Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management 11.5.x/12.1.x to 12.2 Upgrade Procedure Georedundancy Enabled

E82611-02

February 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 Policy Management 11.5.x/12.1.x to 12.2 Upgrade Procedure, Georedundancy Enabled
Copyright © 2013, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

TABLE OF CONTENTS

1. INTRODUCTION 6
1.1 Purpose and Scope 6
1.2 Acronyms 6
1.3 Terminology 7
1.4 Software Release Numbering 7
2. UPGRADE OVERVIEW 8
2.1 Upgrade Status Values 8
2.2 Upgrade Paths 8
2.3 Upgrade Information 8
2.3.1 Required Cluster Upgrade Sequence 9
2.3.2 Policy Release Mixed-Version Operation and Limitation 9
2.4 Customer Impacts 10
2.5 Rollback/Backout 10
2.6 TPD Version 10
2.7 Server Hardware Platforms 10
2.8 Loading Application Software 10
2.9 Required Materials and Remote Access 10
2.9.1 Upgrade Media 11
2.9.2 Login User IDs and Passwords 11
3. THEORY OF OPERATION 13
3.1 Upgrade Manager Page 13
3.1.1 The Upgrade Log 14
3.1.2 Optional Actions 14
3.1.3 The ISO Select 14
3.1.4 Introducing Upgrade Director Behavior 15
4. UPGRADE PREPARATION 18
4.1 Pre-requisites 19
4.2 TVOE and PM&C Server Upgrade 19
4.3 Firmware Upgrade 19
4.4 Plan and Track Upgrades 20
4.5 Convert to Using Interval Statistics 21
4.6 Perform System Health Check 22

4.7 Deploy Policy Upgrade Software 22
4.7.1 Deploying Policy Upgrade Software to Servers 22
4.7.2 Copy ISO image files to Management Server (PM&C) 23
4.7.3 Distribute Application ISO Image Files to Servers 26
4.7.4 Backups and Backup Locations 30
4.7.5 Changing Non-Default *root* and *admusr* Passwords 32

5. UPGRADE CMP CLUSTERS (11.5.X TO 12.2) WIRELESS MODE 36
5.1 Upgrade CMP Clusters Overview 36
5.1.1 Upgrade Primary CMP Cluster 37
5.1.2 Upgrade Secondary CMP Cluster 50

6. UPGRADE CMP CLUSTERS (11.5.X TO 12.2) CABLE MODE 53
6.1 Upgrade CMP Clusters Overview 53
6.1.1 Upgrade Primary CMP Cluster 54
6.1.2 Upgrade Secondary CMP Cluster 66

7. UPGRADE CMP CLUSTERS (12.1.X TO 12.2) 68
7.1 Upgrade CMP Clusters Overview 68
7.1.1 Upgrade Primary CMP Cluster 69
7.1.2 Upgrade Secondary CMP Cluster 80

8. UPGRADE NON-CMP CLUSTERS (MPE, MRA) 11.5.X/12.1.X WIRELESS MODE 84
8.1 Upgrade Preparation 84
8.1.1 Configuration Preparation 84
8.2 Upgrade MRA and MPE Servers 85

9. UPGRADE NON-CMP CLUSTERS (MA, MPE-R, MPE-S, BOD) 11.5.X TO 12.2 CABLE MODE 95
9.1 Site/Segment Upgrade Preparation 95
9.1.1 Configuration Preparation 95
9.2 Upgrade MA Servers 96
9.3 Upgrade MPE-R/S Servers 102
9.4 Upgrade BOD Servers 112

10. POST UPGRADE HEALTH CHECK FOR BOTH CABLE AND WIRELESS SYSTEMS ... 118

11. BACKOUT (ROLLBACK) 11.5.X/12.1.X WIRELESS MODE 120
11.1 Backout Sequence 120
11.2 Pre-requisites 120
11.3 Backout of Fully Upgraded Cluster 120

11.3.1 Backout Sequence 120
11.3.2 Backout of a Partially Upgraded Cluster 122
11.3.3 Backout Fully Upgraded MPE/MRA Cluster 123
11.3.4 Backout Fully Upgraded Secondary CMP Cluster 128
11.3.5 Backout Fully Upgraded Primary CMP Cluster 132

12. BACKOUT (ROLLBACK) CABLE MODE 138
12.1 Backout Sequence 138
12.2 Pre-requisites 138
12.3 Backout of Fully Upgraded Cluster 138
12.3.1 Backout Sequence 138
12.3.2 Backout of a Partially Upgraded Cluster 140
12.3.3 Backout Fully Upgraded BOD Cluster(s) 141
12.3.4 Backout Fully Upgraded MPE-S/R Cluster(s) 144
12.3.5 Backout Fully Upgraded MA Cluster(s) 148
12.3.6 Backout Fully Upgraded Secondary/Primary CMP Cluster 152

APPENDIX A. TVOE AND PM&C SERVER UPGRADE 157
A.1 TVOE Upgrade 158
A.2 PM&C Upgrade 163
A.3 Verify PM&C Upgrade 165

APPENDIX B. TVOE AND PM&C SERVER BACKOUT 172

APPENDIX C. CORRECTING SERVER CORE FILE DETECTED ALARMS 177

APPENDIX D. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE AND HOTLINES 180

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform a software upgrade of Oracle Communications Policy Management Release 11.5.x/12.1.x to Release 12.2 when georedundancy is enabled.

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

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

1.2 Acronyms

Acronym	Definition
BoD	Bandwidth on Demand - a type of component in a cable Policy Management solution
CMP	Configuration Management Platform
DR-CMP	Configuration Management Platform for Disaster Recovery NOTE: It refers to the CMP on the secondary site
DSR	Diameter Signaling Router
GUI	Graphical User Interface
IPM	Initial Product Manufacture
LVM	Logical Volume Manager
MA	Management Agent - a type of component in a cable Policy Management solution
MPE	Multimedia Policy Engine
MPE-LI	MPE for Lawful Intercept - a type of Multimedia Policy Engine
MPE-R	Routing MPE - a type of component in a cable Policy Management solution
MPE-S	Servicing MPE - a type of component in a cable Policy Management solution
MRA	Multiprotocol Routing Agent (also known as the Policy Front End or PFE)
OCS	Online Charging System
OOS	Out of Service
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rules Function—Oracle MPE
PM&C	Platform Management and Configuration
Segment	A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster may be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment

Acronym	Definition
UE	User Equipment

1.3 Terminology

Primary Site (Site1)—Site where the MPE/MRA/MA/BoD Server-A and Server-B are deployed

Secondary Site (Site2)—Site where the MPE/MRA/MA/BoD Server-C is deployed.

Spare Server or Server-C—Server that is ready to take over from the Active server if both the Active and Standby servers fail. It is generally in a different location than the Active and Standby servers.

1.4 Software Release Numbering

- Firmware
  - Oracle: 3.1.5
  - HP Solutions Firmware Upgrade Pack: 2.2.9 or higher
- COMCOL: 6.4
- PM&C: 6.0.3
- TPD: 7.0.3
- TVOE: 3.0.3
- Policy Management release 12.2

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute Policy Management release 12.2 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 11.5.x (cable and wireless) to 12.2
2. Policy Management 12.1.x to 12.2

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, MA, or BoD.

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

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-12.2 release and release 12.2 mixed configuration would support the performance and capacity of pre-12.2 release. The mixed version Policy Management configuration would support pre-12.2 release features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the release 12.2 CMP will be managing servers in both the previous release and release 12.2. In this mixed version configuration release 12.2 CMP will 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 12.2 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/BoD 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 R12.2	MRA R12.2	MPE R12.2	MA R12.2	BoD 12.2
CMP 11.5.x, 12.1.x	Yes	No	No	No	No
MRA 11.5.x, 12.1.x	Yes	Yes	Yes	N/A	N/A
MPE 11.5.x, 12.1.x	Yes	Yes	Yes	Yes	Yes
MA 11.5.x	Yes	N/A	Yes	Yes	Yes
BoD 11.5.x	Yes	N/A	Yes	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of the CMP and DR-CMP from the previous release to release 12.2. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to release 12.2.

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 12.2.

2.7 Server Hardware Platforms

The Policy Management release 12.2 software upgrade can be applied on any server that previously had Policy Management release 11.5.x, or 12.1.x

2.8 Loading Application Software

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

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

2.9 Required Materials and Remote Access

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

1. Policy 12.2 software ISO files and TPD software ISO
2. Policy 12.2 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 will need to 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/MA/BoD servers	**admusr** password:
Target iLO	iLO Administrator Login User/Password
Target OA	OA Administrator Login User/Password
PM&C server	GUI Administrator Login User/Password
	admusr password
Software Upgrade Target Release[1]	Target Release Number
	Policy 12.2 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.

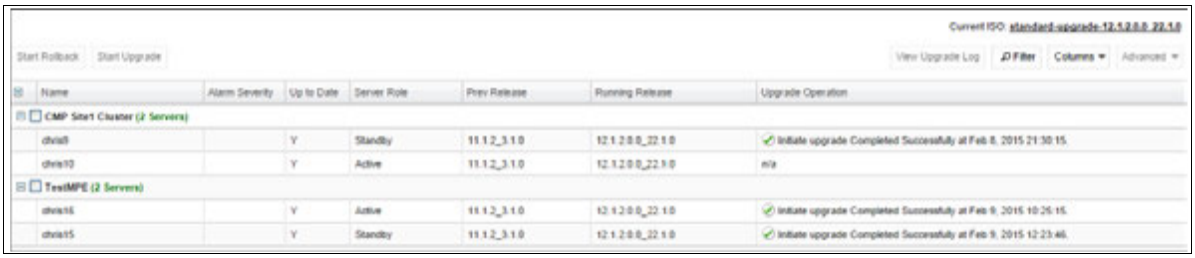


Figure 1 Sample display of the Upgrade Manager page

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 will cause 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 will raise alarms to indicate that it is initiating upgrade activity.
    - Servers will 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 will display 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.

upgradeDirectorTicketsDialog.jsp - Google Chrome

10.148.242.110/mi/pages/upgradeDirectorTicketsDialog.jsp?id=C2013&name=TestMPE

Upgrade Log

Cluster Name: TestMPE
Last Update: 2/9/2015 14:12:58

Filter Columns

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 will upgrade 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 will ONLY be populated with legal/reasonable actions. Actions that are wrong or inconsistent will 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 will search 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.

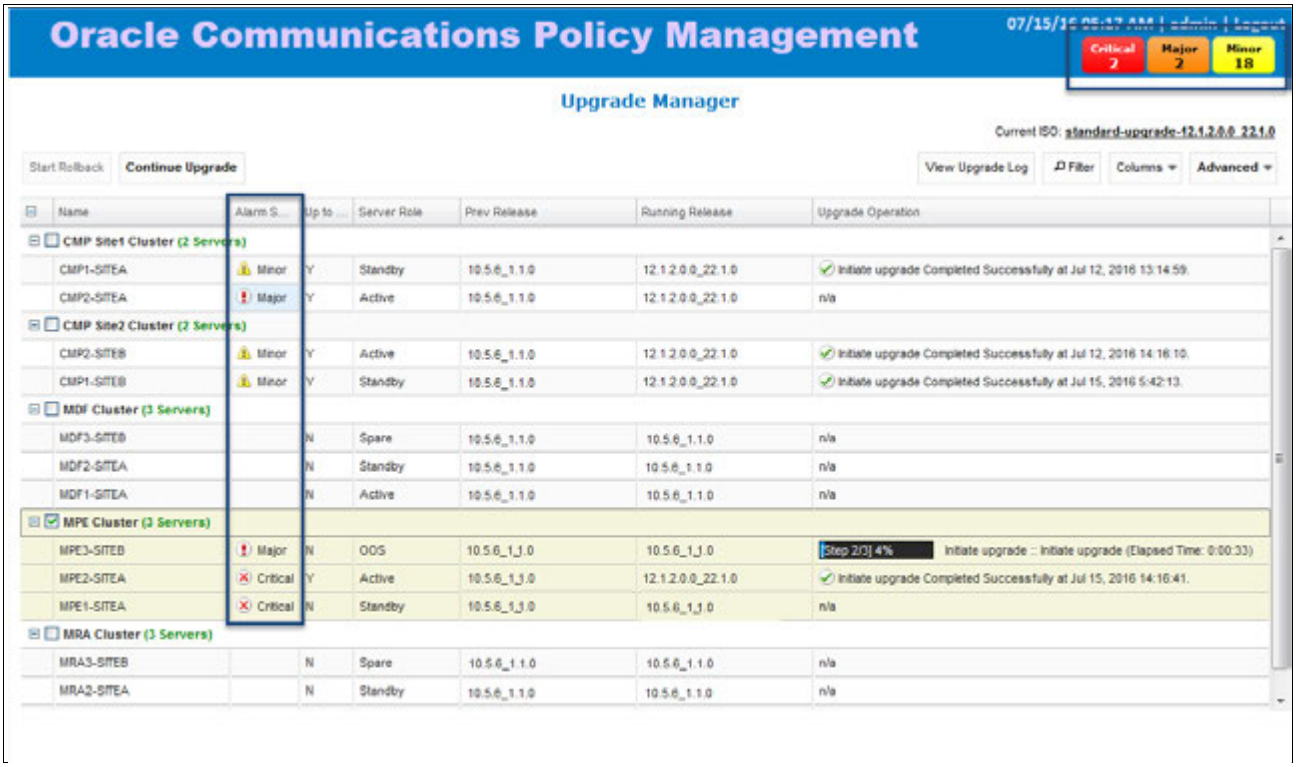


Figure 3 Upgrade in Progress Showing Transient Alarms

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

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

The Upgrade Manager will also assert 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 12.2, 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] The name of alarm 31283 changed in 12.1.2: Before 12.1.2, it was “HA Server Offline,” with 12.1.2 it became “Lost Communication with Server.” Depending on the original release and the upgrade progress, you might see the alarm with one or the other name.

2. Failover
3. Upgrade the remaining server.

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

- For upgrade:
    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 will wait until it can contact the unreachable server before it will take 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 will not be 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 will require 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 executed 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.

TVOE, PM&C and Firmware might need to be upgraded prior to upgrade to Policy Management release 12.2.		
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 12.2 Release Notes (E72271) 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.**
THIS PROCEDURE HAS BEEN COMPLETED		

4.2 TVOE and PM&C Server Upgrade

Policy Management release 12.2 requires PM&C Version 6.0.3 to support IPM of TPD 7.0.3 on c-Class servers.

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

See Appendix A to upgrade the TVOE and PM&C.

4.3 Firmware Upgrade

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

4.4 Plan and Track Upgrades

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

1. **Prerequisite:** 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 will take approximately 1 and ½ hours to complete	Site Names _____ and _____		3 hrs
4. ☐	Upgrade Site1 MPE/MRA clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site2 clusters for Segment-1	Site Names _____ Cluster List:		2 hrs

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

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 will no longer be available. You must migrate to Interval statistics before upgrading to Release 12.2. Upon upgrade to R12.2, Oracle Communications Policy Management will only use Interval statistics and any Manual statistics not saved will be lost.

Statistics affected by this change will be 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 12.2

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 executed 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 (i.e., 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.
		• Validate the IP connectivity between the server and NTP servers by PING.
		• Confirm that time is synchronized on each server using the following CLI shell command:
		`ntpq -np`
		• Confirm that date is correct on each server.
		• Check that BIOS clock is synced with the clock using the following CLI shell command:
		`hwclock`

THIS PROCEDURE HAS BEEN COMPLETED		

4.7 Deploy Policy Upgrade Software

Software should be deployed to each Policy server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This will typically be 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 12.2, 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, MA, and BoD). A single image must be deployed to the `/var/TKLC/upgrade` directory of each server to be upgraded, where the image is the correct type for that server. That is, the CMP software image must be deployed to the CMP servers, the MPE image deployed to the MPE servers, and so on.

IMPORTANT: If the deployed image type (CMP, MPE, MRA, etc.) does not match the existing installed software type, the upgrade will fail. Example: An attempt to upgrade a CMP with a MPE software image will fail 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 will fail.

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.

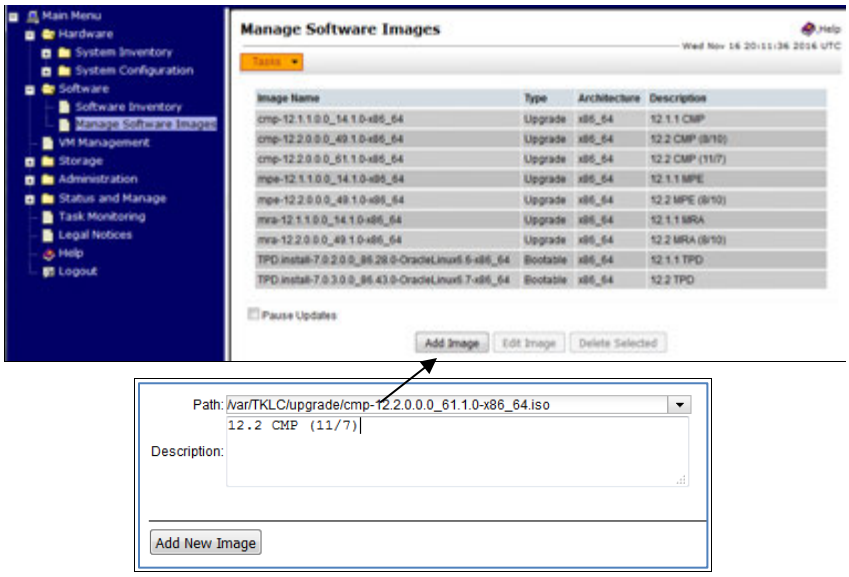
IMPORTANT: PM&C is not used for the upgrade activities. The purpose of this procedure is to be prepared for server recovery activities in case a server needs to be re-installed with software.

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 12.2 ISO files on the server	Log on to the PM&C Server GUI **Software → Manage Software Images** Confirm that the release 12.2 ISO files do not exist. If there are files, remove them.

2. ☐	SSH to PM&C server as admusr	• Log on as admusr to the PM&C server.
		• 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 12.2 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.
4. ☐	**PM&C GUI:** Adding the new release 12.2 ISO files	**Software → Manage Software Images** • Click **Add Image** to select the ISO files that were transferred to the PM&C server.  • Click **OK** on the pop-up

Step	Procedure	Result
5. ☐	**PM&C GUI:** Verify that the ISO files were added successfully	**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: **Background Task Monitoring** Mon Sep 28 13:43: Filter | ID | Task | Target | Status | State | Running Time | Start Time | Progress | | 610 | Add Image | | Done: cmp-12.1.2.0.0_22.1.0.x86_64 | COMPLETE | 0:00:20 | 2015-09-28 13:43:09 | 100% | **NOTE:** The added ISO files are now stored in the `/var/TKLC/smac/image/repository` directory
THIS PROCEDURE HAS BEEN COMPLETED		

4.7.3 Distribute Application ISO Image Files to Servers

This procedure applies to all server types. It assumes that the ISO image files will be 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 12.2 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 will be used to upload to the rest of the servers.
THIS PROCEDURE HAS BEEN COMPLETED		

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

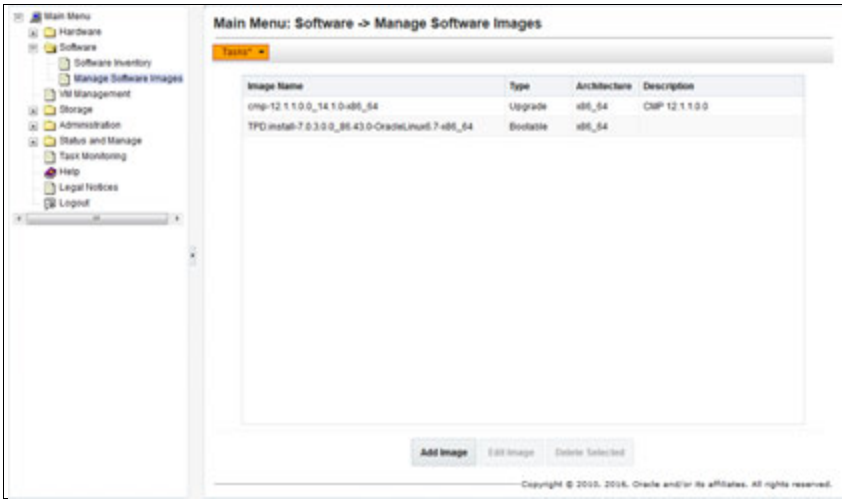
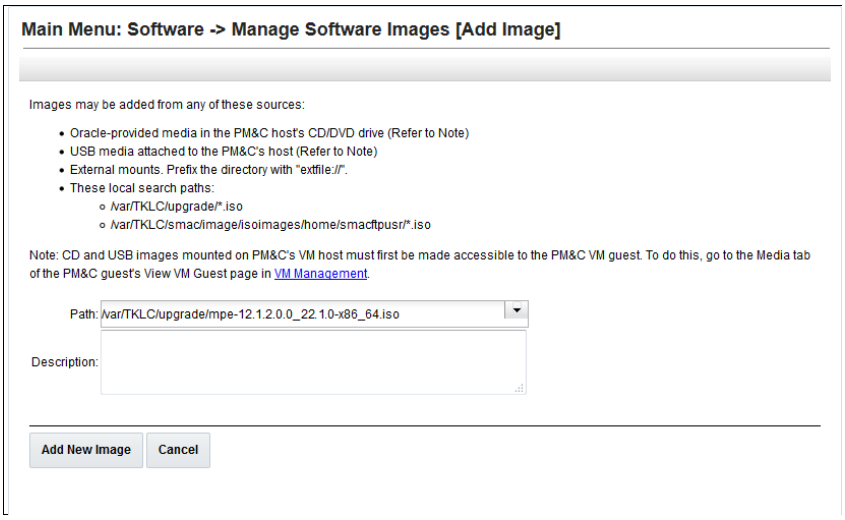
Note: You can instead add images from the following sources:

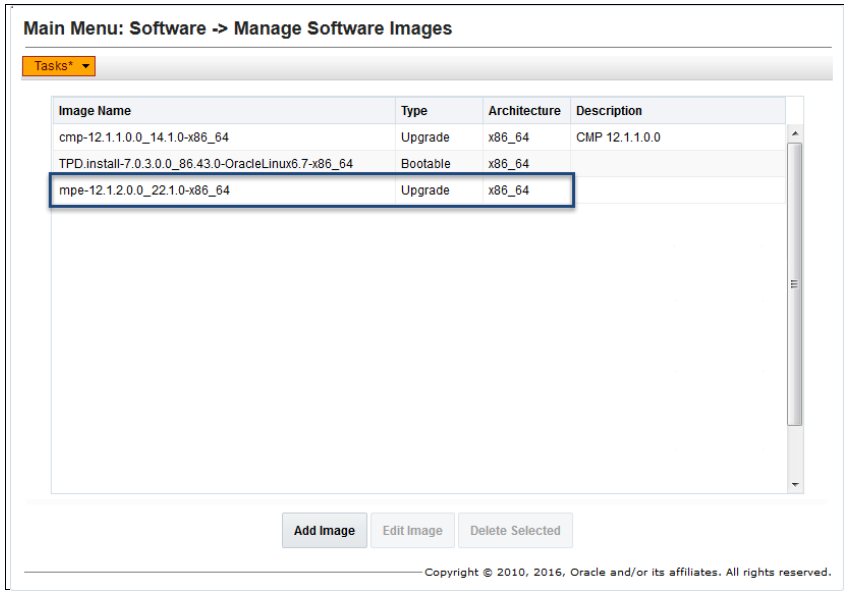
- Media mounted in the CD/DVD drive of the PM&C host
- USB media attached to the PM&C host
- External mounts (prefix the directory with `extfile://`)
- These local search paths:
  - `/var/TKLC/upgrade/`
  - `/var/TKLC/smac/image/isoimages/home/smacftpusr/`

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	• Select **Main Menu** > **Software** > **Manage Software Images** The **Manage Software Images** page opens. For example:  • Click **Add Image** (at the bottom of the page).The **Manage Software Images [Add Image]** page opens. For example:  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 appears in the list. For example: 

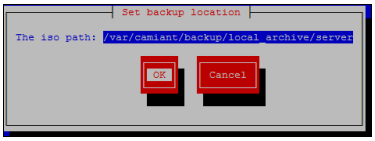
4. ☐	Verify that the image is no longer in the directory	Enter the following command:
		
		`$ sudo ls /var/TKLC/upgrade`
		`$`

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

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.
		
		• Login into the active Primary CMP server.
		• Navigate to the following through platcfg utility.
		`$sudo su - platcfg`
		• **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`
		 
		
		• Go back to the previous menu (**Policy Configuration→Backup and Restore)** and select now **→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`

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`

Step	Procedure	Result

3. ☐	Copy backup files.	• 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>`
		• 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: _____ _____ _____
THIS PROCEDURE HAS BEEN COMPLETED		

4.7.5 Changing Non-Default *root* and *admusr* Passwords

4.7.5.1 Improve Password Security

The default password hash prior to Policy 12.0 is MD5. MD5 is now considered a weak hash that can be brute force cracked in a reasonable amount of time. The best hash to use is SHA512. This is currently the strongest hash supported on the platform. Due to this change, during upgrade, all non-default passwords are automatically expired. This will cause issues during upgrade from pre-12.1.1to 12.2 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 will be 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 12.2, they will be expired post upgrade.

IMPORTANT: The following procedure should be executed prior to the upgrade to 12.2 only if the root or admusr passwords are non-default.

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

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

Step	Procedure	Result

1. ☐	Login to the active CMP server	• **For an upgrade from 11.5.x/12.1.x**, login as *admusr* and change to *root* using the following command:
		`$sudo su`
		`login as: admusr`
		`Using keyboard-interactive authentication.`
		`Password:`

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

Step	Procedure	Result
3. ☐	Order to perform the change	Perform steps 4-15 on each server in the following order: • Standby CMP • Active CMP • Standby non-CMP servers • Spare non-CMP servers • Active non-CMP servers

4. ☐	Login to the Server	• **For an upgrade from 11.5.x/12.1.x**, login as *admusr* and change to *root* using the following command:
		`$sudo su`
		`login as: admusr`
		`Using keyboard-interactive authentication.`
		`Password:`

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

6. ☐	Modify the `system-auth` file	• Open the `system-auth` file.
		`#vi /etc/pam.d/system-auth`
		• 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`
		`#%PAM-1.0`
		`# This file is auto-generated.`
		`# User changes will be destroyed the next time authconfig is run.`
		`auth required pam_env.so`
		`auth sufficient pam_unix.so nullok try_first_pass`
		`auth requisite pam_succeed_if.so uid >= 500 quiet`
		`auth required pam_deny.so`
		`account required pam_unix.so`
		`account sufficient pam_localuser.so`
		`account sufficient pam_succeed_if.so uid < 500 quiet`
		`account required pam_permit.so`
		`password requisite pam_cracklib.so try_first_pass retry=3 type= enforce_for_root minclass=3`
		`password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok`
		`password required pam_deny.so`
		`session optional pam_keyinit.so revoke`
		`session required pam_limits.so`
		`session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid`
		`session required pam_unix.so`

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`

Step	Procedure	Result

8. ☐	Checkout revisions for `login.defs` file	`#rcstool co /etc/login.defs`
		`[root@cmp-1a ~]# rcstool co /etc/login.defs`
		`RCS_VERSION=1.1`

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

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`
		`[root@cmp-1a ~]# rcstool co /etc/libuser.conf`
		`RCS_VERSION=1.1`

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

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

Step	Procedure	Result

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.
THIS PROCEDURE HAS BEEN COMPLETED		

5. UPGRADE CMP CLUSTERS (11.5.X TO 12.2) WIRELESS MODE

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

5.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster
   a. Use the CMP GUI—System Maintenance (11.5.x) to place Primary Standby CMP into Force-Standby
   b. Use the CMP GUI—System Maintenance (11.5.x) to upgrade the Primary Force-Standby CMP server
   c. Use the CMP GUI—System Maintenance (11.5.x) to perform Switch Force-Standby on the Primary CMP cluster
   d. Log back into the CMP GUI and upgrade the remaining Primary CMP that is the Force-Standby server using the 12.2 Upgrade Manager
2. Upgrade the Secondary CMP cluster (if applicable)
   a. Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2
   b. Start upgrade
   c. Continue upgrade—failover
   d. 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 Georedundant Status	Operator Site Name	Site Designation from Topology Form (Site1 or Site2)
Primary Site		
Secondary Site		

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP Address _____

Server-A Status _____

Server-B Hostname _____

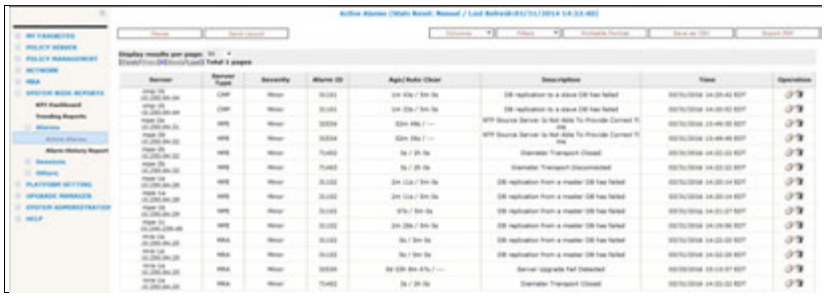
Server-B IP Address _____

Server-B Status _____

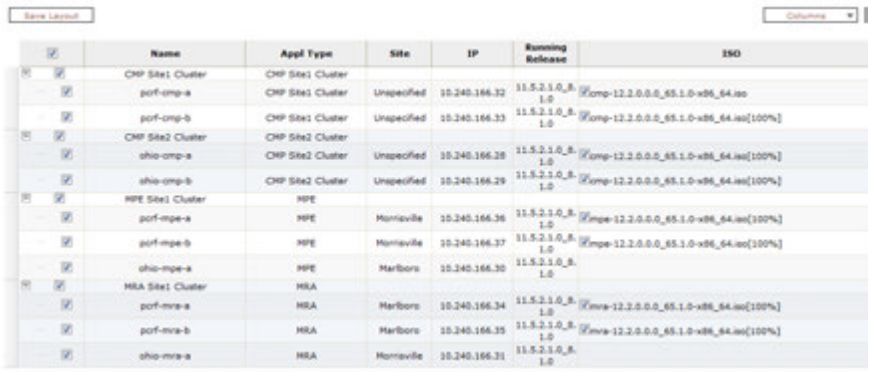
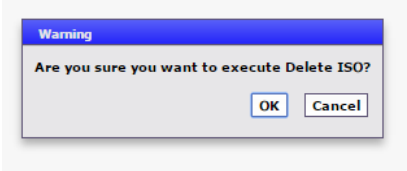
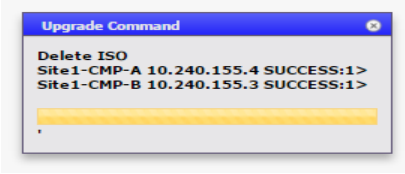
IMPORTANT:

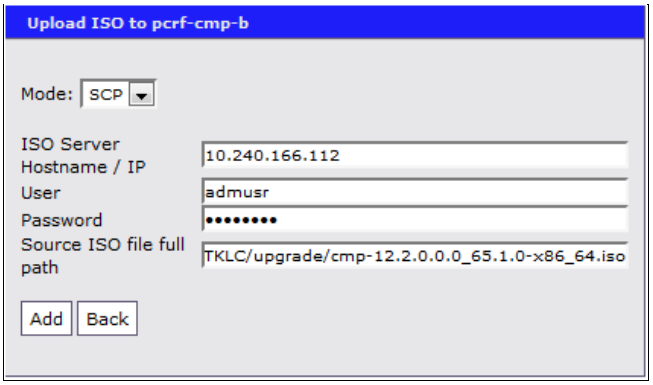
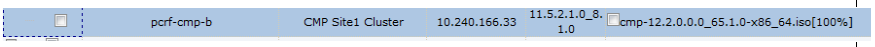
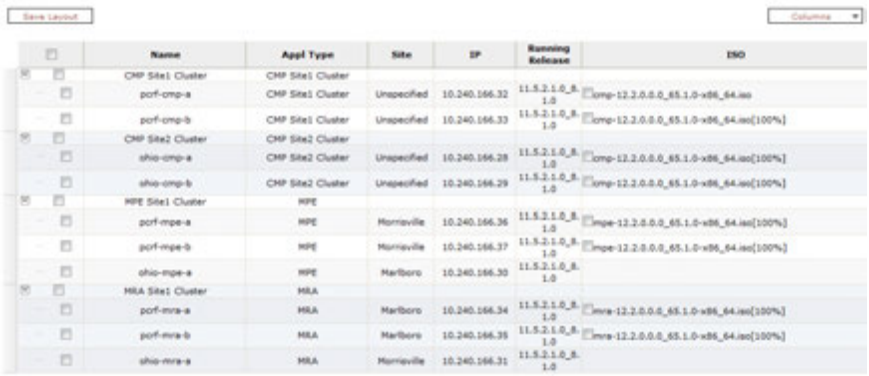
- *CMP servers MUST be upgraded first, before the MPE or MRA clusters*
- *Site1 CMP MUST be upgraded to the new release first, before the Site2 CMP (if applicable)*

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 no impact to the upgrade procedure. • Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and record the CMP cluster(s)	Navigate to **Platform Setting→Topology Settings → All Clusters** Cluster Configuration Add CMP Site1 Cluster Add CMP Site2 Cluster Add MPE/MRA Cluster Cluster Settings • 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. • Save a screenshot for future reference.
3. ☐	**CMP GUI**: Verify status of CMP clusters	**Upgrade Manager → System Maintenance** Confirm the CMP clusters have the following: • Active/Standby status • Running release of 11.5.x version • Replication ON • Corresponding Release 12.2 ISO files copied to at least one of each server types (CMP/MRA/MPE)—Meaning, a copy of the MPE ISO file is on one of the MPE servers, an MRA ISO file is on one of the MRA servers and a copy of the CMP ISO file is on one CMP server

Name	Appl Type	Site Preference	OAM VIP	Server-A	Server-B	Server-C	Operation
CMP Site1 Cluster (P)	CMP Site1 Cluster	N/A	10.240.166.24	10.240.166.32	10.240.166.33	N/A	View Demote
CMP Site2 Cluster (S)	CMP Site2 Cluster	N/A	10.240.166.60	10.240.166.28	10.240.166.29	N/A	View Delete
MPE Site1 Cluster	MPE	Normal	<None> (P) <None> (S)	10.240.166.36	10.240.166.37	10.240.166.30	View Delete
MRA Site1 Cluster	MRA	Normal	<None> (P) <None> (S)	10.240.166.34	10.240.166.35	10.240.166.31	View Delete

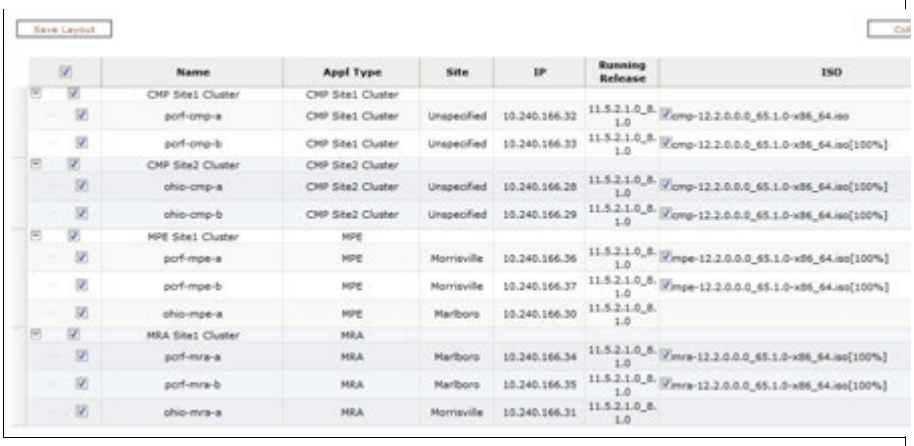
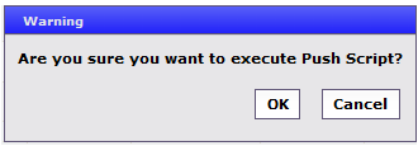
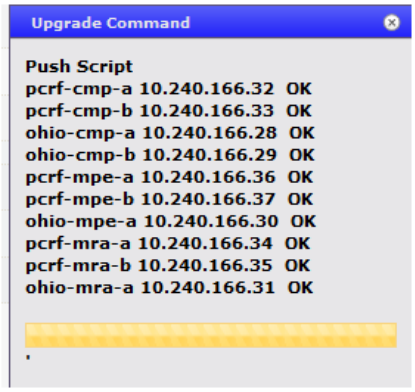
Step	Procedure	Result
4. ☐	**CMP GUI Access** into Primary CMP Server: Remove old ISO files from servers.	**Upgrade Manager → ISO Maintenance** • Select the servers that show old ISO files. • Select the server cluster and select **Operations→ Delete ISO** for any of the older ISO files in the list. •  • Click **OK** to continue  • wait until the successful deletion message appears •  • Wait until the ISO Maintenance page refreshes to show there is not an ISO file in the ISO column.
5. ☐	**CMP GUI:** Distribute ISO files to CMP/MPE/MRA servers **NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly.	**Upgrade Manager → ISO Maintenance** • (Optional but Preferred) Filter CMP/MPE/MRA servers • One application at a time, select one server type (MPE, MRA, or CMP) to be upgraded. **NOTE:** The ISO files for each application type must already be copied over to at least one server. See 4.6.3 "Distribute Application ISO Image Files to Servers" on page 26. • Select **Operations → Upload ISO** • Fill in the dialog with the following information: **Mode**: Select **SCP** **ISO Server Hostname/IP**: *<IP_address_where_ISO_files_are_located>*

Step	Procedure	Result
		User: admusr **Password**: *<admusr_password_for_the_server>* **Source ISO file full path**: */var/TKLC/upgrade/<ISO file>*  • Click **Add** and wait till filename appears under the "ISO" column and file is 100% transferred: •  When completed, the ISO column will be populated with the ISO filename and a notification of [100%]  NOTE: For those servers the ISO file was transferred from the local machine, there will not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management screen of CMP GUI.

6. ☐	**SSH CLI Primary Active CMP:** Copy latest upgrade scripts and Exchange keys	• Ssh to active CMP, login as admusr user then mount the upgrade iso file to copy the latest upgrade scripts as follows:
		`$sudo mount -o loop /var/TKLC/upgrade/cmp-12.2.0.0.0_65.1.0-x86_64.iso /mnt/upgrade/`
		`$sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		`$sudo umount /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.2.0.0.0_65.1.0-x86_64.iso /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		`[admusr@pcrf-cmp-a ~]$ sudo umount /mnt/upgrade/`
		`[admusr@pcrf-cmp-a ~]$`
		• Run the following command to exchange the SSH keys with all servers in the topology:

Step	Procedure	Result

		`$sudo qpSSHKeyProv.pl --prov`
		
		NOTE: You need to supply the PASSWORD of *admusr* for command to process
		
		`[admusr@pcrf-cmp-a ~]$ sudo qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		`Connecting to admusr@pcrf-mra-a ...`
		`Connecting to admusr@ohio-mpe-a ...`
		`Connecting to admusr@pcrf-mpe-a ...`
		`Connecting to admusr@ohio-cmp-a ...`
		`Connecting to admusr@pcrf-mra-b ...`
		`Connecting to admusr@pcrf-cmp-b ...`
		`Connecting to admusr@pcrf-cmp-a ...`
		`Connecting to admusr@ohio-cmp-b ...`
		`Connecting to admusr@ohio-mra-a ...`
		`Connecting to admusr@pcrf-mpe-b ...`
		
		`[1/10] Provisioning SSH keys on pcrf-mra-a ...`
		
		`[2/10] Provisioning SSH keys on ohio-mpe-a ...`
		
		`[3/10] Provisioning SSH keys on pcrf-mpe-a ...`
		
		`[4/10] Provisioning SSH keys on ohio-cmp-a ...`
		
		`[5/10] Provisioning SSH keys on pcrf-mra-b ...`
		
		`[6/10] Provisioning SSH keys on pcrf-cmp-b ...`
		
		`[7/10] Provisioning SSH keys on pcrf-cmp-a ...`
		
		`[8/10] Provisioning SSH keys on ohio-cmp-b ...`
		
		`[9/10] Provisioning SSH keys on ohio-mra-a ...`
		
		`[10/10] Provisioning SSH keys on pcrf-mpe-b ...`
		
		`SSH keys are OK.`
		
		`[admusr@pcrf-cmp-a ~]$`
		
		• Verify that the Keys are exchanged successfully with all the server clusters as follows :
		
		`$sudo qpSSHKeyProv.pl --check`
		
		NOTE: You need to supply the PASSWORD of *admusr* for command to process
		
		`[admusr@pcrf-cmp-a ~]$ sudo qpSSHKeyProv.pl --check`
		
		`The password of admusr in topology:`
		`Connecting to admusr@pcrf-mra-a ...`
		`Connecting to admusr@ohio-mpe-a ...`
		`Connecting to admusr@pcrf-mpe-a ...`
		`Connecting to admusr@ohio-cmp-a ...`
		`Connecting to admusr@pcrf-mra-b ...`
		`Connecting to admusr@pcrf-cmp-b ...`
		`Connecting to admusr@pcrf-cmp-a ...`
		`Connecting to admusr@ohio-cmp-b ...`
		`Connecting to admusr@ohio-mra-a ...`
		`Connecting to admusr@pcrf-mpe-b ...`
		
		`[1/10] Checking SSH keys on pcrf-mra-a ...`
		
		`[2/10] Checking SSH keys on ohio-mpe-a ...`
		
		`[3/10] Checking SSH keys on pcrf-mpe-a ...`
		
		`[4/10] Checking SSH keys on ohio-cmp-a ...`
		
		`[5/10] Checking SSH keys on pcrf-mra-b ...`
		
		`[6/10] Checking SSH keys on pcrf-cmp-b ...`
		
		`[7/10] Checking SSH keys on pcrf-cmp-a ...`
		
		`[8/10] Checking SSH keys on ohio-cmp-b ...`
		
		`[9/10] Checking SSH keys on ohio-mra-a ...`
		
		`[10/10] Checking SSH keys on pcrf-mpe-b ...`
		
		`SSH keys are OK.`
		
		`[admusr@pcrf-cmp-a ~]$`

Step	Procedure	Result
7. ☐	**CMP GUI**: Push the release 12.2 upgrade scripts to all servers in the segment topology	**Upgrade Manager → ISO Maintenance** • Select all the servers in the topology as shown in the figure. • Under **Operations** menu, select the "**Push Script**" operation. (It is safe to run the push script multiple times as needed)  • At the popup warning to execute Push Script click "**OK**" to continue the operation.  • After a minute or so, a successful popup window similar to this should appear:  **NOTE:** Give the push script a minute to complete

Save Layout

	Name	Appl Type	Site	IP	Running Release	ISO
☑	CMP Site1 Cluster	CMP Site1 Cluster				
☑	pcrf-cmp-a	CMP Site1 Cluster	Unspecified	10.240.166.32	11.5.2.1.0_8.1.0	☑cmp-12.2.0.0.0_65.1.0-x86_64.iso
☑	pcrf-cmp-b	CMP Site1 Cluster	Unspecified	10.240.166.33	11.5.2.1.0_8.1.0	☑cmp-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	CMP Site2 Cluster	CMP Site2 Cluster				
☑	ohio-cmp-a	CMP Site2 Cluster	Unspecified	10.240.166.28	11.5.2.1.0_8.1.0	☑cmp-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	ohio-cmp-b	CMP Site2 Cluster	Unspecified	10.240.166.29	11.5.2.1.0_8.1.0	☑cmp-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	MPE Site1 Cluster	MPE				
☑	pcrf-mpe-a	MPE	Morrisville	10.240.166.36	11.5.2.1.0_8.1.0	☑mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	pcrf-mpe-b	MPE	Morrisville	10.240.166.37	11.5.2.1.0_8.1.0	☑mpe-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	ohio-mpe-a	MPE	Marlboro	10.240.166.30	11.5.2.1.0_8.1.0	
☑	MRA Site1 Cluster	MRA				
☑	pcrf-mra-a	MRA	Marlboro	10.240.166.34	11.5.2.1.0_8.1.0	☑mra-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	pcrf-mra-b	MRA	Marlboro	10.240.166.35	11.5.2.1.0_8.1.0	☑mra-12.2.0.0.0_65.1.0-x86_64.iso[100%]
☑	ohio-mra-a	MRA	Morrisville	10.240.166.31	11.5.2.1.0_8.1.0	

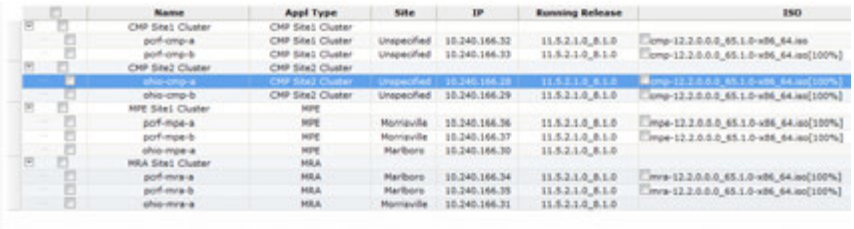
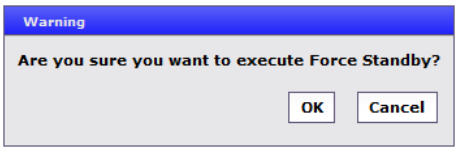
Warning

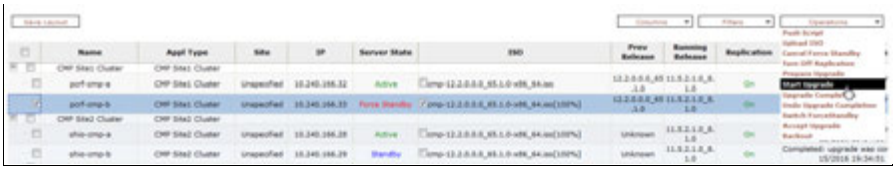
Are you sure you want to execute Push Script?

OK Cancel

Upgrade Command

Push Script
pcrf-cmp-a 10.240.166.32 OK
pcrf-cmp-b 10.240.166.33 OK
ohio-cmp-a 10.240.166.28 OK
ohio-cmp-b 10.240.166.29 OK
pcrf-mpe-a 10.240.166.36 OK
pcrf-mpe-b 10.240.166.37 OK
ohio-mpe-a 10.240.166.30 OK
pcrf-mra-a 10.240.166.34 OK
pcrf-mra-b 10.240.166.35 OK
ohio-mra-a 10.240.166.31 OK

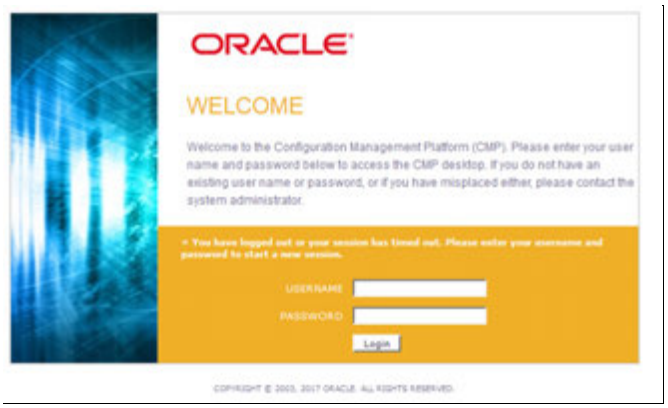
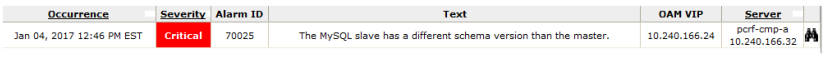
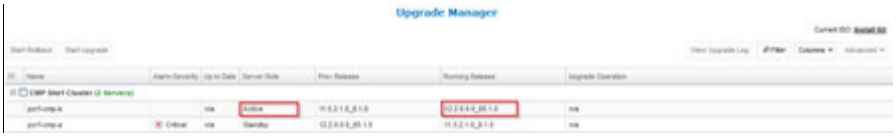
Step	Procedure	Result
8. ☐	**CMP GUI:** Verify ISO file distribution to all the servers	**Upgrade Manager → ISO Management** • Verify that the release 12.2.x.0 ISO file of the correct type is shown for each server. • When completed, the ISO column is populated with the ISO filename and a notification of [100%] **NOTE:** For servers where the ISO was copied to from the local machine, there will not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management feature. 
9. ☐	**CMP GUI**: Set Force Standby mode on the Standby CMP in the Primary cluster	**Upgrade Manager → System Maintenance** • Select the checkbox for the Standby CMP Server at Primary Site • Select **Operations→Force Standby** • Click **OK** to confirm and continue with the operation.  • The Standby CMP server state will be changed to Force Standby.

Step	Procedure	Result
10. ☐	**CMP GUI:** Upgrade the **Force-Standby** CMP server at the primary site **NOTE:** This will take approximately 40 minutes to complete.	**Upgrade Manager → System Maintenance** • Check Force-Standby CMP Server at the Primary Site. • Under **Operations drop down menu, Click 'Start Upgrade'** operation  • Click **OK** to continue with the operation. • Monitor the upgrade status activities from the 'Upgrade Status' column During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical alarm</u>** **31283** HA Server Offline Occurrence: Jan 04, 2017 11:36 AM EST; Severity: Critical; Alarm ID: 31283; Text: High availability server is offline; OAM VIP: 10.240.166.24; Server: pcrf-cmp-a 10.240.166.32 **<u>Expected Major Alarm</u>** **70004** QP Processes has been brought down for maintenance **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master **31233** High availability path loss of connectivity Occurrence: Jan 04, 2017 11:35 AM EST; Severity: Major; Alarm ID: 70004; Text: The QP processes have been brought down for maintenance.; OAM VIP: 10.240.166.24; Server: pcrf-cmp-b 10.240.166.33 Occurrence: Jan 04, 2017 05:07 PM EST; Severity: Major; Alarm ID: 70022; Text: The MySQL slave failed synchronizing with the master; OAM VIP: 10.240.166.24; Server: pcrf-cmp-a 10.240.166.32 Occurrence: Jan 04, 2017 05:07 PM EST; Severity: Major; Alarm ID: 70021; Text: The MySQL slave is not connected to the master; OAM VIP: 10.240.166.24; Server: pcrf-cmp-a 10.240.166.32 Occurrence: Jan 04, 2017 05:41 PM EST; Severity: Major; Alarm ID: 31233; Text: High availability path loss of connectivity; OAM VIP: 10.240.166.60; Server: ohio-cmp-a 10.240.166.28 **<u>Expected Minor Alarms</u>** **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 Wait until '**Completed: upgrade was completed**…' appears in the Upgrade Status column ***IMPORTANT: If a status message other than the '…upgrade was completed…' message appears, stop here and contact Oracle Technical Services to troubleshoot and determine if a rollback should be executed.***

Step	Procedure	Result
11. ☐	**CMP GUI:** Verify that the upgrade completed successfully	**Upgrade Manager → System Maintenance** • Successful upgrade status will show release 12.2 in the Running Release and Upgrade Operation columns. **NOTE:** Expect the Server State column to show Force Standby. This is the same as the status prior to the upgrade. ***IMPORTANT: Any Sync Broken indicator ( ) signifies that the data replication between the two servers of the cluster is not synced yet. This may take up to 45 minutes depending on the database size. Do not continue if there is a Sync Broken indicator on the server that was upgraded.***

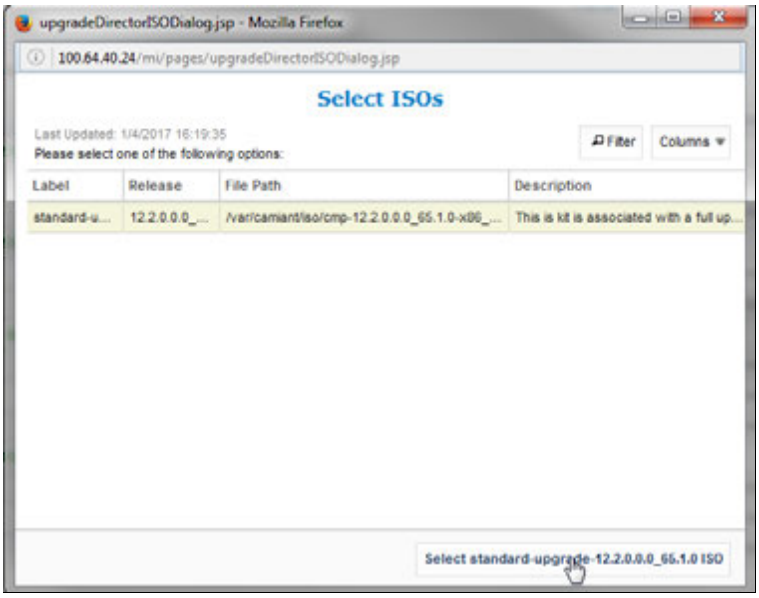
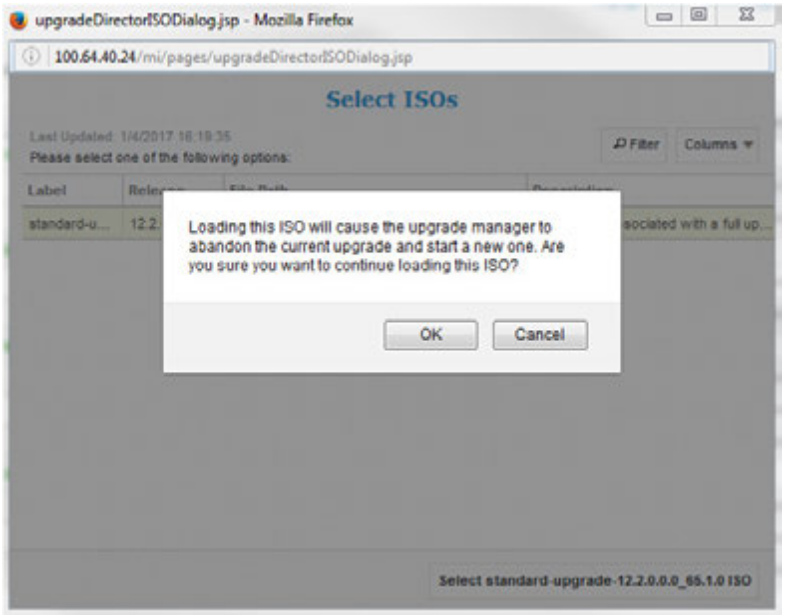
12. ☐	**Upgraded server SSH:** verify upgrade log file	SSH to upgraded server and check the upgrade log (at `/var/TKLC/log/upgrade`) file to validate 'Upgrade returned success!'
		`[admusr@pcrf-cmp-b ~]$ cd /var/TKLC/log/upgrade`
		`[admusr@pcrf-cmp-b upgrade]$ tail upgrade.log`
		`1483548973::Updating platform revision file...`
		`1483548973::RCS VERSION=1.3`
		`1483548974::Upgrade returned success!`
		`1483548974::Creating RC script to set alarm on next boot`
		`1483548974::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus'`
		`1483548974::Cleaning up chroot environment...`
		`1483548974::`
		`1483549284:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute`
		`1483549321:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm`
		`1483549321:: /etc/rc4.d/S99TKLCupgradeStatus -`
		`[admusr@pcrf-cmp-b upgrade]$`

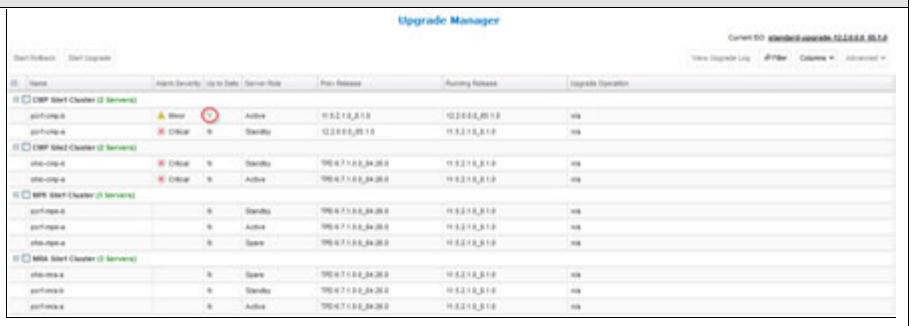
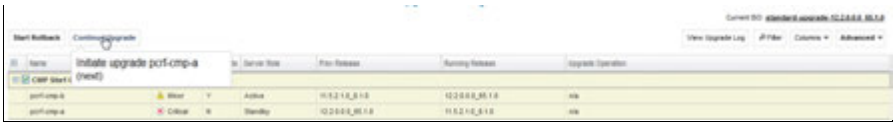
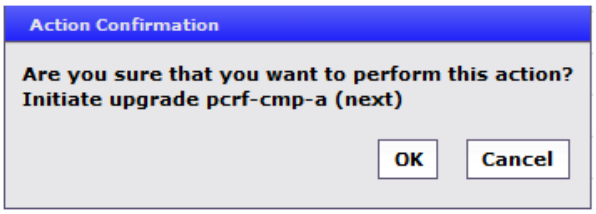
13. ☐	**CMP GUI:** Verify alarms	**System Wide Reports → Active Alarms** Alarm **70025 The MySQL slave has a different schema version than the master**, is expected. The alarm will be cleared after the cluster is fully upgraded to the same release. Occurrence: Jan 04, 2017 12:01 PM EST; Severity: Critical; Alarm ID: 70025; Text: The MySQL slave has a different schema version than the master.; OAM VIP: 10.240.166.24; Server: pcrf-cmp-b 10.240.166.33
14. ☐	**CMP GUI:** Switch the upgraded release 12.2 CMP server to Active	**Upgrade Manager → System Maintenance** • Select the checkbox for the CMP cluster to be switched—primary cluster only, and • Select **Operations→Switch ForceStandby** • Click **OK** to continue with the operation and a successful message appears. Warning Are you sure you want to execute Switch ForceStandby? OK Cancel • **NOTE:** The current CMP GUI browser connection is lost. If this is the primary CMP cluster, you will have to log back into the CMP system as shown in the next step. • Close the browser and re-open.

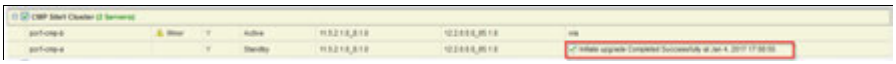
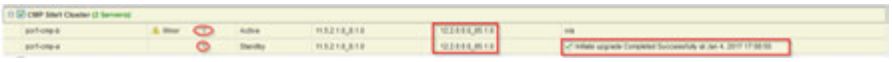
Step	Procedure	Result
15. ☐	**CMP GUI:** Login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management release 12.2 CMP GUI login form should appear as shown—login username and password credentials are the same as the pre-upgrade. 
16. ☐	**CMP GUI: V**erify new Policy Management release	Navigate to **Help→About**. Verify the release displayed is 12.2 12.2.0.0.0_65.1.0 Copyright (C) 2003, 2017 Oracle. All Rights Reserved.
17. ☐	**CMP GUI:** Critical alarms	The following critical alarm will be seen until the SQL Database matches the master (12.2): **70025** The MySQL slave has a different schema version than the master  Occurrence: Jan 04, 2017 12:46 PM EST; Severity: Critical; Alarm ID: 70025; Text: The MySQL slave has a different schema version than the master.; OAM VIP: 10.240.166.24; Server: pcrf-cmp-a 10.240.166.32 These alarms are expected and will remain until all CMPs have been upgraded to the same version. **NOTE:** The Upgrade Manager will show the same alarms.
18. ☐	**CMP GUI:** Verify the Policy Management release 12.2 CMP is Active	**Upgrade→ Upgrade Manager**  As noted, the Active CMP server is now running release 12.2.

19. ☐	**Primary Active CMP:** ssh to primary active CMP and copy iso to `/var/camiant/iso`	• Logon to the primary active CMP as admusr and copy the 12.2 ISO file to the `/var/camiant/iso` directory:
		`$sudo cp /var/TKLC/upgrade/cmp-12.2.x…x.iso /var/camiant/iso/`
		• Verify the copy by using the following command:
		`$ ls /var/camiant/iso/`

20. ☐	**CMP GUI:** Locate the new 12.2 upgrade manual	**Upgrade → Upgrade Manager** • Select the **Current ISO.** In this case it is labeled Install Kit. This will open a dialog box with a description of the ISO that was copied into

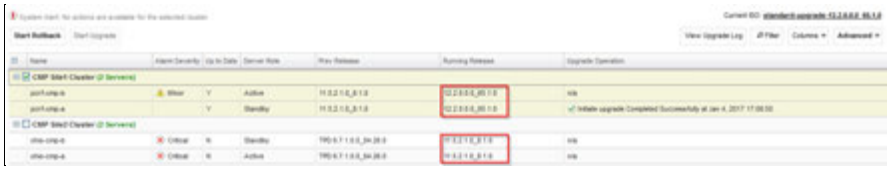
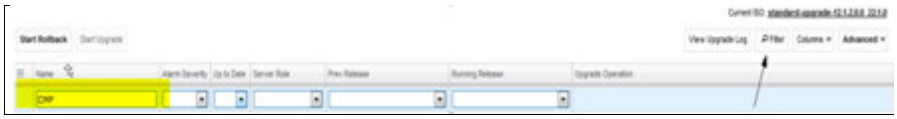
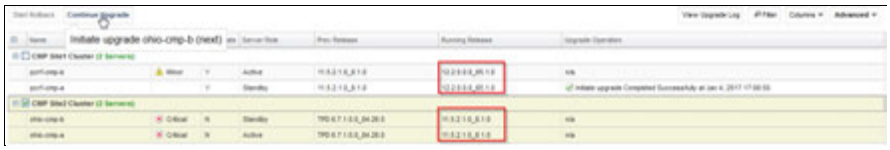
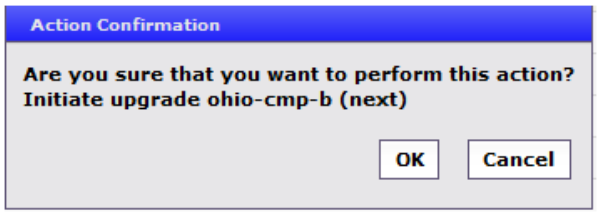
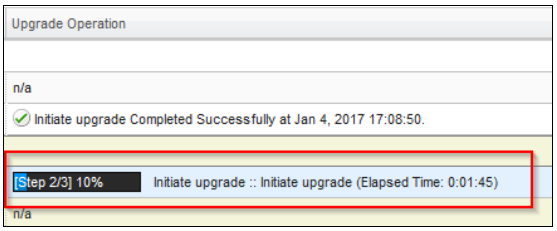
Step	Procedure	Result
		`/var/camiant/iso` • Highlight the ISO file and click the button located in the bottom right-hand corner of the window.  • When the confirmation dialog displays, click **OK**.  • Within a few seconds, the Up to Date column transitions from n/a to Y (meaning up-to-date) or N (meaning needs upgrade).

Step	Procedure	Result
		
21. ☐	**CMP GUI:** New alarms introduced with 12.2	The following minor alarms, along with the already active critical alarms, will now be active. **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **2 Alarms found, displaying all Alarms.** Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 04:21 PM EST | Minor | 70500 | The system is running different versions of software | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:21 PM EST | Minor | 70501 | The Cluster is running different versions of software | 10.240.166.24 | pcrf-cmp-b 10.240.166.33
22. ☐	**CMP GUI:** Complete the upgrade of the Primary CMP cluster **NOTE:** Remaining CMP server will take approximately 40 minutes to complete.	**Upgrade → Upgrade Manager** • Select the Primary Site 1 CMP cluster • Click **Continue Upgrade.** Notice that just hovering over the "**Continue Upgrade**" button will displays what is the next step which in this case the un-upgraded CMP server  • Click **OK** to continue the upgrade on the remaining server in the CMP cluster • 

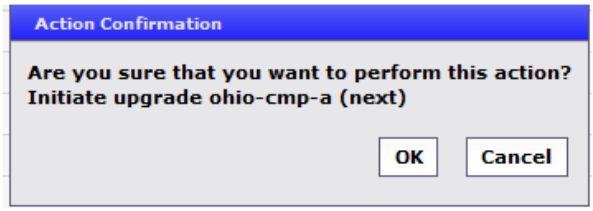
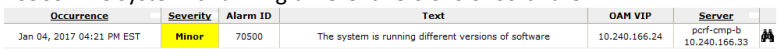
Step	Procedure	Result
23. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	**Upgrade → Upgrade Manager** Notice the upgrade operation column displays the steps of the upgrade process: • At end of the upgrade process, upgrade operation column should display successful upgrade completion message for the upgraded CMP server as follows:  • Successful upgrade status will now show both servers running the Release 12.2 under the "Running Release" column.- • A "Y'" in the Up to Date column • Active/standby state for both servers in the Primary CMP Cluster.  During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical alarm</u>** **31283** HA Server Offline **70025** The MySQL slave has a different schema version than the master Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 04:42 PM EST | Critical | 31283 | High availability server is offline | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 12:46 PM EST | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.240.166.60 | ohio-cmp-b 10.240.166.29 Jan 04, 2017 12:46 PM EST | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.240.166.60 | ohio-cmp-a 10.240.166.28 **<u>Expected Major Alarm</u>** **70004** QP Processes has been down for maintenance **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master **31233** High availability path loss of connectivity Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 04:41 PM EST | Major | 70004 | The QP processes have been brought down for maintenance. | 10.240.166.24 | pcrf-cmp-a 10.240.166.32 Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 05:07 PM EST | Major | 70022 | The MySQL slave failed synchronizing with the master | 10.240.166.24 | pcrf-cmp-a 10.240.166.32 Jan 04, 2017 05:07 PM EST | Major | 70021 | The MySQL slave is not connected to the master | 10.240.166.24 | pcrf-cmp-a 10.240.166.32 Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 05:41 PM EST | Major | 31233 | High availability path loss of connectivity | 10.240.166.60 | ohio-cmp-a 10.240.166.28 **<u>Expected Minor Alarms</u>** **70503** The server is in forced standby **70507** An upgrade/back out action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 04, 2017 04:42 PM EST | Minor | 31114 | DB Replication of configuration data via SOAP has failed | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:42 PM EST | Minor | 31106 | DB merging to the parent Merge Node has failed | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:42 PM EST | Minor | 31107 | DB merging from a child Source Node has failed | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:42 PM EST | Minor | 31101 | DB replication to a slave DB has failed | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:41 PM EST | Minor | 70503 | The server is in forced standby | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:41 PM EST | Minor | 70507 | An upgrade/backout action on a server is in progress | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:21 PM EST | Minor | 70500 | The system is running different versions of software | 10.240.166.24 | pcrf-cmp-b 10.240.166.33 Jan 04, 2017 04:21 PM EST | Minor | 70501 | The Cluster is running different versions of software | 10.240.166.24 | pcrf-cmp-b 10.240.166.33

Step	Procedure	Result
24. ☐	Proceed to next upgrade procedure	Verify the following information: • Primary Site1 is running release 12.2 • Secondary site—if applicable, is on release 11.5.x • All C level nodes will be on release 11.5.x Proceed to the next procedure if there is a disaster recovery CMP to upgrade. If not, skip to section 8
THIS PROCEDURE HAS BEEN COMPLETED		

5.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP cluster	**Upgrade → Upgrade Manager** • Primary CMP is completely upgraded to 12.2 • Secondary CMP cluster is on 11.5.x 
2. ☐	**CMP GUI:** Upgrade Secondary CMP cluster **NOTE:** This will take approximately 30 minutes to complete.	**Upgrade → Upgrade Manager** **NOTE:** The **Filter** button can be used to show only the CMP servers. Enter CMP in the Name field.  • Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. Notice that just hovering over the "**Continue Upgrade**" button will displays what is the next step which in this case the un-upgraded CMP server  • Click **OK** to confirm and continue with the operation.  • The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed. This will continue 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	Result
		Expected Critical alarm **31283** HA Server Offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarm** **70004** QP Processes has been down for maintenance **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master **31233** High availability path loss of connectivity **Expected Minor Database replication Alarms** **70503** The server is in forced standby **70507** An upgrade/back out action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed **View Upgrade Log from the GUI showing complete on the 1st server on the secondary site.** Upgrade Log Cluster Name: CMP Site2 Cluster Last Update: 1/4/2017 17:33:11 Filter Columns ID | Pare... | Action Name | Start Time | End Time | Durat... | Scope | Hostname | Result | Mode | Description 6 | 0 | Preflight Check | 1/4/2017 17:25:20 | 1/4/2017 17:25:30 | 0:00:10 | Server | ohio-cmp-b | Success | Manual | User initiated action: ... 7 | 6 | Initiate upgrade | 1/4/2017 17:25:30 | In Progress | In Pro... | Server | ohio-cmp-b | | Automatic | Automatic action initi... 8 | 6 | Modify the role/replication ... | 1/4/2017 17:25:30 | 1/4/2017 17:25:31 | 0:00:01 | Cluster | CMP Site2 ... | Success | Automatic | Automatic action for ...
3. ☐	**CMP GUI**: Continue upgrade of the Secondary CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. Notice the message 'Failover to new version…' • Click **OK** to confirm and continue with the operation. Action Confirmation Are you sure that you want to perform this action? Failover to new version CMP Site2 Cluster (next) OK Cancel • The specific action will take a minute to complete. Wait until the upgraded server is active, as shown below. • Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. When hovering over the button, the message will display the next action, which is to **initiate the upgrade of the remaining CMP**.

Step	Procedure	Result
		 • 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** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarm** **70004** QP Processes has been down for maintenance **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master **31233** High availability path loss of connectivity **Expected Minor Database replication Alarms** **70503** The server is in forced standby **70507** An upgrade/back out action on a server is in progress **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31101** DB replication to a slave DB has failed
4. ☐	**CMP GUI:** Verify that the upgrade completed successfully.	**Upgrade → Upgrade Manager** Successful upgrade status will show the release 12.2 in the Running Release and the Upgrade Operation columns.
5. ☐	**CMP GUI:** Verify alarms	**System Wide Reports → Alarms → Active Alarms** The following Minor alarm is expected: **70500** The system is running different versions of software  Occurrence: Jan 04, 2017 04:21 PM EST; Severity: Minor; Alarm ID: 70500; Text: The system is running different versions of software; OAM VIP: 10.240.166.24; Server: pcrf-cmp-b 10.240.166.33
6. ☐	Procedure is complete.	Verify the following information: • All CMP clusters upgrades are complete and running release 12.2. • All MRA and MPE clusters are running release 11.5.x • The Policy Management system is running in mixed-version mode.
		THIS PROCEDURE HAS BEEN COMPLETED

6. UPGRADE CMP CLUSTERS (11.5.X TO 12.2) CABLE MODE

This procedure will upgrade the Site-1 CMP cluster first, and if needed, upgrade the Site-2 CMP cluster in Cable Mode.

6.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster:
   a. Use the CMP GUI—System Maintenance (11.5.X), to place Primary Standby CMP into Force-Standby
   b. Use the CMP GUI—System Maintenance (11.5.X), to upgrade the Primary Force-Standby CMP server
   c. Use the CMP GUI—System Maintenance (11.5.X), to perform Switch Force-Standby on the Primary CMP cluster
   d. Log back into the CMP GUI and upgrade the remaining Primary CMP that is the Force-Standby server using the 12.2 Upgrade Manager
2. Upgrade the Secondary CMP cluster (if applicable)

   Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2
   a. Start upgrade
   b. Continue upgrade—failover
   c. Continue upgrade

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

It is assumed that the CMPs may be deployed as 2 Disaster Recovery (DR) clusters, identified as Site-1 and Site-2 as displayed on the CMP GUI. When deployed as such, one site is designated as the Primary Site (which is the site that is managing the Policy 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 Disaster Recovery Status	Operator Site Name	Site Designation from Topology Form (Site-1 or Site-2)
Primary Site		
Secondary Site		

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP _____

Server-A Status _____

Server-B Hostname _____

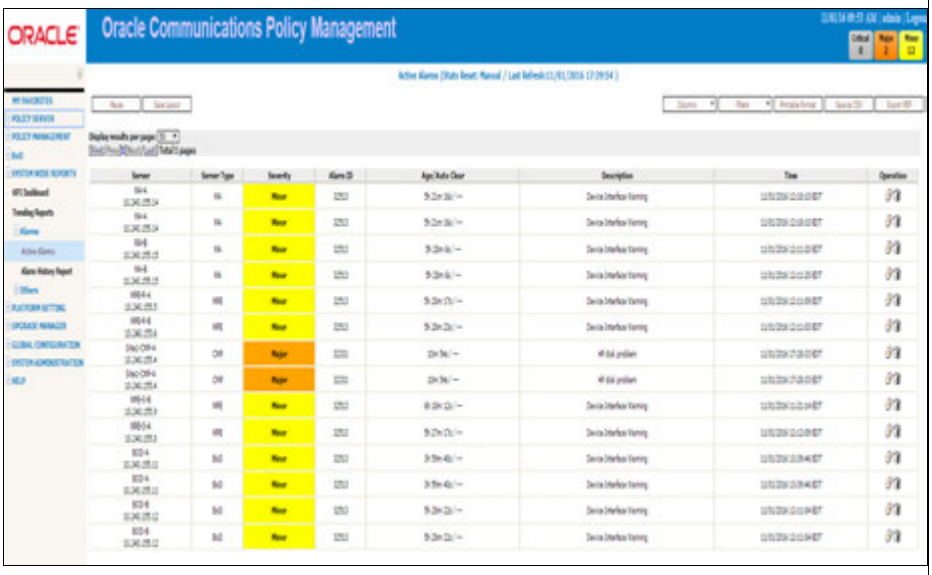
Server-B IP Address _____

Server-B Status _____

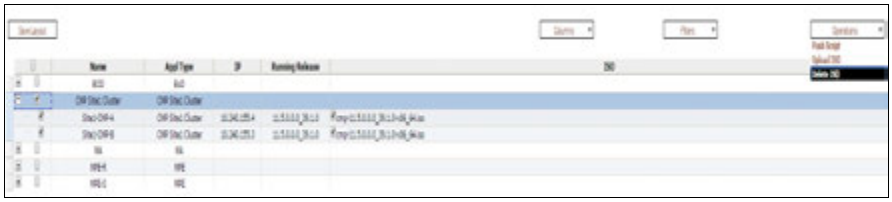
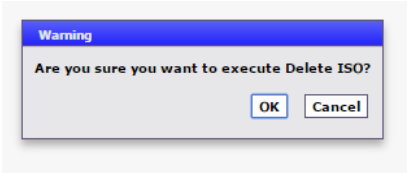
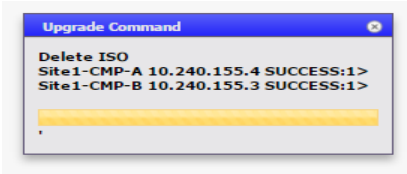
IMPORTANT:

- CMP servers MUST be upgraded first, before the MPE-R, MPE-S, BOD or MA clusters
- Site-1 CMP MUST be upgraded to the new release first, before the Site-2 CMP (if applicable)

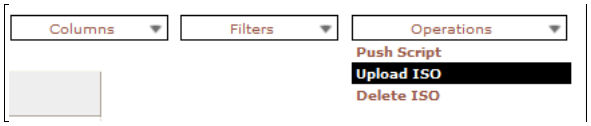
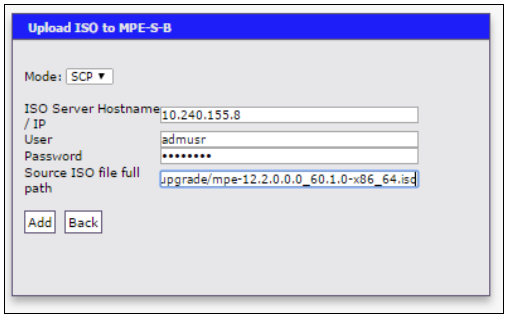
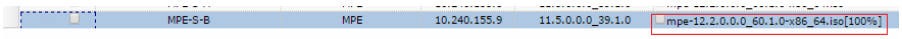
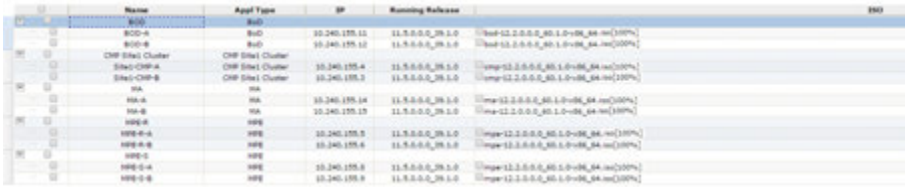
6.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	**System Wide Reports →Alarms→ Active Alarms** • Confirm that any existing alarm is well understood and no impact to the upgrade procedure. ○ Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and record the CMP cluster(s)	Navigate to **Platform Setting→Topology Settings → All Clusters** Cluster Settings • 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. • Save a screenshot for future reference.
3. ☐	**CMP GUI:** Verify status of CMP clusters	**Upgrade Manager → System Maintenance** Confirm the CMP clusters have the following: • Active/Standby status • Running show of 11.5.X version • Replication ON • Release 12.2 ISO files copied to at least one of each server types (CMP/MRA/MPE)—Meaning, a copy of the MPE ISO file is on one of the MPE servers, an MRA ISO file is on one of the MRA servers and a copy of the CMP ISO file is on one CMP server

Name	Appl Type	OAM VIP	Server-A	Server-B	Operation
BOD	BoD	10.240.155.13	10.240.155.11	10.240.155.12	View Delete
CMP Site1 Cluster (P)	CMP Site1 Cluster	10.240.155.2	10.240.155.4	10.240.155.3	View
MA	MA	10.240.155.16	10.240.155.14	10.240.155.15	View Delete
MPE-R	MPE	10.240.155.7	10.240.155.5	10.240.155.6	View Delete
MPE-S	MPE	10.240.155.10	10.240.155.8	10.240.155.9	View Delete

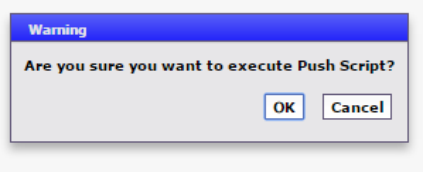
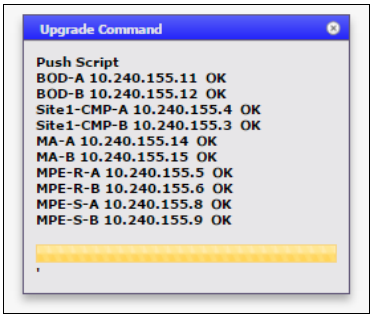
Step	Procedure	Result
4. ☐	**CMP GUI Access** into Primary CMP Server—Remove old ISO files from servers.	**Upgrade Manager → ISO Maintenance** • Select the servers that show old ISO files. • Select the server cluster and select **Operations→ Delete ISO** for any of the older ISO files in the list.  •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

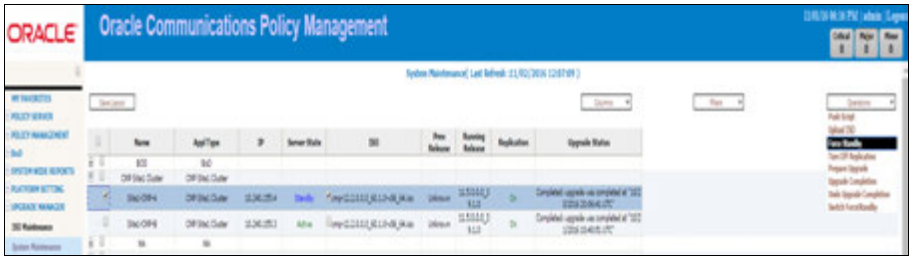
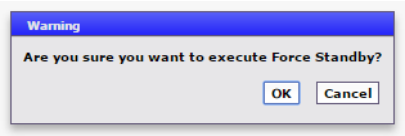
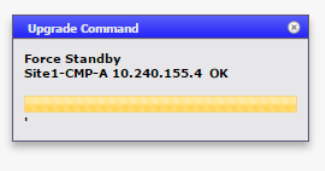
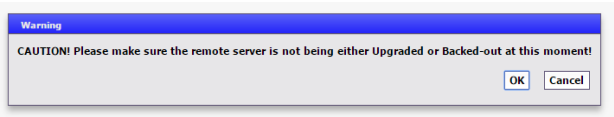
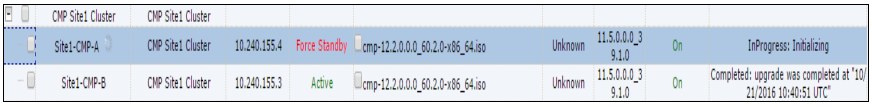
Step	Procedure	Result

5. ☐	**CMP GUI:** Upload relevant upgrade ISO file to each CMP/MPE-R/MPE-S/BOD/MA server
	
	NOTE: This step depends on the ISO file type. Distribute ISO files accordingly.
		Upgrade Manager → ISO Maintenance
		
		• (Optional but Preferred) Filter CMP/MPE/MRA servers
		  ○ One application at a time, select one server type (MPE-R/S, MA, BOD or CMP) to upload its upgrade ISO file.
		
		NOTE: The ISO files for each application type must already be copied over to at least one server. See 4.6.3 "Distribute Application ISO Image Files to Servers" on page **Error! Bookmark not defined.**.
		
		  ○ Select **Operations → Upload ISO**
		
		 
		
		  ○ 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/
		
		 
		
		  ○ Click **Add** and wait till filename appears under the "ISO" column and file is 100% transferred:
		
		 
		
		  ○ When completed for all servers, the ISO column will be populated with the ISO filename and indication of 100% transfer completion
		
		 
		
		NOTE: For those servers the ISO file was transferred from the local machine, there will not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management screen of CMP GUI.

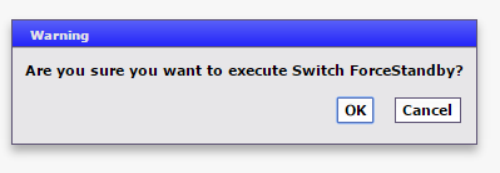
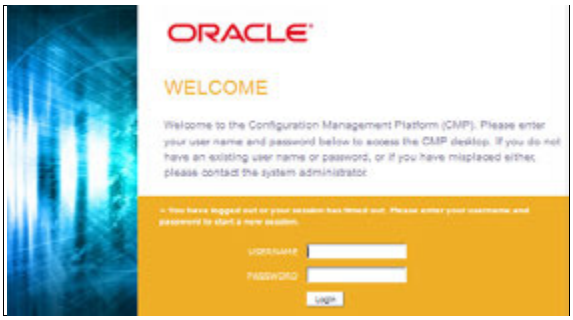
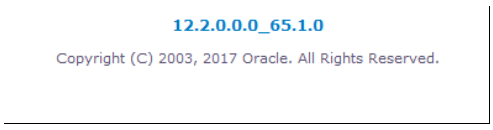
Step	Procedure	Result

6. ☐	**SSH CLI Primary Active CMP:** Copy latest upgrade scripts and Exchange keys	• Ssh to active CMP, login as admusr user then mount the upgrade iso file to copy the latest upgrade scripts as follows:
		`[admusr@Site1-CMP-B ~]$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.2.0.0.0_60.1.0-x86_64.iso /mnt/upgrade/`
		`[admusr@Site1-CMP-B ~]$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		`[admusr@Site1-CMP-B ~]$ sudo umount /mnt/upgrade/`
		`[admusr@Site1-CMP-B ~]$`
		• Run the following command to exchange the SSH keys with all servers in the topology:
		`$sudo qpSSHKeyProv.pl --prov`
		NOTE: You need to supply the admusr PASSWORD for command to process
		`[admusr@Site1-CMP-B ~]$ cd /opt/camiant/bin`
		`[admusr@Site1-CMP-B bin]$ sudo qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:`
		`Connecting to admusr@MA-B ...`
		`Connecting to admusr@Site1-CMP-B ...`
		`Connecting to admusr@BOD-B ...`
		`Connecting to admusr@MPE-S-B ...`
		`Connecting to admusr@MPE-R-B ...`
		`Connecting to admusr@MPE-R-A ...`
		`Connecting to admusr@MA-A ...`
		`Connecting to admusr@MPE-S-A ...`
		`Connecting to admusr@Site1-CMP-A ...`
		`Connecting to admusr@BOD-A ...`
		`[1/10] Provisioning SSH keys on MA-B ...`
		`[2/10] Provisioning SSH keys on Site1-CMP-B ...`
		`[3/10] Provisioning SSH keys on MPE-R-B ...`
		`[4/10] Provisioning SSH keys on MPE-S-B ...`
		`[5/10] Provisioning SSH keys on BOD-B ...`
		`[6/10] Provisioning SSH keys on MPE-R-A ...`
		`[7/10] Provisioning SSH keys on MA-A ...`
		`[8/10] Provisioning SSH keys on MPE-S-A ...`
		`[9/10] Provisioning SSH keys on BOD-A ...`
		`[10/10] Provisioning SSH keys on Site1-CMP-A ...`
		`SSH keys are OK.`
		`[admusr@Site1-CMP-B bin]$`
		• Verify that the Keys are exchanged successfully with all the server clusters as follows :
		`[admusr@Site1-CMP-B bin]$ sudo qpSSHKeyProv.pl --check`
		`The password of admusr in topology:`
		`Connecting to admusr@MA-B ...`
		`Connecting to admusr@Site1-CMP-B ...`
		`Connecting to admusr@BOD-B ...`
		`Connecting to admusr@MPE-S-B ...`
		`Connecting to admusr@MPE-R-B ...`
		`Connecting to admusr@MPE-R-A ...`
		`Connecting to admusr@MA-A ...`
		`Connecting to admusr@MPE-S-A ...`
		`Connecting to admusr@Site1-CMP-A ...`
		`Connecting to admusr@BOD-A ...`
		`[1/10] Checking SSH keys on MA-B ...`
		`[2/10] Checking SSH keys on Site1-CMP-B ...`
		`[3/10] Checking SSH keys on MPE-R-B ...`
		`[4/10] Checking SSH keys on MPE-S-B ...`
		`[5/10] Checking SSH keys on BOD-B ...`
		`[6/10] Checking SSH keys on MPE-R-A ...`
		`[7/10] Checking SSH keys on MA-A ...`
		`[8/10] Checking SSH keys on MPE-S-A ...`
		`[9/10] Checking SSH keys on BOD-A ...`
		`[10/10] Checking SSH keys on Site1-CMP-A ...`
		`SSH keys are OK.`
		`[admusr@Site1-CMP-B bin]$`

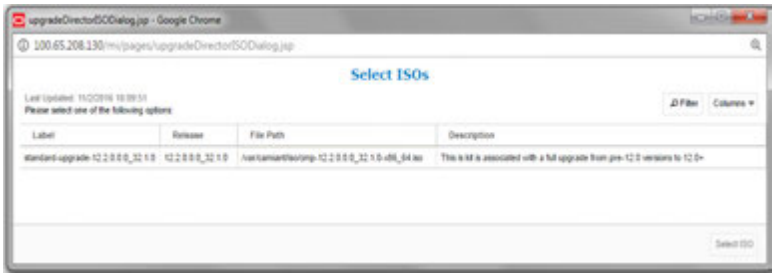
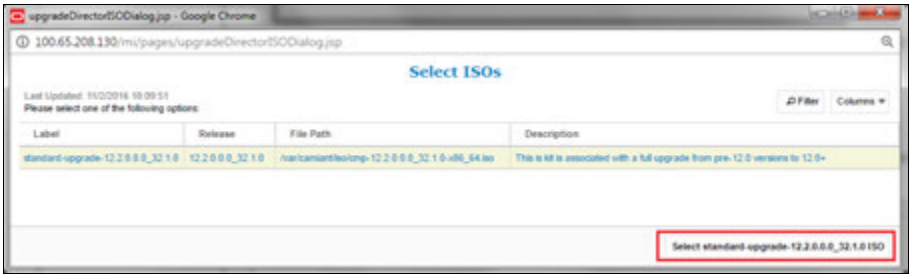
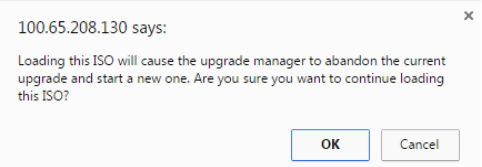
Step	Procedure	Result
7. ☐	**CMP GUI:** Push the latest 12.2 upgrade scripts to all servers in the segment topology	Login to CMP GUI and navigate to **Upgrade Manager → ISO Maintenance** • Select all the servers in the topology as shown in the figure. ○ Select **Operations→Push Scripts**. **NOTE:** It is safe to run the push script multiple times as needed. ○ Click **OK** to continue the operation:  ○ Confirm command completes successfully.  **NOTE:** Give the push script a minute to complete

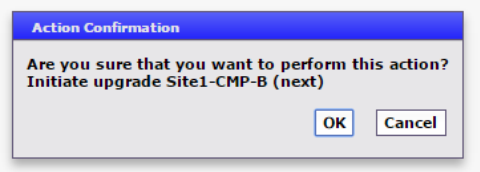
Step	Procedure	Result
8. ☐	**CMP GUI:** Set Force Standby mode on the Standby CMP in the Primary cluster	**Upgrade Manager → System Maintenance** • Select the checkbox for the Standby CMP Server at Primary Site ○ Click **Operations→ Force Standby**.  ○ Click **OK** to confirm and continue with the operation.  ○ Confirm the step completes successfully:  ○ Standby CMP server state will be changed to Force Standby
9. ☐	**CMP GUI:** Upgrade the **Force-Standby** CMP server at the primary site **NOTE:** This will take approximately 40 minutes to complete.	**Upgrade Manager → System Maintenance** • Select the Force-Standby CMP Server at the Primary Site. ○ Select **Operations→Start Upgrade** operation. ○ Click **OK** to continue with the operation:  ○ Monitor the upgrade status activities from the "Upgrade Status" column.  During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical Alarm</u>**

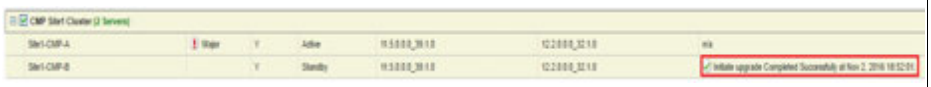
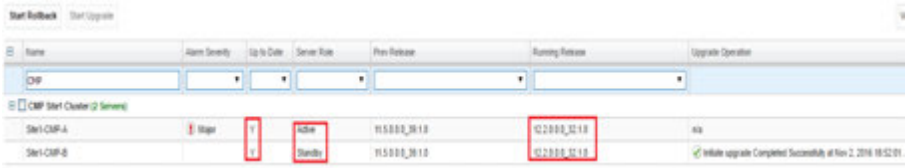
Step	Procedure	Result
		31283 HA Server Offline Nov 02, 2016 01:29 PM EDT | Critical | 31283 | High availability server is offline | 10.240.155.2 | Site1-CMP-B 10.240.155.3 **Expected Major Alarm** 70004 The QP processes have been brought down for maintenance. Nov 02, 2016 01:29 PM EDT | Major | 70004 | The QP processes have been brought down for maintenance. | 10.240.155.2 | Site1-CMP-A 10.240.155.4 **Expected Minor Alarms** 31114 DB Replication over SOAP has failed 31106 DB Merge To Parent Failure 31107 DB Merge From Child Failure 31101 DB replication to slave DB has failed Nov 02, 2016 01:44 PM EDT | Minor | 31101 | DB replication to a slave DB has failed | 10.240.155.2 | Site1-CMP-B 10.240.155.3 Nov 02, 2016 01:44 PM EDT | Minor | 31106 | DB merging to the parent Merge Node has failed | 10.240.155.2 | Site1-CMP-B 10.240.155.3 Nov 02, 2016 01:44 PM EDT | Minor | 31107 | DB merging from a child Source Node has failed | 10.240.155.2 | Site1-CMP-B 10.240.155.3 Nov 02, 2016 01:44 PM EDT | Minor | 31114 | DB Replication of configuration data via SOAP has failed | 10.240.155.2 | Site1-CMP-B 10.240.155.3 ○ Wait until 'Completed: upgrade was completed…' appears in the Upgrade Status column Site1-CMP-A | CMP Site1 Cluster | 10.240.155.4 | Force Standby | cmp-12.2.0.0.0_32.1.0-x86_64.iso | 11.5.0.0.0_39.1.0 | 12.2.0.0.0_32.1.0 | On | Completed: upgrade was completed at "11/02/2016 19:07:01 UTC" ***IMPORTANT: If a status message other than the '…upgrade was completed…' message, stop here and contact Oracle Technical Services to troubleshoot and determine if a rollback should be executed.***
10. ☐	**CMP GUI:** Verify that the upgrade completed successfully	**Upgrade Manager → System Maintenance** Successful upgrade status will show 12.2 in the Running Release and Upgrade Operation columns. Site1-CMP-A | CMP Site1 Cluster | 10.240.155.4 | Force Standby | cmp-12.2.0.0.0_32.1.0-x86_64.iso | 11.5.0.0.0_39.1.0 | 12.2.0.0.0_32.1.0 | On | Completed: upgrade was completed at "11/02/2016 19:07:01 UTC" **NOTE:** Expect the server state role is still shown as Force Standby—same as prior to the upgrade. ***IMPORTANT Any Sync Broken indicator ( ) signifies that the data replication between the two servers of the cluster is not synced yet. This may take up to 45 minutes depending on the database size. Do not continue if there is a Sync Broken indicator on the server that was upgraded.***
11. ☐	**Upgraded server SSH:** Verify upgrade log file	SSH to upgraded server and check the upgrade log file to validate it completed successfully: [admusr@Site1-CMP-A upgrade]$ pwd /var/TKLC/log/upgrade [admusr@Site1-CMP-A upgrade]$ tail upgrade.log 1478113314::Updating platform revision file... 1478113314::RCS VERSION=1.2 1478113314::Upgrade returned success! 1478113314::Creating RC script to set alarm on next boot 1478113314::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus' 1478113314::Cleaning up chroot environment... 1478113314:: 1478113595:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute 1478113621:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm 1478113621:: /etc/rc4.d/S99TKLCupgradeStatus - [admusr@Site1-CMP-A upgrade]$
12. ☐	**CMP GUI:** Verify alarms	**System Wide Reports → Active Alarms** Alarm **70025, QP Slave database is a different version than the master**, is expected. The alarm will be cleared after the cluster is fully upgraded to the same release. Nov 02, 2016 03:06 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.240.155.2 | Site1-CMP-A 10.240.155.4

Step	Procedure	Result
13. ☐	**CMP GUI:** Switch force Standby so the 12.2 upgraded server be the Active CMP server	**Upgrade Manager → System Maintenance** • Select the checkbox for the CMP cluster to be switched—primary cluster only, and ○ Select **Operations→Switch ForceStandby**. ○ Click **OK** to continue with the operation and a successful message appears.  **NOTE:** Current CMP GUI browser connection will be lost. You will need to log back into the CMP system as shown in the next step.
14. ☐	**CMP GUI:** Login to the CMP server VIP	Re-login to the CMP GUI. The Policy Manager shows 12.2 CMP GUI login form opens. The username and password credentials are the same as the pre-upgrade. 
15. ☐	**CMP GUI**: Verify new Policy Manager version	Navigate to **Help→About**. Verify the release number is displayed as 12.2. 
16. ☐	**CMP GUI:** Critical alarms	The following critical alarm will be seen until the SQL Database matches the master (12.2): **70025** QP Slave database is a different version than the master: This alarm is expected and will remain until all CMPs have been upgraded to the same version.

Step	Procedure	Result
17. ☐	**CMP GUI:** Verify that Policy Manager shows 12.2 CMP is Active	**Upgrade→Upgrade Manager** As noted, the active CMP server is now running release 12.2

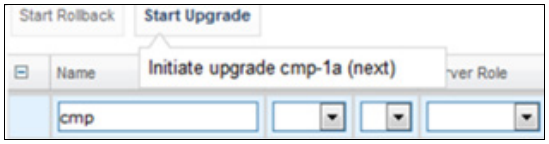
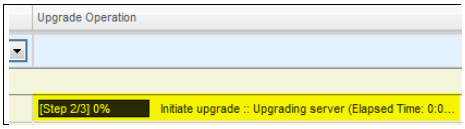
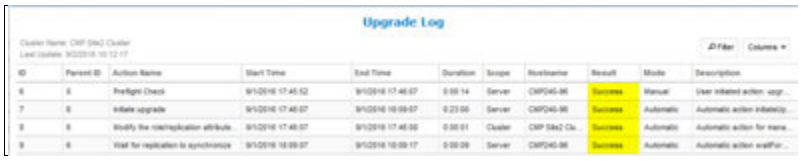
Step	Procedure	Result
18. ☐	**CMP GUI:** Choose the new 12.2 Upgrade ISO file	**Upgrade → Upgrade Manager** • Select "**Install Kit" link** This will open a dialog box with a description of the ISO file that was copied into `/var/camiant/iso` directory"  ○ Highlight the ISO file and click the button located in the bottom right-hand corner of the window.  • Click **OK** to confirm and continue with the operation:  100.65.208.130 says: Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO? OK Cancel Notice that "Up to Date" column transitions from "n/a" to Y (meaning up-to-date) for the upgraded CMP server and N (meaning needs upgrade) for the other CMP server. Also, the "Install Kit" link now displays the selected CMP ISO file.
19. ☐	**CMP GUI:** New alarms introduced with 12.2	The following minor alarms, along with the already active Critical alarms, will now be active. Nov 02, 2016 06:13 PM EDT | Minor | 70500 | The system is running different versions of software | 10.240.155.2 | Site1-CMP-A 10.240.155.4 Nov 02, 2016 06:13 PM EDT | Minor | 70501 | The Cluster is running different versions of software | 10.240.155.2 | Site1-CMP-A 10.240.155.4

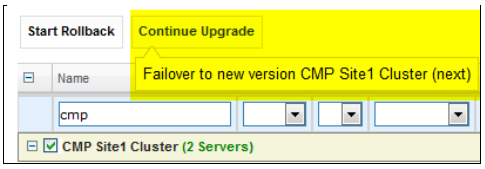
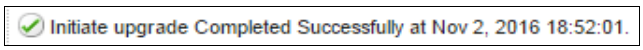
Step	Procedure	Result
20. ☐	**CMP GUI:** Complete the upgrade of the Primary CMP cluster **NOTE:** Remaining CMP server will take approximately 40 minutes to complete.	**Upgrade → Upgrade Manager** • Select the Primary Site 1 CMP cluster • Click **Continue Upgrade.** Notice that just hovering over the "Continue Upgrade" button will displays what is the next step which in this case the un-upgraded CMP server ○ Click **OK** to continue the upgrade on the remaining server in the CMP cluster  Alarms to note: **<u>Expected Critical Alarms</u>** **70025** QP Slave database is a different version than the master **<u>Expected Minor Alarms</u>** **31101** Database replication to slave failure **70507** Upgrade In Progress

Step	Procedure	Result
21. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	**Upgrade Manager → Upgrade Manager** Notice the upgrade operation column displays the steps of the upgrade process: At end of the upgrade process, upgrade operation column should display successful upgrade completion message for the upgraded CMP server as follows:  Successful upgrade status will show the following for both servers in the Primary CMP cluster: • 12.2 in the Running Release column for both server • A "**Y**" in the Up to Date column • Active/Standby roles for each server:  Active alarms to note after the upgrade: **<u>Expected Minor Alarms</u>** **70500** System Mixed Version Nov 02, 2016 06:13 PM EDT | **Minor** | 70500 | The system is running different versions of software | 10.240.155.2 | Site1-CMP-A 10.240.155.4
22. ☐	Proceed to next upgrade procedure	Verify the following information: Primary Site-1 is running release 12.2 • Secondary Site—if applicable is on R11.5.x • All C Level Nodes will be on release 11.5.x
THIS PROCEDURE HAS BEEN COMPLETED		

6.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP cluster	**Upgrade → Upgrade Manager** • Primary CMP is completely upgraded to 12.2 • Secondary CMP cluster is on 11.5.x

2. ☐	**CMP GUI:** Upgrade the Secondary CMP cluster
	
	NOTE: This will take approximately 30 minutes to complete.
		Upgrade → Upgrade Manager
		• Select the checkbox for the Secondary CMP Server cluster at Site-2
		  ○ Click **Start Upgrade**.
		 
		
		  ○ Click **OK** to confirm and continue with the operation.
		The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.
		This will continue to upgrade the standby server only in the CMP cluster.
		The Upgrade Operation column shows a progress bar along with the upgrade activities.
		 
		
		LOG FILE from the GUI showing complete on the 1st server on the secondary site.
		 

3. ☐	**CMP GUI:** Continue to upgrade the Secondary CMP cluster	**Upgrade → Upgrade Manager**
		• Select the checkbox for the Secondary CMP Server cluster at Site-2
		• Click **Continue Upgrade**. Notice the message 'Failover to new version…'
		 
		
		  ○ Click **OK** to confirm and continue with the operation. The "Upgrade Operation" value of the upgraded server will show successful completion when upgrade is successful.
		 
		
		  ○ Select the checkbox for the Secondary CMP Server cluster at Site-2.
		• Click **Continue Upgrade**. When hovering over the button, the message will display the next action, which is to initiate the upgrade of the remaining CMP.

Step	Procedure	Result
		 ○ Click **OK** to confirm and continue with the operation.
4. ☐	**CMP GUI:** Verify that the upgrade completed successfully	**Upgrade → Upgrade Manager** Successful upgrade status will show 12.2 in the Running Release and Upgrade Operation columns.
5. ☐	**CMP GUI:** Verify alarm	**System Wide Reports → Alarms → Active Alarms** The following Minor alarm is expected: **70500** System Mixed Version Nov 02, 2016 06:13 PM EDT | **Minor** | 70500 | The system is running different versions of software | 10.240.155.2 | Site1-CMP-A 10.240.155.4
6. ☐	Procedure is complete.	Verify the following information: • All CMP clusters upgrades are complete and running release 12.2. • All other clusters are running release 11.5.x • The Policy Management system is running in mixed-version mode.
		THIS PROCEDURE HAS BEEN COMPLETED

7. UPGRADE CMP CLUSTERS (12.1.X TO 12.2)

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

7.1 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.

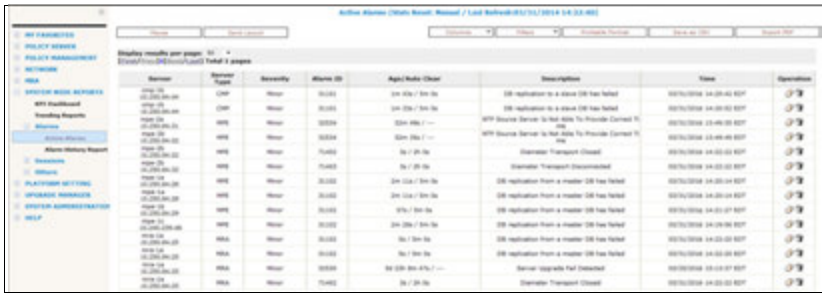
Identify the CMP sites to be upgraded, and verify which site is the Primary site and which site is the Secondary site:

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:

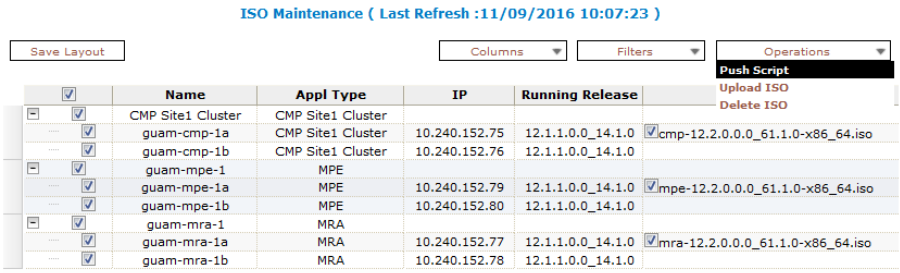
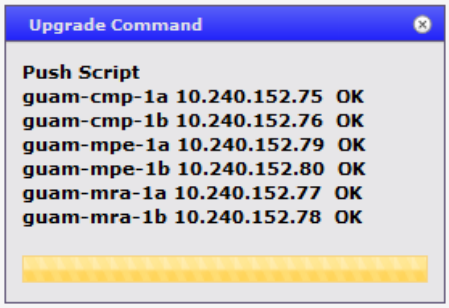
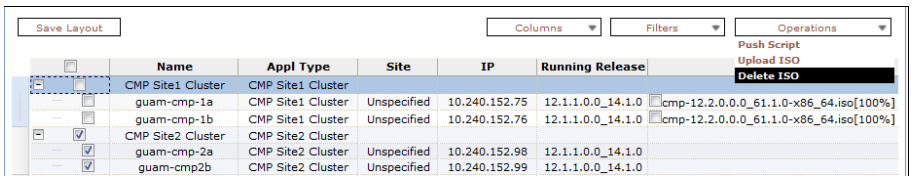
- Site1 CMP MUST be upgraded to the new release first, before the Site2 CMP
- CMP servers MUST be upgraded first, before the non-CMP clusters

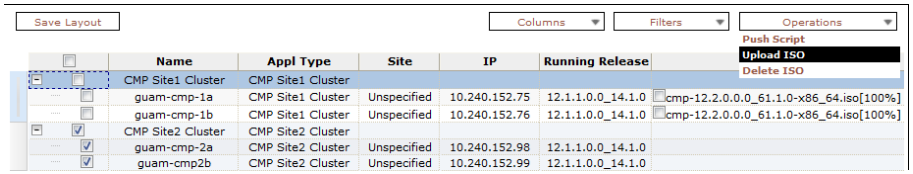
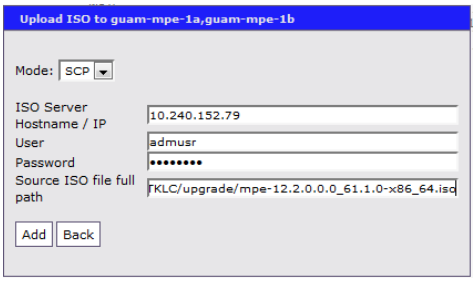
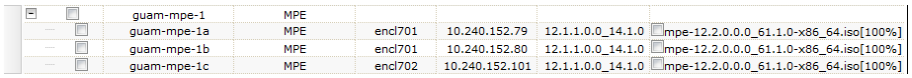
7.1.1 Upgrade Primary CMP Cluster

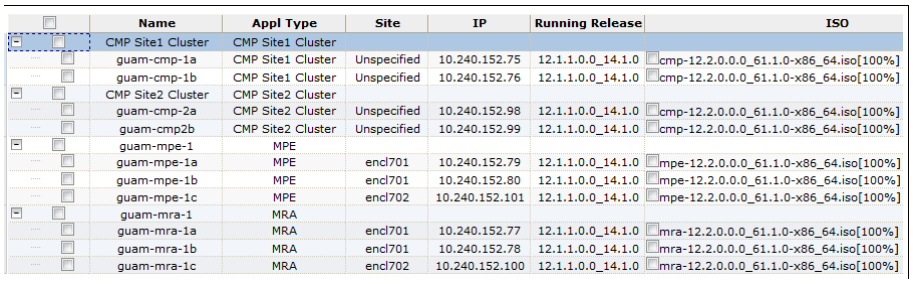
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1. ☐</td><td>CMP GUI: Verify alarm status.</td><td>System Wide Reports → Alarms→Active Alarms
• Confirm that any existing alarm is well understood and is ono impact to the upgrade procedure.
• Capture a screenshot and save it into a file for reference.
  </td></tr>
<tr><td>2. ☐</td><td>CMP GUI: Identify and record the CMP cluster(s)</td><td>Navigate to Platform Setting→Topology Settings → All Clusters
Cluster Settings
<table>
<tr><th>Name</th><th>Appl Type</th><th>Site Preference</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Server-C</th><th>Operation</th></tr>
<tr><td>CMP Site1 Cluster (P)</td><td>CMP Site1 Cluster</td><td>N/A</td><td>10.240.152.88/26</td><td>10.240.152.75</td><td>10.240.152.76</td><td>N/A</td><td>View Demote</td></tr>
<tr><td>CMP Site2 Cluster (S)</td><td>CMP Site2 Cluster</td><td>N/A</td><td>10.240.152.89/26</td><td>10.240.152.98</td><td>10.240.152.99</td><td>N/A</td><td>View Delete</td></tr>
<tr><td>guam-mpe-1</td><td>MPE</td><td>Normal</td><td>N/A (P)
N/A (S)</td><td>10.240.152.79</td><td>10.240.152.80</td><td>10.240.152.101</td><td>View Delete</td></tr>
<tr><td>guam-mra-1</td><td>MRA</td><td>Normal</td><td>N/A (P)
N/A (S)</td><td>10.240.152.77</td><td>10.240.152.78</td><td>10.240.152.100</td><td>View Delete</td></tr>
</table>
• 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.
• Save a screenshot for future reference.</td></tr>
<tr><td>3. ☐</td><td>CMP GUI: Verify the status of the CMP clusters</td><td>Upgrade → Upgrade Manager
Confirm the CMP clusters have the following:
• Active/Standby status
• Running release 12.1.x

Upgrade -> ISO Maintenance
• Release 12.2 ISO files copied to at least one of each server types (CMP/MRA/MPE)—Meaning, a copy of the MPE ISO file is on one of the MPE servers, an MRA ISO file is on one of the MRA servers and a copy of the CMP ISO file is on one CMP server</td></tr>
</table>

Step	Procedure	Result
4. ☐	**SSH CLI Primary Active CMP:** Exchange Keys	• Exchange keys to all servers from the Site1 (Primary) Active CMP. Login as *admusr* user and execute the following command: **$sudo qpSSHKeyProv.pl --prov** [admusr@guam-cmp-1a ~]$ sudo qpSSHKeyProv.pl -prov The password of admusr in topology: • Enter the password for user *admusr* • 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.

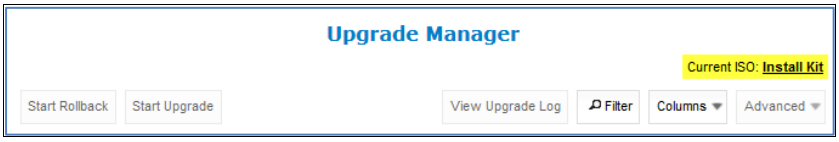
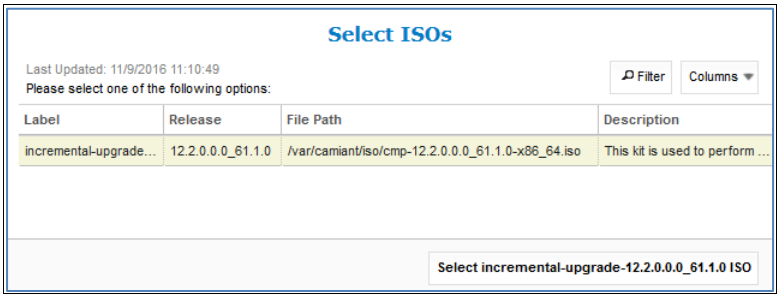
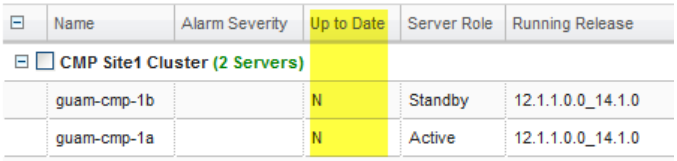
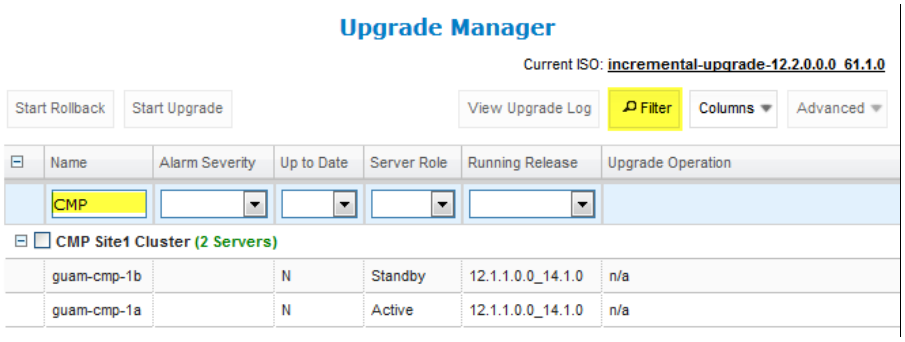
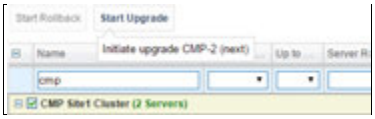
Step	Procedure	Result
5. ☐	**CMP GUI**: Push the Release 12.2 upgrade scripts to all servers	**Upgrade → ISO Maintenance** • Select all the servers in the topology as shown. • Under **Operations** menu, select the "**Push Script**" operation.  • At the popup warning to execute Push Script click "OK" to continue the operation. • After a minute or so, a successful popup window similar to this should appear: 
6. ☐	**CMP GUI Access** into Primary CMP Server—Remove old ISO files from servers.	**Upgrade → ISO Maintenance** • Select the servers that show old ISO files. • Select the server cluster and select **Operations →Delete ISO** to remove any older ISO files.  • Click **OK** to continue and wait until seeing the successful deletion message • Wait until the ISO Maintenance page is refreshed and the ISO column doesn't show any old ISOs.

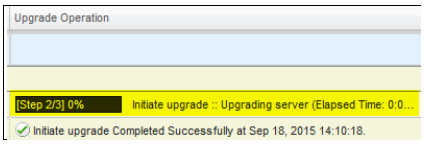
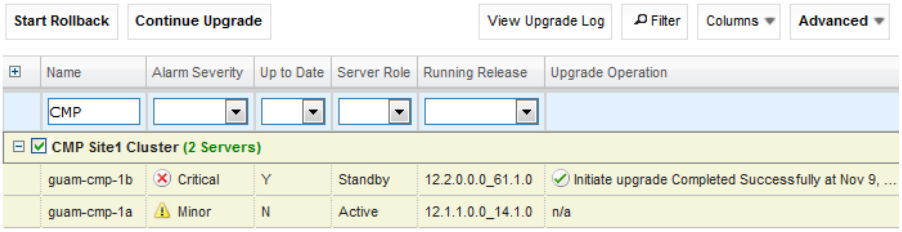
Step	Procedure	Result
7. ☐	CMP GUI: Distribute ISO files to CMP/MPE /MRA/etc., servers **NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly.	**Upgrade → ISO Maintenance** • Filter by server type (optional, but preferred step) • One application at a time, select one server 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". • Select **Operations → Upload ISO**  • 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>*  • Click **Add**. When completed, the ISO column will be populated with the ISO filename and a notification of [100%]  Repeat for all cluster types.

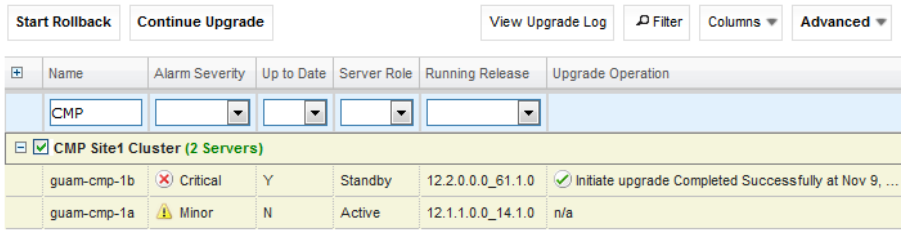
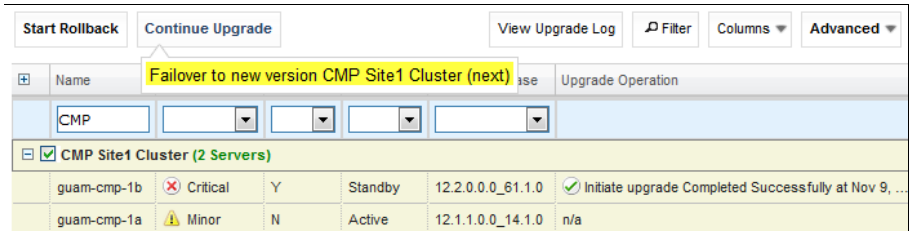
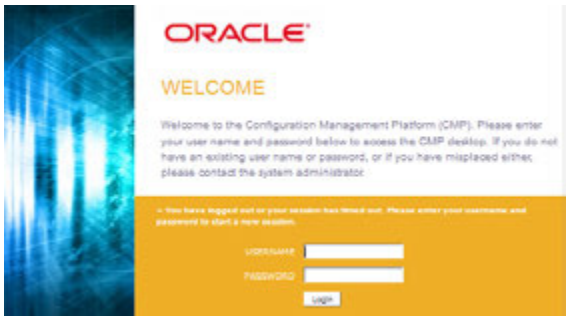
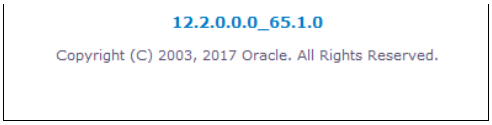
Step	Procedure	Result
8. ☐	**CMP GUI:** Verify ISO distribution to all the server	**Upgrade → ISO Maintenance** • Verify that the release 12.2 ISO file of the correct type is shown for each server. • When completed, the ISO column is populated with the ISO filename and a notification of [100%] **NOTE**: For those servers where the ISO file was copied from the local machine, there will not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management feature. 

9. ☐	**Primary Active CMP:** ssh to primary active CMP and copy iso to /var/camiant/iso	• Logon to the primary active CMP as *admusr* and copy the 12.2 ISO file to the `/var/camiant/iso` directory:
		`$sudo cp /var/TKLC/upgrade/cmp-12.2.x…x.iso /var/camiant/iso/`
		• Verify the copy by using the following command:
		`$ ls /var/camiant/iso/`

Name	Appl Type	Site	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster				
guam-cmp-1a	CMP Site1 Cluster	Unspecified	10.240.152.75	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-cmp-1b	CMP Site1 Cluster	Unspecified	10.240.152.76	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
CMP Site2 Cluster	CMP Site2 Cluster				
guam-cmp-2a	CMP Site2 Cluster	Unspecified	10.240.152.98	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-cmp2b	CMP Site2 Cluster	Unspecified	10.240.152.99	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1	MPE				
guam-mpe-1a	MPE	encl701	10.240.152.79	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1b	MPE	encl701	10.240.152.80	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1c	MPE	encl702	10.240.152.101	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1	MRA				
guam-mra-1a	MRA	encl701	10.240.152.77	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1b	MRA	encl701	10.240.152.78	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1c	MRA	encl702	10.240.152.100	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]

Step	Procedure	Result
10. ☐	**CMP GUI:** Locate the new 12.2 upgrade manual	**Upgrade → Upgrade Manager** • 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. • Highlight the ISO file and click the "Select incremental-upgrade-12.2..." button located in the bottom right-hand corner of the window.  • 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 will take approximately 30 minutes to complete.	**Upgrade → Upgrade Manager** **NOTE:** The **Filter** button can be used to show only the CMP servers. Enter in CMP in the Name field.  • Select the checkbox for the Primary CMP Server cluster • Click **Start Upgrade**. 

Step	Procedure	Result
		• Click **OK** to confirm and continue with the operation. This will continue 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 will change to completed when done. During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical alarm</u>** **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 **<u>Expected Major Alarm</u>** **70004** QP Processes down for maintenance **<u>Expected Minor Database replication Alarms</u>** **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 appears in the Upgrade Operation column. 
12. ☐	**CMP GUI:** Verify that the upgrade is successful	**Upgrade → Upgrade Manager** View the cluster. Verify the following information: • The standby server is on 12.2 • The other server in the cluster is on 12.1.x • The Up to Date column shows Y for the 12.2 server and N for the 12.0 server.

Step	Procedure	Result
		
13. ☐	**CMP GUI:** Continue to upgrade CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Server cluster • Click **Continue Upgrade**. Notice the message 'Failover to new version CMP Site1 Cluster'  • Click **OK** to confirm and continue with the operation. The specific action will take 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 12.2 CMP GUI login form should appear as shown—login and password credentials are the same as the pre-upgrade. 
15. ☐	**CMP GUI: V**erify new Policy Management release	Navigate to **Help→About**. Verify the release displayed is 12.2 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></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 (12.2). This alarm is expected and remains until all CMP servers are upgraded to the same version.

Current Critical Alarms

70025 QP Slave database is a different version than the master:

3 Alarms found, displaying all Alarms.
<table><tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th></tr><tr><td>Sep 28, 2015 07:44 PM EDT</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td></tr><tr><td>Sep 28, 2015 07:44 PM EDT</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td></tr><tr><td>Sep 28, 2015 07:44 PM EDT</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td></tr></table>
Current Minor Alarms

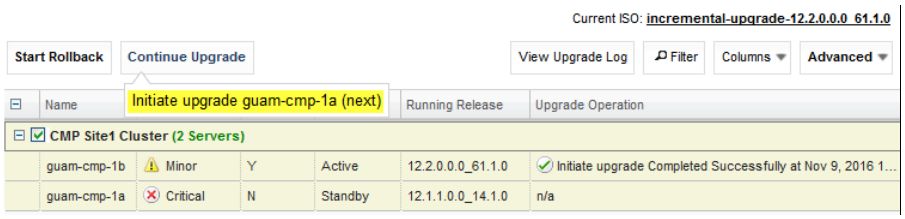
70503 Server Forced Standby
70500 System Mixed Version
70501 Cluster Mixed Version

3 Alarms found, displaying all Alarms.
<table><tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th></tr><tr><td>Sep 28, 2015 07:43 PM EDT</td><td>Minor</td><td>70503</td><td>The server is in forced standby</td></tr><tr><td>Sep 28, 2015 07:43 PM EDT</td><td>Minor</td><td>70501</td><td>The Cluster is running different versions of software</td></tr><tr><td>Sep 28, 2015 07:43 PM EDT</td><td>Minor</td><td>70500</td><td>The system is running different versions of software</td></tr></table>
NOTE: The Upgrade Manager will show alarms as well.</td></tr>
<tr><td>17. ☐</td><td>CMP GUI: Verify the Policy Management release 12.2 CMP is Active</td><td>Upgrade→ Upgrade Manager

Verify the following

• Active server is running release12.2
• Standby server is on the previous release

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

Step	Procedure	Result
18. ☐	**CMP GUI:** Complete the upgrade of the Primary CMP cluster **NOTE:** Remaining CMP server will take approximately 30 minutes to complete.	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Server cluster • Click **Continue Upgrade**. Notice the message 'Initiate upgrade <*standbyserver*> (next)' when hovering over the button.  • Click **OK** to continue the upgrade on the remaining server in the CMP cluster **NOTE:** The server that is being upgraded will go into an OOS state. **Expected Critical Alarms** **31227** HA availability status failed **31283** Lost Communication with server **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault

Step	Procedure	Result
19. ☐	**CMP GUI:** Tracking the upgrade complete	**Upgrade → Upgrade Manager** The last step in the upgrade for the first CMP cluster will be to wait for replication to complete. With the CMP cluster checkbox still checked, click on the "View Upgrade Log" button, a popup window will appear where you can verify that synchronization has taken place: **Upgrade Log** Cluster Name: CMP Site1 Cluster Last Update: 11/10/2016 9:01:00

ID	Parent ID	Action Name	Duration	Scope	Hostname	Result	Mode
1	0	Preflight Check	0:00:15	Server	guam-cmp-1b	Success	Manual
2	1	Upgrading server	0:22:00	Server	guam-cmp-1b	Success	Automatic
3	1	Modify the role/replication attributes of the server	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic
4	1	Wait for replication to synchronize	0:00:09	Server	guam-cmp-1b	Success	Automatic
5	0	Failover to new version	0:00:00	Cluster	CMP Site1 Cluster	Success	Manual
6	0	Preflight Check	0:00:15	Server	guam-cmp-1a	Success	Manual
7	6	Upgrading server	0:21:50	Server	guam-cmp-1a	Success	Automatic
8	6	Modify the role/replication attributes of the server	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic
9	6	Wait for replication to synchronize	0:00:29	Server	guam-cmp-1a	Success	Automatic
10	6	Modify the role/replication attributes of the server	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic

Step	Procedure	Result
20. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	**Upgrade Manager → Upgrade Manager**

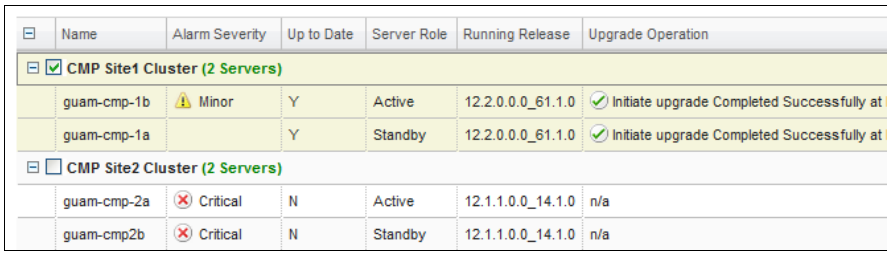
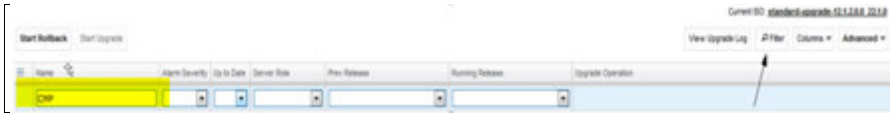
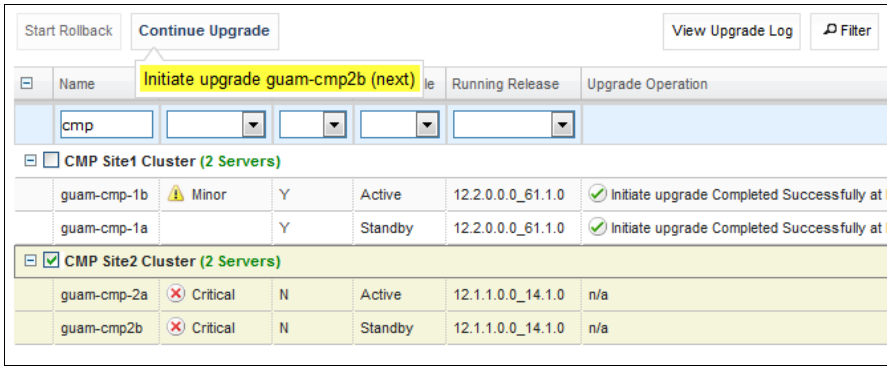
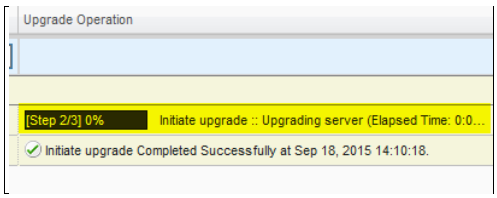
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
guam-cmp-1b	Minor	Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at...
guam-cmp-1a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate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

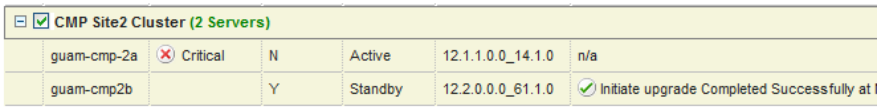
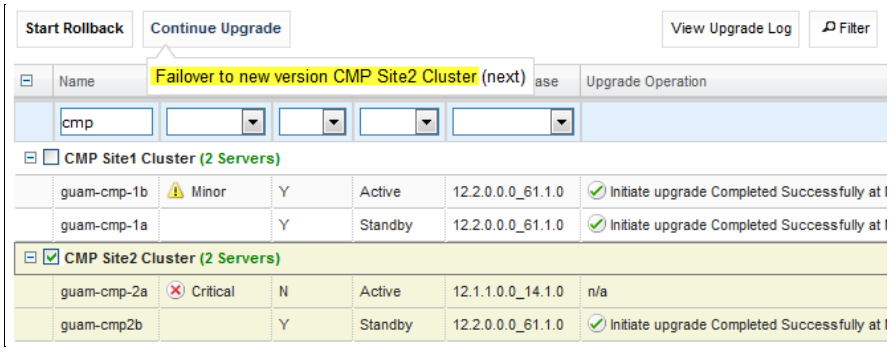
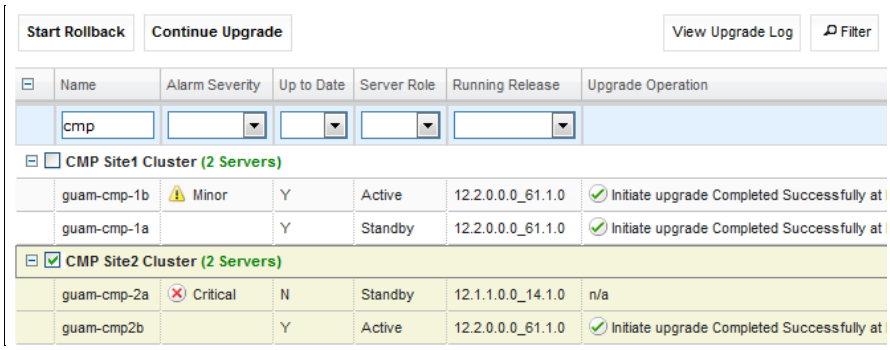
Successful upgrade status will show the following for both servers in the Primary CMP cluster:

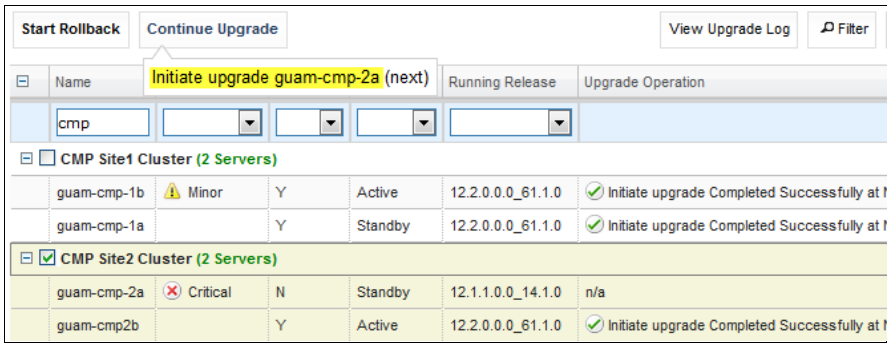
- 12.2 in the Running Release column for both servers
- A Y in the Up to Date column
- Active or Standby state for both servers in the Primary CMP cluster.

Step	Procedure	Result
21. ☐	Proceed to next upgrade procedure	Verify the following information: • Primary Site1 is running release 12.2 • Secondary Site is on release 12.1.x • Proceed to the next procedure to upgrade the secondary CMP cluster.
		THIS PROCEDURE HAS BEEN COMPLETED

7.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify status of CMP cluster	**Upgrade → Upgrade Manager** • Primary CMP is completely upgraded to 12.2 • Secondary CMP cluster is on 12.1.x 
2. ☐	**CMP GUI:** Upgrade Secondary CMP cluster **NOTE:** This will take approximately 30 minutes to complete.	**Upgrade → Upgrade Manager** **NOTE:** The **Filter** button can be used to show only the CMP servers. Enter CMP on the Name field.  • Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. When hovering over the button, it will read 'Initiate upgrade *<site2_standbyserver>* (next)'  • Click **OK** to confirm and continue with the operation. This will continue 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: <u>**Expected Critical alarm**</u> **31283** Lost Communication with server

Step	Procedure	Result
		70001 QP_procmgr failed **70025** QP Slave database is a different version than the master **<u>Expected Major Alarm</u>** **70004** QP Processes down for maintenance **<u>Expected Minor Alarms</u>** **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 appears in the Upgrade Operation column. 
3. ☐	**CMP GUI**: Failover of the Secondary CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. Notice the message 'Failover to new version CMP Site2 Cluster'  • Click **OK** to confirm and continue with the operation. The failover will take about a minute to complete. Wait until the upgraded server is active, running 12.2 as shown below. 

Step	Procedure	Result
4. ☐	**CMP GUI**: Continue upgrade of the Secondary CMP cluster	• Select the checkbox for the Secondary CMP Server cluster at Site2 • Click **Continue Upgrade**. When hovering over the button, the message will display the next action, which is upgrading the remaining CMP in standby, still running 12.1.x.  • Click **OK** to confirm and continue with the operation. During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical alarm</u>** **31283** Lost Communication with server **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **<u>Expected Major Alarm</u>** **70004** QP Processes down for maintenance **<u>Expected Minor Alarms</u>** **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
5. ☐	**CMP GUI:** Verify that the upgrade completed successfully.	**Upgrade → Upgrade Manager** Successful upgrade status will show release 12.2 in the Running Release column and the Upgrade Operation. The Upgrade Operation column will show 'Initiate Upgrade Completed Successfully at..' with the correct date and time.

Step	Procedure	Result
		Start Rollback | Start Upgrade | View Upgrade Log | Filter Name | Alarm Severity | Up to Date | Server Role | Running Release | Upgrade Operation cmp CMP Site1 Cluster (2 Servers) guam-cmp-1b | Minor | Y | Active | 12.2.0.0.0_61.1.0 | Initiate upgrade Completed Successfully at guam-cmp-1a | Y | Standby | 12.2.0.0.0_61.1.0 | Initiate upgrade Completed Successfully at CMP Site2 Cluster (2 Servers) guam-cmp-2a | Y | Standby | 12.2.0.0.0_61.1.0 | Initiate upgrade Completed Successfully at guam-cmp2b | Y | Active | 12.2.0.0.0_61.1.0 | Initiate upgrade Completed Successfully at
6. ☐	**CMP GUI:** Verify alarms	**System Wide Reports → Alarms → Active Alarms** **<u>Expected Minor Alarms</u>** **70500** System Mixed Version
7. ☐	Procedure is complete.	Verify the following information: • All CMP clusters upgrades are complete and running release 12.2 • All MRA and MPE clusters are running release 12.1.x The Policy Management system is running in mixed-version mode.
		THIS PROCEDURE HAS BEEN COMPLETED

8. UPGRADE NON-CMP CLUSTERS (MPE, MRA) 11.5.X/12.1.X WIRELESS MODE

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

NOTES:

- An upgrade of up to 4 clusters (8 for 12.1.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.

8.1 Upgrade Preparation

8.1.1 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 12.2 ISO files	**Upgrade → Upgrade Manager** • Verify that all CMP clusters have both Active, Standby status. • Verify that all MPE and MRA clusters have an Active, Standby, and Spare server. • Verify that Policy Management release 12.2 ISO files are available for all MPE, and MRA clusters. One ISO per server • Verify that the CMP cluster is upgraded successfully and running Policy Management release 12.2
THIS PROCEDURE HAS BEEN COMPLETED		

8.2 Upgrade MRA and MPE Servers

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

This procedure is applicable for an 11.5.x (wireless mode) or 12.1.x upgrade to 12.2.

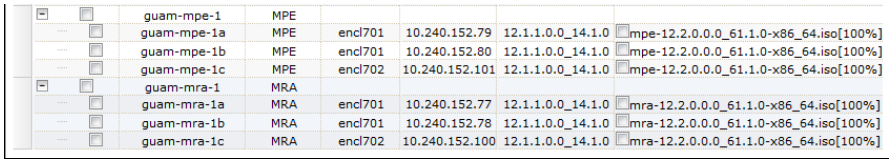
This section can be replicated for each site/segment to be upgraded, allowing you to add cluster and site specific information.

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

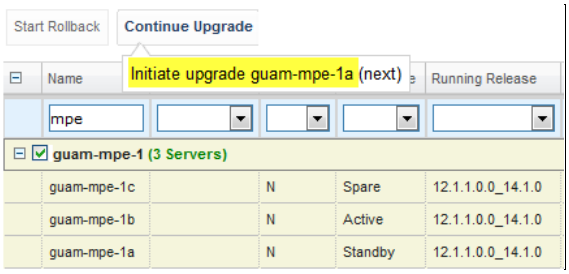
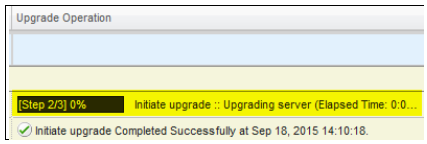
1. Select and start upgrade on the standby server
2. Failover
3. Re-apply configuration
4. Continue to upgrade the spare server
5. Continue upgrade on remaining server
6. (MPE only) Re-apply configuration one MPE cluster at a time

NOTES:

- All CMP clusters must be upgraded to Policy Management release 12.2 prior to executing the following procedures.
- Four (4) clusters (8 for 12.1.x) can be running the upgrade at one time.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 12.2.

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the MPE/MRA servers to be upgraded	Perform the following: • Check for current active alarms • 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** • Go to the KPI Dashboard and capture a screenshot. **System Wide Reports → KPI Dashboard**
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	**Upgrade → Upgrade Manager** Verify information for the MRA/MPE servers: • Current release 11.5.x, or 12.1.x installed • Active/Standby/Spare status • ISO version to be deployed is 12.2 (verify the current ISO files are 12.2 by going to **Upgrade→ ISO Maintenance)** 

guam-mpe-1	MPE					
guam-mpe-1a	MPE	encl701	10.240.152.79	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1b	MPE	encl701	10.240.152.80	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mpe-1c	MPE	encl702	10.240.152.101	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1	MRA				
guam-mra-1a	MRA	encl701	10.240.152.77	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1b	MRA	encl701	10.240.152.78	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]
guam-mra-1c	MRA	encl702	10.240.152.100	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]

Step	Procedure	Result
3. ☐	**CMP GUI**: Upgrade clusters **NOTE:** The upgrade of a single server takes approximately 40 minutes to complete.	**NOTE:** Start the upgrade on ONE cluster. Wait until the cluster shows "OOS", and then continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running upgrade at any time. **Upgrade → Upgrade Manager** • Select the checkbox for the cluster to be upgraded, it can be an MRA or MPE • Click **Continue Upgrade**  • Click **OK** to confirm and continue with the operation. It will begin to upgrade the standby server of that cluster. Wait until the cluster reports OOS before selecting the next cluster Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical Alarms</u>** **31283** HA Server Offline / Lost Communication with server **70001** QP_procmgr failed **31227** HA availability status failed **<u>Expected Major Alarm</u>** **31233** High availability path loss of connectivity **70004** QP Processes down for maintenance Severity: Major; Alarm ID: 31233; Text: High availability path loss of connectivity Severity: Major; Alarm ID: 70004; Text: The QP processes have been brought down for maintenance. **<u>Expected Minor Alarms</u>** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault

Step	Procedure	Result
		78001 Rsync Failed

Severity	Alarm ID	Text
Minor	31107	DB merging from a child Source Node has failed
Minor	31107	DB merging from a child Source Node has failed
Minor	31107	DB merging from a child Source Node has failed
Minor	31107	DB merging from a child Source Node has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	31114	DB Replication of configuration data via SOAP has failed
Minor	70501	The Cluster is running different versions of software
Minor	70503	The server is in forced standby
Minor	70507	An upgrade/backout action on a server is in progress

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

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

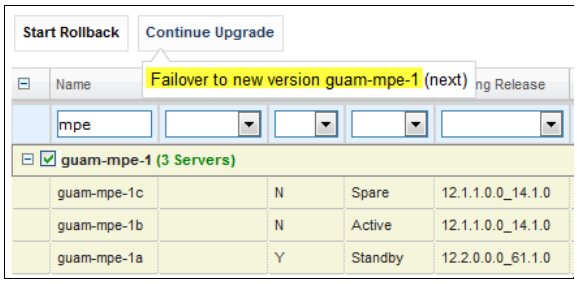
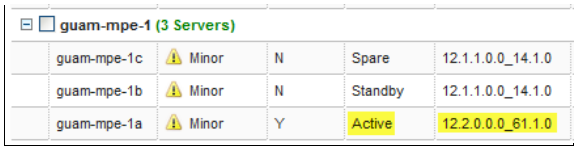
guam-mpe-1 (3 Servers)					
guam-mpe-1c		N	Spare	12.1.1.0.0_14.1.0	n/a
guam-mpe-1b		N	Active	12.1.1.0.0_14.1.0	Initiate backout Completed Successfully at I
guam-mpe-1a		Y	Standby	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at

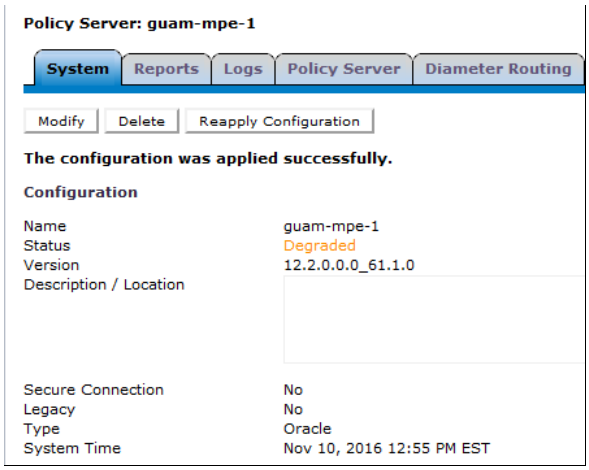
During the upgrade activities, the following alarms may be generated and considered normal reporting events.

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

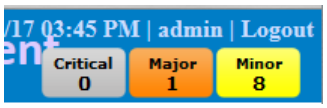
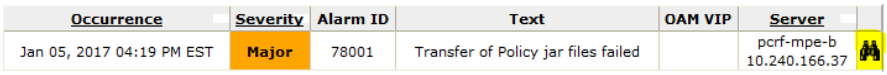
Expected Minor Alarms

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

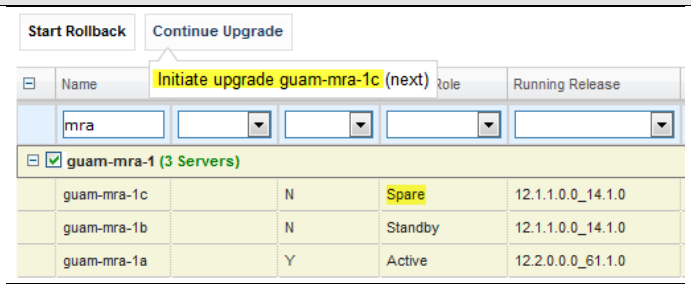
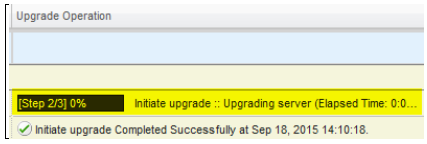
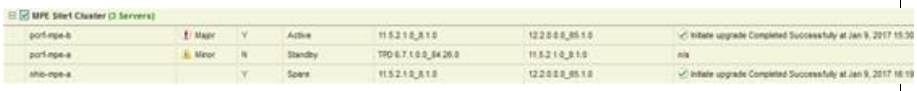
Step	Procedure	Result
4. ☐	**CMP GUI**: Continue to upgrade the MRA/MPE clusters. Next operation is a **failover** **NOTE:** 4 clusters (8 for 12.1.x) can be running the upgrade process at one time.	Fail over **ONE** cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster. **Upgrade → Upgrade Manager** • Select the checkbox for the cluster being upgraded (it can be an MRA or MPE) • Click **Continue Upgrade**. When hovering over the button, it will say 'Failover to new version…'  • Click **OK** to confirm and continue with the operation. It will start to failover the cluster. Wait until failover completes before failing over the next cluster, this will take a minute or two to complete. Verify the 12.2 server is now active. The process is complete when there is an active/standby at site 1 and spare at site 2. 

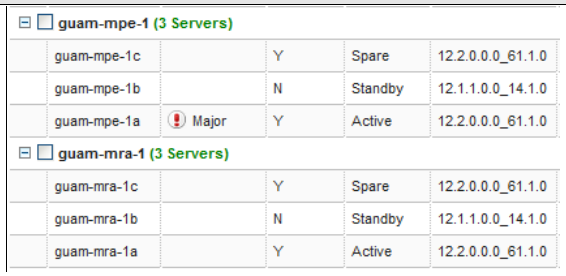
Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the upgrade successfully.	For MPE: **PolicyServer → Configuration →** *<MPE_cluster_name>* **→ System** For MRA: **MRA→Configuration→**<*MRA_cluster*>**→System** The selected cluster will show status "Degraded" as it has different releases for the Active and Standby servers. It may display "Config mismatch" as well. This is expected. • Click **Reapply Configuration** **NOTE:** A progress bar appears for the MPE reapply configuration only. The MRA reapply configuration does not display the progress bar. • Note the version is successfully changed to the upgraded release 12.2. **NOTE:** The status will appear as Degraded as the servers are still in different releases. 

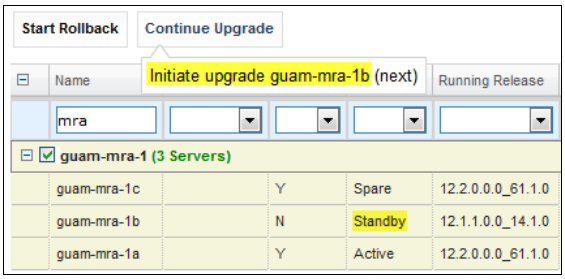
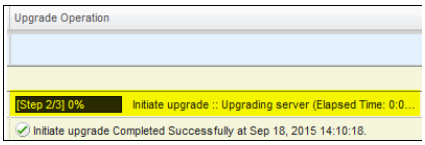
Step	Procedure	Result
6. ☐	**CMP GUI:** Current alarms	During the upgrade activities, the following alarms may be generated and considered normal reporting events. **Expected Critical alarm** None **Expected Major Alarm** **78001** Rsync Failed Severity: Major; Alarm ID: 78001; Text: Transfer of Policy jar files failed **Expected Minor Alarms** **70503** Server Forced Standby **70502** Cluster Replication Inhibited **70500** System Mixed Version **70501** Cluster Mixed Version **71402** Connectivity Lost **31101** Database replication to slave failure
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	**Upgrade Manager → System Maintenance** If traffic is active, go to step 9. If traffic does not become active within 90 seconds: • Select the checkbox for the partially upgraded cluster, and select **Operations → Rollback**. • The pre-12.2 MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	• **Policy Server → Configuration →** *<mpe_cluster name>* **→ System** tab or **MRA → Configuration →** *<mra_cluster name>* **→ System** tab • Click **Reapply Configuration** • Verify that the version is changed back to 11.5.x or 12.1.x, and the action report success. • If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.

Step	Procedure	Result
9. ☐	**CMP GUI:** 78001 Major Alarm	During the upgrade activities, *Major* alarm 78001 in particular may be generated. And even though it's a normal event, the alarm will not clear by itself. Before continuing we should make sure that the alarm is cleared. Click on the Major alarms button in the upper right part to display the alarms:  Now click on the binoculars icon on the right to display details about the 78001 Major alarm  Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 05, 2017 04:19 PM EST | Major | 78001 | Transfer of Policy jar files failed | | pcrf-mpe-b 10.240.166.37 You should see in the last line of the details that the reason for the major alarm is "Version check failed". **Date/Time** Jan 05, 2017 04:19 PM EST **Severity** Major **Text** Transfer of Policy jar files failed **Count** 1 **First Occurrence** Jan 05, 2017 04:19 PM EST **Last Occurrence** Jan 05, 2017 04:19 PM EST **Server** pcrf-mpe-b,10.240.166.37 **Details** RSYNC: Policy jar files sync to standby failed. Reason: Version check failed Cancel If you see a different reason, stop and contact My Oracle Support. If you see the "Version check failed" reason, continue here. Navigate to System Wide Reports > Alarms > Active Alarms and select the 78001 Major alarm pcrf-mpe-b 10.240.166.37 | MPE | Major | 78001 | 5m 35s / --- | Transfer of Policy jar files failed | 01/05/2017 16:19:53 EST Click on 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 12.1.x) can be running the upgrade process at one time.
		
		Upgrade → Upgrade Manager
		
		• Select the checkbox for a cluster.
		  - Select one cluster at a time
		  - Can be an either an MRA or MPE cluster
		• Click **Continue Upgrade**. When hovering over the button, it will read 'Initiate upgrade…' on the spare server

Step	Procedure	Result
		 • 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 will be cleared after the MPE cluster is completely upgraded. **<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 **<u>Expected Minor Alarms</u>** **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 message 'Initiate upgrade Completed Successfully…' shows in the Upgrade Operation column.  • The server goes back to the Spare state. • The Up to Date column shows a Y (YES). The Active and Spare servers are on release 12.2 and the current Standby will be 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 12.1.x) may be running the upgrade at one time.
		
		Upgrade → Upgrade Manager
		
		• Select the checkbox for a cluster
		  - Select one cluster at a time
		  - Can be an either an MRA or MPE cluster
		• Click **Continue Upgrade**. When hovering over the button, the message will display the next action, which is to initiate the upgrade of the standby server.
		 
		• Click **OK** to confirm and continue with the operation. It will begin the final server upgrade of the cluster
		Wait until the cluster reports OOS before selecting the next cluster
		
		Follow the progress in the Upgrade Operation column.
		 
		During the upgrade activities, the following alarms may be generated and considered normal reporting events—these will be cleared after the MPE cluster is completely upgraded.
		
		<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
		
		<u>Expected Minor Alarms</u>
		
		70503 Server Forced Standby
		70507 Upgrade In Progress

Step	Procedure	Result
		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 12.2
12. ☐	**CMP GUI: (MPE only)** Reapply configuration on the fully upgraded MPE clusters.	**MPE only** • **PolicyServer → Configuration →** <*MPE_cluster*> **→ System** • Click **Reapply Configuration** **NOTE:** A progress bar appears for the MPE reapply configuration. Reapply Settings to the RC Re-applying Settings to the RC... Applying Configuration to Policy Server
13. ☐	Repeat steps 1–14 for the next MPE or MRA clusters	Proceed with next cluster(s)
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
		THIS PROCEDURE HAS BEEN COMPLETED

9. UPGRADE NON-CMP CLUSTERS (MA, MPE-R, MPE-S, BOD) 11.5.X TO 12.2 CABLE MODE

The following procedures will upgrade a site/segment containing one or more clusters of Cable components including MA, MPE and BOD.

NOTES:

- An upgrade of up to 4 clusters can be running at the same time.
- The following is the Cable Policy components upgrade sequence:
  - MA
  - MPE-R
  - MPE-S
  - BoD-AM

9.1 Site/Segment Upgrade Preparation

9.1.1 Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	Use a supported browser to login using the admin user ID or with a user ID that has admin privileges.
2. ☐	**CMP GUI:** Verify current Upgrade Manager status and software release 12.2 ISO files	**Upgrade → Upgrade Manager** • Verify that all CMP clusters have both Active, Standby status. • Verify that all other components clusters (MA, MPE, BoD) have both Active, Standby. • Verify that Policy Management release 12.2 ISO files are staged on each of the components servers in the topology • Verify that the CMP cluster is upgraded successfully and running Policy Management release 12.2
THIS PROCEDURE HAS BEEN COMPLETED		

9.2 Upgrade MA Servers

This procedure will upgrade one or more MA clusters at a site/segment.

This procedure is applicable for all 11.5.X releases upgrading to 12.2

This section can be replicated for each site/segment to be upgraded.

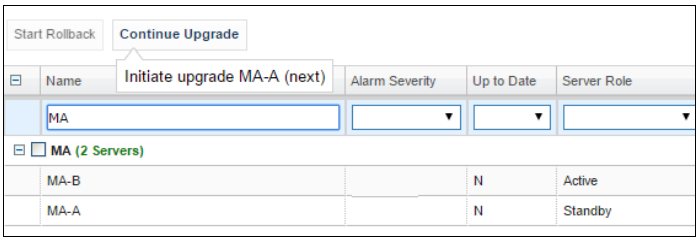
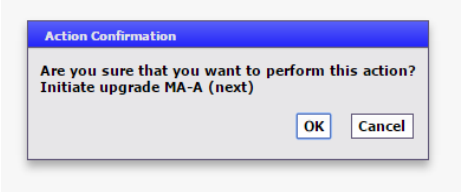
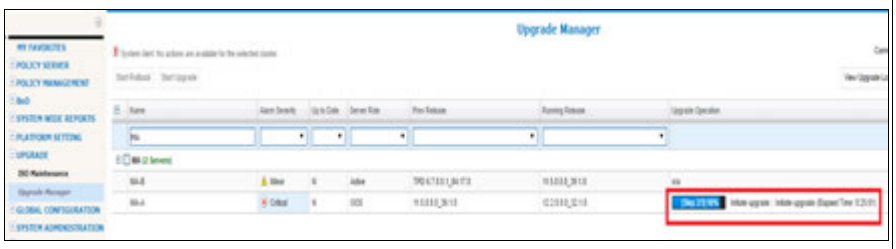
The upgrade procedure is essentially the same for MA, MPE-R/S and BOD clusters.

1. Select and start upgrade on Standby server
2. Failover one cluster at a time
3. Re-apply configuration one cluster at a time
4. Continue upgrade on remaining server

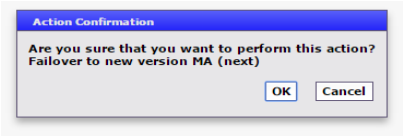
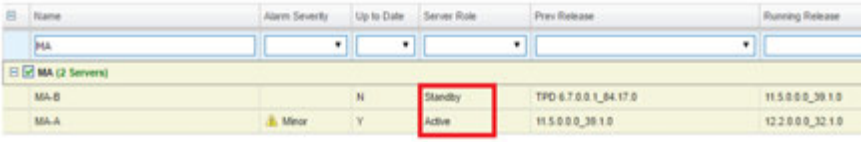
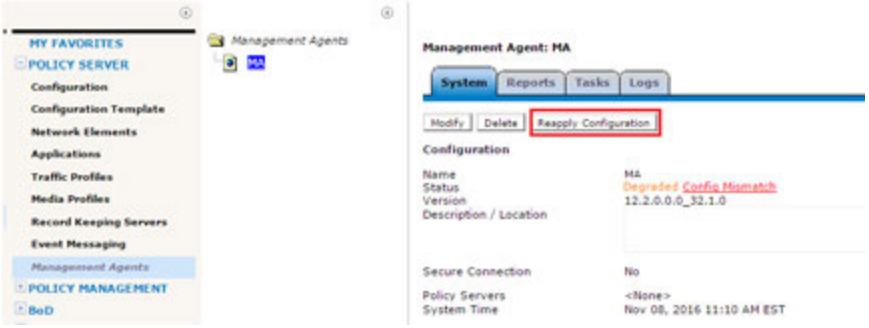
NOTES:

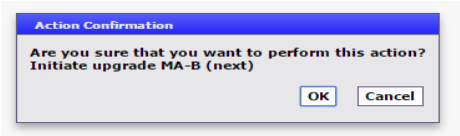
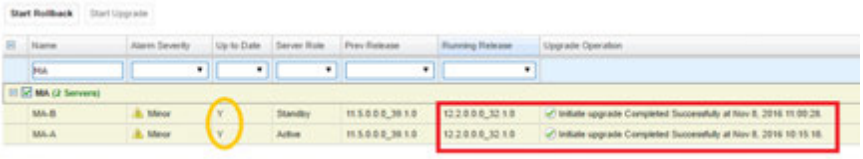
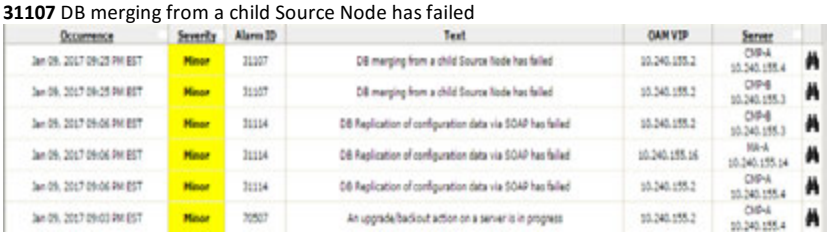
- MA component is an optional component that customer can choose to use or not use it so this procedure would be skipped in case customer's Cable system does not include MA component deployed.
- All CMP clusters must be upgraded to Policy Management release 12.2 prior to executing the following procedures.
- Four (4) clusters 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 12.2

Step	Procedure	Result
1. ☐	**CMP GUI:** Health Checks on the MA servers to be upgraded	Perform the following: • Check for current Active Alarms and confirm non affects the MA cluster upgrade: Note that some alarms are expected since the whole system's upgrade is not completed.

Step	Procedure	Result
2. ☐	**CMP GUI:** Verify the upgrade status of selected MA Cluster(s)	**Upgrade →Upgrade Manager** Verify information for the MAs: • Current release 11.5.X • Active/Standby status for the servers in the MA cluster • Current ISO version to be deployed is 12.2
3. ☐	**CMP GUI:** Upgrade clusters	**NOTE:** Start the upgrade on ONE cluster. Wait for a minute, and then continue with the next cluster and so on. Up to 4 clusters maximum may be running upgrade at any one time. **Upgrade → Upgrade Manager** Select the checkbox for the MA cluster (one cluster at a time) ○ Click **Continue Upgrade**.  ○ Click **OK** to confirm and continue with the operation. It will begin to upgrade the standby Server of that cluster.  Wait until the cluster reports OOS before selecting the next cluster Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and considered normal reporting events—these will be cleared after the MA cluster is completely

Step	Procedure	Result
		upgraded. Upgrade is complete on the first server in the cluster when the 'Completed Successfully…' message shows in the Upgrade Operation column and up to date flag has "Y" value. The server will go back to Standby state when the upgrade completes. During the upgrade activities, the following alarms may be generated and considered normal reporting events. The following minor alarms may be present: **Expected Critical Alarms** **70025** QP Slave database is a different version than the master **Expected Major Alarms** **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70501** The Cluster is running different versions of software

Step	Procedure	Result
4. ☐	**CMP GUI:** Failover to upgraded server **NOTE:** 4 clusters 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. **Upgrade → Upgrade Manager** Select the checkbox for the MA cluster (one cluster at a time) a. Click **Continue Upgrade**. When hovering over the button, it will say 'Failover to new version…' b. Click **OK** to confirm and continue with the operation. It will begin to failover the cluster:  Wait until failover completes before failing over the next cluster. And verify the 12.2 upgraded MA server is now active. 
5. ☐	**CMP GUI:** Reapply configuration on the upgraded MA cluster	**Policy Server→Management Agents→<*Upgraded* MA cluster>→System** Push **Reapply Configuration**.  **Note:** ▪ Cluster is in degraded state, this is expected due to different versions of software between the servers in the MA cluster ▪ Notice the version should be successfully changed to the release 12.2

Step	Procedure	Result
6. ☐	**CMP GUI:** Upgrade the other MA server	**Upgrade → Upgrade Manager** a) Click **Continue Upgrade**. When hovering over the button, it will say 'Initiate upgrade' for the other MA server b) Click OK to confirm and continue with the operation. It will begin to failover the cluster:  Wait until upgrade operation of the MA server indicates successfully completion, up to date flag indicates "Y" and running release has the 12.2 release 
7. ☐	**CMP GUI**: Current alarms	During the upgrade activities, the following alarms may be generated and considered normal reporting events. **<u>Expected Critical Alarm</u>** **31283** HA Server Offline **<u>Expected Minor Alarms</u>** **70507** An upgrade/back out action on a server is in progress **31114** DB Replication of configuration data via SOAP has failed **31107** DB merging from a child Source Node has failed 
8. ☐	**CMP GUI:** Verify traffic is active	If traffic is not active and issues or non-expected alarms are observed, a rollback to 11.5.X might be needed, contact Oracle support to back out of a partially upgraded cluster.

Step	Procedure	Result
9. ☐	Repeat steps 1–10 for the next MA cluster(s) if deployed	Proceed with next cluster(s): MA Cluster _____ MA Cluster _____ MA Cluster _____
THIS PROCEDURE HAS BEEN COMPLETED		

9.3 Upgrade MPE-R/S Servers

This procedure will upgrade one or more MPE-R and MPE-S clusters at a site/segment.

This procedure is applicable for all 11.5.X releases upgrading to 12.2

This section can be replicated for each site/segment to be upgraded.

The upgrade procedure is essentially the same for MA, MPE-R/S and BOD clusters.

1. Select and start upgrade on Standby server
2. Failover one cluster at a time
3. Re-apply configuration one cluster at a time
4. Continue upgrade on remaining server
5. Re-apply configuration on the fully upgraded cluster

NOTES:

- In case solution is geo-redundant, same process could be followed to upgrade the 3 servers of the MPE-S cluster(s) starting with StandBy server then spare server in secondary site and finally the Active server.
- All CMP clusters must be upgraded to Policy Management release 12.2 prior to executing the following procedures.
- Four (4) clusters 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 12.2

Step	Procedure	Result
1. ☐	**CMP GUI:** Health Checks on the MPE-R servers to be upgraded	Perform the following: • Check for current Active Alarms and confirm non affects the MPE-R/S clusters' upgrade: Note that some alarms are expected since the whole system's upgrade is not completed.

Step	Procedure	Result
2. ☐	**CMP GUI:** Verify the upgrade status of selected MPE-R Cluster(s)	**Upgrade →Upgrade Manager** Verify information for the MPE-Rs: • Current release 11.5.X • Active/Standby status for the servers in the MPE-R cluster • Current ISO version to be deployed is 12.2 Start Rollback Start Upgrade Name | Alarm Severity | Up to Date | Server Role | Prev Release | Running Release | Upgrade Operation MPE-R MPE-R (2 Servers) MPE-R-B | N | Standby | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a MPE-R-A | N | Active | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a
3. ☐	**CMP GUI:** Upgrade MPE-R clusters	**NOTE:** Start the upgrade on ONE cluster. Wait for a minute, and then continue with the next cluster and so on. Up to 4 clusters maximum may be running upgrade at any one time. **Upgrade → Upgrade Manager** Select the checkbox for the MPE-R cluster (one cluster at a time) ○ Click **Continue Upgrade**. Start Rollback Continue Upgrade Initiate upgrade MPE-R-B (next) Name | Server Role | Prev Release | Running Release | Upgrade Operation MPE-R MPE-R (2 Servers) MPE-R-B | N | Standby | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a MPE-R-A | N | Active | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a ○ Click **OK** to confirm and continue with the operation. It will begin to upgrade the standby Server of that cluster. Action Confirmation Are you sure that you want to perform this action? Initiate upgrade MPE-R-B (next) OK Cancel 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 will be cleared after the MPE-R cluster is completely upgraded. Upgrade is complete on the first server in the cluster when the 'Completed Successfully…' message shows in the Upgrade Operation column and up to date flag has "Y" value. The server will go back to Standby state when the upgrade completes.

Step	Procedure	Result

MPE-R (2 Servers)					
MPE-R-B	Y	Standby	11.5.0.0.0_38.1.0	12.2.0.0.0_32.1.0	Initiate upgrade Completed Successfully at Nov 8, 2016 20:04:48
MPE-R-A	N	Active	TPD 6.7.0.0.1_84.17.0	11.5.0.0.0_38.1.0	n/a

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

The following minor alarms may be present:

Expected Critical Alarms

31227 HA availability status failed

Jan 10, 2017 09:07 AM EST	Critical	31283	High availability server is offline	10.240.155.10	MPE-S-A 10.240.155.8

Expected Major Alarms

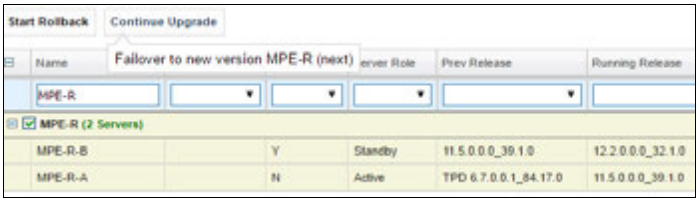
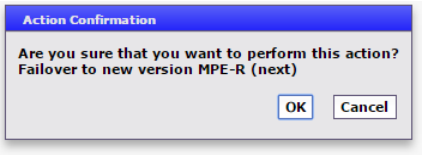
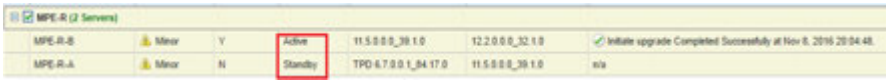
70004 QP Processes down for maintenance

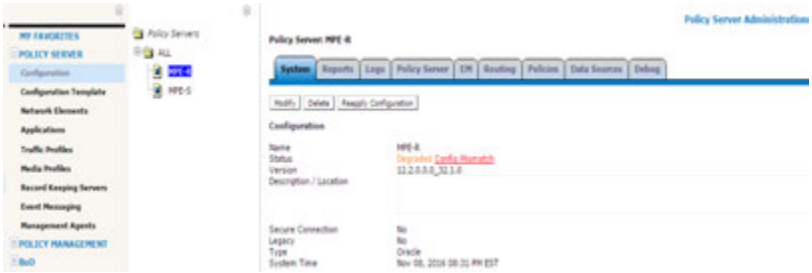
Jan 09, 2017 09:30 PM EST	Major	70004	The QP processes have been brought down for maintenance.	10.240.155.7	MPE-R-A 10.240.155.5

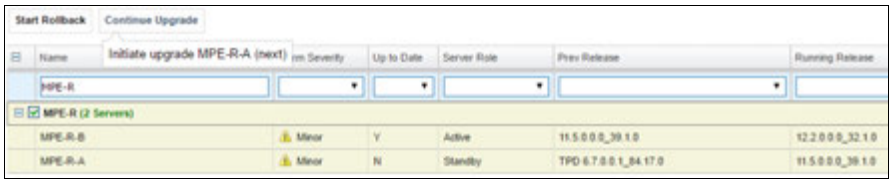
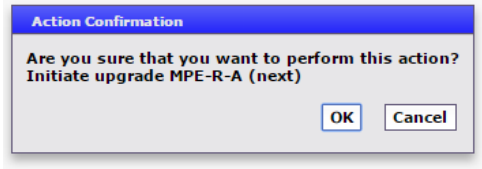
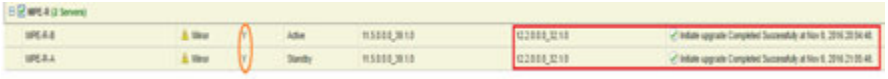
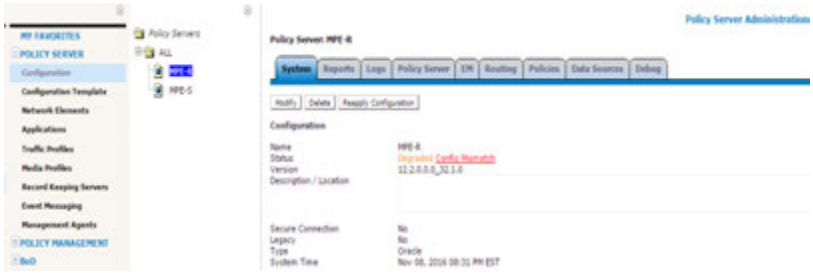
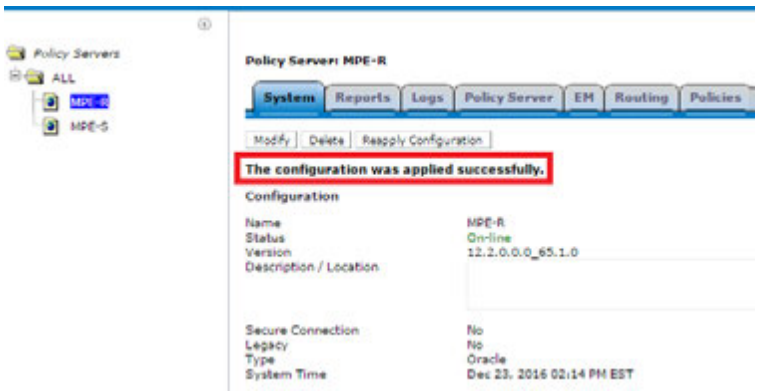
Expected Minor Alarms

70507 Upgrade In Progress
31000 S/W Fault
31101 Database replication to slave failure
31102 DB Replication from Master Failure
31114 DB replication over SOAP has failed
31107 Database merge from child failure
31113 DB replication manually disabled
32513 Device Interface Warning

Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 09, 2017 09:32 PM EST	Minor	31114	DB Replication of configuration data via SOAP has failed	10.240.155.2	CMP-B 10.240.155.3
Jan 09, 2017 09:32 PM EST	Minor	31114	DB Replication of configuration data via SOAP has failed	10.240.155.7	MPE-R-B 10.240.155.6
Jan 09, 2017 09:32 PM EST	Minor	31000	Program impaired by s/w fault	10.240.155.7	MPE-R-B 10.240.155.6
Jan 09, 2017 09:32 PM EST	Minor	31107	DB merging from a child Source Node has failed	10.240.155.2	CMP-A 10.240.155.4
Jan 09, 2017 09:32 PM EST	Minor	31101	DB replication to a slave DB has failed	10.240.155.2	CMP-A 10.240.155.4
Jan 09, 2017 09:32 PM EST	Minor	31107	DB merging from a child Source Node has failed	10.240.155.2	CMP-B 10.240.155.3
Jan 09, 2017 09:32 PM EST	Minor	31101	DB replication to a slave DB has failed	10.240.155.7	MPE-R-B 10.240.155.6
Jan 09, 2017 09:32 PM EST	Minor	32513	Device Interface Warning	10.240.155.7	MPE-R-A 10.240.155.5
Jan 09, 2017 09:31 PM EST	Minor	31102	DB replication from a master DB has failed	10.240.155.7	MPE-R-A 10.240.155.5
Jan 09, 2017 09:30 PM EST	Minor	70507	An upgrade/backout action on a server is in progress	10.240.155.2	CMP-A 10.240.155.4

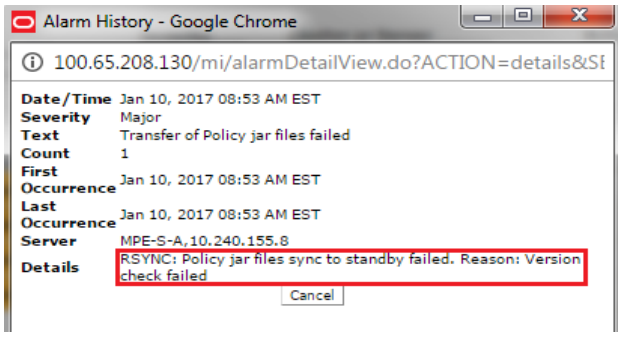
Step	Procedure	Result
4. ☐	**CMP GUI:** Failover to upgraded server **NOTE:** 4 clusters can be running the upgrade process at one time.	Fail over **ONE** cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster. **Upgrade → Upgrade Manager** Select the checkbox for the MPE-R cluster (one cluster at a time) a. Click **Continue Upgrade**. When hovering over the button, it will say 'Failover to new version…'  b. Click **OK** to confirm and continue with the operation. It will begin to failover the cluster:  Wait until failover completes before failing over the next cluster. And verify the 12.2 upgraded MPE-R server is now active. 

Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on the upgraded MPE-R server	**Policy Server→Configuration→<*Upgraded* MPE-R cluster>→System** Push **Reapply Configuration**.  **Note:** ▪ Cluster is in degraded state, this is expected due to different versions of software between the servers in the MPE-R cluster ▪ Notice the version should be successfully changed to the release 12.2 ▪ After successful reapplying the configuration , the config mismatch message clears out : **Policy Server: MPE-R** System | Reports | Logs | Policy Server | EM Modify | Delete | Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: MPE-R Status: Degraded Version: 12.2.0.0.0_32.1.0 Description / Location:

Step	Procedure	Result
6. ☐	**CMP GUI:** Upgrade the other MPE-R server	**Upgrade → Upgrade Manager** a. Click **Continue Upgrade**. When hovering over the button, it will say 'Initiate upgrade' for the other MPE-R server  b. Click OK to confirm and continue with the operation. It will begin to failover the cluster:  Wait until upgrade operation of the MPE-R server indicates successfully completion, up to date flag indicates "Y" and running release has the 12.2 release 
7. ☐	**CMP GUI:** Reapply configuration on the upgraded MPE-R cluster	**Policy Server→Configuration→<*Upgraded* MPE-R cluster>→System** Push **Reapply Configuration**.  **Note:** After successful reapplying the configuration , the config mismatch message clears out : 

Step	Procedure	Result
8. ☐	**CMP GUI**: Current alarms	During the upgrade activities, the following alarms may be generated and considered normal reporting events. **Expected Critical Alarm** **31227** HA availability status failed Jan 10, 2017 09:07 AM EST | Critical | 31283 | High availability server is offline | 10.240.155.10 | MPE-S-A 10.240.155.8 **Expected Major Alarm** **78001** Rsync Failed Jan 10, 2017 07:38 AM EST | Major | 78001 | Transfer of Policy jar files failed | 10.240.155.7 | MPE-R-A 10.240.155.5 **Expected Minor Alarms** **78001** Rsync Failed **71103** PCMM Conn Lost **70502** Cluster Replication Inhibited **31113** DB Replication Manually Disabled Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Jan 10, 2017 07:34 AM EST | Minor | 78001 | Transfer of Policy jar files failed | 10.240.155.7 | MPE-R-B 10.240.155.6 Jan 10, 2017 07:34 AM EST | Minor | 71103 | PCMM Conn Lost | 10.240.155.10 | MPE-S-B 10.240.155.9 Jan 10, 2017 07:34 AM EST | Minor | 31113 | Replication Manually Disabled | 10.240.155.7 | MPE-R-B 10.240.155.6 Jan 10, 2017 07:33 AM EST | Minor | 70502 | Replication is inhibited in the cluster | 10.240.155.2 | CMP-A 10.240.155.4
9. ☐	**CMP GUI:** duri MPE-R cluster upgrade	If traffic is not active and issues or non-expected alarms are observed, then rollback to 11.5.X is decided, skip to section 12 for backing out.
10. ☐	Repeat steps 1–8 for the next MPE-R cluster(s) if deployed	Proceed with next cluster(s): MPE-R Cluster _____ MPE-R Cluster _____ MPE-R Cluster _____
11. ☐	CMP GUI: Upgrade MPE-S clusters	Follow same steps outlined in this procedure for upgrading MPE-R clusters to upgrade deployed MPE-S clusters. **Note:** In case solution is geo-redundant, same process could be followed to upgrade the 3 servers of the MPE-S cluster(s) starting with StandBy server then spare server in secondary site and finally the Active server. Successful upgrade operation of the MPE-S servers indicates successfully completion, up to date flag indicates "Y" and running release has the 12.2 release for both MPE-S servers. MPE-S (2 Servers) MPE-S-A | Y | Standby | 11.5.0.0.0_30.1.0 | 12.2.0.0.0_32.1.0 | Initiate upgrade Completed Successfully at Nov 9, 2016 8:47:50 MPE-S-B | Y | Active | 11.5.0.0.0_30.1.0 | 12.2.0.0.0_32.1.0 | Initiate upgrade Completed Successfully at Nov 9, 2016 8:15:40
12. ☐	**CMP GUI:** If traffic does not become active within 90 seconds	If traffic is not active and issues or non-expected alarms observed, then rollback to 11.5.X is decided, skip to section 12 for backing out.

Step	Procedure	Result
13. ☐	Repeat steps 1–7 for the next MPE-S cluster(s) if deployed	Proceed with next cluster(s): MPE-S Cluster _____ MPE-S Cluster _____ MPE-S Cluster _____

Step	Procedure	Result
14.	**CMP GUI:** Residual upgrade Major Alarm 78001	During the course of MPE clusters upgrade activities, alarm 78001 in particular may be generated either as Minor or Major alarm. And even though it's a normal event during the upgrade, major alarm 78001 will not clear automatically after the upgrade of MPE cluster completes. This alarm does not indicate an issue or problem in the system and we should clear it manually as follows: Click on the Major alarms button in the upper right part to display the alarms: Before manually clearing it, click on the binoculars icon on the right to confirm the details of the alarm: The details that indicate it is safe to clear out the alarm should be "Version check failed".  **Note:** If you see a different reason in the details, stop and contact My Oracle Support. To manually clear it, navigate to System Wide Reports > Alarms > Active Alarms and Click on the trash can icon on the far right of the 78001 Major alarms: Click "OK" in the confirmation message that follows: In few seconds the alarm will clear out from CMP GUI.

Step	Procedure	Result
THIS PROCEDURE HAS BEEN COMPLETED		

9.4 Upgrade BOD Servers

This procedure will upgrade one or more BOD clusters at a site/segment.

This procedure is applicable for all 11.5.X releases upgrading to 12.2

This section can be replicated for each site/segment to be upgraded.

The upgrade procedure is essentially the same for MA, MPE-R/S and BOD clusters.

1. Select and start upgrade on Standby server
2. Failover one cluster at a time
3. Re-apply configuration one cluster at a time
4. Continue upgrade on remaining server

NOTES:

- In case solution is geo-redundant, same process could be followed to upgrade the 3 servers of the BOD cluster(s) starting with StandBy server then spare server in secondary site and finally the Active server.
- All CMP clusters must be upgraded to Policy Management release 12.2 prior to executing the following procedures.
- Four (4) clusters 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 12.2

Step	Procedure	Result
1. ☐	**CMP GUI:** Health Checks on the BOD servers to be upgraded	Perform the following: • Check for current Active Alarms and confirm non affects the BOD cluster upgrade: Note that some alarms are expected since the whole system's upgrade is not completed.

Step	Procedure	Result
2. ☐	**CMP GUI:** Verify the upgrade status of selected BOD Cluster(s)	**Upgrade →Upgrade Manager** Verify information for the BOD clusters: • Current release 11.5.X • Active/Standby status for the servers in the BOD cluster • Current ISO version to be deployed is 12.2 Start Rollback Start Upgrade Name | Alarm Severity | Up to Date | Server Role | Prev Release | Running Release | Upgrade Operation BOD BOD (2 Servers) BOD-B | N | Active | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a BOD-A | N | Standby | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a
3. ☐	**CMP GUI:** Upgrade BOD clusters	**NOTE:** Start the upgrade on ONE cluster. Wait for a minute, and then continue with the next cluster and so on. Up to 4 clusters maximum may be running upgrade at any one time. **Upgrade → Upgrade Manager** Select the checkbox for the BOD cluster (one cluster at a time) ○ Click **Continue Upgrade**. Start Rollback Continue Upgrade Initiate upgrade BOD-A (next) Name | Server Role | Prev Release | Running Release | Upgrade Operation BOD BOD (2 Servers) BOD-B | N | Active | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a BOD-A | N | Standby | TPD 6.7.0.0.1_84.17.0 | 11.5.0.0.0_39.1.0 | n/a ○ Click **OK** to confirm and continue with the operation. It will begin to upgrade the standby Server of that cluster. Action Confirmation Are you sure that you want to perform this action? Initiate upgrade BOD-A (next) OK Cancel 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 will be cleared after the BOD cluster is completely upgraded. Upgrade is complete on the first server in the cluster when the 'Completed Successfully…' message shows in the Upgrade Operation column and up to date flag has "Y" value. The server will go back to Standby state when the upgrade completes.

Step	Procedure	Result

BOD (2 Servers)						
BOD-B	Minor	N	Active	TPD 6.7.0.0.1_84.17.0	11.5.0.0.0_39.1.0	n/a
BOD-A	Minor	Y	Standby	11.5.0.0.0_39.1.0	12.2.0.0.0_32.1.0	Initiate upgrade Completed Successfully at Nov 9, 2016 19:22:09

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

The following minor alarms may be present:

Expected Critical Alarms

31283 HA Server Offline

Jan 10, 2017 09:26 AM EST	Critical	31283	High availability server is offline	10.240.155.13	BOD-B 10.240.155.12	

Expected Major Alarms

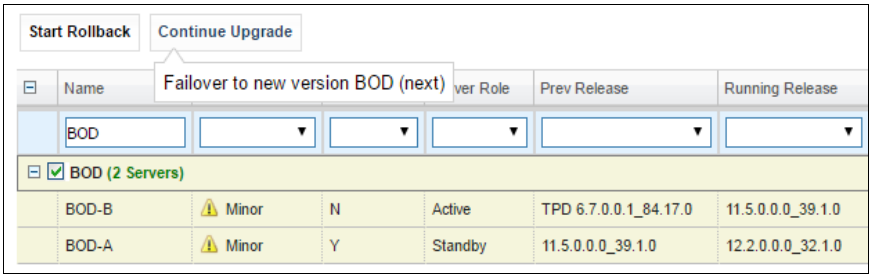
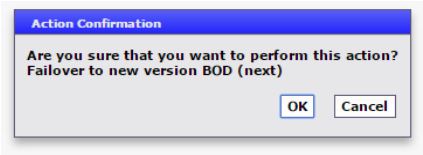
70004 QP Processes has been down for maintenance

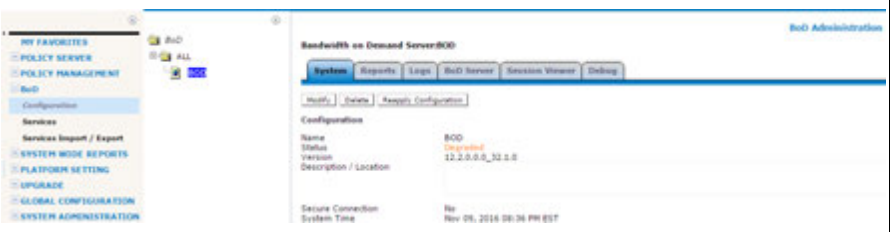
Jan 10, 2017 09:26 AM EST	Major	70004	The QP processes have been brought down for maintenance.	10.240.155.13	BOD-A 10.240.155.11	

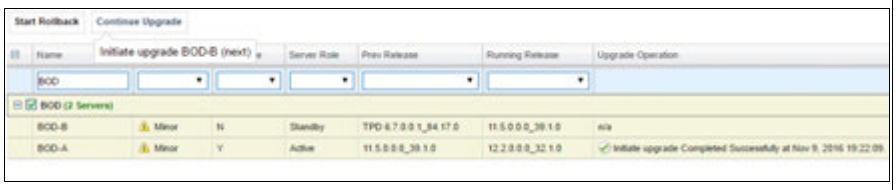
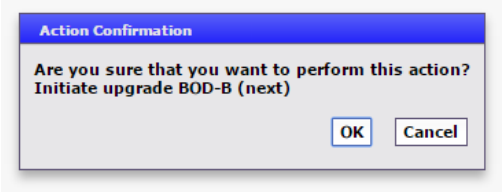
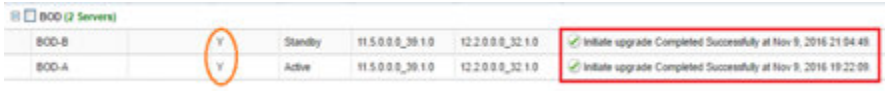
Expected Minor Alarms

70503 The server is in forced standby
70507 An upgrade/back out action on a server is in progress
70501 The Cluster is running different versions of software
31114 DB Replication of configuration data via SOAP has failed
31107 DB merging from a child Source Node has failed
31102 Database replication from master failure
31101 DB replication to a slave DB has failed

Occurrence	Severity	Alarm ID	Text	OAM VIP	Server
Jan 10, 2017 09:26 AM EST	Minor	31114	DB Replication of configuration data via SOAP has failed	10.240.155.2	CMP-A 10.240.155.4
Jan 10, 2017 09:26 AM EST	Minor	31114	DB Replication of configuration data via SOAP has failed	10.240.155.13	BOD-B 10.240.155.12
Jan 10, 2017 09:26 AM EST	Minor	31101	DB replication to a slave DB has failed	10.240.155.13	BOD-B 10.240.155.12
Jan 10, 2017 09:26 AM EST	Minor	31107	DB merging from a child Source Node has failed	10.240.155.2	CMP-A 10.240.155.4
Jan 10, 2017 09:26 AM EST	Minor	31101	DB replication to a slave DB has failed	10.240.155.2	CMP-A 10.240.155.4
Jan 10, 2017 09:26 AM EST	Minor	31107	DB merging from a child Source Node has failed	10.240.155.2	CMP-B 10.240.155.3
Jan 10, 2017 09:26 AM EST	Minor	31102	DB replication from a master DB has failed	10.240.155.13	BOD-A 10.240.155.11
Jan 10, 2017 09:25 AM EST	Minor	70501	The Cluster is running different versions of software	10.240.155.2	CMP-A 10.240.155.4
Jan 10, 2017 09:25 AM EST	Minor	70507	An upgrade/backout action on a server is in progress	10.240.155.2	CMP-A 10.240.155.4
Jan 10, 2017 09:25 AM EST	Minor	70503	The server is in forced standby	10.240.155.2	CMP-A 10.240.155.4

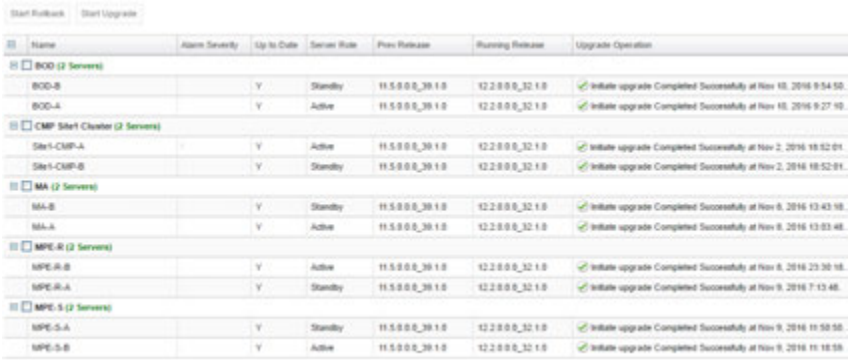
Step	Procedure	Result
4. ☐	**CMP GUI:** Failover to upgraded server **NOTE:** 4 clusters can be running the upgrade process at one time.	Fail over **ONE** cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster. **Upgrade → Upgrade Manager** Select the checkbox for the BOD cluster (one cluster at a time) a. Click **Continue Upgrade**. When hovering over the button, it will say 'Failover to new version…'  b. Click **OK** to confirm and continue with the operation. It will begin to failover the cluster:  Wait until failover completes before failing over the next cluster. And verify the 12.2 upgraded BOD server is now active.

Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on the upgraded BOD cluster	**BOD→Configuration→<*Upgraded* BOD cluster>→System** Push **Reapply Configuration**.  **Note:** ▪ Cluster is in degraded state, this is expected due to different versions of software between the servers in the BOD cluster ▪ Notice the version should be successfully changed to the release 12.2 ▪ After successful reapplying the configuration , the config mismatch message clears out : **Bandwidth on Demand Server:BOD** System | Reports | Logs | BoD Server | Session Viewer | Debug Modify | Delete | Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: BOD Status: Degraded Version: 12.2.0.0.0_32.1.0 Description / Location: Secure Connection: No System Time: Nov 09, 2016 08:38 PM EST
6. ☐	**CMP GUI:** Upgrade the spare BOD server	**Upgrade → Upgrade Manager** Click **Continue Upgrade**. When hovering over the button, it will say 'Initiate upgrade' for the spare BOD server. Click OK to confirm and follow the upgrade operation column value till it completes successfully and running release shows 12.2

Step	Procedure	Result
7. ☐	**CMP GUI:** Upgrade the other BOD server	**Upgrade → Upgrade Manager** a. Click **Continue Upgrade**. When hovering over the button, it will say 'Initiate upgrade' for the other BOD server  b. Click OK to confirm and continue with the operation. It will begin to failover the cluster:  Wait until upgrade operation of the BOD server indicates successfully completion, up to date flag indicates "Y" and running release has the 12.2 release 
8. ☐	**CMP GUI**: Current alarms	At this point the whole system would be upgraded to 12.2 and no active alarms should be present in the system. If there are still active alarms, please contact Oracle Customer Support.
9. ☐	**CMP GUI:** Roll back BOD cluster upgrade	If traffic is not active and issues or non-expected alarms observed, then rollback to 11.5.X is decided, skip to the section describing backing out.
10. ☐	Repeat steps 1–8 for the next BOD cluster(s) if deployed	Proceed with next cluster(s): BOD Cluster _____ BOD Cluster _____ BOD Cluster _____

10. POST UPGRADE HEALTH CHECK FOR BOTH CABLE AND WIRELESS SYSTEMS

NOTE: This section is used when the entire topology is running release 12.2

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

Step	Procedure	Result
4. ☐	**CMP GUI:** Replication stats	Navigate to **System Wide Reports→Others→MPE/MRA Rep Stats** (for a wireless system) Navigate to **System Wide Reports→Others→MPE/BOD Rep Stats** (for a cable system) Verify all clusters and servers are in OK state. Wireless: **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 Cable:
THIS PROCEDURE HAS BEEN COMPLETED		

11. BACKOUT (ROLLBACK) 11.5.X/12.1.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 will be backed out to the previous release.

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

11.1 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.

11.2 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.

11.3 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 will be on a pre-12.2 release with Active, Standby, or Spare status.

Expected pre-conditions:

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

11.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, MPE, MA, or BoD) will be 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.

11.3.1.1 Overview on Backout/Rollback MRA/MPE cluster

The following sequence will preserve 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

11.3.1.2 Backout Secondary CMP (if applicable)

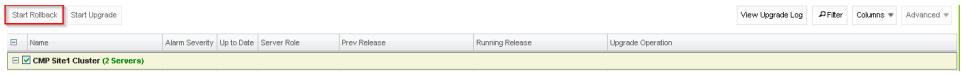
NOTE: At this time, all MPEs and MRAs must already be backed out to the previous release.

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

11.3.1.3 Backout Primary CMP (11.5.x)

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

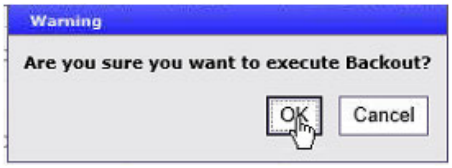
1. Use the CMP GUI (Upgrade Manager) to backout the Primary standby CMP cluster
2. Select the CMP cluster and click on the 'Rollback' button on the top left , would initiate backout on Standby CMP



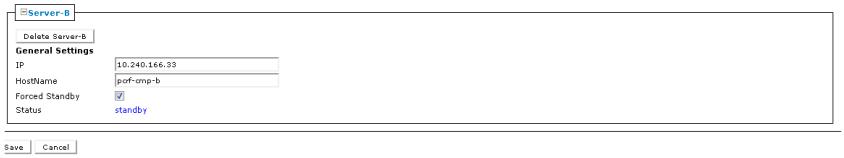
3. Continue Rollback, which would failover to older version CMP cluster.

4. Log back in to the Primary CMP VIP
5. Use the 11.5.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 > click on 'Reapply Configuration'

11.3.1.4 Backout Primary CMP (12.1.x)

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

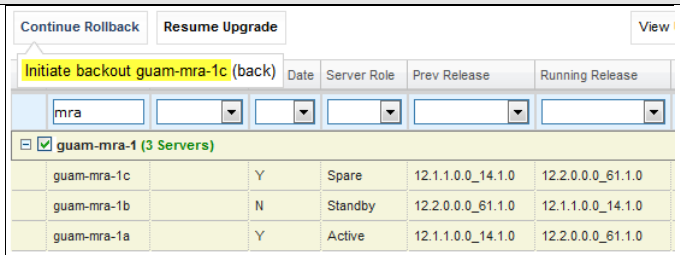
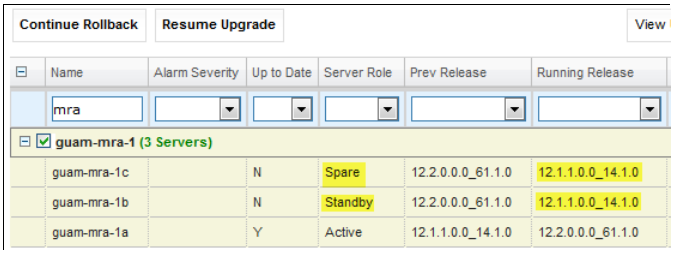
11.3.2 Backout of a Partially Upgraded Cluster

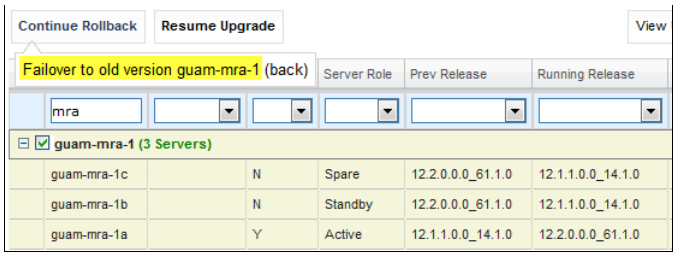
A partially upgraded cluster occurs when the version is not correct or the success message does not appear. If this happens, contact Oracle Support and report a partially upgraded cluster.

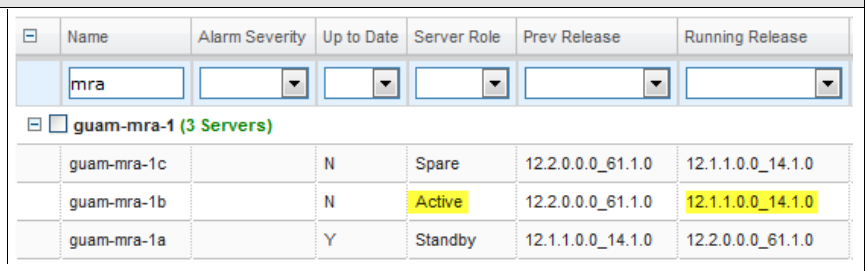
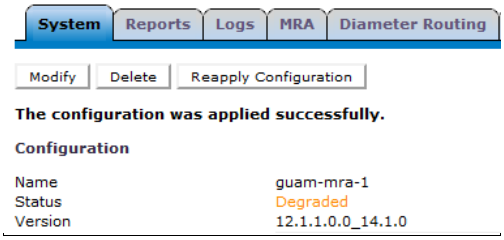
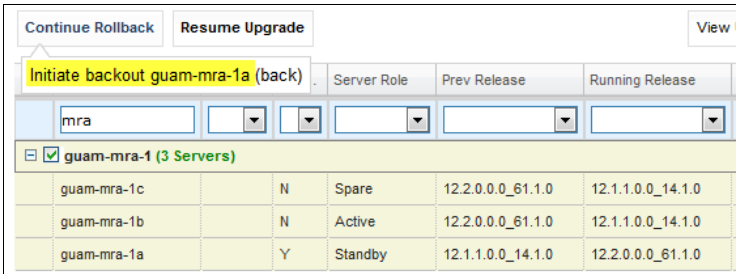
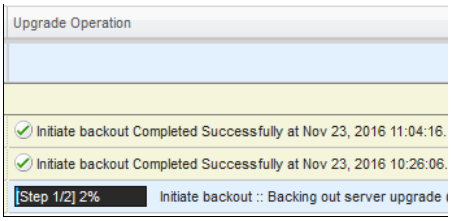
11.3.3 Backout Fully Upgraded MPE/MRA Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	**Upgrade → Upgrade Manager** Confirm status of the cluster to be backed out: • Primary CMP is on release 12.2 • MPE/MRA is on release 12.2 • Up to Date column shows Y for all servers **EXAMPLE** ☐ 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
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 out at the same time, selecting one at a time.	**Upgrade → Upgrade Manager** • Select the checkbox for the cluster. - Select one cluster at a time. - It can be an MRA or MPE cluster. • Click **Start Rollback**. When hovering over the button, it will inform you of the server to backout, in this case it will be the current standby server. Start Rollback / Start Upgrade / View Initiate backout guam-mra-1b (back) / Date / Server Role / Prev Release / Running Release mra ☑ **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 • Click **OK** to confirm and continue with the operation. It will begin the backout process. Follow the progress in the Upgrade Operation column. Upgrade Operation [Step 2/3] 0% — Initiate upgrade :: Upgrading server (Elapsed Time: 0:0... Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:18.

Step	Procedure	Result
		The server backing out will go into the OOS state and the spare server will now take 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 will be 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 message 'Initiate backout completed successfully at…' appears in the Upgrade Operation column. The server will be running a pre-12.2 release and return to standby with an N in the Up to Date column. Start Rollback Start Upgrade View Name Alarm Severity Up to Date Server Role Prev Release Running Release mra 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 N Standby 12.2.0.0.0_61.1.0 12.1.1.0.0_14.1.0 guam-mra-1a Y Active 12.1.1.0.0_14.1.0 12.2.0.0.0_61.1.0
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	Select the partially backed out cluster. **Upgrade → Upgrade Manager** • Click **Continue Rollback**. When hovering over the button, it will inform you it will initiate backout on the spare server.

Step	Procedure	Result
	one at a time.	 • Click **OK** to confirm and continue with the operation. Follow the progress in the Server Role column. The Server will show 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 will be 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 **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 will go back to running a pre-12.2 release. 

Step	Procedure	Result
4. ☐	**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.	• 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 12.2 **Upgrade → Upgrade Manager** • Click **Continue Rollback**. When hovering over the button, it will inform you that a failover to the old version will occur  • Click **OK** to confirm and continue with the operation. It will begin to fail over. Wait until the server fails over before selecting the next cluster. This will take a minute or two. **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 State of the cluster will look like the following when the failover completes. The active server is now running the previous release:

Step	Procedure	Result
		
5. ☐	**CMP GUI:** Reapply the configuration to the MPE/MRA cluster that completed the failover successfully.	For MPE: **Policy Server → Configuration →** <*MPE_cluster*> **→ System** For MRA: **MRA→Configuration→**<*MRA_cluster*>**→System** The selected cluster will have the status shown as Degraded running release 12.2 • Click **Reapply Configuration**. - The MPE opens a popup box showing the progress of the reapply process. - The MRA will not show anything. • Note the version is successfully changed to the previous release:  **NOTE:** The status still showing Degraded is a normal reporting event because the servers currently have different releases.
6. ☐	**CMP GUI**: Complete backout of cluster(s) **NOTE:** The backout of a single server takes approximately 30 minutes to complete. **NOTE:** Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.	**Upgrade → Upgrade Manager** • Select the partially upgraded cluster to backout. • Click **Continue Rollback**. When hovering over the button, it will inform you of the current standby server to be backed out:  • Click **OK** to confirm and continue with the operation. It will begin the backout process. Follow the progress in the Upgrade Operation column. 

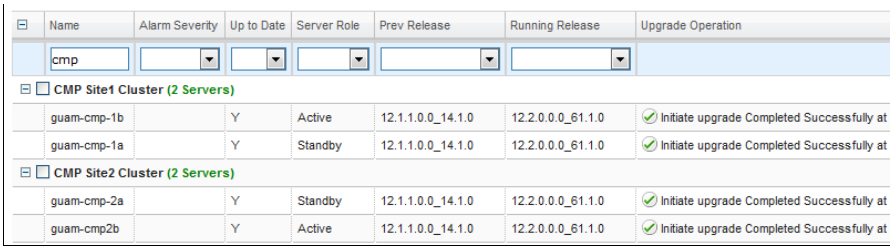
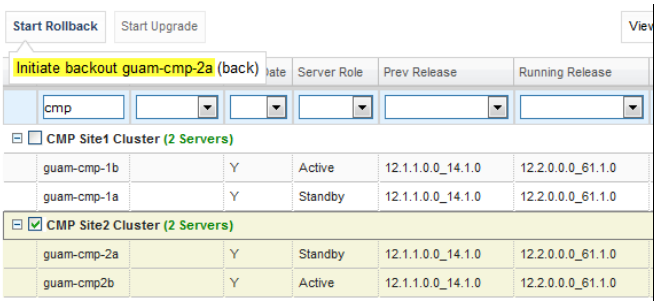
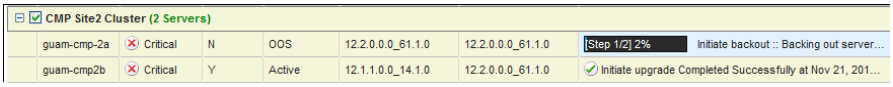
Step	Procedure	Result
		During the backout activities, the following alarms may be generated and considered normal reporting events—these will be cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **31227** HA 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 shows in the Upgrade Operation column. All of the servers will be on the pre-12.2 release and show active/standby/spare Name | Alarm Severity | Up to Date | Server Role | Prev Release | Running Release | Upgrade Operation mra guam-mra-1 (3 Servers) guam-mra-1c | N | Spare | 12.2.0.0.0_61.1.0 | 12.1.1.0.0_14.1.0 | Initiate backout Completed Successfully at guam-mra-1b | N | Active | 12.2.0.0.0_61.1.0 | 12.1.1.0.0_14.1.0 | Initiate backout Completed Successfully at guam-mra-1a | N | Standby | 12.2.0.0.0_61.1.0 | 12.1.1.0.0_14.1.0 | Initiate backout Completed Successfully at
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.
THIS PROCEDURE HAS BEEN COMPLETED		

11.3.4 Backout Fully Upgraded Secondary CMP Cluster

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

Step	Procedure	Result

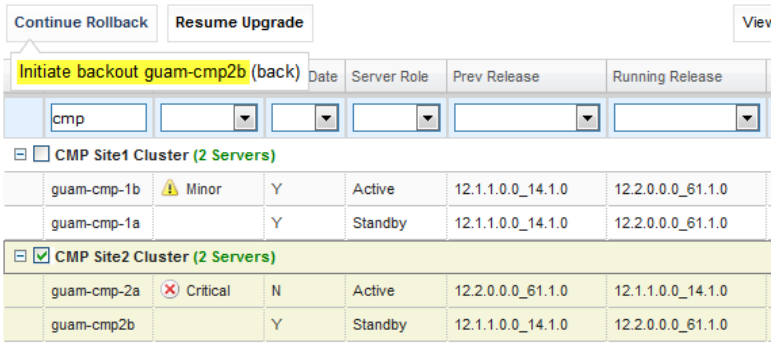
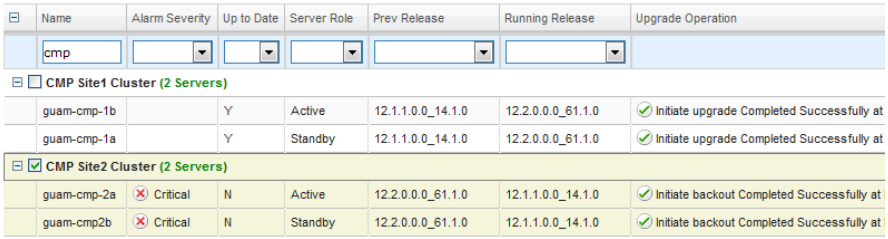
NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site1 cluster.

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP clusters	**Upgrade → System Maintenance** Confirm status of the cluster to be backed out • Primary CMP is on release 12.2 • All other non-CMP clusters are on pre-12.2 • Up to Date column shows Y for all servers **NOTE:** The **Filter** button can be used to show only the CMP servers. Enter CMP in the Name field. 
2. ☐	**CMP GUI:** backout secondary CMP cluster **NOTE:** The backout of a single server takes approximately 40 minutes to complete.	**Upgrade → Upgrade Manager** • Select the checkbox for the secondary CMP cluster • Click **Start Rollback**. When hovering over the button, it will inform you that the standby server will be backed out.  • Click **OK** to confirm and continue with the operation. It will begin to backout. The server will go 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 will be 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 **70025** The MySQL slave has a different schema version than the master. **<u>Expected Major Alarm</u>**

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

Step	Procedure	Result
		70004 QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **<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 Backout of the server is complete when the "Initiate backout completed successfully at…" message shows in the Upgrade Operation column. The server will go back to standby state and show the previous release. Name | Alarm Severity | Up to Date | Server Role | Prev Release | Running Release cmp CMP Site1 Cluster (2 Servers) guam-cmp-1b | Minor | Y | Active | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0 guam-cmp-1a | Y | Standby | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0 CMP Site2 Cluster (2 Servers) guam-cmp-2a | Critical | N | Standby | 12.2.0.0.0_61.1.0 | 12.1.1.0.0_14.1.0 guam-cmp2b | Y | Active | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0
3. ☐	**CMP GUI:** Continue the backout. Next operation is failover	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Click **Continue Rollback**. When hovering over the button, it will inform you it will fail over to the previous version. Continue Rollback | Resume Upgrade | View Failover to old version CMP Site2 Cluster (back) Role | Prev Release | Running Release cmp CMP Site1 Cluster (2 Servers) guam-cmp-1b | Minor | Y | Active | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0 guam-cmp-1a | Y | Standby | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0 CMP Site2 Cluster (2 Servers) guam-cmp-2a | Critical | N | Standby | 12.2.0.0.0_61.1.0 | 12.1.1.0.0_14.1.0 guam-cmp2b | Y | Active | 12.1.1.0.0_14.1.0 | 12.2.0.0.0_61.1.0 • Click **OK** to confirm and continue with the operation. It will begin the failover process. Wait until the previous release becomes active before continuing

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

Step	Procedure	Result
		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
4. ☐	**CMP GUI**: Continue the backout. Next operation is initiate backout	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Click **Continue Rollback**. When hovering over the button, it will inform you it will back out the new standby server.  • Click **OK** to confirm and continue with the operation. It will begin the failover process. 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. 
THIS PROCEDURE HAS BEEN COMPLETED		

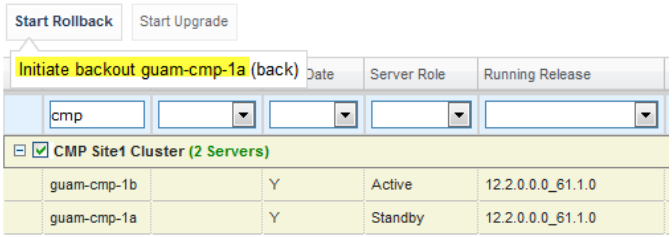
11.3.5 Backout Fully Upgraded Primary CMP Cluster

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 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP clusters	**Upgrade Manager → System Maintenance** Confirm status of the cluster to be backed out: • Primary Active CMP is on release 12.2 • Secondary CMP cluster is on pre-12.2 release • Up to Date column shows Y for all servers in the primary CMP cluster

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

Step	Procedure	Result
2. ☐	**CMP GUI**: backout standby Primary CMP cluster **NOTE:** backout of one server will take approximately 40 minutes to complete.	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP cluster (you can use the Filter button to show the CMP clusters only) • Click **Start Rollback**. When hovering over the button, it will inform you of the server to get backed out.



• Click **OK** to confirm and continue with the operation. It will begin to backout. The server will go 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 will be 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
31236 HA Link Down

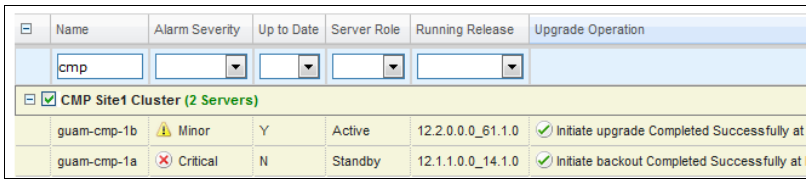
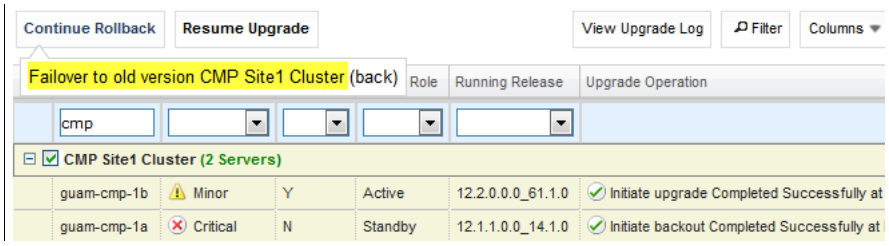
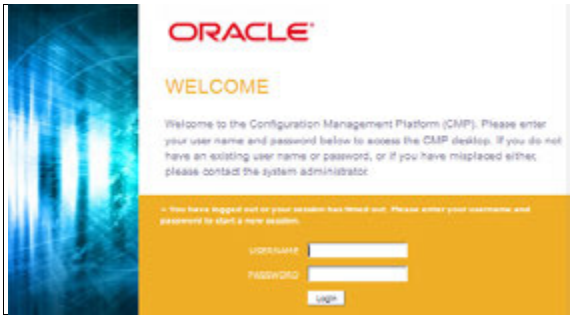
Expected Major Alarm

70004 QP Processes down for maintenance
31233 HA Path Down

Expected Minor Alarms

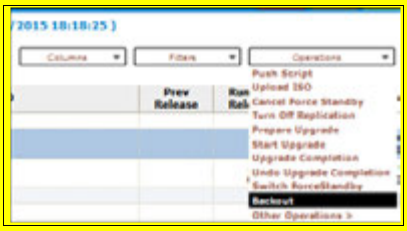
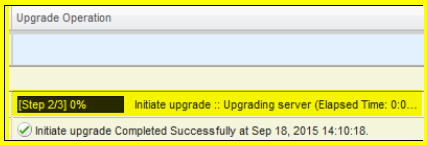
31114 DB replication over SOAP has failed

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 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.

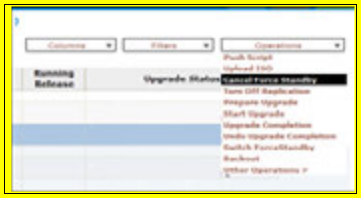
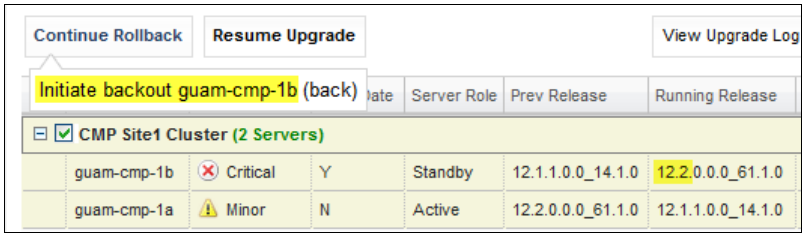
Step	Procedure	Result
		31106 Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31102** Database replication from master failure **31113** DB replication manually disabled **70503** Server Forced Standby **70507** Upgrade In 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 will go back to standby state and show the previous release. 
3. ☐	**CMP GUI:** Continue the backout. Next operation is failover	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP cluster • Click **Continue Rollback**. When hovering over the button, it will inform you it will fail over.  • Click **OK** to confirm and continue with the operation. It will begin the failover process. Failover takes a couple minutes.
4. ☐	**CMP GUI**: Log back in to the Primary CMP VIP	After failover, you will be required to log back in to the CMP GUI using the Primary CMP VIP. 

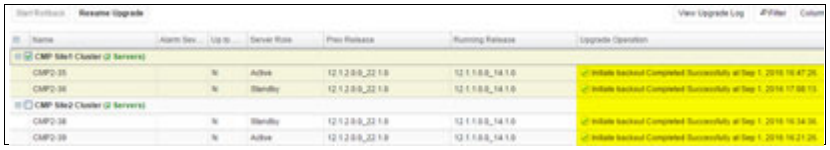
NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site1 cluster. For rollback to 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.		
Step	**Procedure**	**Result**
5. ☐	**CMP GUI:** Verify release	Navigate to **Help→About**. Verify the release number is not 12.2 anymore. • If the rollback is for release 11.5.x, continue with step 6. • If the rollback is for release 12.1.x, continue with step 8

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 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.

Step	Procedure	Result
6. ☐	**CMP GUI (release 11.5.x):** Continue the backout of the Primary CMP cluster **NOTE**: backout of one server will take approximately 30 minutes to complete.	**Upgrade → System Maintenance** • Select the checkbox for the remaining server in the Primary CMP cluster. The server will be on 12.2 and show Forced Standby in the Server State column. • Select **Operations→Backout**  • 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 will be 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 **<u>Expected Major Alarm</u>** **70004** QP Processes down for maintenance **<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

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 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.

Step	Procedure	Result
7. ☐	**CMP GUI**: Remove Forced Standby	**Upgrade → System Maintenance** Select the checkbox for the remaining server in the Primary CMP cluster. The server will be on 11.5.x and show Forced Standby in the Server State column. **NOTE:** A refresh of the current screen may be necessary at the 40 minute mark. Select **Operations→Cancel Forced Standby** 
		The backout procedure is now completed for release 11.5.x.
8. ☐	**CMP GUI (release 12.1.x)**: Continue the backout of the Primary CMP cluster **NOTE:** The backout of one server takes approximately 40 minutes to complete.	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP cluster • Click **Continue Rollback**. When hovering over the button, it will inform you of the server to back out. In this case, it will be the current standby server still running 12.2.  • Click **OK** to confirm and continue with the operation. It will begin to backout. Server will go in 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 will be 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

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 11.5.x, use both the Upgrade Manager and System Maintenance. For rollback to release 12.1.x, only use the Upgrade Manager.		
Step	**Procedure**	**Result**
		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 will go back to standby state and show 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.
THIS PROCEDURE HAS BEEN COMPLETED		

12. BACKOUT (ROLLBACK) CABLE 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 will be backed out to the previous release.

Oracle strongly recommends consulting Technical Services and Escalation team before initiating the backout procedure. They will determine the appropriate course of recovery options if any.

12.1 Backout Sequence

The backout sequence order is the reverse of the upgrade order as in the following sequence:

1. Backout BOD cluster(s)
2. Backout MPE-S cluster(s)
3. Backout MPE-R cluster(s)
4. Backout MA cluster(s)
5. Backout Secondary CMP cluster (if applicable)
6. Backout Primary CMP cluster:

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

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

12.2 Pre-requisites

1. No new policies or features have been configured or executed on the upgraded release.
2. The CMP cluster cannot be backed out if other Policy components (MPEs, MAs and BODs) are still on the upgraded release.

12.3 Backout of Fully Upgraded Cluster

Prior to executing this procedure, Oracle recommends first consulting the Technical Services team, 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 will be on release 11.5.X (MA, MPE, BOD, CMP) with Active, Standby status.

Expected pre-conditions:

1. Primary Active CMP is on release 12.2
2. Cluster is of MPE, MA, BOD or CMP
3. One server of target cluster is on release 12.2 in Active role
4. One server of target cluster is on release 12.2 in either Standby or Force Standby

12.3.1 Backout Sequence

This procedure applies to an Active/Standby group of servers. This group of servers will be referred to as a cluster or HA cluster. The cluster types are CMP, MA, BOD or MPE. For CMP cluster, the cluster status may also be Site-1 and/or Site-2.

12.3.1.1 Overview on Backout/Rollback BOD cluster

NOTE: The following procedure should be used to backout a 12.2 cluster to Policy 11.5.X.

1. Use the CMP GUI to begin the backout of the BOD cluster
2. Wait until successfully complete
3. Failover
4. Reapply the configuration
5. Use the CMP GUI (Upgrade Manager) to continue the backout of the BOD cluster

12.3.1.2 Overview on Backout/Rollback MPE-S/R cluster

NOTE: The following procedure should be used to backout a 12.2 cluster to Policy 11.5.X.

1. Use the CMP GUI to begin the backout of the MPE-S cluster
2. Wait until successfully complete
3. Failover
4. Reapply the configuration
5. Use the CMP GUI (Upgrade Manager) to continue the backout of the MPE-R cluster
6. Use the CMP GUI to begin the backout of the MPE-R cluster
7. Wait until successfully complete
8. Failover
9. Reapply the configuration
10. Use the CMP GUI (Upgrade Manager) to continue the backout of the MPE-R cluster

12.3.1.3 Overview on Backout/Rollback MA cluster

NOTE: The following procedure should be used to backout a 12.2 cluster to Policy 11.5.X.

1. Use the CMP GUI to begin the backout of the MA cluster
2. Wait until successfully complete
3. Failover
4. Reapply the configuration
5. Use the CMP GUI (Upgrade Manager) to continue the backout of the MA cluster

12.3.1.4 Backout Secondary CMP (If Applicable)

At this time, all MPEs, BOD and MAs must already be backed out.

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

12.3.1.5 Backout Primary CMP (11.5.X)

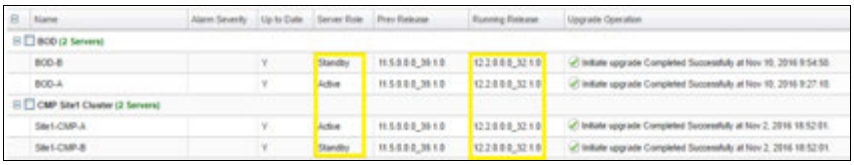
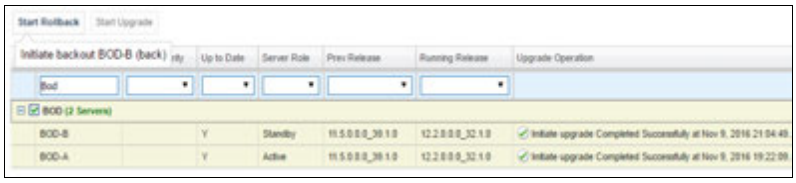
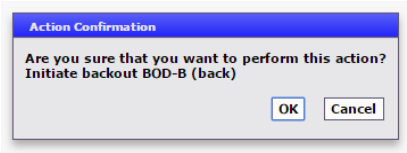
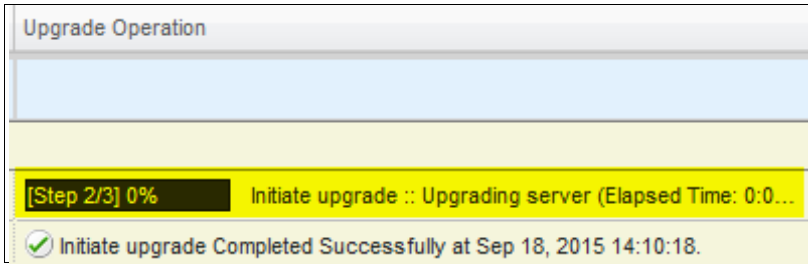
NOTE: Secondary CMP must already be backed out and all of the MPE/MRA clusters

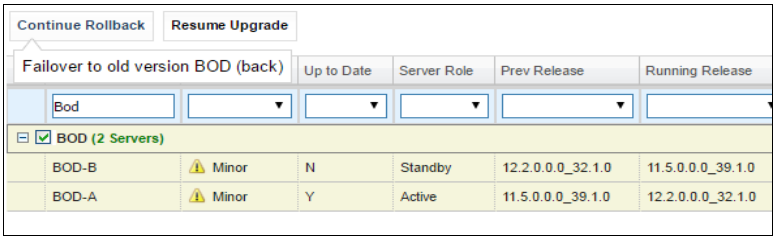
1. Use the CMP GUI (Upgrade Manager) to backout the Primary standby CMP cluster
2. Log back in to the Primary CMP VIP
3. Use the 11.5.X System Maintenance to complete backout of the Primary CMP cluster

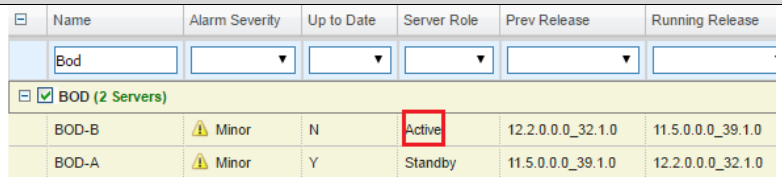
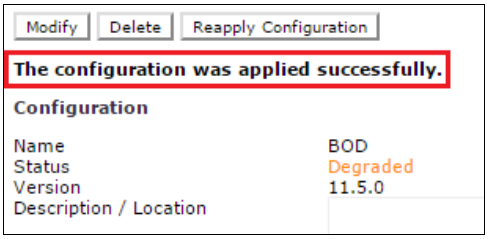
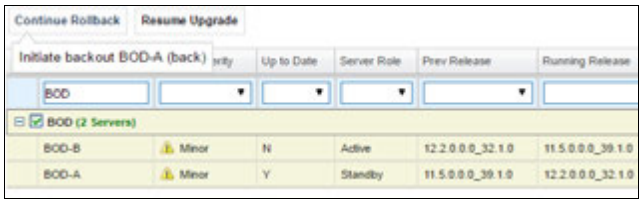
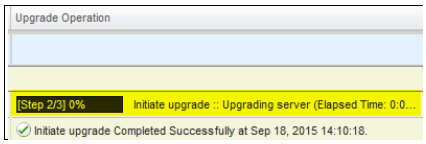
12.3.2 Backout of a Partially Upgraded Cluster

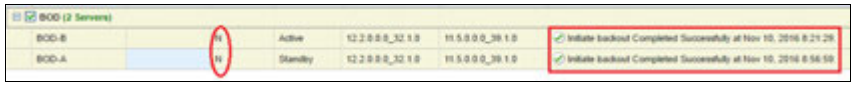
A partially upgraded cluster occurs when the version is not correct or the success message does not appear. If this happens, contact Oracle Support and report a partially upgraded cluster.

12.3.3 Backout Fully Upgraded BOD Cluster(s)

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	**Upgrade Manager → Upgrade Manager** Confirm status of the cluster to be backed out: • Primary Active CMP is on release 12.2 • All Standby servers are on release 12.2 • Up to Date column shows Y for all servers **EXAMPLE** 
2. ☐	**CMP GUI:** Rollback standby BOD server **NOTE:** The backout of a single server takes approximately 40 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the upgraded clusters to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Start Rollback**. When hovering over the button, it will inform you of the server to backout, in this case it will be the current standby server.  ○ Click **OK** to confirm and continue with the operation. It will begin to backout.  Follow the progress status in the Upgrade Operation column.  The server backing out will go into OOS state. 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. These will be cleared after the cluster is completely backed out.

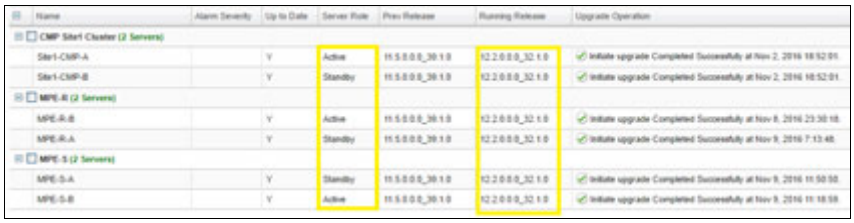
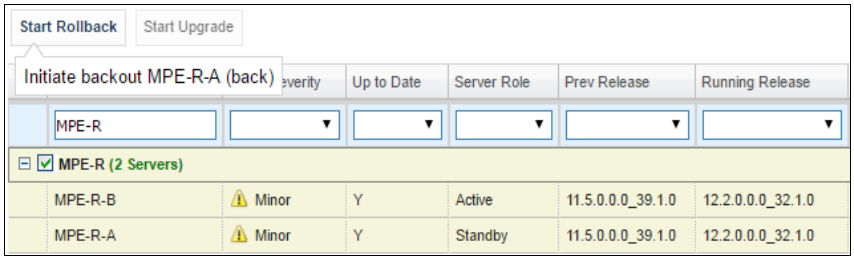
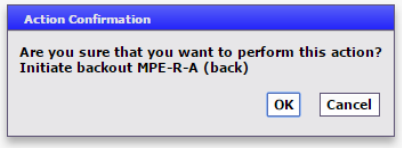
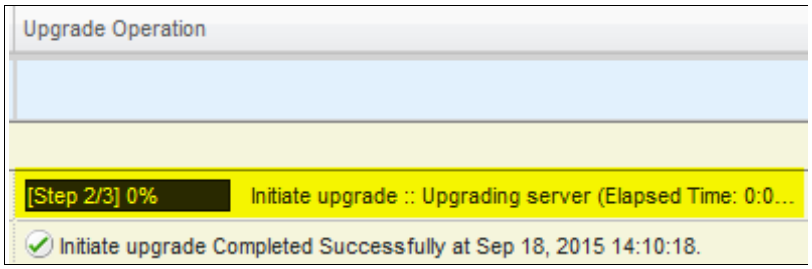
Step	Procedure	Result
		Expected Critical Alarms **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** 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 'Initial backout Completed Successfully…' shows in the Upgrade Operation column. The server will show running release of 11.5.X , role is back to standby role and up to date value is set to "N".
3. ☐	**CMP GUI:** Continue the backout of the BOD clusters. Next operation is failover to the 11.5.X server. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the partially backed out cluster to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you to failover to old version.  ○ Click **OK** to confirm and continue with the operation. It will begin to failover the cluster. Wait until the server fails over before selecting the next cluster. This will take a minute or two.

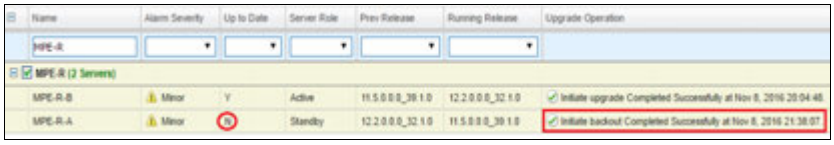
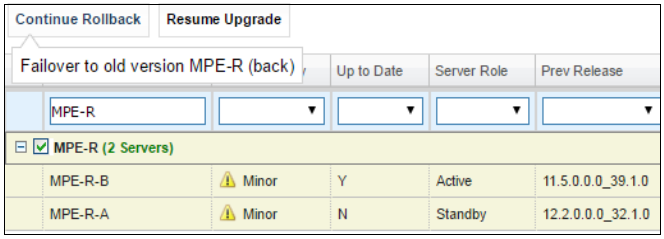
Step	Procedure	Result
		
4. ☐	**CMP GUI:** Reapply the configuration to the BOD cluster that completed the failover successfully.	Navigate to: **BOD → Configuration →** *<BOD cluster name>* **→ System** The selected cluster will have the status of Degraded. This is expected Click **Reapply Configuration**. The running version is successfully changed to the previous 11.5.X release  **NOTE:** The status still showing Degraded is a normal reporting event because the servers currently have different releases.
5. ☐	**CMP GUI:** Upgrade the spare BOD server	**Upgrade → Upgrade Manager** Click **Continue Rollback**. When hovering over the button, it will say 'Initiate backout' for the spare BOD server. Click OK to confirm and follow the upgrade operation column value till it completes successfully and running release shows 11.5.X.
6. ☐	**CMP GUI:** Complete backout of cluster(s) **NOTE:** The backout of a single server takes approximately 35 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the partially Backed out cluster **Upgrade → Upgrade Manager** Select the checkbox for the cluster (one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you of the server to get backed out.  ○ Click **OK** to confirm and continue with the operation. It will begin to backout. Follow the progress status in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events. These will be cleared after the cluster is completely backed out.

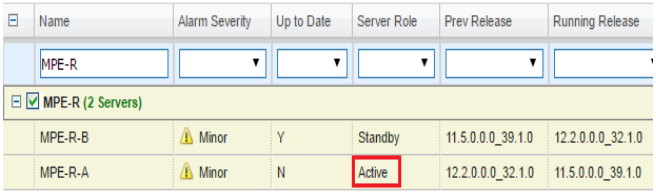
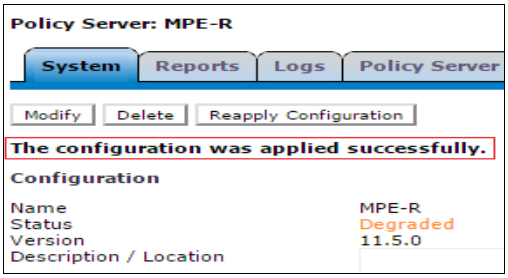
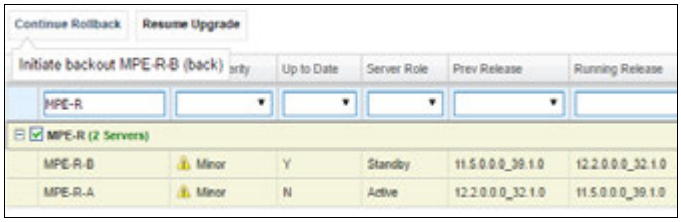
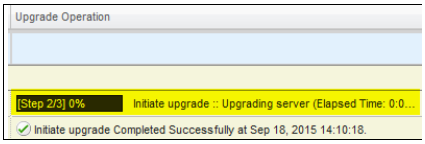
Step	Procedure	Result
		Expected Critical Alarms **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** 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 servers is complete when the message 'Initiate backout Completed Successfully…' shows in the Upgrade Operation column. All of the servers will be on the previous release, up to date value is set to "N" and show active/standby. 
THIS PROCEDURE HAS BEEN COMPLETED		

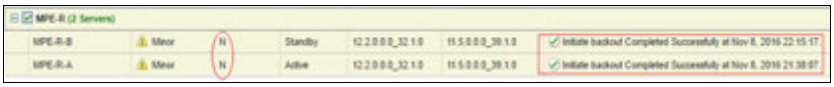
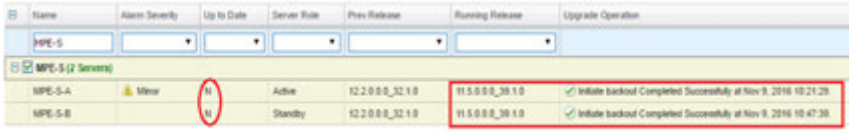
12.3.4 Backout Fully Upgraded MPE-S/R Cluster(s)

Step	Procedure	Result

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	**Upgrade Manager → Upgrade Manager** Confirm status of the cluster to be backed out: • Primary Active CMP is on release 12.2 • All Standby servers are on release 12.2 • Up to Date column shows Y for all servers **EXAMPLE** 
2. ☐	**CMP GUI:** Rollback standby MPE-R server **NOTE:** The backout of a single server takes approximately 40 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the upgraded clusters to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Start Rollback**. When hovering over the button, it will inform you of the server to backout, in this case it will be the current standby server.  ○ Click **OK** to confirm and continue with the operation. It will begin to backout.  Follow the progress status in the Upgrade Operation column.  The server backing out will go into OOS state. Wait until the server goes to an OOS state before selecting the next cluster to backout.

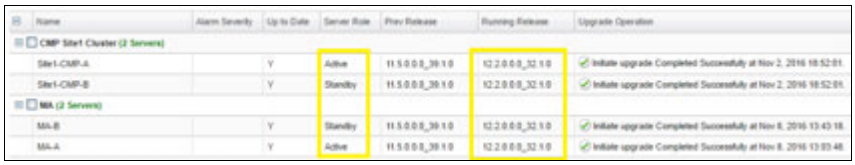
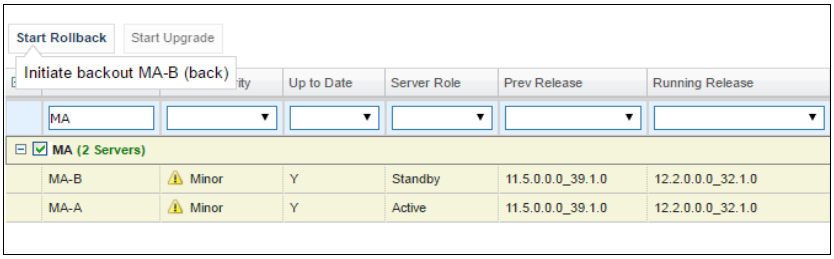
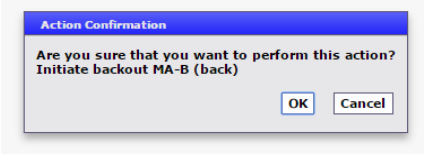
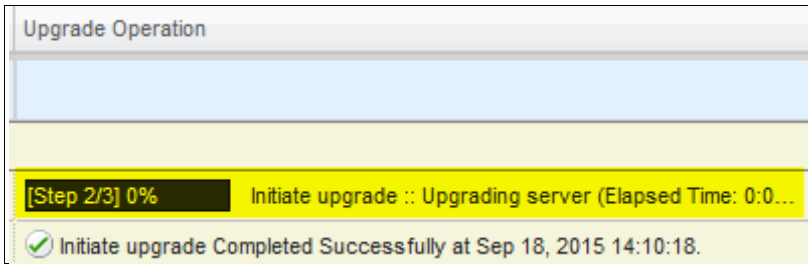
Step	Procedure	Result
		During the backout activities, the following alarms may be generated and considered normal reporting events. These will be cleared after the cluster is completely backed out. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **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 servers is complete when the 'Initial backout Completed Successfully…' shows in the Upgrade Operation column. The server will show running release of 11.5.X , role is back to standby role and up to date value is set to "N". 
3. ☐	**CMP GUI:** Continue the backout of the MPE-R clusters. Next operation is failover to the 11.5.X server. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the partially backed out cluster to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you to failover to old version.  ○ Click **OK** to confirm and continue with the operation. It will begin to failover the cluster. Wait until the server fails over before selecting the next cluster. This will take a

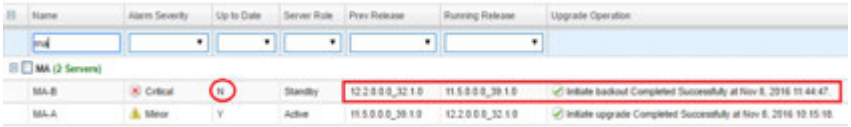
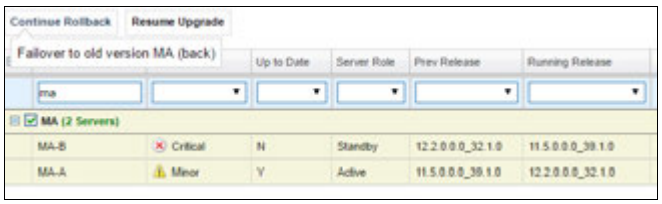
Step	Procedure	Result
		minute or two. 
4. ☐	**CMP GUI:** Reapply the configuration to the MPE-R cluster that completed the failover successfully.	Navigate to: **Policy Server → Configuration →** <*MPE-R cluster name*> **→ System** The selected cluster will have the status of Degraded. This is expected Click **Reapply Configuration**. The running version is successfully changed to the previous 11.5.X release  **NOTE:** The status still showing Degraded is a normal reporting event because the servers currently have different releases.
5. ☐	**CMP GUI:** Complete backout of cluster(s) **NOTE:** The backout of a single server takes approximately 35 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	• Select the partially Backed out cluster **Upgrade → Upgrade Manager** Select the checkbox for the cluster (one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you of the server to get backed out.  ○ Click **OK** to confirm and continue with the operation. It will begin to backout. Follow the progress status in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events. These will be cleared after the cluster is completely backed out. <u>**Expected Critical Alarms**</u>

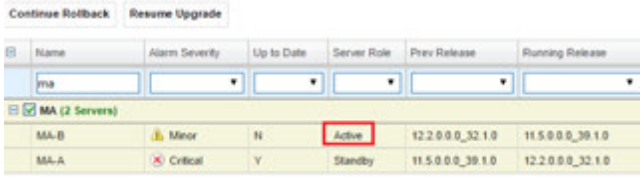
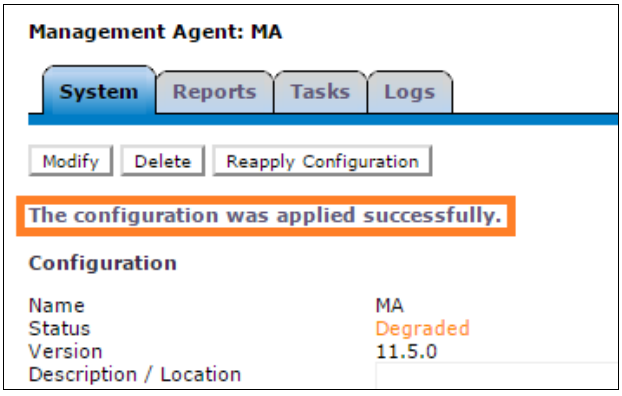
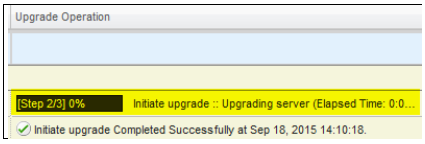
Step	Procedure	Result
		31283 HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** 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 message 'Initiate backout Completed Successfully…' shows in the Upgrade Operation column. All of the servers will be on the previous release, up to date value is set to "N" and show active/standby. 
6. ☐	**CMP GUI:** Rollback standby MPE-S cluster(s)	Follow same instructions above in this procedure to roll back upgraded MPE-S cluster(s) including spare servers configured in Site 2. Successful Roll back operation of the MPE-S servers indicates successfully completion, up to date flag indicates "N" and running release has the 11.5.X release for both MPE-S servers. 
THIS PROCEDURE HAS BEEN COMPLETED		

12.3.5 Backout Fully Upgraded MA Cluster(s)

Step	Procedure	Result

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected clusters	**Upgrade Manager → Upgrade Manager** Confirm status of the cluster to be backed out: • Primary Active CMP is on release 12.2 • All Standby servers are on release 12.2 • Up to Date column shows Y for all servers **EXAMPLE** 
2. ☐	**CMP GUI:** Rollback standby MA server **NOTE:** The backout of a single server takes approximately 40 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the upgraded clusters to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Start Rollback**. When hovering over the button, it will inform you of the server to backout, in this case it will be the current standby server.  ○ Click **OK** to confirm and continue with the operation. It will begin to backout.  Follow the progress status in the Upgrade Operation column.  The server backing out will go into OOS state. 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. These will be cleared after the cluster is completely backed out.

Step	Procedure	Result
		Expected Critical Alarms **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **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 servers is complete when the 'Initial backout Completed Successfully…' shows in the Upgrade Operation column. The server will show running release of 11.5.X , role is back to standby role and up to date value is set to "N". 
3. ☐	**CMP GUI:** Continue the backout of the MA clusters. Next operation is failover to the 11.5.X server. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	Select the partially backed out cluster to backout. **Upgrade → Upgrade Manager** Select the checkbox for the cluster (Select one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you to failover to old version.  ○ Click **OK** to confirm and continue with the operation. It will begin to failover the cluster. Wait until the server fails over before selecting the next cluster. This will take a minute or two.

Step	Procedure	Result
		
4. ☐	**CMP GUI:** Reapply the configuration to the MA cluster that completed the failover successfully.	Navigate to: **Policy Server → Management Agents →** *<MA cluster name>* **→ System** The selected cluster will have the status of Degraded. This is expected Click **Reapply Configuration**. The running version is successfully changed to the previous 11.5.X release  **NOTE:** The status still showing Degraded is a normal reporting event because the servers currently have different releases.
5. ☐	**CMP GUI:** Complete backout of MA cluster **NOTE:** The backout of a single server takes approximately 35 minutes to complete. **NOTE:** Up to 4 clusters can be backed out at the same time, selecting one at a time.	• Select the partially Backed out cluster **Upgrade → Upgrade Manager** Select the checkbox for the cluster (one cluster at a time) ○ Click **Continue Rollback**. When hovering over the button, it will inform you of the server to get backed out. ○ Click **OK** to confirm and continue with the operation. It will begin to backout. Follow the progress status in the Upgrade Operation column.  During the backout activities, the following alarms may be generated and considered normal reporting events. These will be cleared after the cluster is completely backed out.

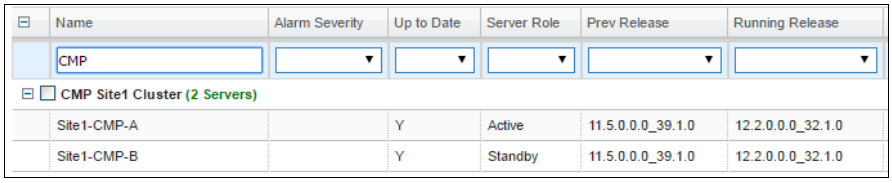
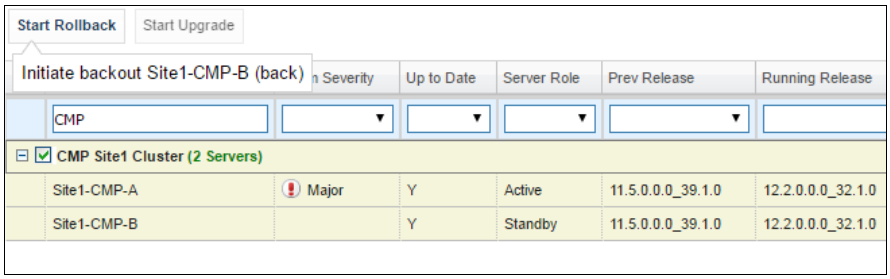
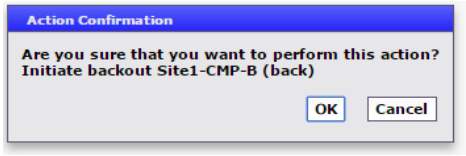
Step	Procedure	Result
		Expected Critical Alarms **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **Expected Major Alarms** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit blocked **Expected Minor Alarms** **70503** 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 message 'Initiate backout Completed Successfully…' shows in the Upgrade Operation column. All of the servers will be on the previous release, up to date value is set to "N" and show active/standby.
THIS PROCEDURE HAS BEEN COMPLETED		

12.3.6 Backout Fully Upgraded Secondary/Primary CMP Cluster

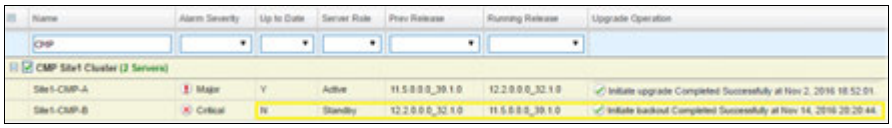
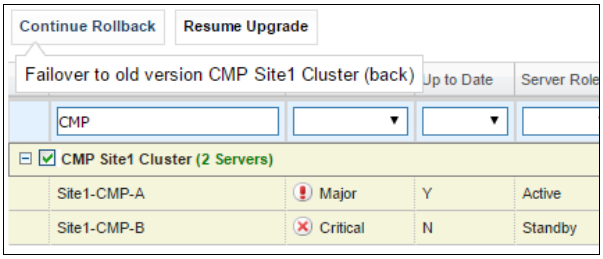
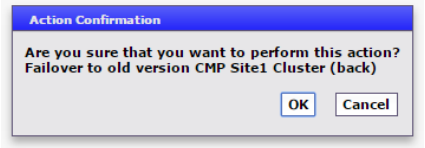
In case a Secondary CMP cluster is deployed, it needs to be backed out first. The following procedure applies to both Primary and Secondary CMP clusters.

NOTE: The Secondary CMP Site-2 cluster should be backed out first if deployed, then followed by the Primary CMP Site-1 cluster.		
Step	**Procedure**	**Result**

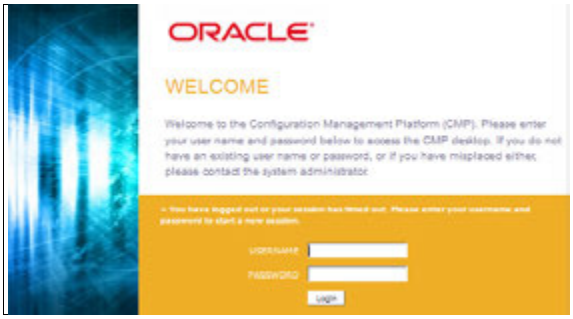
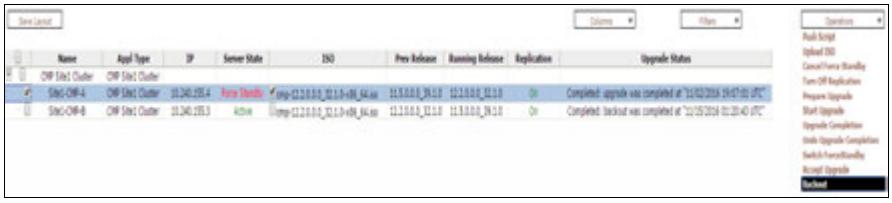
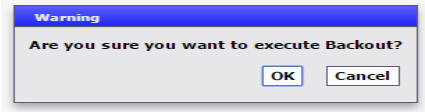
NOTE: The Secondary CMP Site-2 cluster should be backed out first if deployed, then followed by the Primary CMP Site-1 cluster.

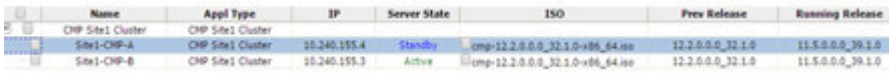
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP clusters	**Upgrade Manager → System Maintenance** Confirm status of the cluster to be backed out: • The CMP is on release 12.2 • The Up to Date column shows Y for all servers in the CMP cluster **NOTE:** The **Filter** button can be used to show only the CMP servers. Enter CMP in the Name field. 
2. ☐	**CMP GUI:** Backout standby CMP cluster **NOTE:** Backout of one server will take approximately 40 minutes to complete.	Select the CMP cluster to backout. **Upgrade → Upgrade Manager** • Select the checkbox for the CMP cluster ○ Click **Start Rollback**. When hovering over the button, it will inform you of the server to get backed out, in this case it will be the current standby server.  a. Click **OK** to confirm and continue with the operation. It will begin to backout. The server will go 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 will be 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

NOTE: The Secondary CMP Site-2 cluster should be backed out first if deployed, then followed by the Primary CMP Site-1 cluster.

Step	Procedure	Result
		31236 HA Link Down **<u>Expected Major Alarm</u>** **70004** QP Processes down for maintenance **31233** HA Path Down **<u>Expected Minor Alarms</u>** **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 message 'Initiate backout Completed Successfully…' shows in the Upgrade Operation column. The server will go back to standby state and show the previous release. 
3. ☐	**CMP GUI:** Continue the backout. Next operation is failover	• Select the CMP cluster. **Upgrade → Upgrade Manager** Select the checkbox for the CMP cluster ○ Click **Continue Rollback**. When hovering over the button, it will say 'Failover to old version…'  ○ Click **OK** to confirm and continue with the operation. It will begin to failover the cluster.  Failover takes a couple minutes.

NOTE: The Secondary CMP Site-2 cluster should be backed out first if deployed, then followed by the Primary CMP Site-1 cluster.

Step	Procedure	Result
4. ☐	**CMP GUI:** Log back in to the CMP VIP	After failover, you will be required to log back in to the CMP GUI using the CMP VIP. 
5. ☐	**CMP GUI:** Verify release	Navigate to **Help→About**. Verify the release number is now back to 11.5.X.
6. ☐	**CMP GUI (release 11.5.X):** Continue the backout of the CMP cluster **NOTE:** Backout of one server will take approximately 30 minutes to complete.	**Upgrade → System Maintenance** • Select the checkbox for the remaining server in the CMP cluster. The server will be on 12.2 and show Forced Standby ○ Select **Operations→Backout**  ○ Click **OK** to continue  Follow the progress in the Upgrade Status 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 will be cleared after the cluster is completely backed out.

NOTE: The Secondary CMP Site-2 cluster should be backed out first if deployed, then followed by the Primary CMP Site-1 cluster.		
Step	**Procedure**	**Result**
		<u>Expected Critical Alarms</u> **31283** HA Server Offline / Lost Communication with server **<u>Expected Major Alarm</u>** **31233** HA Path Down **31236** HA Link Down **70004** QP Processes down for maintenance **<u>Expected Minor Alarms</u>** **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 **31284** HA Remote Subscriber Heartbeat Warning
7. ☐	**CMP GUI:** Remove Forced standby	**Upgrade → System Maintenance** Select the checkbox for the remaining server in the CMP cluster. The server will be on 11.5.X and show Forced Standby **NOTE:** A refresh of the current screen may be necessary at the 40 minute mark. o Select **Operations→Cancel Forced Standby** **Note** that server state updates to "StandBy" : 
8. ☐	Final Syscheck	A Syscheck on all the backed out servers can be performed to ensure all modules are still operationally OK. If the CMP you just backed out of was the Secondary (Site2) CMP, repeat this procedure for the Primary (Site1) CMP before progressing to the next Procedure.
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX A. TVOE AND PM&C SERVER UPGRADE

Adding TVOE software image to TVOE host

STEP	Use this procedure to add the TVOE software image to the TVOE host. *Check off (√) each step as it is completed.* If this procedure fails, contact Oracle Support.	
	Task	**Description**

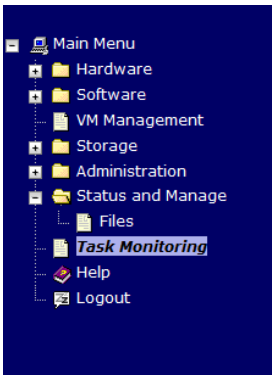
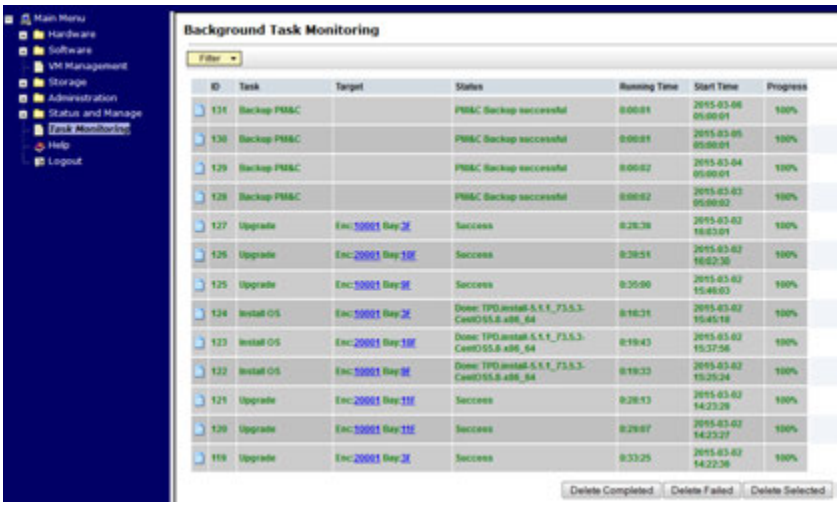
1 ☐	**TVOE Host:**
	Verify there is enough space on the server for TVOE software image
		Log in to the TVOE host and run the following to verify there is sufficient space:
		`$ df -h /var/TKLC/upgrade/`
		
		The system returns output similar to the following to indicate the disk usage of where the TVOE 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
		1. Attach the USB media to the TVOE host.
		1. 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`
		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/`
		2. Unmount the USB media:
		`$ sudo umount /media/usb`

---End of Procedure---		

A.1 TVOE Upgrade

STEP	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 will have to be rejected to allow PM&C 5.5 to be re-deployed.** • **A reject cannot be performed after an upgrade has been accepted.**		
1. ☐		**NOTE:** Upgrade of TVOE host will shut 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.

2. ☐	Check any in-progress task(s) on PM&C	On a supported web browser, log in to PM&C GUI as *pmacadmin* Navigate to PM&C GUI background tasks page: **Main Menu > Task Monitoring**  • 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. 

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

4. ☐	Verify PM&C guest is shut down	Logged on to TVOE host as *admusr*
		Verify that the PM&C is shut down with the following command:
		`[admusr@tvoe ~]# sudo virsh list --all`
		`[admusr@slak-tvoe ~]$ sudo virsh list --all`
		` Id Name State`
		`----------`
		` - pmac shut off`
		NOTE: This should show PM&C guest state as “shut off”

5.	Validate media	Logged on to the TVOE host as admusr
		• Run the platcfg utility
		`$ sudo su - platcfg`
		
		Navigate to **Maintenance → Upgrade → Validate Media**
		• Select the new TVOE ISO
		`lqqqqqqqqqqqqqqqqqqqu Choose Upgrade Media Menu tqqqqqqqqqqqqqqqqqqqqk`
		`x x`
		`x TVOE-3.0.3.0.0_86.46.0-x86_64.iso - 3.0.3.0.0_86.46.0 x`
		`x Exit x`
		`x x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`
		• Press [Enter] to validate the ISO file
		
		The TVOE ISO image will be 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 15 minutes
		Press [Enter] to return to platcfg and then press Exit to go back to the Upgrade menu. Do not quit platcfg.
		
		Select: **Maintenance → Upgrade → Initiate Upgrade**
		• Select the new TVOE ISO filename
		`lqqqqqqqqqqqqqqqqqqqu Choose Upgrade Media Menu tqqqqqqqqqqqqqqqqqqqqk`
		`x x`
		`x TVOE-3.0.3.0.0_86.46.0-x86_64.iso - 3.0.3.0.0_86.46.0 x`
		`x Exit x`
		`x x`
		`mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj`
		• Press [Enter] to initiate the upgrade
		
		NOTE: TVOE host will be rebooted at the end of the upgrade process (around 15 minutes) and will return to the login prompt. At this point the upgrade is complete.

7. ☐	Verify the Upgrade status	Log in to TVOE as *admusr*
		`login as: admusr`
		`admusr@100.64.31.173's password:`
		`Last login: Wed Dec  7 08:10:12 2016 from 10.75.12.57`
		`|==========|`
		`| This system has been upgraded but the upgrade has not yet |`
		`| been accepted or rejected.  Please accept or reject the |`
		`| upgrade soon. |`
		`|==========|`
		
		Verify the upgraded TVOE revision by executing the following command:
		`$appRev`
		You'll get an output similar to this:
		`[admusr@slak-tvoe ~]$ appRev`
		`Install Time: Wed Dec  7 09:44:48 2016`
		`Product Name: TVOE`
		`Product Release: 3.0.3.0.0_86.46.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.3.0.0_86.46.0`
		`Base Distro ISO: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso`
		`ISO name: TVOE-3.0.3.0.0_86.46.0-x86_64.iso`
		`OS: OracleLinux 6.7`
		
		Execute now:
		`$sudo verifyUpgrade`
		No output is expected from this command. Any output will display potential issues.
		
		And finally, a syscheck:
		`$sudo syscheck`
		`[admusr@slak-tvoe ~]$ sudo syscheck`
		`Running modules in class disk...`
		`OK`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class upgrade...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[admusr@slak-tvoe ~]$`

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 will have to be rejected to allow older PM&C to be re-deployed. • A reject cannot be performed once an upgrade has been accepted.

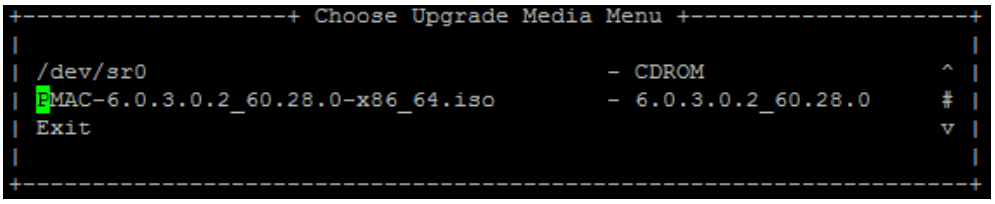
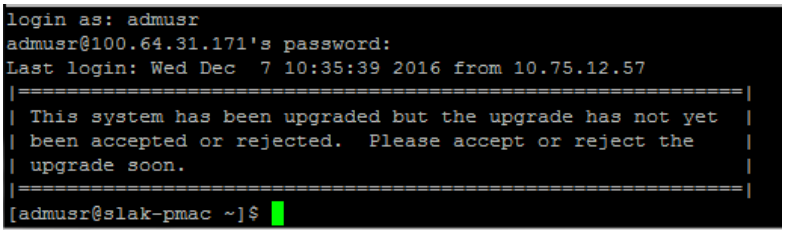
A.2 PM&C Upgrade

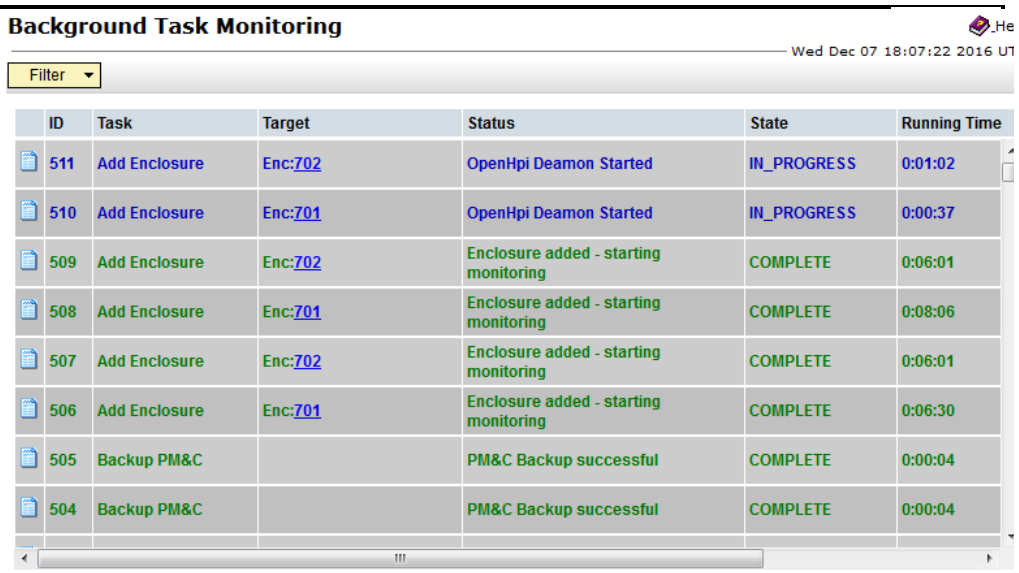
STEP	This procedure provides instructions to perform software upgrade of the PM&C. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	

1. ☐	Start the PM&C guest	If not already logged in to the TVOE host as *admusr*, do so.
		
		Start the PM&C guest if not already started:
		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's running, skip to the next step.
		If it's 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	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 hit <ENTER> twice
		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.
		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`
5. ☐	In "platcfg" utility select "Initiate Upgrade" to start the upgrade process	**platcfg: Maintenance→Upgrade→Initiate Upgrade** • Select "Initiate Upgrade" to start the upgrade process • Wait for the "Choose Upgrade Media Menu" screen to display before proceeding to the next step  • Select the new PM&C 6.0.3 target ISO filename and press the [ENTER] key to start the upgrade process • The upgrade will begin and after 20 minutes, the connection will be lost as it reboots. • Do not take any action on the PM&C until the server reboots. The reboot takes approximately 5 minutes. • Once you log back in to PM&C you will see something similar to this: 
6. ☐	**PM&C GUI:** Verify the upgrade after 30 minutes	**Open a browser and type in the IP address of the PM&C server** Login as *pmacadmin* Verify the release at the top of the page. 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:



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

A.3 Verify PM&C Upgrade

S T E P #	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.	

1. ☐	Access PM&C guest console	• Log on to TVOE host SSH as *admusr*
		• Verify that the PM&C console is running by issuing the following command
		`$ sudo virsh list`
		`[admusr@brbg-tvoe-host ~]$ sudo virsh list`
		`Id  Name  State`
		`----------`
		`1  brbgpmac  running`
		
		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+]**

2. ☐	Verify the date/timestamp	• 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 ~]$`
		
		And 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	• Execute 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	• Execute 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`

6. ☐

PM&C SSH CLI: Recreate the ssh_service with admusr credentials on PM&C guest console if it doesn't exist

Verify that the ssh service exists with admusr credentials by executing the following command:

```
$ sudo netConfig --repo showService name=ssh_service
```

```
[admusr@westlakelab-pmac ~]$ sudo netConfig --repo showService name=ssh_service
    Service Name:    ssh_service
            Type:    ssh
            Host:    172.16.18.12
            Options:
               password: 390F1FAE4A420C1F2ABB05C372E30FA9
               usr: admusr
```

If the results are similar to the above, i.e., Options include "usr: admusr" and an encrypted password, skip to the next step.

If the results do not include the "usr: admusr" option or if the service does not exist, continue with this step:

- Delete the ssh_service if it exists

```
$ sudo netConfig --repo deleteService name=ssh_service
```

--answer YES to the message if prompted--

- Recreate ssh_service with *admusr* user -

```
$ sudo netConfig --repo addService name=ssh_service
Service type? (tftp, ssh, conserver, oa) ssh
Service host? <pm&c_ip_address>
Enter an option name (q to cancel): user
Enter a value for user: admusr
Enter an option name(q to cancel): password
Enter a value for password: Duk******
Verify Password : Duk******
Enter an option name(q to cancel): q
```

Example output

```
Service type? (tftp, ssh, conserver, oa)ssh
Service host? 10.250.84.122
Enter an option name <q to cancel>: user
Enter the value for user: admusr
Enter an option name <q to cancel>: password
Enter the value for password:
Verify password:
Enter an option name <q to cancel>: q
Add service for ssh_service successful
```

- Ensure the information entered is correct by executing the following command and compare the output with the configuration in the last step -

```
$ sudo netConfig --repo showService name=ssh_service
```

Example output

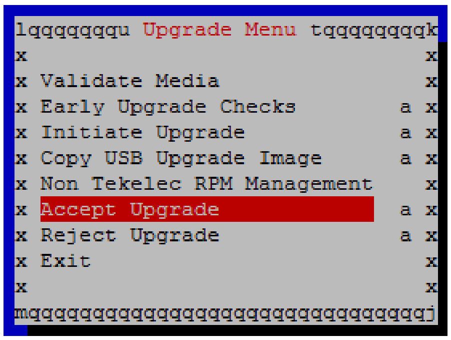
```
[admusr@westlakelab-pmac ~]$ sudo netConfig --repo showService name=ssh_service
    Service Name:    ssh_service
            Type:    ssh
            Host:    172.16.18.12
            Options:
               password: 390F1FAE4A420C1F2ABB05C372E30FA9
               usr: admusr
```

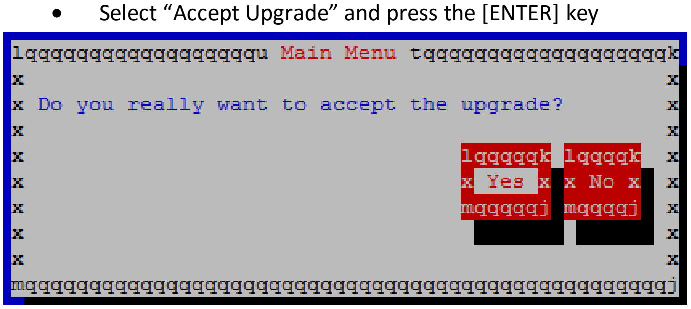
<table>
<tr>
<td>7.
☐</td>
<td></td>
<td>If ALL health checks passed, accept PM&C server and TVOE upgrades.

If health checks do not pass or a backout is needed, skip to Appendix B to reject/backout the upgrade in entirety. This will include both the PM&C server and the TVOE host.</td>
</tr>
<tr>
<td>8.
☐</td>
<td>Accept the upgrade for PM&C

NOTE:Accept takes 5 minutes</td>
<td>Close any open PM&C GUI browsers

NOTE: After accepting the upgrade, you will not be able to ‘roll back’ to the previous release.
• Logon to PM&C guest console
• Run the platcfg utility –
<code>$ sudo su – platcfg</code>

Maintenance→Upgrade→Accept Upgrade


• Select “Accept Upgrade” and press the [ENTER] key


Select ‘Yes’ to start accept upgrade process.

If a message shows up prompting to hit any key to continue, DO NOT hit any key, the server will reboot on its own.
The connection will be lost while the PM&C reboots (approximately 5 minutes)….</td>
</tr>
</table>

9.	Health Checks	**$sudo syscheck** **Open a browser and launch the PM&C GUI.** Verify the release at the top of the page. ORACLE Platform Management & Configuration 6.0.3.0.2-60.28.0 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. **Background Task Monitoring** Help Wed Dec 07 18:07:22 2016 UTC Filter

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

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:

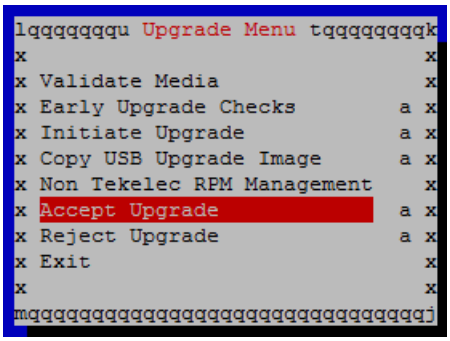
- **Some older PM&C releases cannot be deployed on upgraded TVOE 3.0.3 system.**
- **If issues occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade will have to be rejected to allow older PM&C to be re-deployed.**
- **A reject cannot be performed once an upgrade has been accepted.**

NOTE: Once the upgrade is accepted, you will not be able to 'roll back' to the previous release.

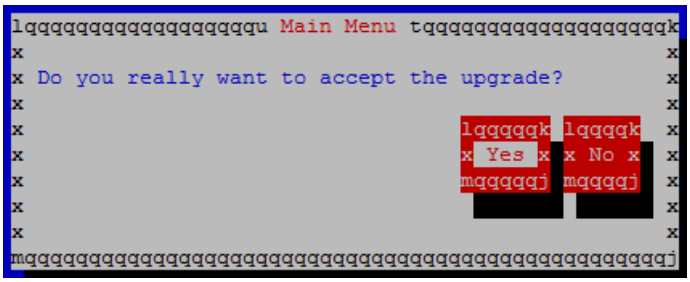
Login as *admusr* to **TVOE** host CLI and run the platcfg utility:

```
$ sudo su - platcfg
```

Maintenance→Upgrade→Accept Upgrade

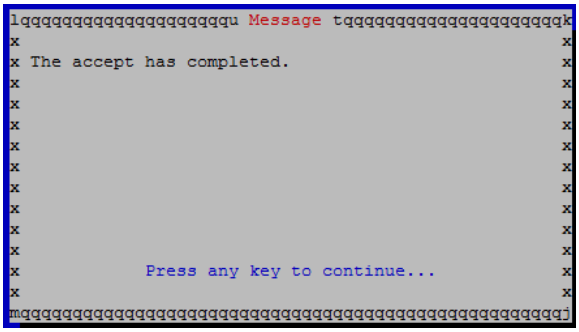


- Select "Accept Upgrade" and press the [ENTER] key



Select 'Yes' to start accept upgrade process.

NOTE: A screen session is launched when accepting the upgrade, pres "q" to close the window and return to platcfg.



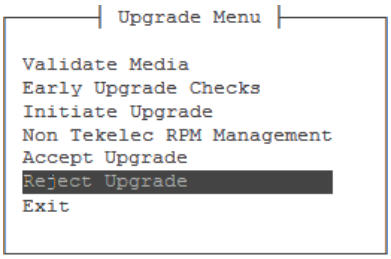
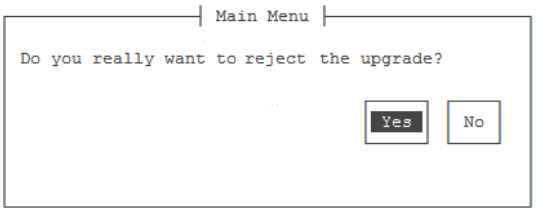
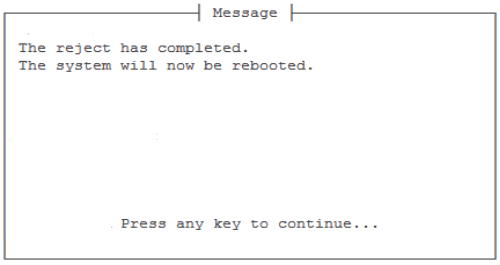
Select and press enter on "Exit" or press F12 until exiting platcfg.

The upgrade process is now complete.

APPENDIX B. TVOE AND PM&C SERVER BACKOUT

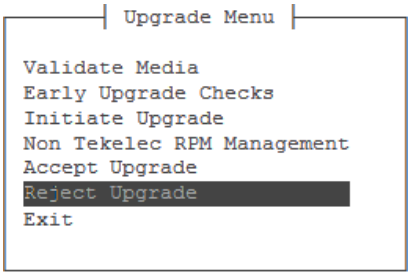
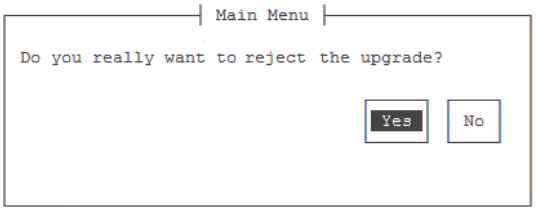
S T E P #	This procedure provides instructions to backout/reject the PM&C server upgrade. **NOTE: A reject cannot be performed after an upgrade has been accepted.** Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
1. ☐	Close any active browser sessions of PM&C	Close any open browsers connected to PM&C before proceeding.

2. ☐	If necessary, access PM&C guest console	• Log on to TVOE host as *admusr*
		• Verify PM&C console is running by issuing the following command
		`$sudo virsh list`
		`[root@brbgpmac-tvoe ~]# virsh list`
		`Id  Name  State`
		`----------`
		`1  brbgpmac  running`
		
		Log on to PM&C guest console by issuing the following command
		`$sudo virsh console <pmacname>`
		`[root@brbgpmac-tvoe ~]# virsh list`
		`Id  Name  State`
		`----------`
		`1  brbgpmac  running`
		
		`[root@brbgpmac-tvoe ~]# virsh console brbgpmac`
		`Connected to domain brbgpmac`
		`Escape character is ^]`
		
		`CentOS release 6.4 (Final)`
		`Kernel 2.6.32-358.18.1.el6prerel6.5.1_82.26.0.x86_64 on an x86_64`
		
		`brbgpmac login:`
		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, enter CTRL+]

3. ☐	Run "platcfg" utility on the PM&C Server	At the prompt, execute: `$sudo su - platcfg` Navigate to **Maintenance→Upgrade**  Select "Reject Upgrade" and press the [ENTER] key to start the reject process. The following window pops up, enter yes to begin the backout.  **NOTE**: 5 minutes into the backout, a reboot will complete 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 will reboot on its own.  **NOTE:** From this point on, it will take 20 minutes to complete the backout
5. ☐	Wait for PM&C login prompt	Upon successful completion of backout, the user should be returned to a login prompt. **Login as admusr.**

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 will be 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.

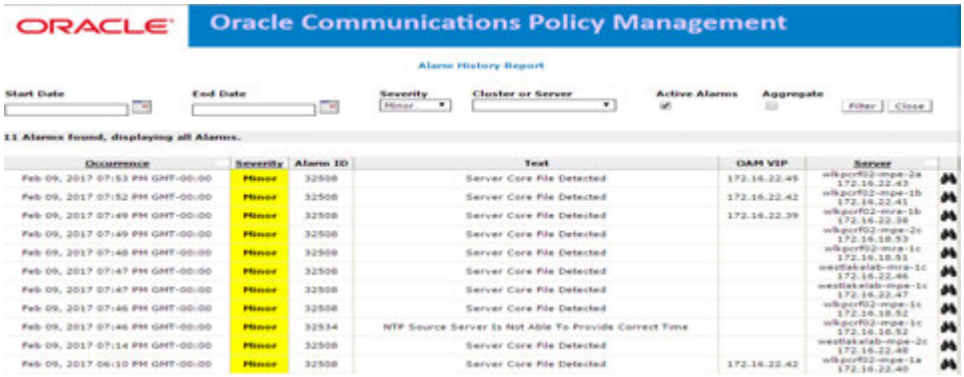
8.	**TVOE Server iLO:** **manually backout upgrade**	At the prompt execute: `$sudo su - platcfg` Navigate to **Maintenance→Upgrade**  Select "Reject Upgrade" and press the [ENTER] key to start the reject process. The following window pops up, enter yes to begin the backout.  The system will undergo a backout. As part of the process the system will reboot several times. After completing the final reboot the login prompt will be presented. Some of the final startup output along with an example of the login prompt is shown below: 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`
		
		`Install Time: Wed Nov 12 20:41:30 2014`
		`Product Name: TVOE`
		`Product Release: 2.5.2_82.37.0`
		`Part Number ISO: 872-2525-101`
		`Part Number USB: 872-2525-101`
		`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`

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

APPENDIX C. CORRECTING SERVER CORE FILE DETECTED ALARMS

Appendix C: Correcting Server Core File Detected Alarms

S **T** **E** **P** **#**	After the upgrades, if old core file detected alarms are generated, this procedure corrects these alarms. This procedure should be 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 TECHNICAL SERVICES AND ASK FOR ASSISTANCE. NOTE: THIS PROCEDURE SHOULD TAKE APPROXIMATELY 10 MINUTES PER BLADE OR RMS SERVER.	
1. ☐	**CMP GUI: Login into the CMP GUI using VIP address as 'admin' or user with admin 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'** alarm(s) 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 down the server IP(s) for which **'Server Core File Detected'** alarm was generated	Note down the server IP addresses for which **'Server Core File Detected'** alarm was generated.

4.
☐
	SSH CLI: Login to each of the servers and verify that core files are present	Login as **'admusr'** to each of the noted servers using SSH
		Change the user to **'root'** and change directory to **/var/TKLC/core**
		`$ sudo su -`
		`# cd /var/TKLC/core`

Appendix C: Correcting Server Core File Detected Alarms

		# ls Example: core.java.9499 core.java.9499.bt **# ls /var/camiant/cores** Example: core.java.9499 Note: Where **'9499'** is the java's **proc_id** and will be different for each server.
5. ☐	**SSH CLI:** cat the **core.java.<proc_id>.bt** file	'cat' 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: - /var/camiant/cores/corefile.java.<proc_id> - /var/TKLC/core/corefile.java.<proc_id>.bt - /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>**

Appendix C: Correcting Server Core File Detected Alarms

		`# exit` `$`
7. ☐	**CMP GUI:** Verify alarms	On the CMP GUI, verify that the corresponding **'Server Core File Detected'** alarms have been cleared.
This procedure has been completed.		

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