions Firmware Upgrade Pack 2.2.9 (or higher) documentation and ISO files (if applicable).
5. 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 the customer network firewall policy allows the required application and corresponded ports.
6. The capability to secure copy (`scp`) from the local workstation being used to perform this upgrade to the target server, or otherwise be able to transfer binary files to the target server.
7. User login IDs, passwords, IP addresses, and other administration information.
8. 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 Manager GUI, and the PM&C GUI.

2.9.1 Upgrade Media

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

2.9.2 Login 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 SSH login.	GUI Administrator Login User/Password
	admusr password:
MPE/MRA/Mediation	**admusr** password:
Target iLO	iLO Administrator Login User/Password
Target OA	OA Administrator Login User/Password
PM&C server	GUI Administrator Login User/Password
	admusr password
Software Upgrade Target Release[1]	Target Release Number
	Policy 12.3 software ISO image 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 a 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

1. Begin/continue upgrading a cluster
2. 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 no longer 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 first.

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.

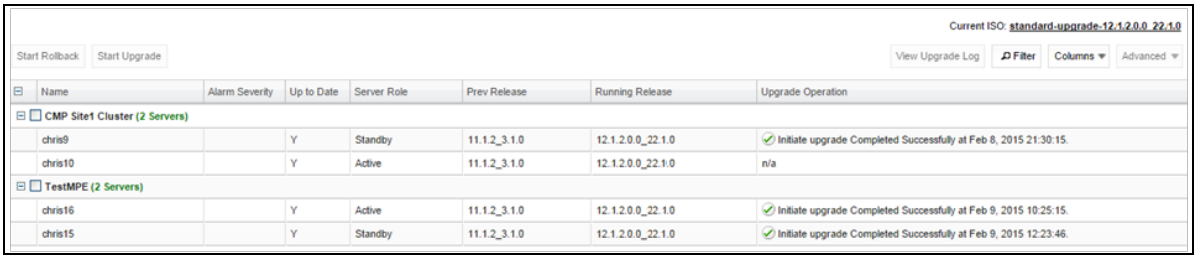


Figure 1 Sample display of the Upgrade Manager page

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

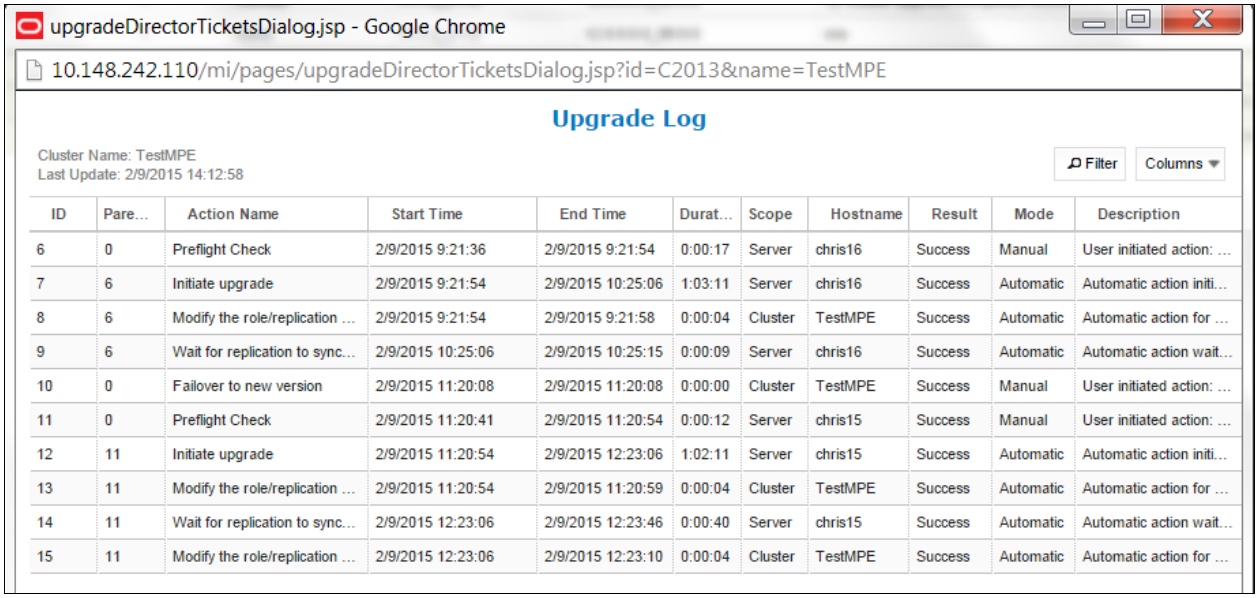
- **Start Rollback** and **Start Upgrade** buttons (upper left): If a cluster is selected and these buttons are disabled (grey), it means that there is not an appropriate action to take at this time. However, if a button is not disabled (white), then it means that there is a preferred action that can 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 report alarms to indicate that their mate servers are offline.

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

- **Up to Date:** This column is used to indicate the state of the code on the server.
  - N—Server is running old code needs to 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 be 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:

- A standard (full) upgrade to version *XXX*
- An incremental 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. From a user perspective, the Upgrade Director is hidden. However, there are conventions/operating principles that have visible effects.

3.1.4.1 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.

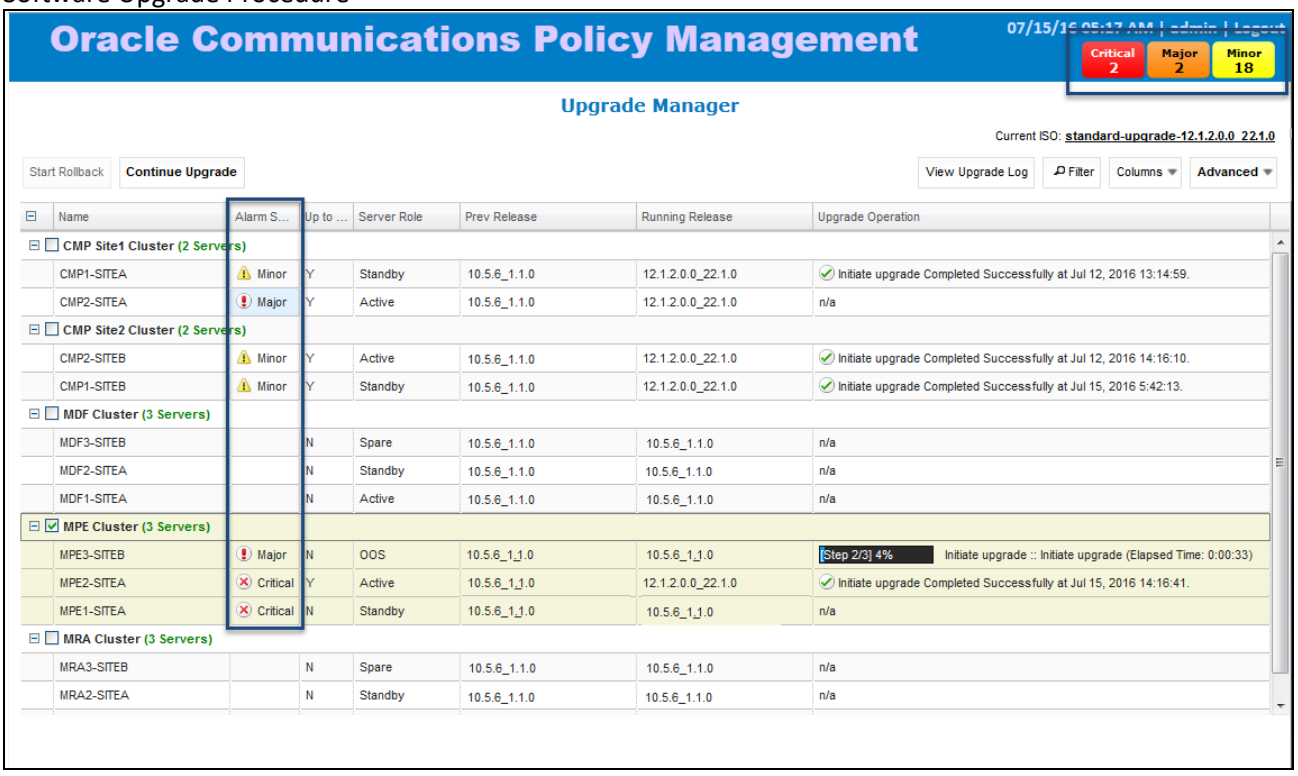


Figure 3 Upgrade in Progress Showing Transient Alarms

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

[2] The name of alarm 31283 changed in 12.2.2: Before 12.2.2, it was "HA Server Offline," with 12.2.2 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.

Alarm Number	Severity	Name
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.

3.1.4.2 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
   a. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.
   b. Preflight checks are VERY narrow. This prevents false positives for an otherwise valid upgrade.
2. The upgrade itself
3. Wait for replication to synchronize.

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

3.1.4.3 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

3.1.4.4 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.

3.1.4.5 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.

3.1.4.6 Mixed version and Forced Standby

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

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

3.1.4.7 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 execution. These procedures are performed 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:

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

4.1 Pre-requisites

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

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

Step	Procedure	Result
1. ☐	Verify all required materials are present	As listed in section 2.9, "Required Materials and Remote Access"
2. ☐	Review Release Notes	Review Policy 12.3 Release Notes for the following information: • Individual software components and versions included in target release. • New features included in target release. • 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 12.2, 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 and higher 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:

Prerequisites:

1. TVOE and PM&C Server upgraded. Firmware upgrade deployed if necessary.
2. Upgrade CMP clusters
3. Upgrade MPE/MRA clusters

Table 4 can be completed first before performing the upgrade, to identify the clusters to be upgraded and plan the work. It can also be used to track the completion of the upgrades, and assign work to different engineers.

NOTES:

- Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.
- Time estimates are for upgrade 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
3. ☐	Upgrade Site1 and Site2 CMP clusters. Each cluster takes approximately 90 minutes 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 user-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 12.2, Manual statistics is no longer available. You must migrate to Interval statistics before upgrading to Release 12.2. After the upgrade to R12.2, Oracle Communications Policy Management uses Interval statistics only and any Manual statistics not saved are lost.

Statistics affected by this change are reset to zero when migrating to Interval statistics. This affects both the information presented 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:

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

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

For addition information, see the following publications:

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

4.6 Perform System Health Check

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

Step	Procedure	Result
1. ☐	CMP GUI Access	Open a supported browser (Mozilla Firefox or Google Chrome) to access the Primary CMP GUI on its VIP address and login to verify access.
2. ☐	View Active Alarms	Identify the cause of any existing active alarms, and determine if these may have impact on the upgrade. Export current alarms to save into a file. ***IMPORTANT: Before starting any upgrade activity, ensure that all active alarms are understood and resolved.***
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 first 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:
		`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:
		`hwclock`

---End of Procedure---		

4.7 Deploy Policy Upgrade Software

Software should be deployed to each Policy server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This is typically done 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 Upgrade Software to Servers

There are six possible software images in this upgrade (CMP, MPE, MPE-LI, MRA, 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, Mediation) does not match the existing installed software type, the upgrade fails. Example: An attempt to upgrade a CMP with a MPE software image fails during the Upgrade action.

NOTE: To change a server from one application type to another, the server must first be cleaned of all application software by an Install OS action 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.

This procedure transfers 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 the upgrade activities. The purpose of this procedure is to be prepared for server recovery activities in case a server needs to be re-installed with software.

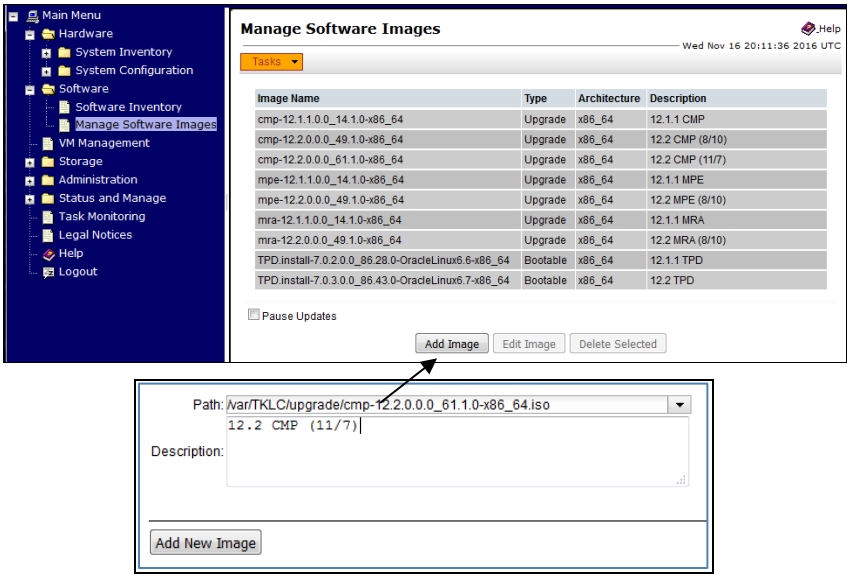
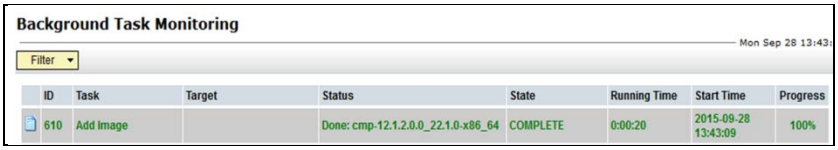
NOTES:

- 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 there are no release 12.3 ISO files 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	Transfer all release 12.2 ISO files (CMP and non-CMP) into directory `/var/TKLC/upgrade` using one of the following methods: • 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	**Software → Manage Software Images** 1. Click **Add Image** to select the ISO files that were transferred to the PM&C server.  2. Click **OK** on the confirmation dialog.
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 screen 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 are electronically copied to the sites to be upgraded.

NOTE: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to 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 server.	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 If the images are on a server in the same network, `scp` the files using the CLI, for example, for CMP: • Copy CMP software ISO file to ONE of the other CMP servers: `$sudo scp cmp-12.2.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/` Repeat for one server of all clusters. **NOTE:** After copying the ISO to one of the respective servers, the ISO Maintenance function 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:

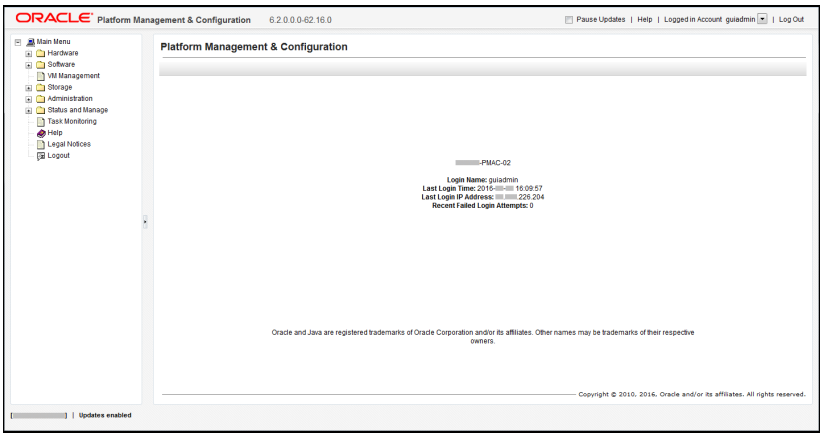
- The URL of the PM&C server and the `guiadmin` password
- The Policy Management ISO files, loaded into the directory `/var/TKLC/upgrade` on the PM&C server

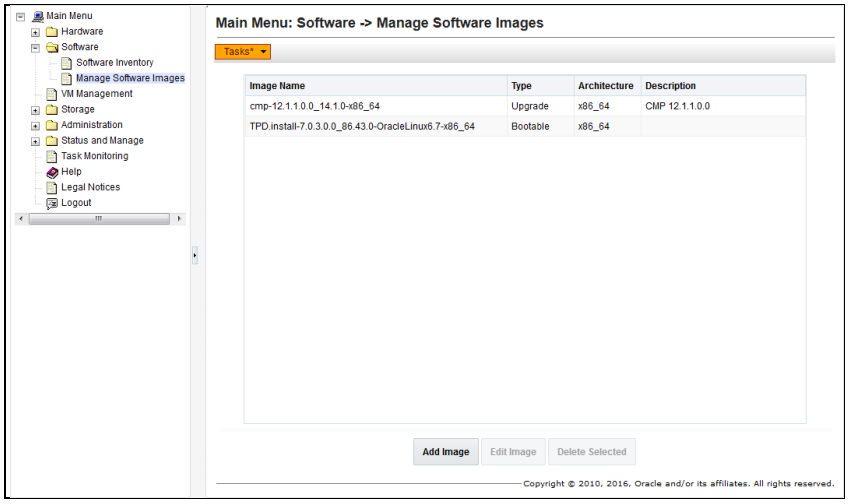
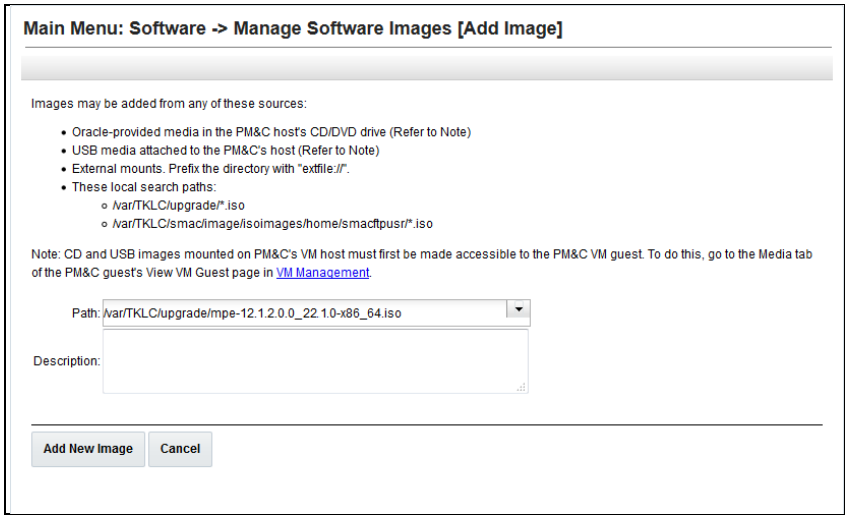
NOTE: You can instead add images from the following sources:

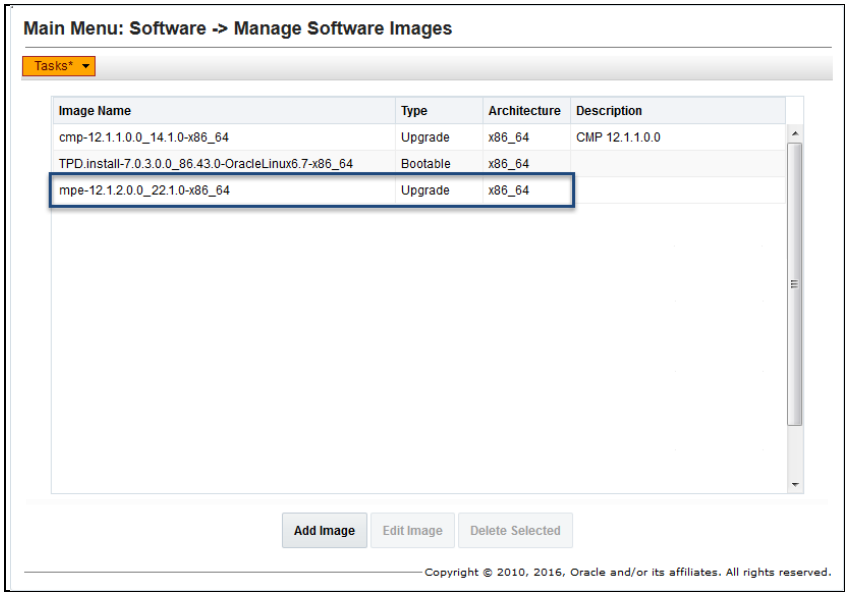
- Media mounted in the CD/DVD drive of the PM&C host
- USB media attached to the PM&C host
- External mounts (prefix the directory with `extfile://`)
- These local search paths:
  - `/var/TKLC/upgrade/`
  - `/var/TKLC/smac/image/isoimages/home/smacftpusr/`

NOTE: CD, DVD, and USB images mounted on the PM&C VM host must first 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.

The following procedure assumes the ISO file is located in the directory `/var/TKLC/upgrade` 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. Select **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** dropdown 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 the **Tasks** dropdown list to check the progress of the task. When the upload is complete, the ISO file displays in the list. For example: 

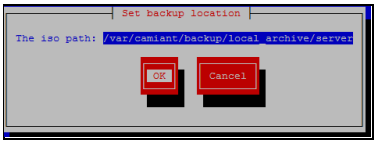
4. ☐	Verify that the image is no longer in the directory	Enter the following command:
		`$ sudo ls /var/TKLC/upgrade`
		`$`

5. ☐	Load addition files	If you are loading multiple ISO files into the image repository, repeat steps 2 through 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.

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. Navigate to the following through platcfg utility.
		
		`$sudo su - platcfg`
		
		3. **Policy Configuration→Backup and Restore→Server Backup**
		
		Provide (or use the suggested) ISO backup filename in the default backup location path of:
		
		`/var/camiant/backup/local_archive/serverbackup/<filename>.iso`
		
		 
		
		4. Go back to the previous menu (**Policy Configuration → Backup and Restore)** and select **System Backup**
		
		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-_12.2.x…x-serverbackup-<yyyy><mm><dd><hhmm>.iso`
		And for the system backup:
		`$ cd /var/camiant/backup/local_archive/systembackup`
		`$ ls <hostname>-cmp_12.2.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	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 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-12.2.1to 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 are hashed with the strongest possible method, SHA512.

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

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

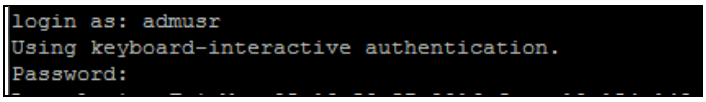
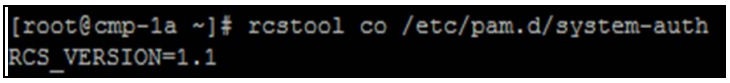
Order to perform the upgrade on an In-Service Policy Management system:

1. Standby CMP servers
2. Active CMP servers
3. Standby MPE/MRA/Mediation servers
4. Spare MPE/MRA/ Mediation servers
5. Active MPE/MRA/ Mediation servers

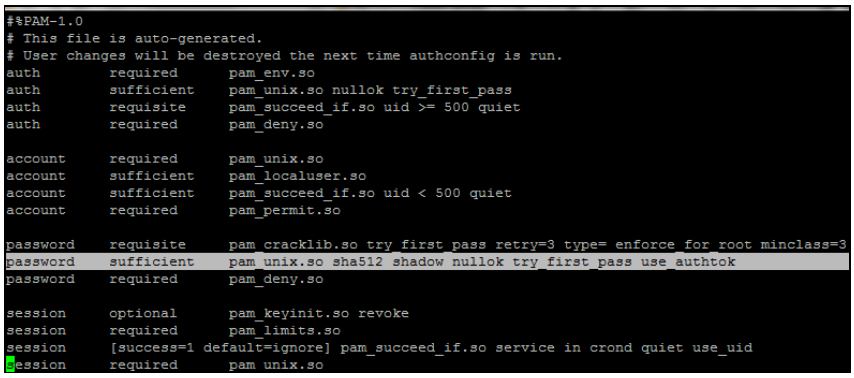
Step	Procedure	Result
1. ☐	Login to the active CMP server	For an upgrade from 12.2.x, login as admusr and change to root using the following command: **$**sudo **su** login as: admusr Using keyboard-interactive authentication. Password:

Step	Procedure	Result

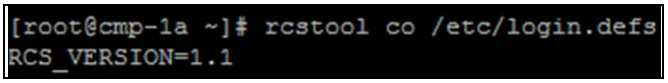
2. ☐	Check the password field of root and admusr	Issue the following
		`#egrep '^(root|admusr)' /etc/shadow`
		EXAMPLE OUTPUT
		`root:$6$mErKrEsA$83n5G8dR3CgBJjMEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc.Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7:::`
		`admusr:$6$mUstAfa$gn2B8TsW1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825::::::`
		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	For an upgrade from 12.2.x/12.2.x, login as admusr and change to root using the following command: `$sudo su` 
5. ☐	Checkout revisions	Issue the following command: `#rcstool co /etc/pam.d/system-auth` 

Step	Procedure	Result

6. ☐	Modify the `system-auth` file	1. Open the `system-auth` file.
		`#vi /etc/pam.d/system-auth`
		2. Modify the file. Change the 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`
		 

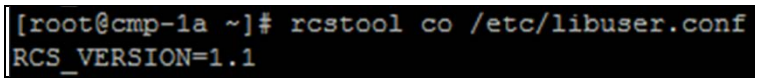
7. ☐	Save the file	• If the file required changing:
		`#rcstool ci /etc/pam.d/system-auth`
		• If the file was already configured:
		`#rcstool unco /etc/pam.d/system-auth`

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

9. ☐	Edit `login.defs` file	**Shadow password suite configuration**
		3. Open the `login.defs` file.
		`#vi /etc/login.defs`
		4. 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.
		5. Comment out the following line if necessary.
		`MD5_CRYPT_ENAB yes`

Step	Procedure	Result

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

11. ☐	Checkout revisions for the `libuser.conf` file	Checkout the file. `# rcstool co /etc/libuser.conf` 

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 already was configured
		`#rcstool unco /etc/libuser.conf`

14. ☐	Set the admusr and root passwords	• For root user
		`#passwd root`
		• For admusr user:
		`#passwd admusr`
		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 (12.2.X TO 12.3)

This procedure upgrades the Site1 CMP cluster first, and if needed, upgrade the Site2 CMP cluster in a single maintenance window.

5.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster
    a. Start upgrade
    b. Failover
    c. Log back into the CMP GUI
    d. Continue upgrade
2. Upgrade Secondary CMP cluster
    a. Start upgrade
    b. Failover
    c. Continue upgrade

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

It is assumed that the CMPs may be deployed as 2 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 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.

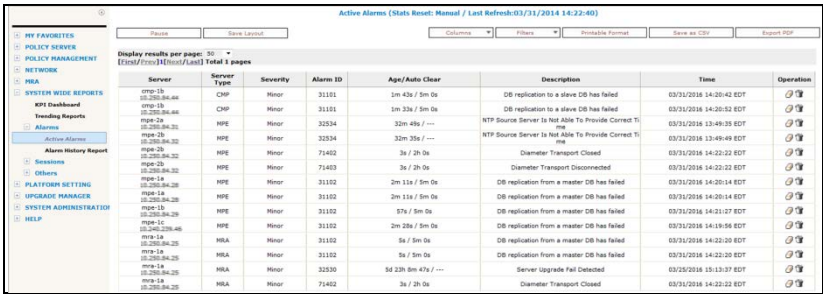
Identify the CMP sites to be upgraded, and verify which site is the Primary site and which site is the Secondary site:

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:

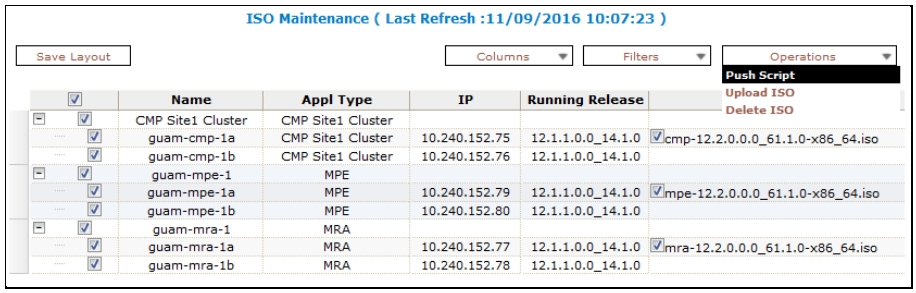
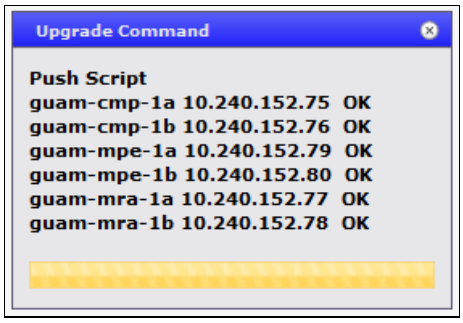
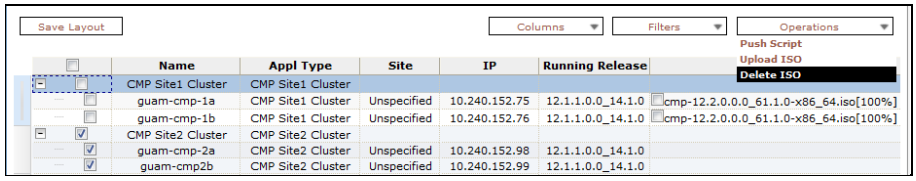
- Site1 CMP MUST be upgraded to the new release first, before the Site2 CMP
- CMP servers MUST be upgraded first, before the non-CMP clusters

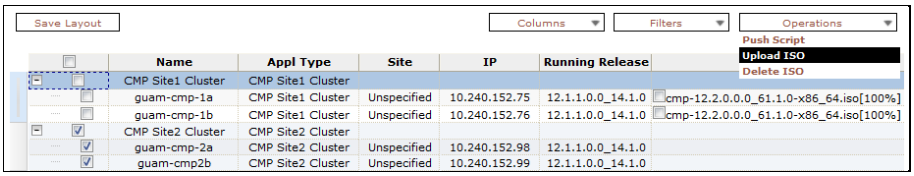
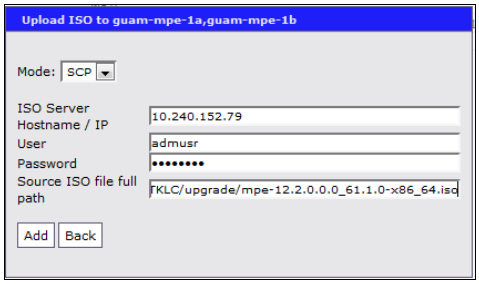
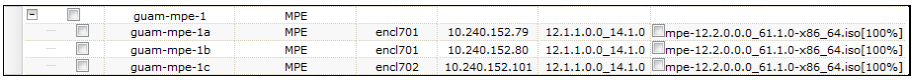
5.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	**System Wide Reports → Alarms→Active Alarms** • Confirm that any existing alarm is well understood and is ono impact to the upgrade procedure. • Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and record the CMP clusters	1. Navigate to **Platform Setting→Topology Settings → 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**. 4. Verify that release 12.3 ISO files are on at least one of each server types (CMP/MRA/MPE/Mediation)—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

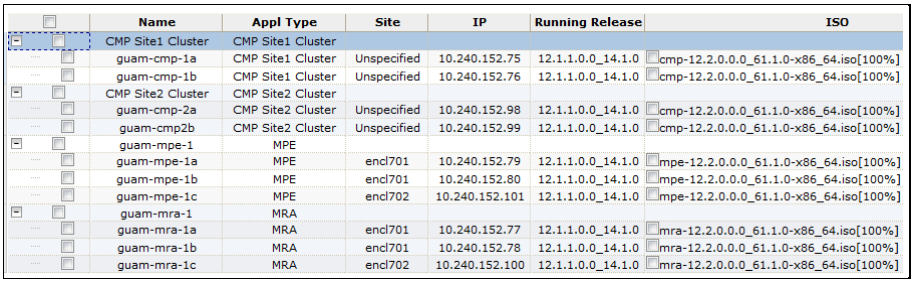
4. ☐	**SSH CLI Primary Active CMP:** Exchange Keys	1. Exchange keys to all servers from the Site1 (Primary) Active CMP.
		2. Login as admusr user and run the following command:
		`$sudo qpSSHKeyProv.pl --prov`
		`[admusr@guam-cmp-1a ~]$ sudo qpSSHKeyProv.pl -prov`
		`The password of admusr in topology:`
		3. Enter the password for user admusr
		4. Ensure that the keys are exchanged successfully with all the server clusters:
		`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.`

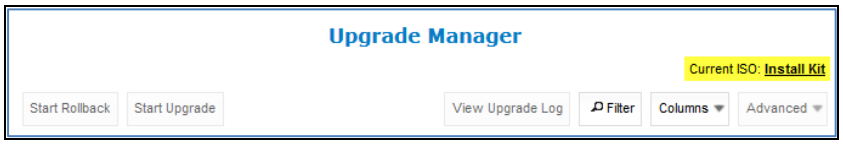
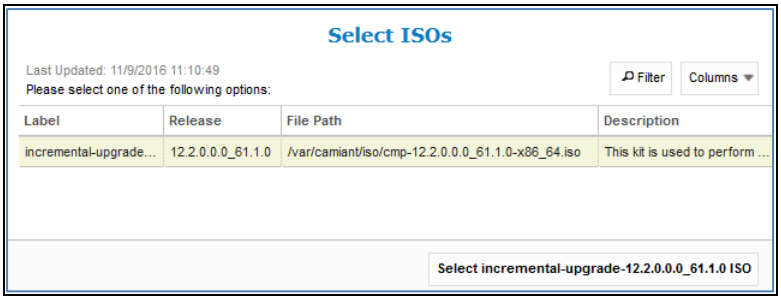
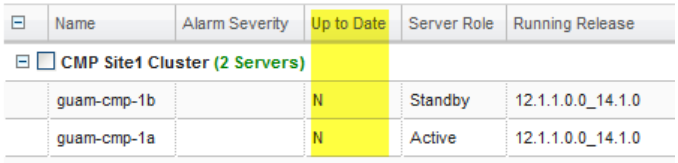
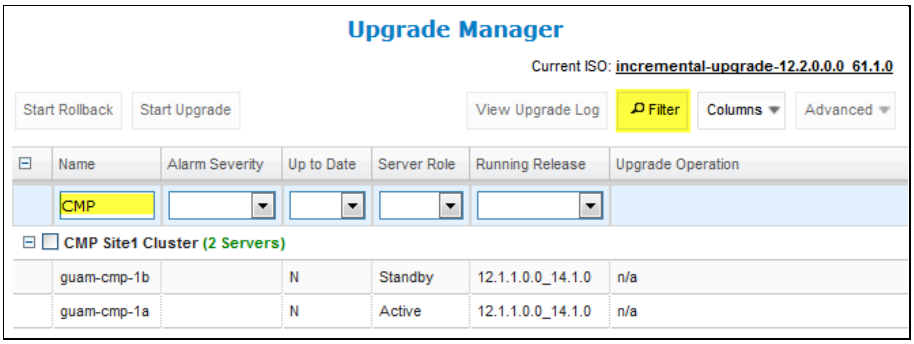
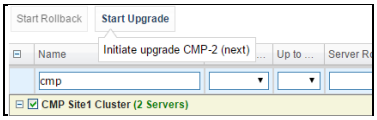
Step	Procedure	Result
5. ☐	**CMP GUI:** Push the Release 12.2 upgrade scripts to all servers	1. Navigate to **Upgrade → ISO Maintenance**. 2. Select all the servers in the topology as shown. 3. Select **Operations → Push Script**.  4. At the popup warning to execute Push Script click "OK" to continue the operation. After approximately a minute, a successful information window similar to this displays: 
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 and select **Operations →Delete ISO** to remove any older ISO files.  4. Click **OK** to continue and wait until seeing the successful deletion message 5. Wait until the ISO Maintenance page is refreshed and the ISO column doesn't show any old ISOs.

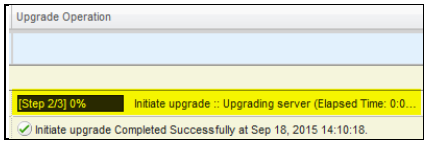
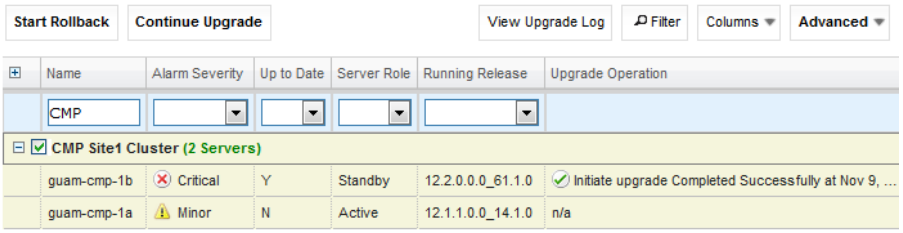
Step	Procedure	Result
7. ☐	CMP GUI: Distribute ISO files to CMP/MPE /MRA/etc., servers **NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly.	1. Navigate to **Upgrade → ISO Maintenance**. 2. Filter by server type (optional, but preferred step) 3. One application at a time, select one server type (CMP, MPE, etc.) to be upgraded. **NOTE:** The ISO files for each application type must already 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%]  Repeat for all cluster types.

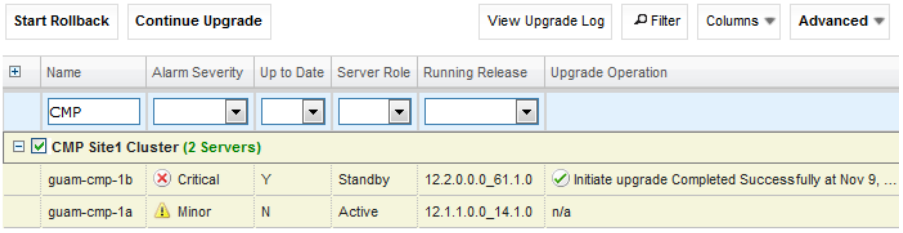
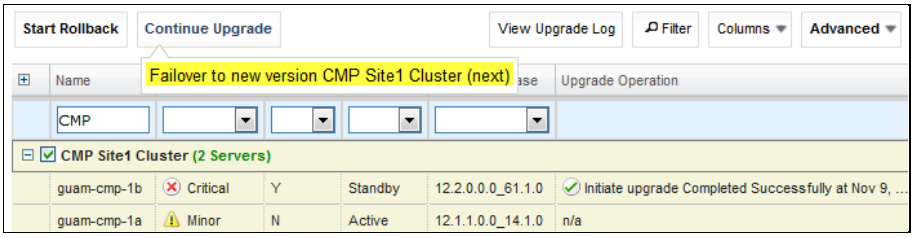
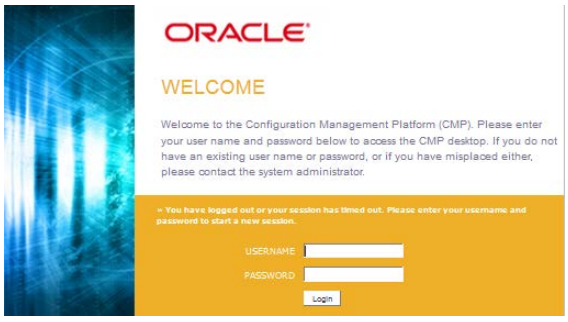
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>8. ☐</td><td>CMP GUI: Verify ISO distribution to all the server</td><td>1. Navigate to Upgrade → ISO Maintenance.
2. Verify that the release 12.3 ISO file of the correct type is shown for each server.
3. When completed, the ISO column is populated with the ISO filename and a notification of [100%]

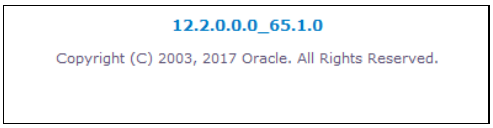
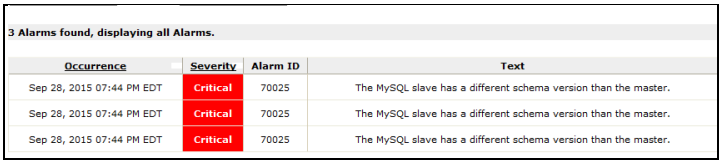
NOTE: For those servers where the ISO file was copied from the local machine, there is not a 100% indicator. This indicator is only available when transferring ISO files using the ISO management feature.

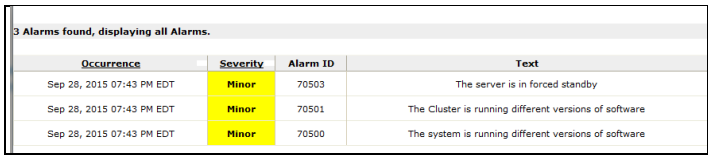
 
<table>
<tr><th></th><th>Name</th><th>Appl Type</th><th>Site</th><th>IP</th><th>Running Release</th><th>ISO</th></tr>
<tr><td>CMP Site1 Cluster</td><td>CMP Site1 Cluster</td><td></td><td></td><td></td><td></td></tr>
<tr><td>guam-cmp-1a</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.240.152.75</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-cmp-1b</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.240.152.76</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>CMP Site2 Cluster</td><td>CMP Site2 Cluster</td><td></td><td></td><td></td><td></td></tr>
<tr><td>guam-cmp-2a</td><td>CMP Site2 Cluster</td><td>Unspecified</td><td>10.240.152.98</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-cmp2b</td><td>CMP Site2 Cluster</td><td>Unspecified</td><td>10.240.152.99</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mpe-1</td><td>MPE</td><td></td><td></td><td></td><td></td></tr>
<tr><td>guam-mpe-1a</td><td>MPE</td><td>encl701</td><td>10.240.152.79</td><td>12.1.1.0.0_14.1.0</td><td>mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mpe-1b</td><td>MPE</td><td>encl701</td><td>10.240.152.80</td><td>12.1.1.0.0_14.1.0</td><td>mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mpe-1c</td><td>MPE</td><td>encl702</td><td>10.240.152.101</td><td>12.1.1.0.0_14.1.0</td><td>mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mra-1</td><td>MRA</td><td></td><td></td><td></td><td></td></tr>
<tr><td>guam-mra-1a</td><td>MRA</td><td>encl701</td><td>10.240.152.77</td><td>12.1.1.0.0_14.1.0</td><td>mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mra-1b</td><td>MRA</td><td>encl701</td><td>10.240.152.78</td><td>12.1.1.0.0_14.1.0</td><td>mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td>guam-mra-1c</td><td>MRA</td><td>encl702</td><td>10.240.152.100</td><td>12.1.1.0.0_14.1.0</td><td>mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
</table></td></tr>
<tr><td>9. ☐</td><td>Primary Active CMP: ssh to primary active CMP and copy iso to /var/camiant/iso</td><td>1. Logon to the primary active CMP as admusr and copy the 12.3 ISO file to the <code>/var/camiant/iso</code> directory:
<code>$sudo cp /var/TKLC/upgrade/cmp-12.2.x…x.iso /var/camiant/iso/</code>
2. Verify the copy by using the following command:
<code>$ ls /var/camiant/iso/</code></td></tr>
</table>

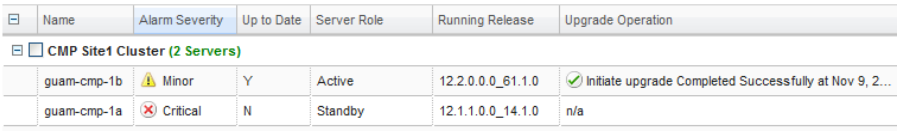
Step	Procedure	Result
10. ☐	**CMP GUI:** Locate the new 12.3 upgrade manual	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the **Current ISO**. In this case it is labeled Install Kit.  A dialog box with a description of the ISO file that was copied into the `/var/camiant/iso` directory opens. 3. Highlight the ISO file and click **Select incremental-upgrade-12.2…** located in the bottom right corner of the window.  4. When the confirmations message displays, click **OK**. Within a few seconds, the Up to Date column transition 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**. 2. (Optional) Click **Filter** and enter `CMP` in the Name field.  3. Select the checkbox for the Primary CMP Server cluster 4. Click **Start Upgrade**. 

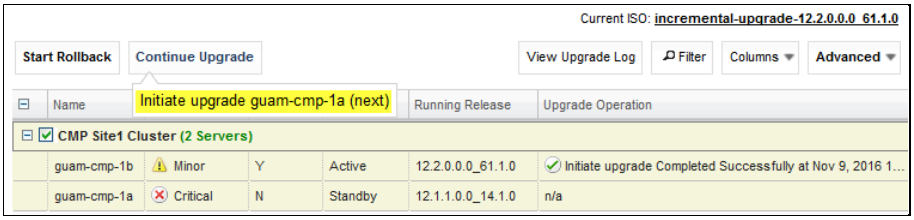
Step	Procedure	Result
		5. Click **OK** to confirm and continue with the operation. This continues to upgrade the standby server only in the CMP cluster The Upgrade Operation column shows a progress bar along with the upgrade activities.  Upgrade Operation changes to completed when done. During the upgrade activities, the following alarms may be generated and 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 12.0 server. 
13. ☐	**CMP GUI:** Continue to upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Primary CMP Server cluster 3. Click **Continue Upgrade**. Notice the Failover to new version CMP Site1 Cluster message.  4. Click **OK** to confirm and continue with the operation. The specific action take approximately 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 form should appear as shown—login and password credentials are the same as the pre-upgrade. 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>15. ☐</td><td>CMP GUI: Verify new Policy Management release</td><td>Navigate to Help→About. Verify the release displayed is 12.3
 
</td></tr>
<tr><td>16. ☐</td><td>CMP GUI: Critical alarms</td><td>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:
 

Current Minor Alarms
70503 Server Forced Standby
70500 System Mixed Version
70501 Cluster Mixed Version
 

NOTE: The Upgrade Manager shows alarms as well.</td></tr>
<tr><td>17. ☐</td><td>CMP GUI: Verify the Policy Management release 12.3 CMP is Active</td><td>1. Navigate to Upgrade→ Upgrade Manager.
2. Verify the following
- Active server is running release12.3
- Standby server is on the previous release
 
</td></tr>
</table>

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 checkbox for the Primary CMP Server cluster 3. Click **Continue Upgrade**. Notice the message Initiate upgrade <*standbyserver*> (next) 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

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

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

2. With the CMP cluster checkbox still selected, click View Upgrade Log. A window opens where you can verify that synchronization has taken place:

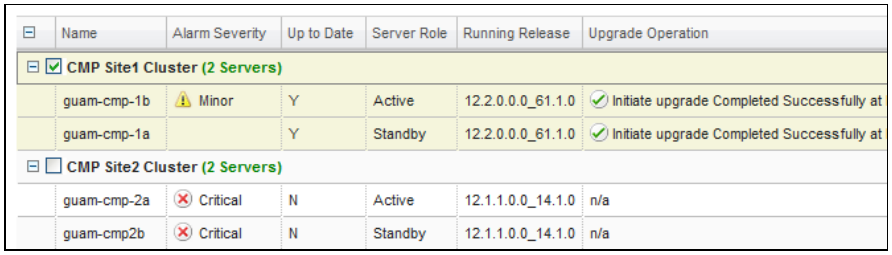
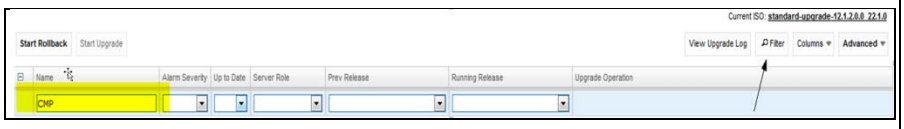
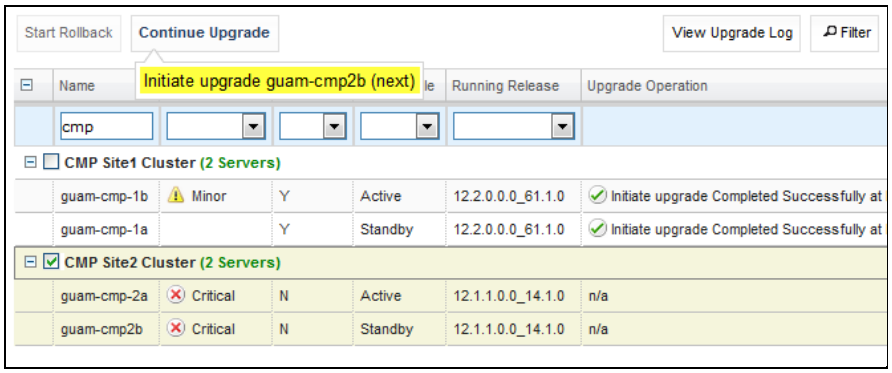
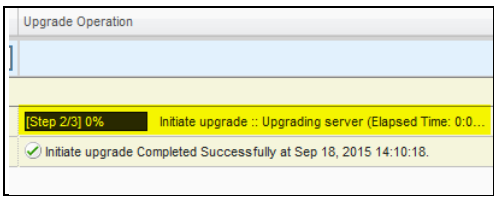
Upgrade Log
Cluster Name: CMP Site1 Cluster
Last Update: 11/10/2016 9:01:00
<table><tr><th>ID</th><th>Parent ID</th><th>Action Name</th><th>Duration</th><th>Scope</th><th>Hostname</th><th>Result</th><th>Mode</th></tr><tr><td>1</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1b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

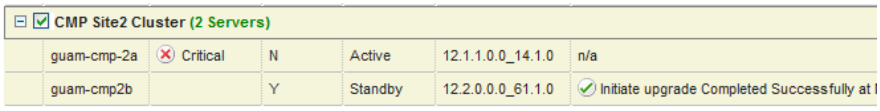
<table><tr><th></th><th>Name</th><th>Alarm Severity</th><th>Up to Date</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr><tr><td colspan="8">CMP Site1 Cluster (2 Servers)</td></tr><tr><td></td><td>guam-cmp-1b</td><td>Minor</td><td>Y</td><td>Active</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr><tr><td></td><td>guam-cmp-1a</td><td></td><td>Y</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr></table>
Successful upgrade status shows the following for both servers in the Primary CMP cluster:

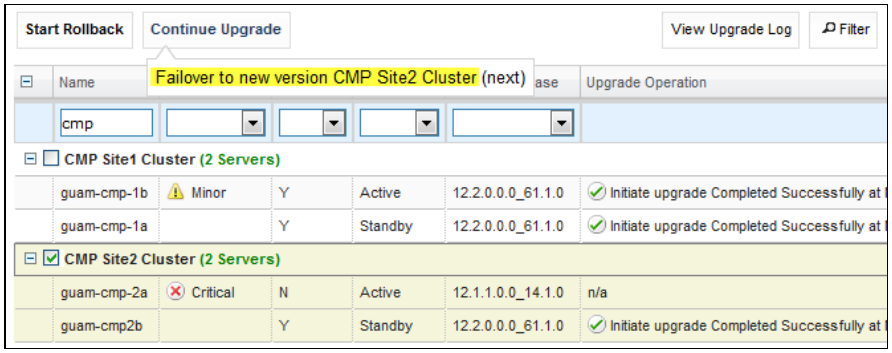
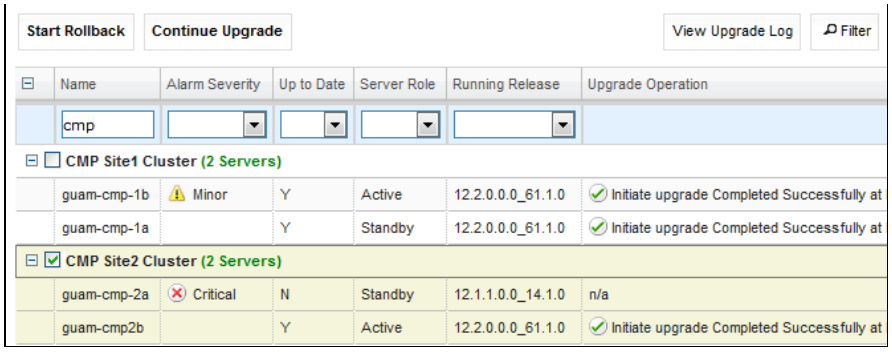
• 12.3 in the Running Release column for both servers
• A Y in the Up to Date column
• Active or Standby state for both servers in the Primary CMP cluster.</td></tr>
<tr><td>21. ☐</td><td>Proceed to next upgrade procedure</td><td>Verify the following information:

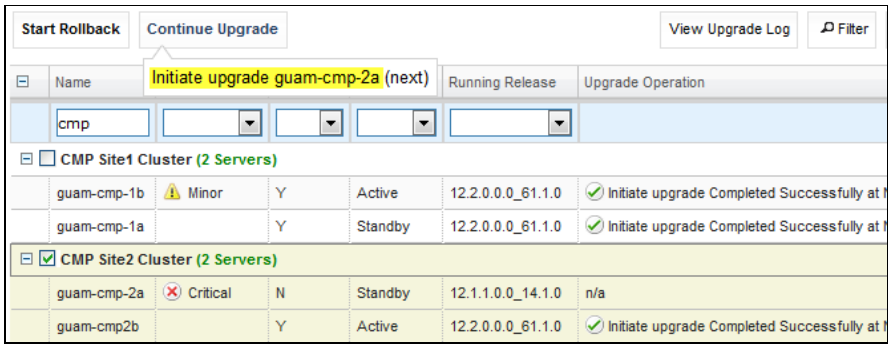
• Primary Site1 is running release 12.3
• Secondary Site is on release 12.2.x
• Proceed to the next procedure to upgrade the secondary CMP cluster.</td></tr>
<tr><td colspan="3">---End of Procedure---</td></tr>
</table>

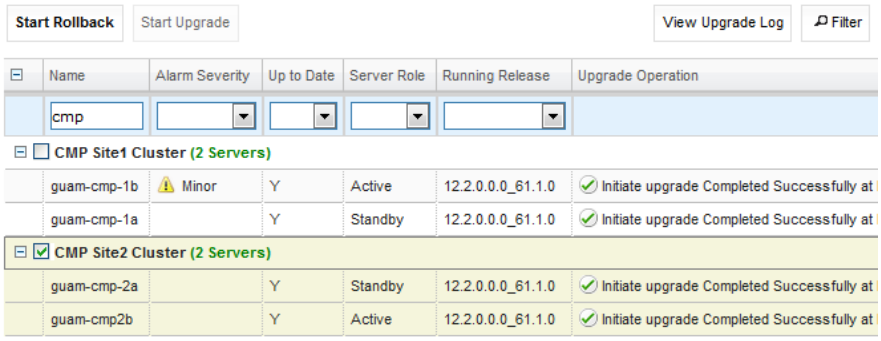
5.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify status of CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that: - 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**. 2. (Optional) Click **Filter** and enter `CMP` in the Name field.  3. Select the checkbox for the Secondary CMP Server cluster at Site2 4. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade <*site2_standbyserver*> (next)  5. 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 considered normal reporting events:

Step	Procedure	Details
		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. 

Step	Procedure	Details
3. ☐	**CMP GUI**: Failover of the Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Secondary CMP Server cluster at Site2 3. Click **Continue Upgrade**. Notice the message 'Failover to new version CMP Site2 Cluster'  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	Details
4. ☐	**CMP GUI**: Continue upgrade of the Secondary CMP cluster	1. Select the checkbox for 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 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	Details
5. ☐	**CMP GUI:** Verify that the upgrade completed successfully.	**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… with 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---		

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

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

NOTES:

- An upgrade of up to 4 clusters (8 for 12.2.x) can be running at the same time.
- Different cluster types can be upgraded at the same time. 2 MPEs and 2 MRAs, for example, can be upgraded in parallel.

6.1 Upgrade Preparation

6.1.1 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---		

6.2 Upgrade MRA and MPE Servers

This procedure upgrades one or more clusters (MPE and/or MRA).

This procedure is applicable for 12.2.x (wireless mode) 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.

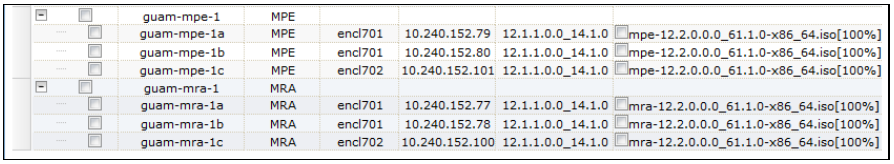
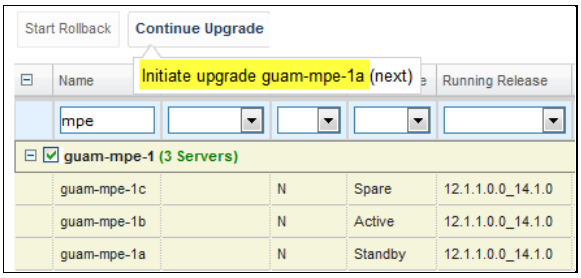
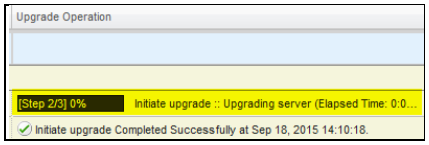
The upgrade procedure is essentially the same for an MRA cluster and an MPE cluster.

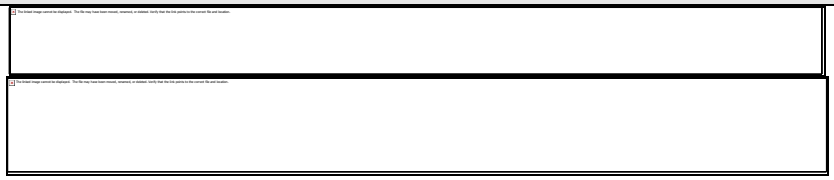
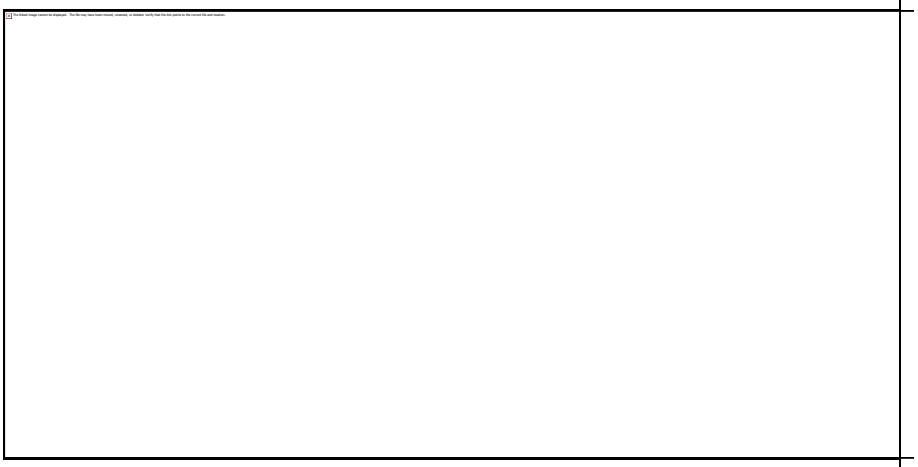
1. Select and start upgrade on the standby server
2. Failover
3. Re-apply configuration
4. Continue to upgrade the spare server
5. Continue upgrade on remaining server
6. (MPE only) Re-apply configuration one MPE cluster at a time

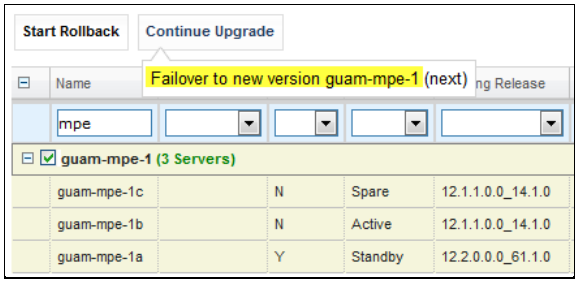
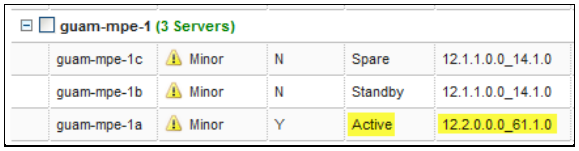
NOTES:

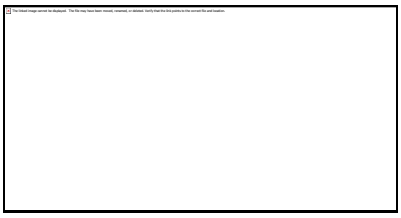
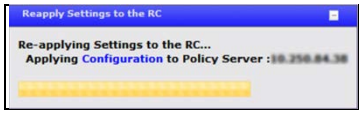
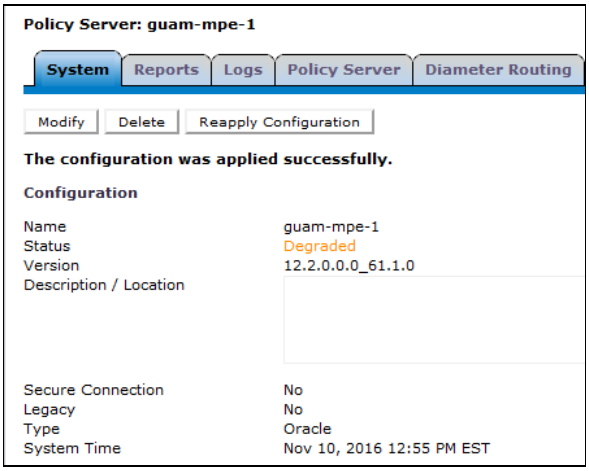
- All CMP clusters must be upgraded to Policy Management release 12.3 prior to executing the following procedures.
- Four (4) clusters (8 for 12.2.x) can be running the upgrade at one time.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 12.3.

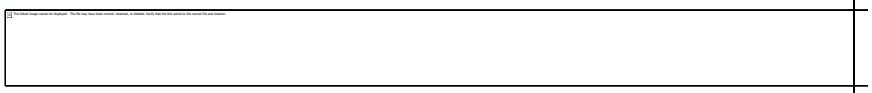
Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the MPE/MRA servers to be upgraded	Perform the following: 1. Check for current active alarms 2. Reset MPE/MRA counters to make a baseline - For the MPE**: Policy Server→Configuration→<***server_name***>→Reports → Reset Counters** - For the MRA**: MRA→Configuration→<***server_name***>→Reports →Reset Counters** 3. Go to the KPI Dashboard and capture a screenshot. **System Wide Reports → KPI Dashboard**

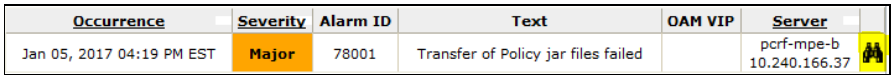
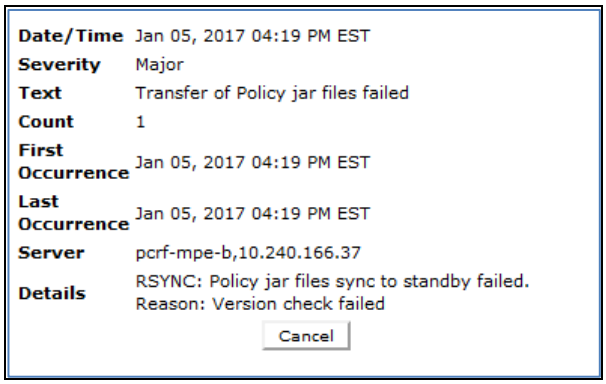
Step	Procedure	Result
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	1. Navigate to Upgrade → Upgrade Manager. 2. Verify information for the MRA/MPE servers: • Current release 12.2.x, or 12.2.x installed • Active/Standby/Spare status • ISO version to be deployed is 12.3 (verify the current ISO files are 12.3 by going to **Upgrade→ ISO Maintenance**) 
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 12.2.x) may be running upgrade at any time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the cluster to be upgraded, it can be an MRA or MPE 3. Click **Continue Upgrade**  4. Click **OK** to confirm and continue with the operation. The upgrade of the standby server of that cluster begins. 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 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

Step	Procedure	Result
		 **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   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 returns to the Standby state when the upgrade completes.  guam-mpe-1 (3 Servers) guam-mpe-1c N Spare 12.1.1.0.0_14.1.0 n/a guam-mpe-1b N Active 12.1.1.0.0_14.1.0 Initiate backout Completed Successfully at guam-mpe-1a Y Standby 12.2.0.0.0_61.1.0 Initiate upgrade Completed Successfully at During the upgrade activities, the following alarms may be generated and 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:

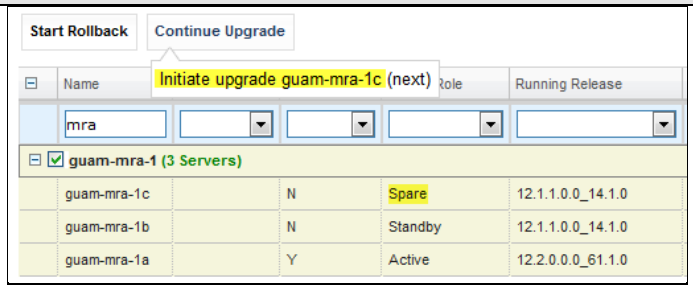
Step	Procedure	Result
		Expected Minor Alarms **78001** Rsync Failed **70500** System Mixed Version **70501** Cluster Mixed Version **70503** Server Forced Standby
4. ☐	**CMP GUI**: Continue to upgrade the MRA/MPE clusters. Next operation is a **failover** **NOTE:** 4 clusters (8 for 12.2.x) can be running 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 checkbox for 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*>**→System** The selected cluster shows a status of 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 as Degraded as 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 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 approximately 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 checkbox for the partially upgraded cluster, and select **Operations → Rollback**. The pre-12.2 MPE server becomes the active server and resumes handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	1. **Policy Server → Configuration →** *<mpe_cluster name>* **→ System** tab or **MRA → Configuration →** *<mra_cluster name>* **→ System** tab 2. Click **Reapply Configuration** 3. Verify that the version is changed back to 10.5, 11.5, 12.0, or 12.1.1, and the action report success. If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.

Step	Procedure	Result
9. ☐	**CMP GUI:** 78001 Major Alarm	During the upgrade activities, Major alarm 78001 in particular may be generated. And even though it is a normal event, the alarm does not clear by itself. Before continuing ensure that the alarm is cleared. 1. Click Major in the upper right part to display the alarms:  2. Click the binoculars icon on the right to display details about the 78001 Major alarm  You should see in the last line of the details that the reason for the major alarm is Version check failed.  - If you see a different reason, stop and contact My Oracle Support. - If you see the Version check failed reason, continue to the next step. 3. Navigate to **System Wide Reports → Alarms → Active Alarms** and select the 78001 Major alarm  4. Click the trash can icon on the right to clear this alarm.
10. ☐	**CMP GUI:** Continue upgrade of the MRA/MPE clusters. Next operation is initiate upgrade on the Spare server	Continue the upgrade on ONE cluster first, when the server goes into OOS, continue with the next cluster and so on. **NOTE:** Up to 4 clusters (8 for 12.2.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

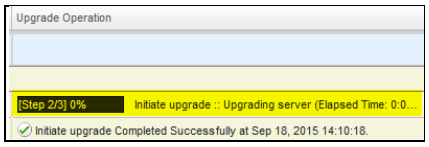
Step	Procedure	Result



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 considered normal reporting events—these are 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

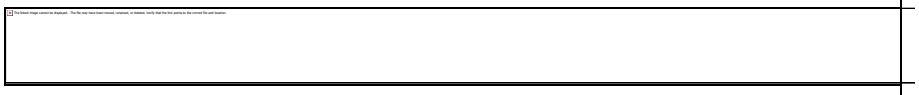
70004 QP Processes down for maintenance

Expected Minor Alarms

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

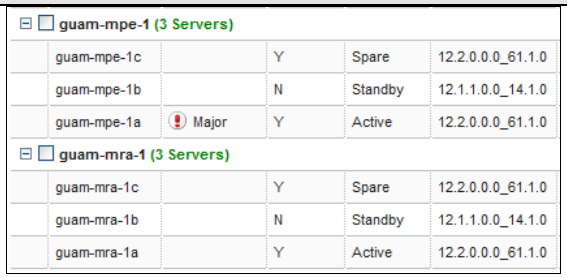
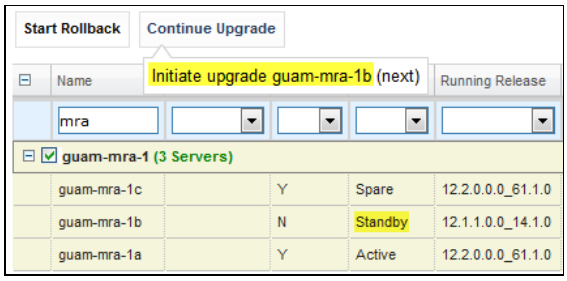
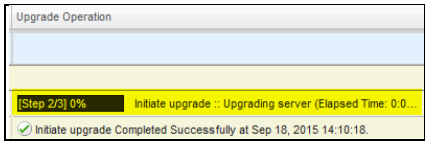
Upgrade is complete on the spare server in the georedundant cluster when:

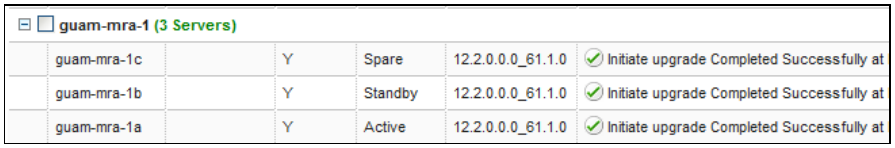
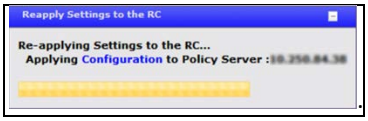
- The Initiate upgrade Completed Successfully… message displays in the Upgrade Operation column.



- 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
		
11. ☐	**CMP GUI:** Continue to upgrade the MRA/MPE clusters. Next operation is Initiate upgrade on the standby server	Continue the upgrade on ONE cluster first, when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters (8 for 12.2.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 displays the next action, which is to initiate the upgrade of the standby server.  4. Click **OK** to confirm and continue with the operation. The final server upgrade of the cluster begins 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 considered normal reporting events—these are 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

Step	Procedure	Result
		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)  guam-mra-1 (3 Servers) guam-mra-1c Y Spare 12.2.0.0.0_61.1.0 Initiate upgrade Completed Successfully at guam-mra-1b Y Standby 12.2.0.0.0_61.1.0 Initiate upgrade Completed Successfully at guam-mra-1a Y Active 12.2.0.0.0_61.1.0 Initiate upgrade Completed Successfully at All servers are now running release 12.3
12. ☐	**CMP GUI: (MPE only)** Reapply configuration on the fully upgraded MPE clusters.	**MPE only** 1. Navigate to **PolicyServer → Configuration → <***MPE_cluster***> → 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 :
13. ☐	Repeat steps 1 through 14 for the next MPE or MRA cluster	Proceed with next cluster

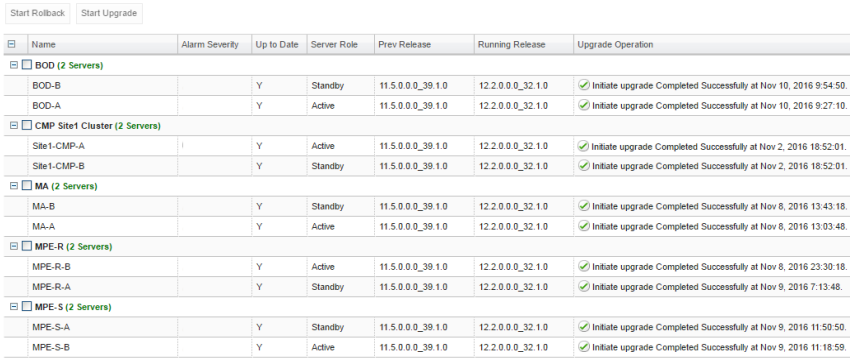
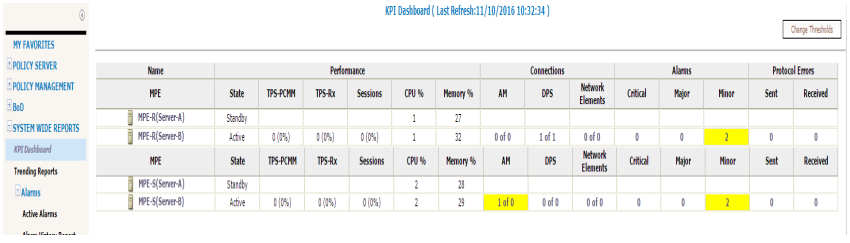
Step	Procedure	Result
14. ☐	Upgrade Completed	At this point all servers have been upgraded.

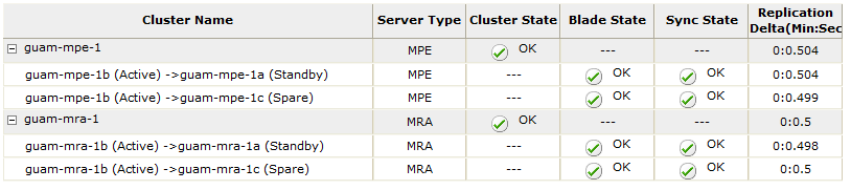
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
guam-cmp-1b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-cmp-1a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
CMP Site2 Cluster (2 Servers)						
guam-cmp-2a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-cmp2b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mpe-1 (3 Servers)						
guam-mpe-1c		Y	Spare	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mpe-1b		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mpe-1a		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mra-1 (3 Servers)						
guam-mra-1c		Y	Spare	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mra-1b		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-mra-1a		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at

---End of Procedure---

7. POST UPGRADE HEALTH CHECK

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

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the upgrade is successful on all CMP/MA/MPE/ Mediation clusters.	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the Up to Date, Running Release, and Upgrade Operation columns and verify that they read Y, 12.2…, and Initiate upgrade completed successfully at… respectively, for all servers in all clusters. 
2. ☐	**CMP GUI:** View current alarms	1. Navigate to **System Wide Reports→Alarms→Active Alarms** 2. Verify that all alarms due to the upgrade have been cleared. 
3. ☐	**CMP GUI**: View current KPIs	1. Navigate to **System Wide Reports→KPI Dashbord.** 2. Verify that everything looks normal. 

Step	Procedure	Result
4. ☐	**CMP GUI:** Replication stats	1. Navigate to **System Wide Reports→Others→MPE/MRA Rep Stats** (for a wireless system) 2. Verify all clusters and servers are in OK state. 

Cluster Name	Server Type	Cluster State	Blade State	Sync State	Replication Delta(Min:Sec
⊟ guam-mpe-1	MPE	OK	---	---	0:0.504
guam-mpe-1b (Active) ->guam-mpe-1a (Standby)	MPE	---	OK	OK	0:0.504
guam-mpe-1b (Active) ->guam-mpe-1c (Spare)	MPE	---	OK	OK	0:0.499
⊟ guam-mra-1	MRA	OK	---	---	0:0.5
guam-mra-1b (Active) ->guam-mra-1a (Standby)	MRA	---	OK	OK	0:0.498
guam-mra-1b (Active) ->guam-mra-1c (Spare)	MRA	---	OK	OK	0:0.5

---End of Procedure---

8. BACKOUT (ROLLBACK) 12.2.X/12.2.X WIRELESS MODE

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

The Policy system is backed out to the previous release.

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

8.1 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 needs to 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.

8.2 Pre-requisites

1. No new policies or features have been configured or executed on the upgraded release.
2. The CMP cluster cannot backout if other non-CMP Policy servers are still on the upgraded release.

8.3 Backout of Fully Upgraded Cluster

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

This procedure is used to backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster are on a pre-12.2 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 12.2

8.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, or MPE) are 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.

8.3.1.1 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

8.3.1.2 Backout Secondary CMP (if applicable)

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

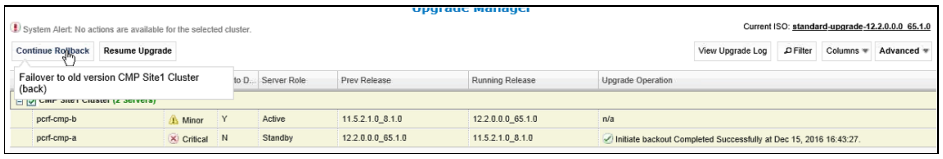
Use the CMP GUI (Upgrade Manager) to backout the Secondary CMP cluster

8.3.1.3 Backout Primary CMP (12.2.x)

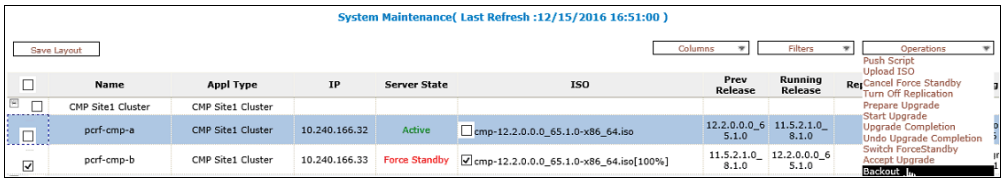
NOTE: At this time, all of the MPE/MRA clusters must already be backed out, the Secondary CMP must also be backed out.

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. Click **Continue Rollback**, which would failover to older version CMP cluster.

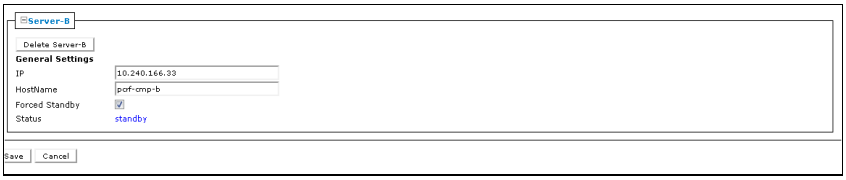


4. Log back in to the Primary CMP VIP
5. Use the 12.2.x System Maintenance to complete backout of the Primary CMP cluster



6. Click **OK** to execute 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**.

8.3.1.4 Backout Primary CMP (12.2.x)

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

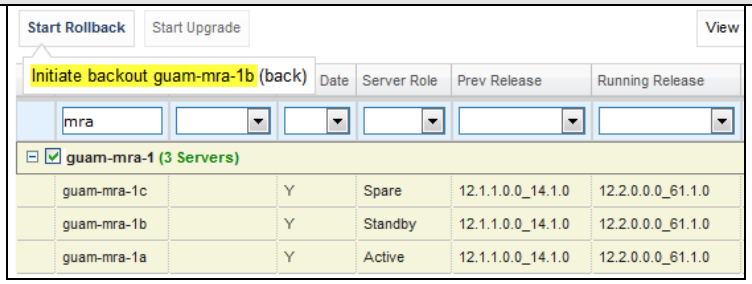
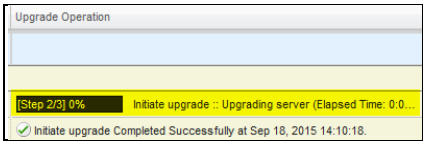
8.3.2 Backout of a Partially Upgraded Cluster

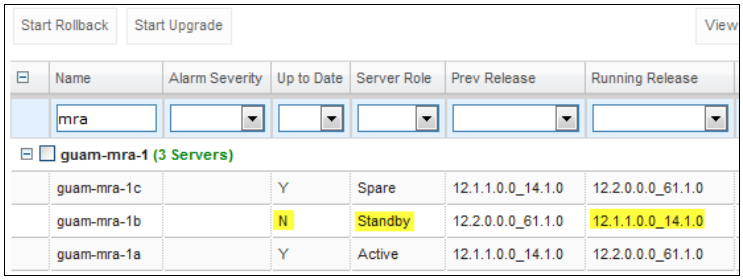
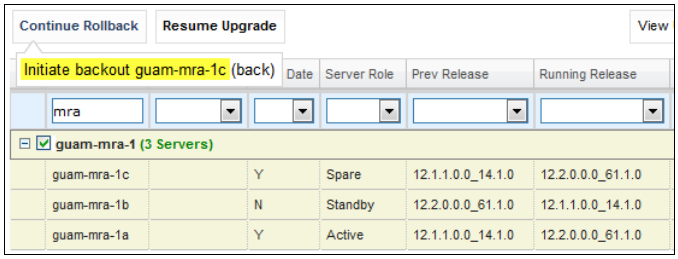
A partially upgraded cluster occurs when the version is not correct or the success message does not display. If this happens, contact Oracle Support and report a partially upgraded cluster.

8.3.3 Backout Fully Upgraded MPE/MRA Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster to be backed out: - Primary CMP is on release 12.3 - MPE/MRA is on release 12.3 - Up to Date column shows Y for all servers **EXAMPLE**
2. ☐	**CMP GUI**: Rollback standby server—MPE/MRA **NOTE:** The backout of a single server takes approximately 40 minutes to complete. **NOTE:** Up to 8 upgraded clusters can be backed	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the cluster. - Select one cluster at a time. - It can be an MRA or MPE cluster. 3. Click **Start Rollback**. When hovering over the button, it informs you of the server to backout, in this case it is the current standby server.

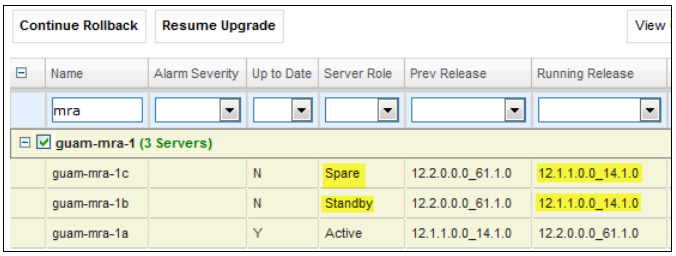
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release
CMP Site1 Cluster (2 Servers)					
guam-cmp-1b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-cmp-1a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
CMP Site2 Cluster (2 Servers)					
guam-cmp-2a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-cmp2b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mpe-1 (3 Servers)					
guam-mpe-1c		Y	Spare	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mpe-1b		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mpe-1a		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mra-1 (3 Servers)					
guam-mra-1c		Y	Spare	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mra-1b		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0
guam-mra-1a		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0

Step	Procedure	Result
	out at the same time, selecting one at a time.	 4. Click **OK** to confirm and continue with the operation. The backout process begins. Follow the progress in the Upgrade Operation column.  The server backing out goes into the OOS state and the spare server now takes over as standby. Wait until the server goes to an OOS state before selecting the next cluster to backout. During the backout activities, the following alarms may be generated and considered normal reporting events. The alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarm** **70004** QP Processes down for maintenance **78001** Rsync Failed **31233** HA Path Down **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 **31282** HA Management Fault Backout of this server is complete when the Initiate backout completed successfully at… message displays in the Upgrade Operation column. The

Step	Procedure	Result
		server is running a pre-12.2 release and returns to standby with an N in the Up to Date column. 
3. ☐	**CMP GUI:** Continue the backout of the MRA/MPE clusters. Next operation is initiate backout on the spare server **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	1. Select the partially backed out cluster. 2. Navigate to **Upgrade → Upgrade Manager**. 3. Click **Continue Rollback**. When hovering over the button, it informs you of a backout on the spare server.  4. Click **OK** to confirm and continue with the operation. Follow the progress in the Server Role column. The Server shows OOS in the server role until the backout completes. During the backout activities, the following alarms may be generated and considered normal reporting events—these are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarm** **78001** Rsync Failed **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **78001** Rsync Failed **70502** Cluster Replication Inhibited **31114** DB replication over SOAP has failed

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>
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
31282 HA Management Fault

Backout of this server is complete when the Initiate backout completed successfully at… message shows in the Upgrade Operation column. The spare server goes back to running a pre-12.2 release.



</td></tr>
<tr><td>4. ☐</td><td>CMP GUI: Continue the backout of the MRA/MPE clusters. Next operation is failover to previous release.

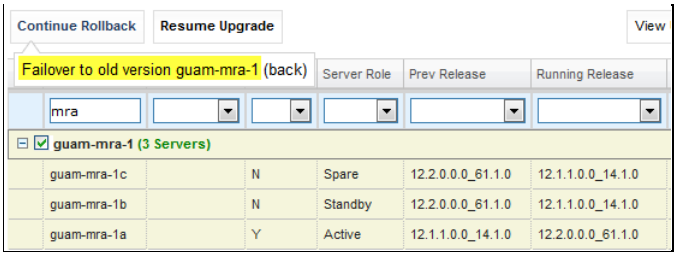
NOTE: Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.</td><td>
1. Select the cluster to backout.

Current state of the cluster should be as follows:

- Spare server on previous release
- Standby server on previous release
- Active server on release 12.3

2. Navigate to Upgrade → Upgrade Manager.

3. Click Continue Rollback. When hovering over the button, it informs you of a failover to the old version.



4. Click OK to confirm and continue with the operation. It begins to fail over.

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

<u>Expected Critical Alarms</u>

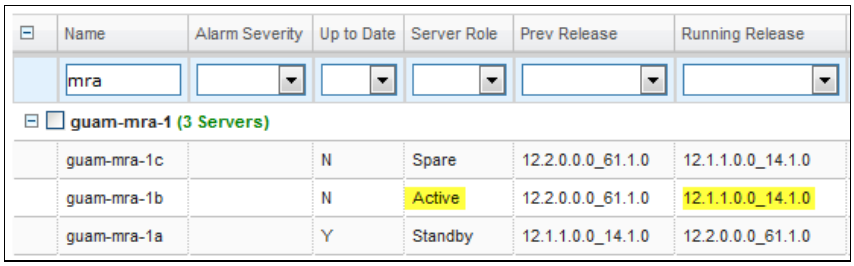
31283 HA Server Offline / Lost Communication with server
31227 HA availability status failed
70001 QP_procmgr failed

<u>Expected Major Alarm</u>

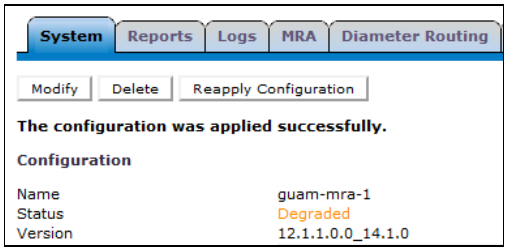
70004 QP Processes down for maintenance
31233 HA Path Down
31126 Audit blocked
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>
<u>Expected Minor Alarms</u>

70503 Server Forced Standby
70507 Upgrade In Progress
70500 System Mixed Version
70501 Cluster Mixed Version
78001 Rsync Failed
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
31282 HA Management Fault

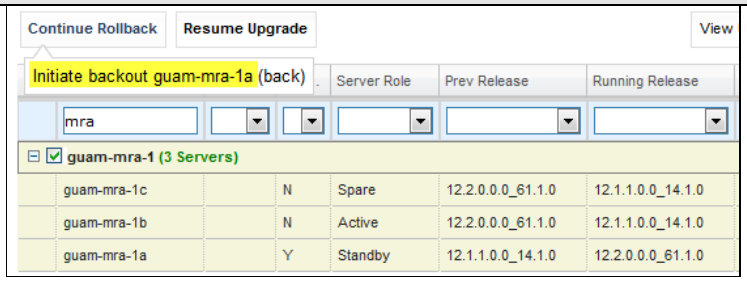
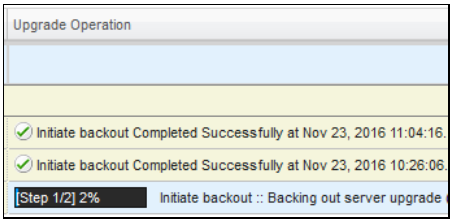
State of the cluster looks like the following when the failover completes. The active server is now running the previous release:


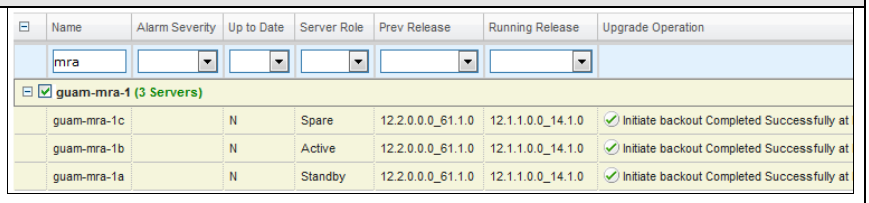
</td></tr>
<tr><td>5. ☐</td><td>CMP GUI: Reapply the configuration to the MPE/MRA cluster that completed the failover successfully.</td><td>
• For MPE: Policy Server → Configuration → <MPE_cluster> → System
• For MRA: MRA→Configuration→<MRA_cluster>→System
The selected cluster has the status shown as Degraded running release 12.2

1. Click Reapply Configuration.
- The MPE opens a popup box showing the progress of the reapply process.
- The MRA does not show anything.
2. Note the version is successfully changed to the previous release:


NOTE: The status showing Degraded is a normal reporting event because the servers currently have different releases.
</td></tr>
<tr><td>6. ☐</td><td>CMP GUI: Complete backout of clusters

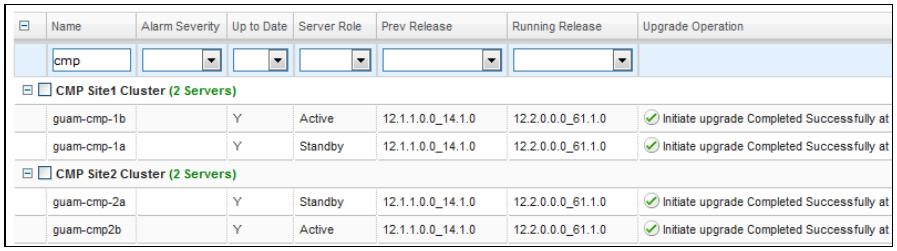
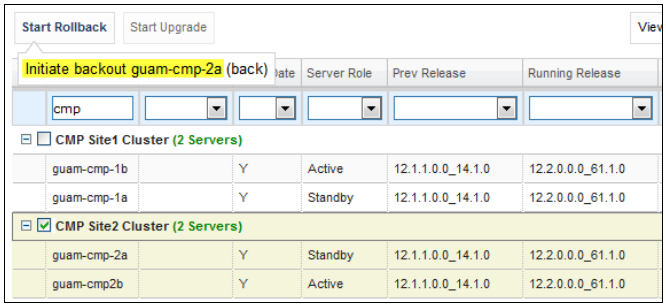
NOTE: The backout of a single server takes approximately 30</td><td>
1. Navigate to Upgrade → Upgrade Manager.
2. Select the partially upgraded cluster to backout.
3. Click Continue Rollback. When hovering over the button, it informs you of the current standby server to be backed out:
</td></tr>
</table>

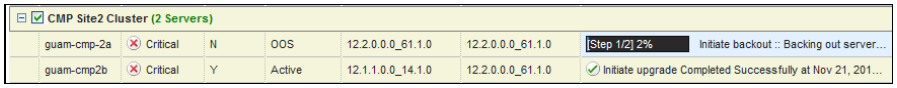
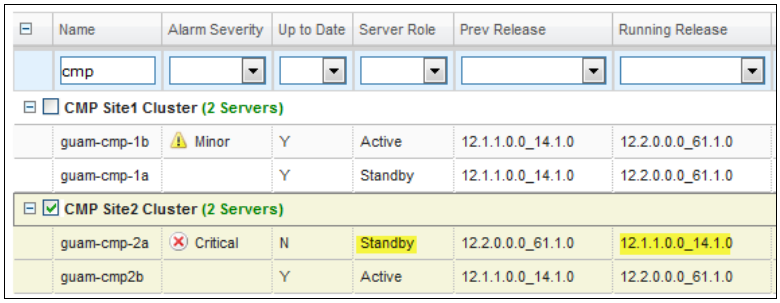
Step	Procedure	Result
	minutes to complete. **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	 4. Click **OK** to confirm and continue with the operation. The backout process begins. Follow the progress in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events—these are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** 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 **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **78001** Rsync Failed **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 **31282** HA Management Fault Backout of the server is complete when the Initiate backout completed successfully message displays in the Upgrade Operation column. All of the servers are on the pre-12.2 release and shows active/standby/spare

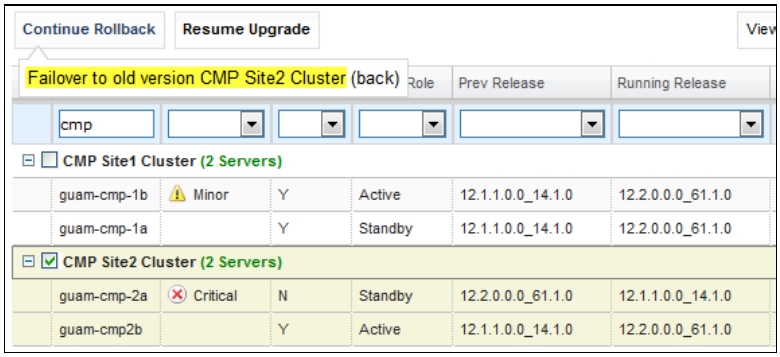
Step	Procedure	Result
		
7. ☐		Repeat this Procedure for remainder of MPE and MRA servers, if not fully backed out yet.
8. ☐	Final Syscheck	Another Syscheck on all the backed out servers can be performed to ensure all modules are still operationally OK before progressing to the next Procedure.
---End of Procedure---		

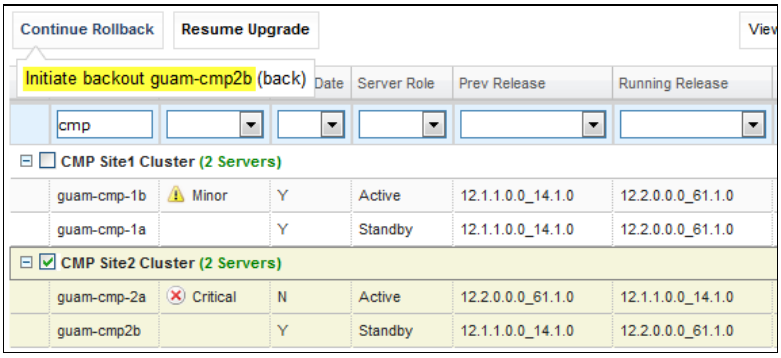
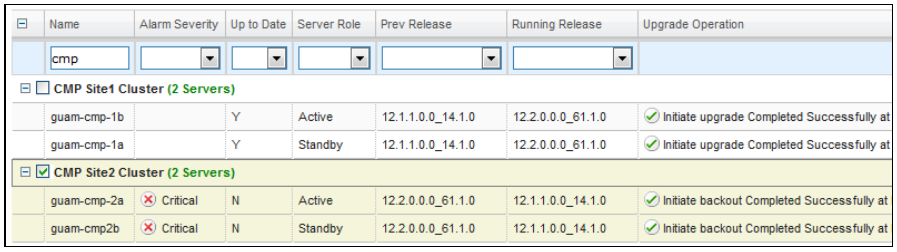
8.3.4 Backout Fully Upgraded Secondary CMP Cluster

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

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP clusters	1. Navigate to **Upgrade → System Maintenance**. 2. (Optional) Click **Filter** and enter `CMP` in the Name field. 3. Confirm status of the cluster to be backed out a. Primary CMP is on release 12.3 b. All other non-CMP clusters are on pre-12.3 c. Up to Date column shows Y for all servers 
2. ☐	**CMP GUI:** backout secondary CMP cluster **NOTE:** The backout of a single server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the secondary CMP cluster 3. Click **Start Rollback**. When hovering over the button, it informs you of a back out of the standby server.  4. Click **OK** to confirm and continue with the operation. The backout begins.

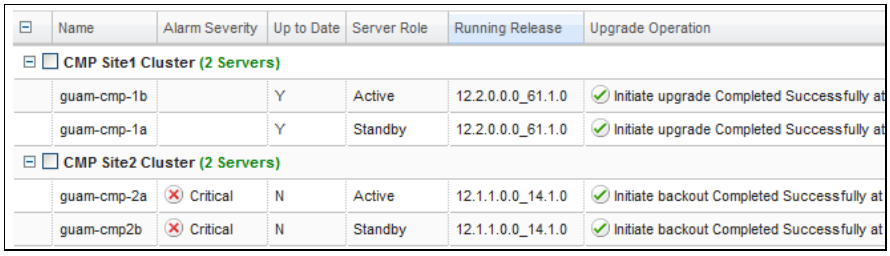
Step	Procedure	Result
		The server goes into an OOS server Role Follow the progress in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events—these are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **70025** The MySQL slave has a different schema version than the master. **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **78001** Rsync Failed **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 **31282** HA Management Fault Backout of the server is complete when the Initiate backout completed successfully at… message shows in the Upgrade Operation column. The server returns to standby state and shows the previous release. 

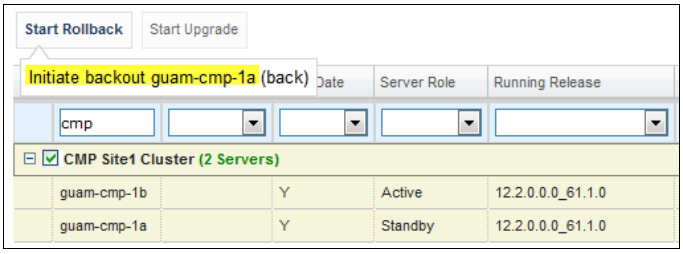
Step	Procedure	Result
3. ☐	**CMP GUI:** Continue the backout. Next operation is failover	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Secondary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of a fail over to the previous version.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

Step	Procedure	Result
4. ☐	**CMP GUI**: Continue the backout. Next operation is initiate backout	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Secondary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of a back out of the new standby server.  4. Click **OK** to confirm and continue with the operation. The failover process begins. Follow the progress of the status in the Upgrade Operation column. **Expected Critical alarm** **70025** QP Slave database is a different version than the master **Expected Minor Alarms** **70500** System Mixed Version The procedure is completed when both servers in the Secondary CMP are in the previous release. 
---End of Procedure---		

8.3.5 Backout Fully Upgraded Primary CMP Cluster

NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site1 cluster. For rollback to 12.2.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.2.x, only use the Upgrade Manager.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1. ☐</td><td>CMP GUI: Verify the status of the CMP clusters</td><td>1. Navigate to Upgrade Manager → System Maintenance.
2. Confirm status of the cluster to be backed out:
- Primary Active CMP is on release 12.3
- Secondary CMP cluster is on pre-12.2 release 10.5, 11.5, 12.0, or 12.1.1
- Up to Date column shows Y for all servers in the primary CMP cluster
 
</td></tr>
<tr><td>2. ☐</td><td>CMP GUI: backout standby Primary CMP cluster

NOTE: Backout of one server takes approximately 40 minutes to complete.</td><td>3. Navigate to Upgrade → Upgrade Manager.
4. Select the checkbox for the Primary CMP cluster
5. (Optional) Click Filter and enter <code>CMP</code> in the Name field.
6. Click Start Rollback. When hovering over the button, it informs you of the server to get backed out.
 

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

Follow the progress of the status in the Upgrade Operation column.

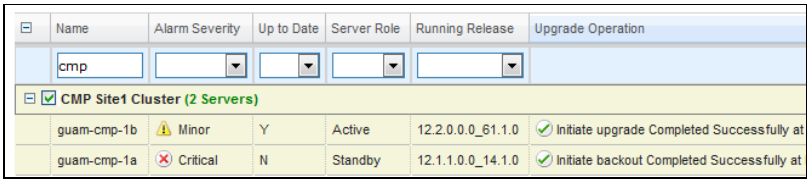
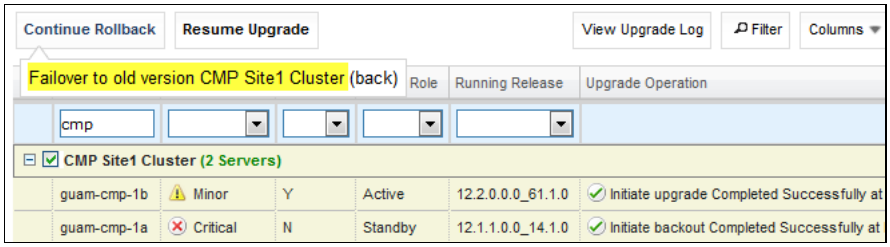
During the backout activities, the following alarms may be generated and considered normal reporting events—these are cleared after the cluster is completely backed out.

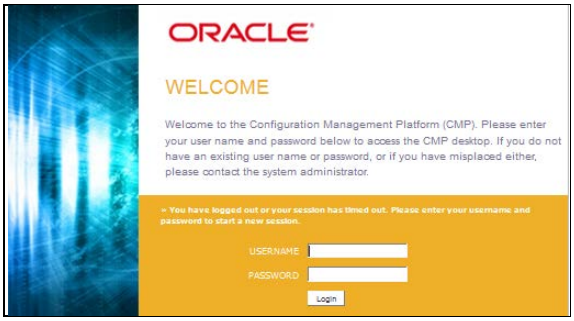
<u>Expected Critical Alarms</u>

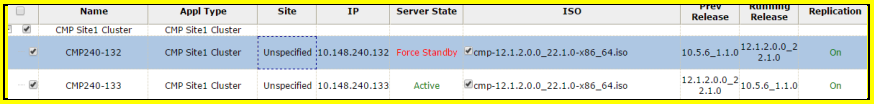
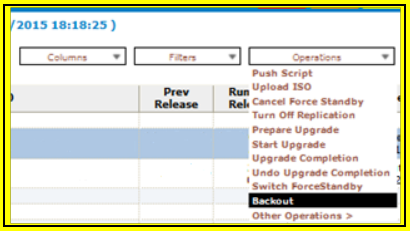
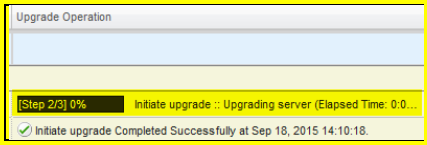
31283 HA Server Offline / Lost Communication with server
31227 HA availability status failed
70001 QP_procmgr failed
31236 HA Link Down

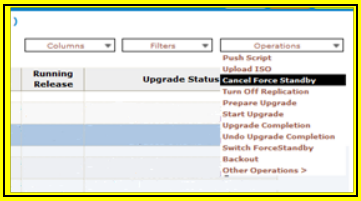
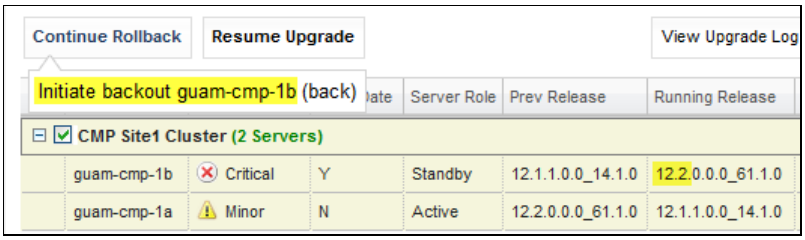
<u>Expected Major Alarm</u>

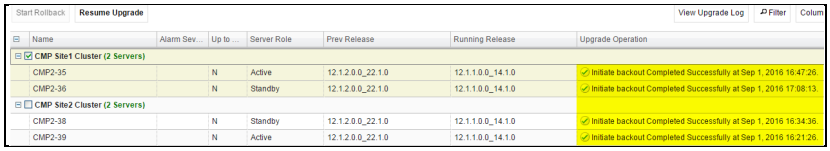
70004 QP Processes down for maintenance
31233 HA Path Down</td></tr>
</table>

Step	Procedure	Result
		Expected Minor Alarms **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 **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **78001** Rsync Failed **70502** Cluster Replication Inhibited Backout of the server is complete when the Initiate backout completed successfully message shows in the Upgrade Operation column. The server returns to the Standby state and shows the previous release. 
3. ☐	**CMP GUI:** Continue the backout. Next operation is failover	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Primary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of a fail over.  4. Click **OK** to confirm and continue with the operation. The failover process begins. Failover takes a couple minutes.

Step	Procedure	Result
4. ☐	**CMP GUI**: Log back in to the Primary CMP VIP	After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP. 
5. ☐	**CMP GUI:** Verify release	Navigate to **Help→About**. Verify the release number is not 12.2 anymore. • If the rollback is for release 12.2.x, continue with step 6. • If the rollback is for release 12.2.x, continue with step 8

Step	Procedure	Result
6. ☐	**CMP GUI (release 12.2.x):** Continue the backout of the Primary CMP cluster **NOTE**: Backout of one server takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → System Maintenance**. 2. Select the remaining server in the Primary CMP cluster. The server is 12.3 and shows Forced Standby in the Server State column.  3. Select **Operations→Backout**  4. Click **OK** to continue Follow the progress in the Upgrade Operation column. Wait until the server to backout comes to backout complete.  During the Backout activities, the following alarms may be generated and considered normal reporting events. These are cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** 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 **78001** Rsync Failed **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

Step	Procedure	Result
7. ☐	**CMP GUI**: Remove Forced Standby	1. Navigate to **Upgrade → System Maintenance**. 2. Select the remaining server in the Primary CMP cluster. The server is on 12.2.x and shows Forced Standby in the Server State column. **NOTE:** A refresh of the current screen may be necessary at approximately the 40 minute mark. 3. Select **Operations→Cancel Forced Standby** 
		The backout procedure is now completed for release 12.2.x.
8. ☐	**CMP GUI (release 12.2.x)**: Continue the backout of the Primary CMP cluster **NOTE:** The backout of one server takes approximately 40 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for the Primary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of the server to back out. In this case, it is the current standby server still running 12.2.  4. Click **OK** to confirm and continue with the operation. The backout process begins. Server goes into an OOS server Role Follow the progress in the Upgrade Operation column. During the backout activities, the following alarms may be generated and are considered normal reporting events. These are cleared after the cluster is completely backed out. **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 **78001** Rsync Failed

Step	Procedure	Result
		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 Backout of the server is complete when the following message (initiate backout completed successfully) shows in the Upgrade Operation column. The server returns to the Standby state and shows the previous release. 
9. ☐	Final syscheck	A syscheck on all the backed out servers, can be performed to ensure all modules are still operationally OK before progressing to the next procedure.
---End of Procedure---		

APPENDIX A. 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.

If this procedure fails, contact Oracle Support.

Adding TVOE software image to TVOE host

Step	Procedure	Description

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 customer PC using Linux
		From the command line of a Linux machine, 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 and <*TVOE_ip*> is the TVOE IP address. <*user*> should be admusr for TVOE releases 2.5 or newer.
		• SCP from customer PC using Windows
		Use WinSCP to copy the TVOE ISO image to the TVOE host.
		• USB Media
		d. Attach the USB media to the TVOE host.
		e. 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`
		f. Replacing <*PATH_TO_TVOE_ISO*> with the output of the command above, copy the ISO to the /var/TKLC/upgrade directory:
		`$ sudo cp <PATH_TO_TVOE_ISO> /var/TKLC/upgrade/`
		g. Unmount the USB media:
		`$ sudo umount /media/usb`

---End of Procedure---		

8.4 TVOE Upgrade

This procedure provides basic steps to upgrade the PM&C Server to 6.0.3 and the TVOE host to 3.0.3

NOTE: The TVOE upgrade procedure can executed 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.

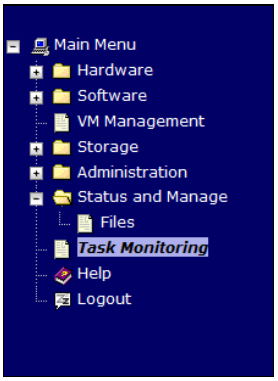
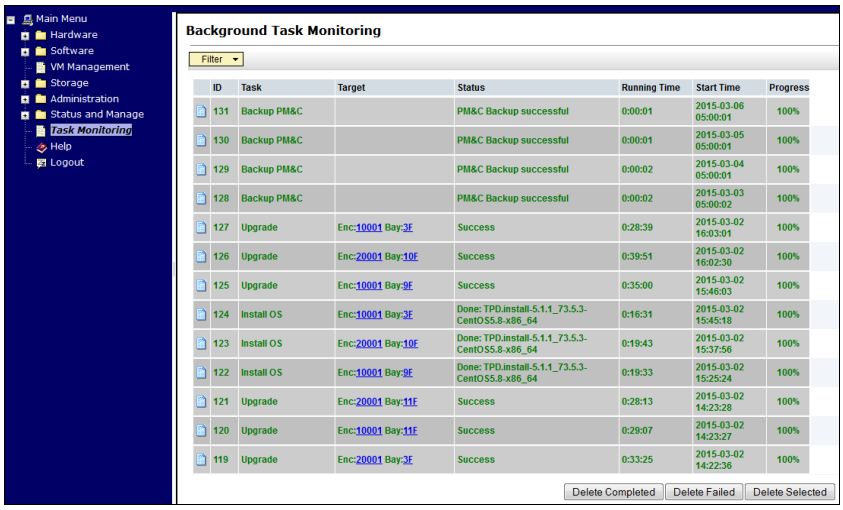
- TVOE Pre-Upgrade Validation
- Pre-Upgrade Backup
- Add TVOE Software Image to TVOE HOST
- Add PM&C Upgrade Software to PM&C Server
- Stand Alone TVOE Host Upgrade
- TVOE Post-Upgrade Validation
- PM&C upgrade
- Stand Alone TVOE Upgrade Accept
- PM&C Upgrade Accept

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

- If you're 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.

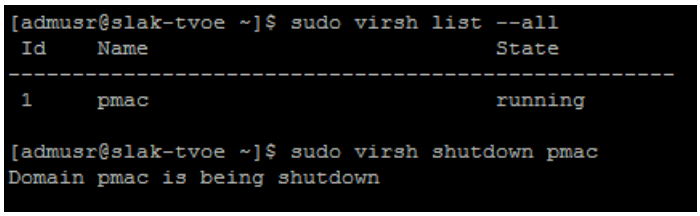
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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.

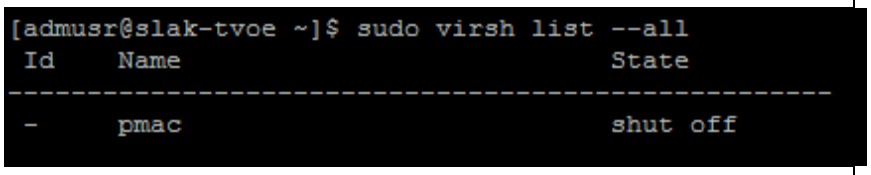
Step	Procedure	Details
2. ☐	Check any in-progress tasks on PM&C	1. On a supported web browser, log in to PM&C GUI as pmacadmin 2. Navigate to PM&C GUI background tasks page: **Main Menu → Task Monitoring**  3. Verify all tasks are complete indicated by green 100% progress **NOTE:** If any task shows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

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>3. ☐</td><td>Shutdown PM&C</td><td>
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

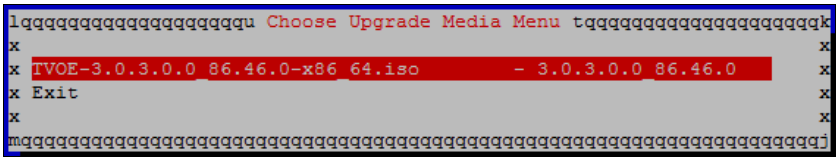
2. Obtain the name of the PM&C guest by executing the following command:
<pre>$ sudo virsh list --all
Id Name   State
----
1 <pmac_name>   running</pre>
3. Stop the PM&C process by using the following command:
<pre>$ sudo virsh shutdown <pmac_name></pre>


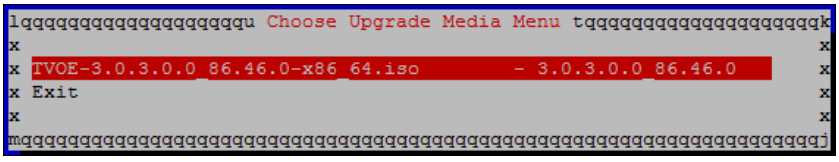
NOTE: It is imperative to log into the TVOE host instead of using ssh to the PM&C guest. The upgrade might fail otherwise.
</td></tr>
<tr><td>4. ☐</td><td>Verify PM&C guest is shut down</td><td>
1. Log into the TVOE host as admusr.

2. Verify that the PM&C is shut down with the following command:
<pre>[admusr@tvoe ~]# sudo virsh list --all</pre>


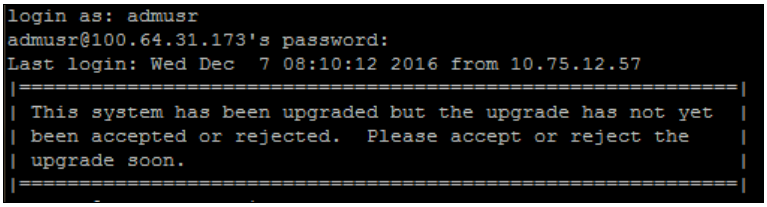
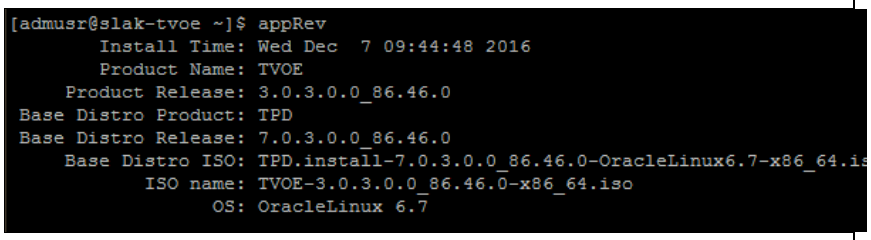
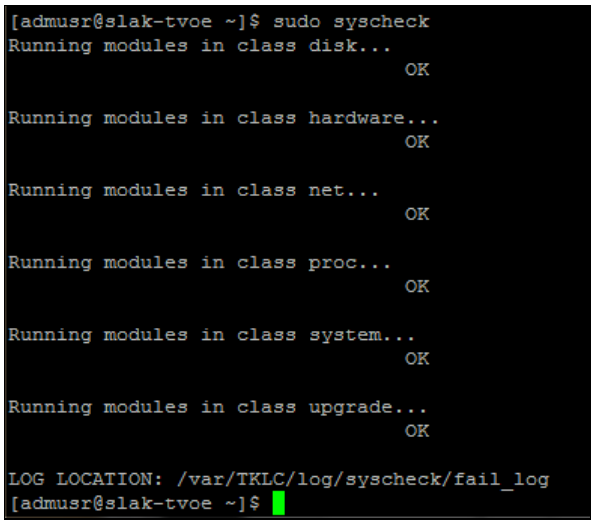
NOTE: This should show PM&C guest state as shut off.
</td></tr>
</table>

Step	Procedure	Details

5. ☐	Validate media	1. Log into 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.

6. ☐	Start TVOE upgrade **NOTE:** The upgrade process takes approximately 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. Navigate to **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 executing the following command:
		`$appRev`
		You get an output similar to this:
		 
		3. Run the following command:
		`$sudo verifyUpgrade`
		No output is expected from this command. Any output displays potential issues.
		4. Perform a syscheck:
		`$sudo syscheck`
		 

Software Upgrade Procedure

Step	Procedure	Details
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 once an upgrade has been accepted.
---End of Procedure---		

8.5 PM&C Upgrade

This procedure provides instructions 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

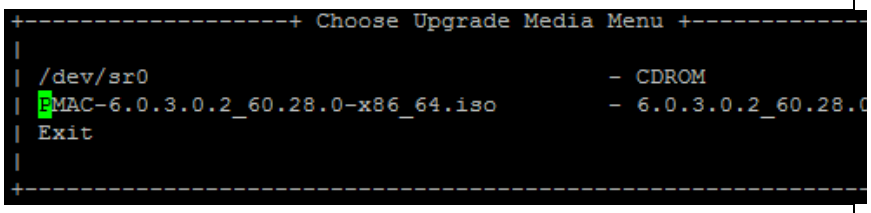
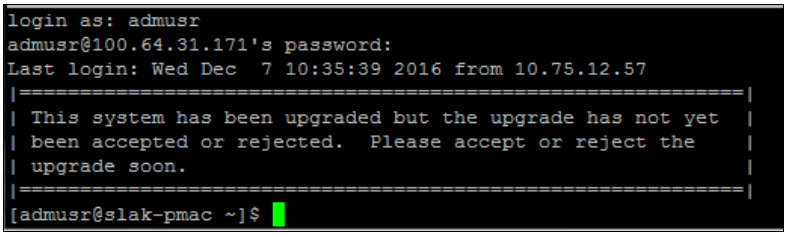
1. ☐	Start the PM&C guest	1. If not already logged in to the TVOE host as admusr, do so.
		2. Start the PM&C guest if not already started:
		3. Query the list of guests to check whether the PM&C guest is in state running.
		`$ sudo virsh list --all`
		`Id Name State`
		`----------`
		`1 <pmac_name> running`
		- 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`

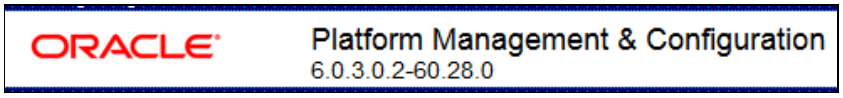
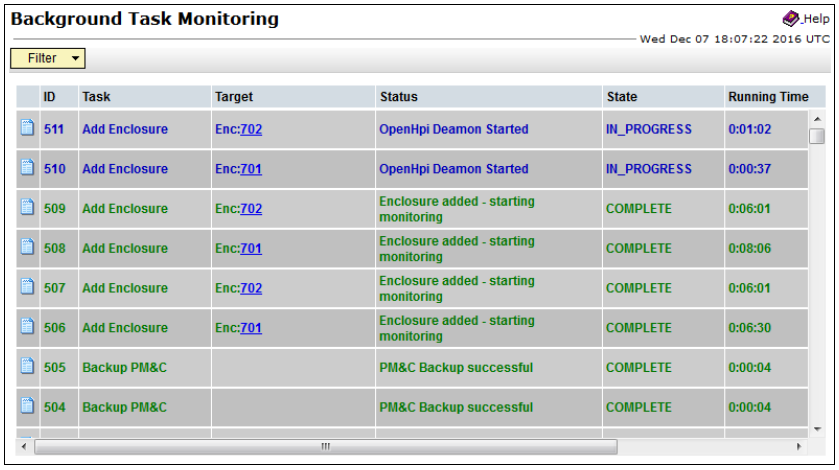
2. ☐	Close any active browser sessions to PM&C	If any open browsers are connected to PM&C, close them before proceeding

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: It might be needed 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. ☐	Execute 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`

Software Upgrade Procedure

Step	Procedure	Details
5. ☐	In the platcfg utility select **Initiate Upgrade** to start the upgrade process	1. In platcfg, navigate to **Maintenance→Upgrade→Initiate Upgrade**. 2. Select **Initiate Upgrade** to start the upgrade process Wait for the Choose Upgrade Media Menu screen to display 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 approximately 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. 4. Log back into PM&C and you see something similar to the following: 

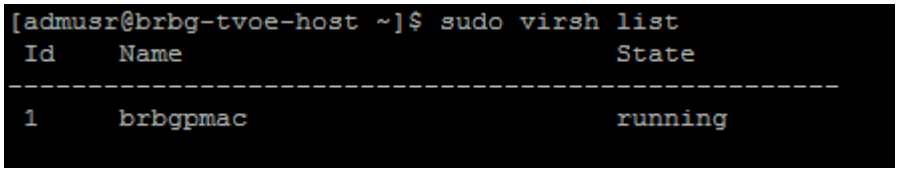
Step	Procedure	Details
6. ☐	**PM&C GUI:** Verify the upgrade after approximately 30 minutes	1. Open a browser and type in the IP address of the PM&C server 2. Login as pmacadmin. 3. Verify the release at the top of the page.  4. Navigate to the task manager and verify all tasks are complete. DO NOT proceed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

8.6 Verify PM&C Upgrade

This procedure provides instructions to verify 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

1. ☐	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`
		 
		
		3. Log on to PM&C guest console by issuing the following command from the TVOE console:
		`$ sudo virsh console <pmac_name>`
		Remember to press **Enter** twice.
		NOTE: If you connected from the TVOE console, the guest session to PM&C is broken with CTRL+]

Software Upgrade Procedure

Step	Procedure	Details

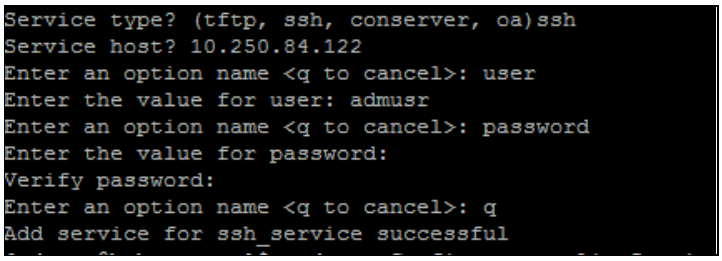
2. ☐	Verify the date/timestamp	1. Logged in to the PM&C console, execute the following command
		`$ ls -l /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@slak-pmac ~]$ ls -l /var/TKLC/log/upgrade/upgrade.log`
		`-rw-rw-r-- 1 platcfg root 127103 Dec 7 11:51 /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@slak-pmac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

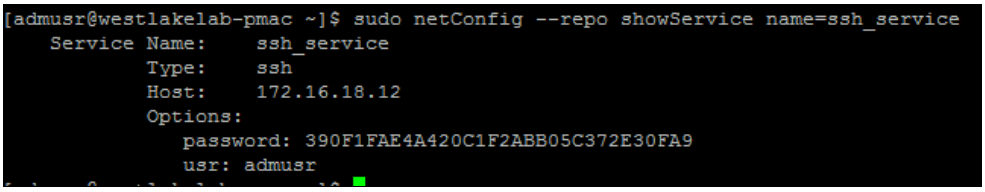
3. ☐	Verify that the release version has been updated	Run the following command and verify the release
		`$ appRev`
		`[admusr@slak-pmac ~]$ appRev`
		`Install Time: Wed Dec 7 11:50:31 2016`
		`Product Name: PMAC`
		`Product Release: 6.0.3.0.2_60.28.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 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`

4. ☐	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.

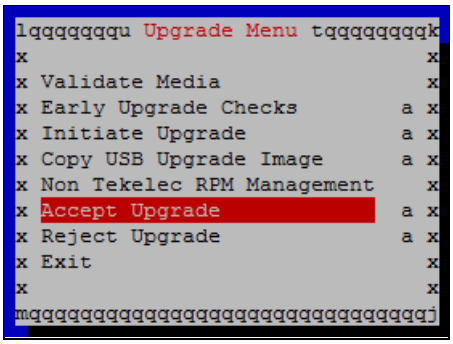
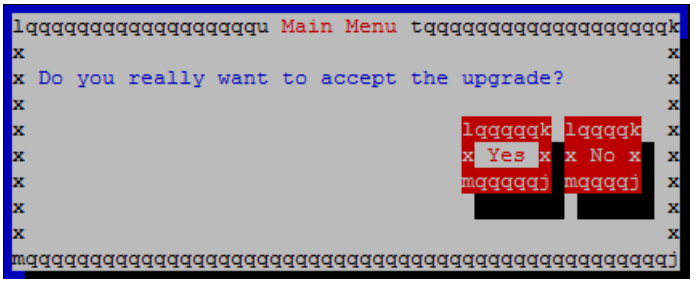
5. ☐	Run syscheck	Run syscheck and verify everything is Ok `$ sudo syscheck`

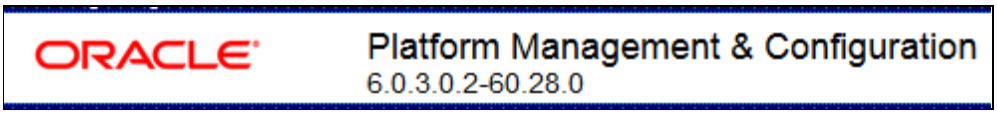
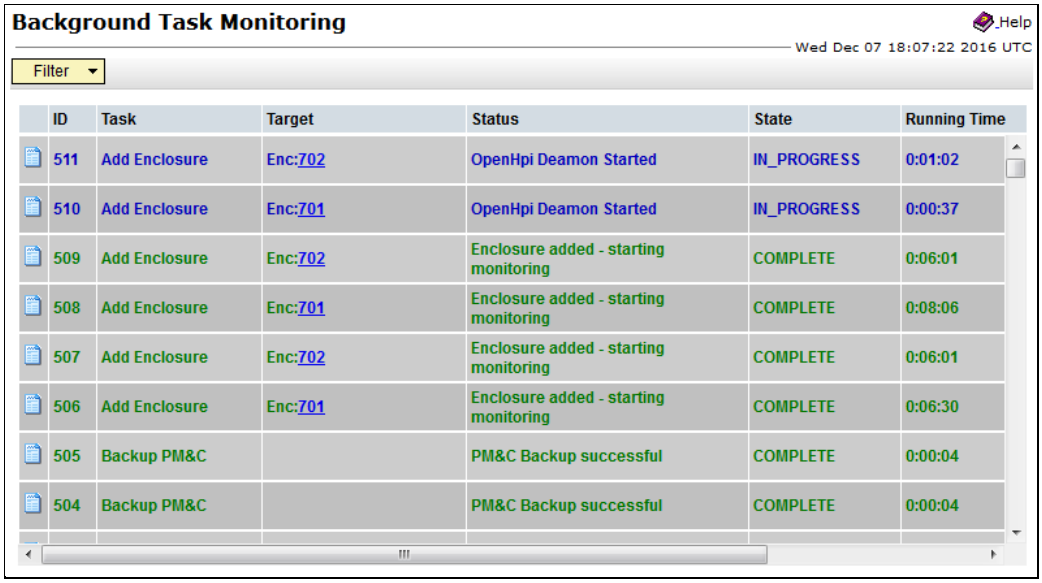
<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>6. ☐</td><td>PM&C SSH CLI: Recreate the ssh_service with admusr credentials on PM&C guest console if it doesn’t exist</td><td>
1. Verify that the ssh service exists with admusr credentials by executing the following command:
<code>$ sudo netConfig --repo showService name=ssh_service</code>


- If the results are similar to the above, that is, the Options field include <code>usr: admusr</code> and an encrypted password, skip to the next step.
- If the Options field does not include the <code>usr: admusr</code> or if the service does not exist, continue with this step:
2. Delete the ssh_service if it exists
<code>$ sudo netConfig --repo deleteService name=ssh_service</code>
Answer <code>YES</code> to the message if prompted.
3. Recreate ssh_service with admusr user.
<code>$ sudo netConfig --repo addService name=ssh_service</code>
<code>Service type? (tftp, ssh, conserver, oa) ssh</code>
<code>Service host? <<i>pm&c_ip_address</i>></code>
<code>Enter an option name (q to cancel): user</code>
<code>Enter a value for user: admusr</code>
<code>Enter an option name(q to cancel): password</code>
<code>Enter a value for password: Duk******</code>
<code>Verify Password: Duk******</code>
<code>Enter an option name(q to cancel): q</code>
Example output


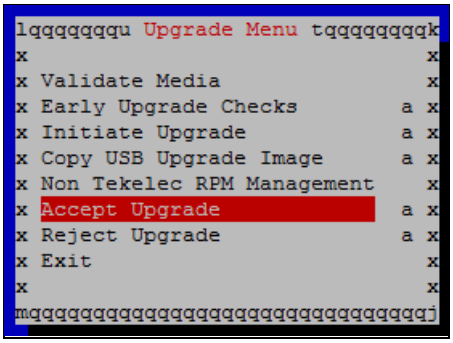
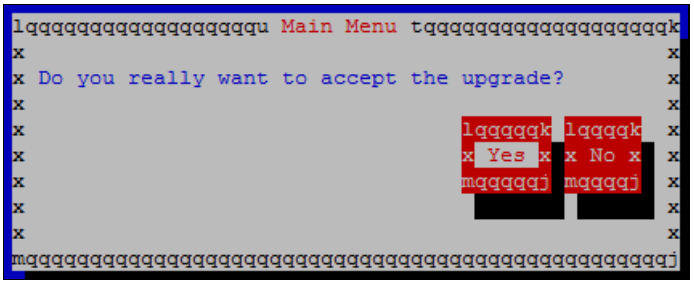
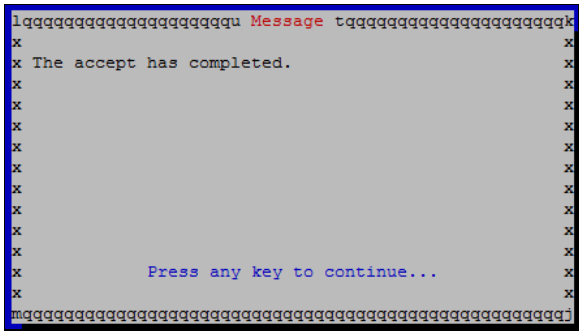
4. Ensure the information entered is correct by executing the following command and compare the output with the configuration in the last step -
<code>$ sudo netConfig --repo showService name=ssh_service</code>
Example output


</td></tr>
</table>

Step	Procedure	Details
7. ☐		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.
8. ☐	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. - Logon to PM&C guest console - Run the platcfg utility. `$ sudo su - platcfg` 2. Navigate to **Maintenance→Upgrade**.  3. Select **Accept Upgrade** and press **Enter.**  4. Click **Yes** to start accept upgrade process. If a message displays prompting you 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).

Step	Procedure	Details
9. ☐	Health Checks	1. Run the following command: `$sudo syscheck` 2. Open a browser and launch the PM&C GUI. 3. Verify the release at the top of the page.  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. 

ID	Task	Target	Status	State	Running Time
511	Add Enclosure	Enc:702	OpenHpi Deamon Started	IN_PROGRESS	0:01:02
510	Add Enclosure	Enc:701	OpenHpi Deamon Started	IN_PROGRESS	0:00:37
509	Add Enclosure	Enc:702	Enclosure added - starting monitoring	COMPLETE	0:06:01
508	Add Enclosure	Enc:701	Enclosure added - starting monitoring	COMPLETE	0:08:06
507	Add Enclosure	Enc:702	Enclosure added - starting monitoring	COMPLETE	0:06:01
506	Add Enclosure	Enc:701	Enclosure added - starting monitoring	COMPLETE	0:06:30
505	Backup PM&C		PM&C Backup successful	COMPLETE	0:00:04
504	Backup PM&C		PM&C Backup successful	COMPLETE	0:00:04

Step	Procedure	Details
10. ☐	Accept the upgrade for TVOE	**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 once an upgrade has been accepted. **NOTE:** After the upgrade is accepted, you are not able to roll back to the previous release. 1. Login as admusr to TVOE host CLI and run the platcfg utility: `$ sudo su - platcfg` 2. Navigate to **Maintenance→Upgrade**.  3. Select **Accept Upgrade** and press the **Enter**.  4. Click **Yes** to start accept upgrade process. **NOTE:** A screen session is launched when accepting the upgrade, press **q** to close the window and return to platcfg utility.  5. Select and press **Enter** on the Exit menu or press **F12** until exiting platcfg. The upgrade process is now complete.
---End of Procedure---		

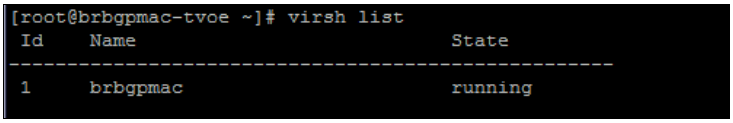
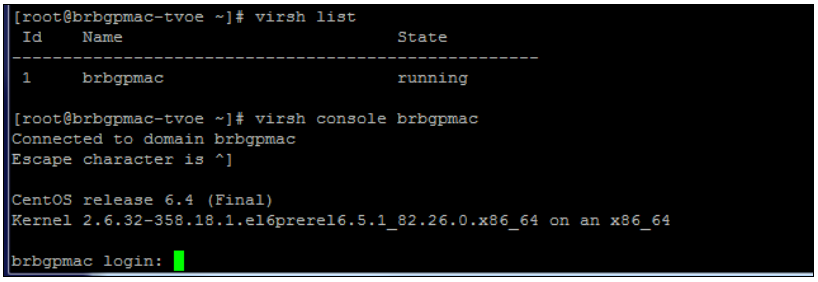
APPENDIX B. TVOE AND PM&C SERVER BACKOUT

This procedure provides instructions to backout/reject the PM&C server upgrade.

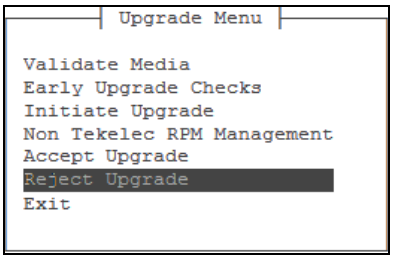
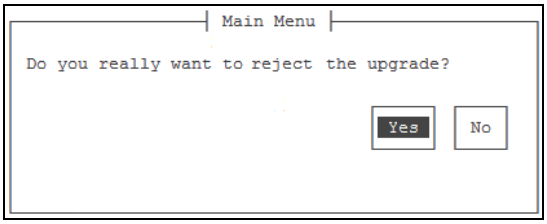
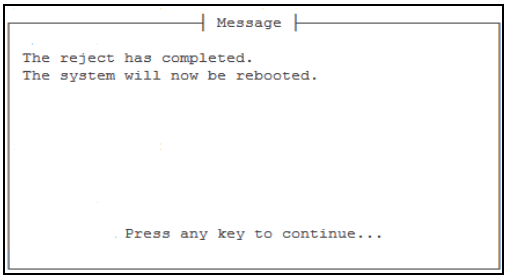
NOTE: A reject cannot be performed after an upgrade has been accepted.

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.

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 <pmacname>`
		 
		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 ~]$`
		NOTE: To break the guest session to go back to TVOE host, press **CTRL+]**

Software Upgrade Procedure

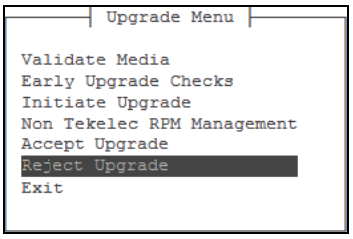
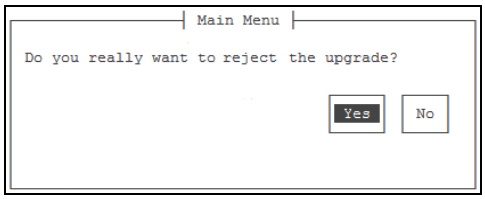
Step	Procedure	Details
3. ☐	Run the platcfg utility on the PM&C Server	1. At the prompt, run: `$sudo su - platcfg` 2. Navigate to Maintenance→Upgrade  3. Select **Reject Upgrade** and press **Enter** to start the reject process. The following window opens, enter yes to begin the backout.  **NOTE:** 5 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, the user is returned to a login prompt. Login as admusr.

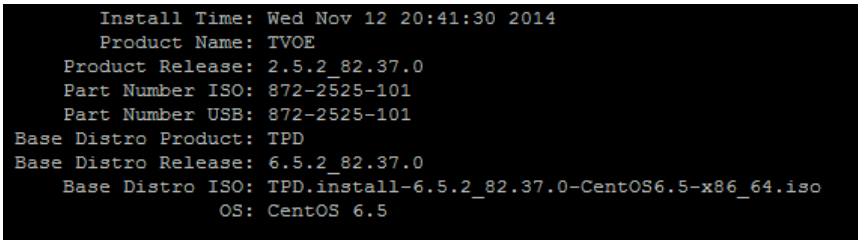
Step	Procedure	Details

6. ☐	Verify backout completed	Execute the following command to verify source PM&C release:
		`[admusr@pmac ~]# 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	As Administrator on the TVOE iLO – log in through the iLO and execute the following command to check the logical drives that are used for the backout.
		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.

Step	Procedure	Details

8. ☐	**TVOE Server iLO:** manually backout upgrade	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.
		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:
		4. Login as admusr.
		`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:`

9. ☐	**TVOE Server iLO:** check server health.	Log in and run the following: `# appRev` 
10. ☐	**TVOE Server iLO:** check server health	Run the following command to check the health of the server: `# sudo alarmMgr --alarmStatus` If any output is produced, an alarm is present on the system. Contact Oracle for information about how to proceed.
11. ☐	Clear browser cache	Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary.
12. ☐	**PM&C GUI**	Login to the PM&C GUI to verify the old PM&C version
---End of Procedure---		

APPENDIX C. CORRECTING SERVER CORE FILE DETECTED ALARMS

After the upgrades, if old core file detected alarms are generated, this procedure corrects these alarms.

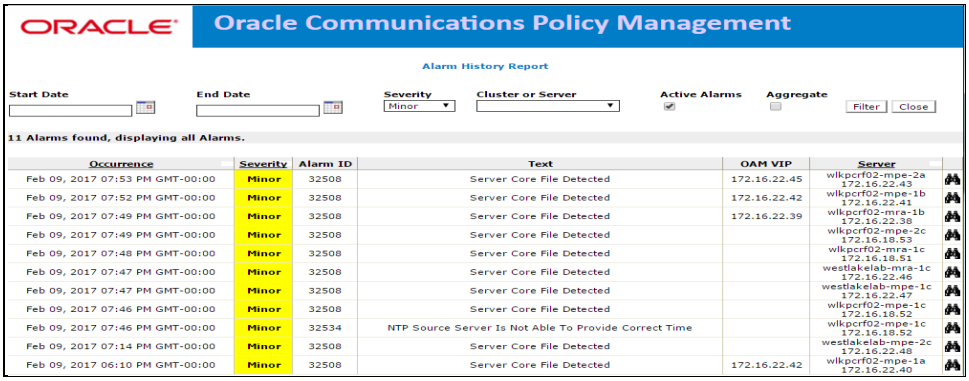
This procedure is performed during a maintenance window.

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

If this procedure fails, contact Oracle Support.

NOTE: this Procedure should take APPROXIMATELY 10 minutes per Blade or RMS server.

Appendix C: Correcting Server Core File Detected Alarms

Step	Procedure	Details
1. ☐	**CMP GUI:** Login into the CMP GUI using VIP address as admin or user with administrative privileges	Login into the PCRF CMP GUI as admin using the VIP IP Address
2. ☐	CMP GUI: Verify active alarms	In the upper right hand corner of the GUI, click on Minor alarms and check if Server Core File Detected alarms are present.  If Server Core File Detected alarms are present, then proceed to the next step, otherwise stop and there is no need to perform this procedure.
3. ☐	**CMP GUI:** Note the server IP addresses where the **Server Core File Detected** alarm was generated	Note down the server IP addresses for which Server Core File Detected alarm was generated.

Step	Procedure	Details

4. ☐	**SSH CLI:** Login to each of the servers and verify that core files are present	1. Login as admusr to each of the noted servers using SSH
		2. Change the user to root and change directory to `/var/TKLC/core`
		`$ sudo su -`
		`# cd /var/TKLC/core`
		`# ls`
		Example:
		`core.java.9499  core.java.9499.bt`
		`# ls /var/camiant/cores`
		Example:
		`core.java.9499`
		NOTE: Where 9499 is the java *proc_id* and is different for each server.

5. ☐	**SSH CLI**: cat the core.java.<*proc_id*>.bt file	Use the cat command on the **core.java.** <*proc_id*>.**bt** file and verify that the core file was generated by **java** due to **Program terminated with signal 3** `# cd /var/TKLC/core` `# cat core.java.<proc_id>.bt` **NOTE:** User may need to scroll up Example below: `==========` `[New Thread 9499]` `[New Thread 9571]` `Core was generated by `/usr/java/jdk1.7.0_72/bin/java -Djava.util.logging.config.file=/opt/camiant/tom'.` `Program terminated with signal 3, Quit.` `#0 0x00000039eba0822d in ?? ()` `==========` If the reason was due to **Program terminated with signal 3,** proceed to the next step; otherwise if the reason was something else then Contact Oracle Support.

6. ☐	**SSH CLI:** Remove the corresponding core files	Remove the following files:
		1. /var/camiant/cores/corefile.java. <*proc_id*>
		2. /var/TKLC/core/corefile.java. <*proc_id*>.bt
		3. /var/TKLC/core/ corefile.java. <*proc_id*>
		`# cd /var/camiant/cores`
		`# rm -rf core.java.<proc_id>`
		`# cd /var/TKLC/core`
		`# rm -rf core.java.<proc_id>.bt`
		`# rm -rf core.java.<proc_id>`
		`# exit`
		`$`

Step	Procedure	Details
7. ☐	**CMP GUI:** Verify alarms	On the CMP GUI, verify that the corresponding Server Core File Detected alarms have been cleared.
---End of Procedure---		

APPENDIX D. 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