

Oracle® Communications

Software Upgrade Procedure

Policy Management 10.5/11.5/12.0/12.1.1 to 12.1.2 Upgrade Procedure, Georedundancy Enabled

E75411-01

September 2016



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 A 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.

Software Upgrade Procedure

Oracle Communications Policy Management 10.5/11.5/12.0/12.1.1 to 12.1.2 Upgrade Procedure, Georedundancy Enabled

Copyright © 2013, 2016, 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 References	6
1.3 Acronyms	7
1.4 Terminology.....	7
1.5 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 Perform System Health Check.....	21

Software Upgrade Procedure

4.6 Deploy Policy Upgrade Software	22
4.6.1 Deploying Policy Upgrade Software to Servers	22
4.6.2 Copy ISO image files to Management Server (PM&C)	22
4.6.3 Distribute Application ISO Image Files to Servers	25
4.6.4 Backups and Backup Locations	29
4.6.5 Changing Non-Default Root and admusr Passwords.....	31
5. SOFTWARE UPGRADE CAUTIONS.....	35
6. UPGRADE CMP CLUSTERS (10.5 TO 12.1.2)	36
6.1 Upgrade CMP Clusters Overview	36
6.1.1 Upgrade Primary CMP Cluster.....	37
6.1.2 Upgrade Secondary CMP Cluster	45
7. UPGRADE CMP CLUSTERS (11.5 TO 12.1.2)	48
7.1 Upgrade CMP Clusters Overview	48
7.1.1 Upgrade Primary CMP Cluster.....	49
7.1.2 Upgrade Secondary CMP Cluster	59
8. UPGRADE CMP CLUSTERS (12.0 TO 12.1.2)	62
8.1 Upgrade CMP Clusters Overview	62
8.1.1 Upgrade Primary CMP Cluster.....	63
8.1.2 Upgrade Secondary CMP Cluster	71
9. UPGRADE CMP CLUSTERS (12.1.1 TO 12.1.2)	74
9.1 Upgrade CMP Clusters Overview	74
9.1.1 Upgrade Primary CMP Cluster.....	75
9.1.2 Upgrade Secondary CMP Cluster	82
10. MPE AND/OR MRA UPGRADE	85
10.1 Upgrade Preparation	85
10.1.1 Configuration Preparation	85
10.2 Upgrade MRA and MPE Servers	86
11. POST UPGRADE HEALTH CHECK.....	93
12. BACKOUT (ROLLBACK).....	94
12.1 Backout Sequence.....	94
12.2 Pre-requisites	94
12.3 Backout of Fully Upgraded Cluster	94
12.3.1 Backout Sequence	94

Software Upgrade Procedure

12.3.2 Backout of a Partially Upgraded Cluster..... 95

12.3.3 Backout Fully Upgraded MPE/MRA Cluster 96

12.3.4 Backout Fully Upgraded Secondary CMP Cluster 101

12.3.5 Backout Fully Upgraded Primary CMP Cluster 104

**APPENDIX A. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE AND
HOTLINES109**

1. INTRODUCTION

1.1 Purpose and Scope

This document describes the methods utilized and procedures executed to perform Oracle Communications Policy Management release 10.5, 11.5, 12.0, or 12.1.1 software upgrade to Policy Management release 12.1.2 with georedundancy enabled.

- Upgrade of the PM&C server including TVoE Host is required, but not covered in this document.
NOTE: Not all Policy Management systems use a PM&C Server, so this is optional.
- Upgrade of firmware may be required, but is not covered in this document.
- In-service Policy Management release 10.5, 11.5, 12.0, or 12.1.1 CMP, MRA servers and MPE servers.

The georedundancy implemented in the MPE and the MRA is using the 2+1 server cluster scheme. The 2 refers to the current Active and Standby servers and the +1 refers to the third Spare server. This Spare server is added into the same cluster so that any server can assume the Active role if necessary. The Spare server is 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 References

Depending on the hardware platform on which your Policy Management software operates, you need some of the following documents before you upgrade the Policy Management software. Collect these documents, and if necessary perform the prerequisite procedures in them, before beginning an upgrade.

The following documents are available at the Oracle Help Center:

- E53018-01—Tekelec Platform TVOE 3.0 Software Upgrade Guide
- E54387-03—Tekelec Platform 5.7 and 6.0 Incremental Upgrade Guide
- E59721-01—Tekelec Platform HP Solutions Firmware Upgrade Pack, Release 2.2.8 Upgrade Guide
- E59722-01—Tekelec Platform HP Solutions Firmware Upgrade Pack, Release 2.2.8 Release Notes
- E64920-01—Tekelec Platform HP Solutions Firmware Upgrade Pack, Release 2.2.9, Upgrade Guide
- E64919-01—Tekelec Platform HP Solutions Firmware Upgrade Pack, Release 2.2.9, Release Notes
- E72398-02—Oracle Communications Policy Management Release Notes for Release 12.1.2
- E70153-01—Oracle Communications Bare Metal Installation Guide 12.1.x
- E54387-04—PM&C Incremental Upgrade, Release 5.7 and 6.0
- E53486-01—Tekelec Platform 7.0.x Configuration Guide, part number
- E71647-01—Policy Management Troubleshooting Reference
- E71641-01—Policy Management Platform Configuration User's Guide

1.3 Acronyms

Acronym	Definition
CMP	Configuration Management Platform
DSR	Diameter Signaling Router
GUI	Graphical User Interface
IPM	Initial product manufacture
LVM	Logical Volume Manager
MPE	Multimedia Policy Engine
MRA	Multiprotocol Routing Agent (also known as the Policy Front End)
OCS	Online Charging System
OOS	Out of service
PCEF	Policy Control Enforcement Function (GGSN, P-GW, DPI)
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
UE	User Equipment

1.4 Terminology

Primary Site (Site-1)—Site where the MPE/MRA Server-A and Server-B are deployed

Secondary Site (Site-2)—Site where the MPE/MRA Server-C is deployed.

Spare Server—Server that is ready to take over from the Active server if the Standby server fails. Server-C is typically designated as the Spare Server and is generally in another location from the Active and Standby servers.

1.5 Software Release Numbering

- PM&C: 6.0.1.0.0_60.21.0
- TVOE: 3.0.2.0.0_86.28.0
- Policy Management release 12.1.2.0.0_22.1.0
- Firmware: Tekelec Platform HP Solutions Firmware Upgrade Pack 2.2.8 or higher

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute Policy Management release 12.1.2 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 12.1.1 to 12.1.2
2. Policy Management 12.0.x to 12.1.2
3. Policy Management 11.5.x to 12.1.2
4. Policy Management 10.5.x to 12.1.2

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 contains all servers. The cluster types are CMP, MRA, or MPE.

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

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 upgrades are not covered in this document, but 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 1.5
2. Upgrade PM&C Server at Site 2—Needed if version is older than what is listed in Section 1.5
3. Firmware upgrade—If needed
4. Upgrade Primary CMP
5. Upgrade Secondary CMP (If Applicable)
6. Site 1 Segment 1—Upgrade MPE and MRA (See Note Below)
7. Site 2 Segment 1—Upgrade MPE and MRA (See Note Below)
8. Site 1 Segment 2—Upgrade MPE and MRA (See Note Below)
9. Site 2 Segment 2—Upgrade MPE and MRA (See Note Below)

NOTE: Up to 4 MPE and MRA 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 release 10.5, 11.5, 12.0, or 12.1.1 and release 12.1.2 mixed configuration would support the performance and capacity of release 10.5, 11.5, 12.0, or 12.1.1. The mixed version Policy Management configuration would support release 10.5, 11.5, 12.0, or 12.1.1 features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the release 12.1.2 CMP will be managing the previous release, and release 12.1.2 MRA and MPE servers. In this mixed version configuration release 12.1.2 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. This is due to the number of permutations involved in testing different mixed version configuration scenarios.

In the mixed version Policy Management configuration release 12.1.2 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 and MRA servers is limited to parameters that are available in the previous version. Specifically, Network Elements can be added

Software Upgrade Procedure

Table 1 Mixed-version configurations supported between release 10.5, 11.5, 12.0, or 12.1.1, and release 12.1.2

Policy Management system components on	CMP R12.1.2	MRA R 12.1.2	MPE R 12.1.2
CMP R10.5, 11.5, 12.0, or 12.1.1	Yes	No	No
MRA R10.5, 11.5, 12.0, or 12.1.1	Yes	Yes	Yes
MPE R10.5, 11.5, 12.0, or 12.1.1	Yes	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of the CMP and DR-CMP from release 10.5, 11.5, 12.0, or 12.1.1 to release 12.1.2. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to release 12.1.2.

2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the standby server, and then switching over from the Active to the Standby, and upgrading the second server. The switchover of each MPE or MRA 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 7.0.2 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 7.0.2 should have been installed prior to upgrading to Policy Management release 12.1.2.

2.7 Server Hardware Platforms

The Policy Management release 12.1.2 software upgrade can be applied on any server that previously had Policy Management release 10.5, 11.5, 12.0, or 12.1.1

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 12.1.2 software ISO files and TPD software ISO
2. Policy 12.1.2 software Release Notes.
3. TVOE, PM&C upgrade/installation documentation, software ISO files and TPD ISO (if applicable).
4. HP Solutions Firmware Upgrade Pack 2.2.8 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.

Software Upgrade Procedure

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

The following list is the ISO image files required for the 12.1.2 Policy Management upgrade.

- cmp-12.1.2.0.0_22.1.0-x86_64.iso
- mpe-12.1.2.0.0_22.1.0-x86_64.iso
- mpe-li-12.1.2.0.0_22.1.0-x86_64.iso
- mra-12.1.2.0.0_22.1.0-x86_64.iso

NOTE: You will need either the MPE or MPE-Li ISO file for the upgrade. The file you use is based on your current Policy Management setup.

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 on page 12.

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.

Software Upgrade Procedure

Table 2 Login IDs, Passwords and release Information

Item	Value
CMP servers NOTE: 10.5 does not use admusr, instead use the default root SSH login.	GUI Administrator Login User/Password
	admusr password:
MPE/MRA servers	admusr password:
Target iLO	iLO Administrator Login User/Password
Target OA	OA Administrator Login User/Password
PM&C server	GUI Administrator Login User/Password
	admusr password
Software Upgrade Target Release ¹	Target Release Number
	Policy 12.1.2 software ISO image filenames <ul style="list-style-type: none">• cmp-12.1.2.0.0_22.1.0-x86_64.iso• mpe-12.1.2.0.0_22.1.0-x86_64.iso or mpe-li-12.1.2.0.0_22.1.0-x86_64.iso• mra-12.1.2.0.0_22.1.0-x86_64.iso

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.

The screenshot shows the Upgrade Manager interface. At the top right, it says 'Current ISO: standard-upgrade-12.1.2.0.0_22.1.0'. Below this are buttons for 'Start Rollback' and 'Start Upgrade'. A 'View Upgrade Log' button is also present. The main table has columns: Name, Alarm Severity, Up to Date, Server Role, Prev Release, Running Release, and Upgrade Operation. There are two expandable sections: 'CMP Start Cluster (2 Servers)' and 'TestIMPE (2 Servers)'. The table lists servers like chris0, chris10, chris16, and chris15 with their respective roles and upgrade statuses.

Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Start Cluster (2 Servers)						
chris0		Y	Standby	11.1.2.3.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Feb 8, 2015 21:30:15.
chris10		Y	Active	11.1.2.3.1.0	12.1.2.0.0_22.1.0	n/a
TestIMPE (2 Servers)						
chris16		Y	Active	11.1.2.3.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Feb 8, 2015 10:26:15.
chris15		Y	Standby	11.1.2.3.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Feb 8, 2015 12:23:46.

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.

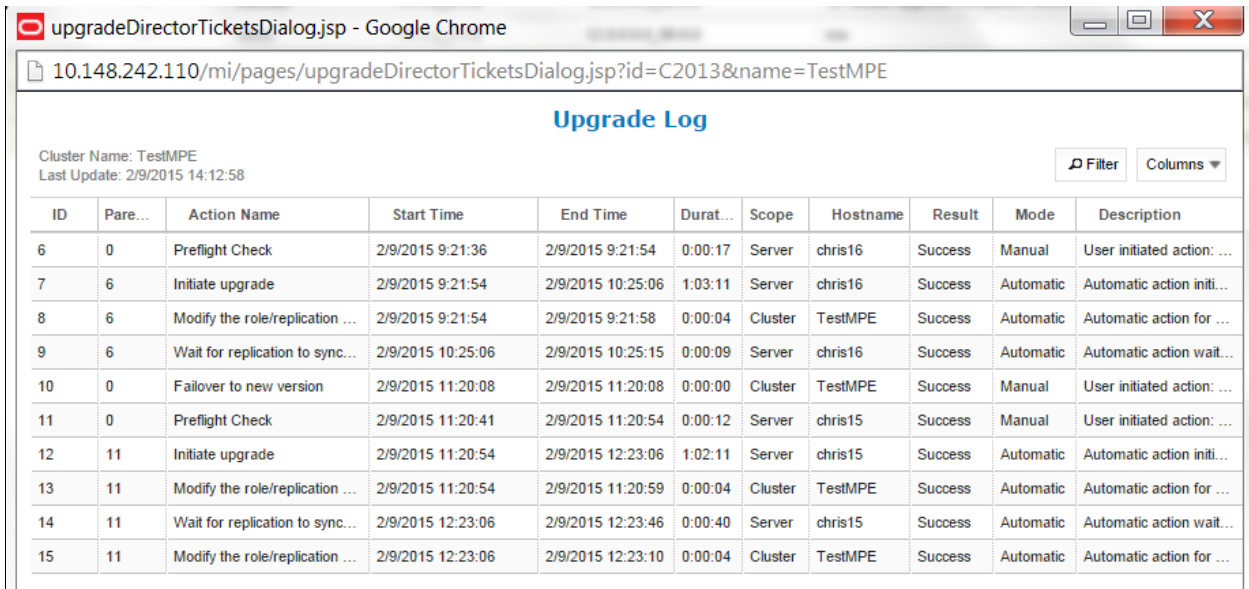
- **Start Rollback and Start Upgrade buttons** (upper left): If a cluster is selected and these buttons are disabled (grey), it means that there is not an appropriate action to take at this time. However, if a button is not disabled (white), then it means that there is a preferred action that can be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

Software Upgrade Procedure

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.



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.

Software 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.

Name	Alarm S...	Up to ...	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
CMP1-SITEA	Minor	Y	Standby	10.5.6_1.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Jul 12, 2016 13:14:59.
CMP2-SITEA	Major	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	n/a
CMP Site2 Cluster (2 Servers)						
CMP2-SITEB	Minor	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Jul 12, 2016 14:16:10.
CMP1-SITEB	Minor	Y	Standby	10.5.6_1.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Jul 15, 2016 5:42:13.
MDF Cluster (3 Servers)						
MDF3-SITEB		N	Spare	10.5.6_1.1.0	10.5.6_1.1.0	n/a
MDF2-SITEA		N	Standby	10.5.6_1.1.0	10.5.6_1.1.0	n/a
MDF1-SITEA		N	Active	10.5.6_1.1.0	10.5.6_1.1.0	n/a
MPE Cluster (3 Servers)						
MPE3-SITEB	Major	N	OOS	10.5.6_1.1.0	10.5.6_1.1.0	Step 2/3 4% Initiate upgrade : Initiate upgrade (Elapsed Time: 0:00:33)
MPE2-SITEA	Critical	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully at Jul 15, 2016 14:16:41.
MPE1-SITEA	Critical	N	Standby	10.5.6_1.1.0	10.5.6_1.1.0	n/a
MRA Cluster (3 Servers)						
MRA3-SITEB		N	Spare	10.5.6_1.1.0	10.5.6_1.1.0	n/a
MRA2-SITEA		N	Standby	10.5.6_1.1.0	10.5.6_1.1.0	n/a

Figure 3 Upgrade in Progress Showing Transient Alarms

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

Table 3 Transient Alarms Asserted During a Typical Upgrade

Alarm Number	Severity	Name
31227	Critical	HA availability status failed
31283	Critical	Lost Communication with server
70001	Critical	QP_procmgr failed
70025	Critical	QP Slave database is a different version than the master

Software Upgrade Procedure

Alarm Number	Severity	Name
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 12.1.2, 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:

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

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

- 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

Software Upgrade Procedure

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

Software Upgrade Procedure

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 will need to be upgraded prior to upgrade to Policy Management release 12.1.2. Firmware upgrade to FUP 2.2.8 will need to be executed prior to the upgrade to Policy Management release 12.1.2.		
Step	Procedure	Result
1. <input type="checkbox"/>	Verify all required materials are present	As listed in section 2.9, "Required Materials and Remote Access," on page 10.
2. <input type="checkbox"/>	Review Release Notes	Review Policy 12.1.2 Release Notes for the following information: <ul style="list-style-type: none">• Individual software components and versions included in target release.• New features included in target release.• Issues (Oracle BUGs) resolved in target release.• Known Issues with target release.• Any further instructions that may be required to complete the software upgrade for the target release.
THIS PROCEDURE HAS BEEN COMPLETED		

4.2 TVOE and PM&C Server Upgrade

Policy Management release 12.1.2 requires PM&C Version 6.0 to support IPM of TPD 7.0 on c-Class server.

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 the following documents to upgrade the TVOE and PM&C:

- E53018-02—Oracle Communications Platform Tekelec Virtualization Operating Environment (TVOE) 3.0 Software Upgrade Procedure
- E54387-04—Oracle Communications Platform PM&C Incremental Upgrade

4.3 Firmware Upgrade

See the following Documents to upgrade the TVOE and PM&C:

1. E59721-01—Oracle Communications Tekelec Platform HP Solutions Firmware Upgrade Pack, Upgrade Guide, Release 2.2.8
2. E59722—Oracle Communications Tekelec Platform HP Solutions Firmware Upgrade Pack Release Notes, Release 2.2.8
3. ISO files
 - a. FW2_MISC-2.2.8.0.0_10.43.0.iso
 - b. FW2_SPP-2.2.8.0.0_10.43.0.iso

Software Upgrade Procedure

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 and FUP 2.2.8 deployed.
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. <input type="checkbox"/>	Use the following checklist to plan the cluster upgrades for the entire system.	Maintenance Windows are planned		
2. <input type="checkbox"/>	Upgrade Site-1 and Site-2 TVOE/PM&C	Site Names _____ and _____		3 hrs
3. <input type="checkbox"/>	Upgrade Site-1 and Site-2 CMP clusters. Each cluster will take approximately 1 and ½ hours to complete	Site Names _____ and _____		3 hrs
4. <input type="checkbox"/>	Upgrade Site-1 MPE/MRA clusters for Segment-1 NOTE: Maximum of 4 clusters performed in parallel	Site Names _____ Cluster List:		2 hrs
5. <input type="checkbox"/>	Upgrade Site-2 clusters for Segment-1 NOTE: Maximum of 4 clusters performed in parallel	Site Names _____ Cluster List:		2 hrs

Software Upgrade Procedure

Step	Procedure	Result	Engineer	Time
6. <input type="checkbox"/>	Upgrade Site-1 clusters for Segment-2 NOTE: Maximum of 4 clusters performed in parallel	Site Names _____ Cluster List:		2 hrs
7. <input type="checkbox"/>	Upgrade Site-2 clusters for Segment-2 NOTE: Maximum of 4 clusters performed in parallel	Site Names _____ Cluster List:		2 hrs
THIS PROCEDURE HAS BEEN COMPLETED				

4.5 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. <input type="checkbox"/>	CMP GUI Access	Open a browser to access the Primary CMP GUI on its VIP address and login to verify access.
2. <input type="checkbox"/>	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. <i>IMPORTANT: Before starting any upgrade activity, ensure that all active alarms are understood and resolved.</i>
3. <input type="checkbox"/>	View KPI reports	Verify that the system is running within expected parameters. Export current the KPIs into a file.

Software Upgrade Procedure

Step	Procedure	Result
4. <input type="checkbox"/>	<p>Confirm NTP servers are reachable from all the servers (CMP, MPEs and MRAs) to be upgraded</p> <p>NOTE: If the time across the servers is out of synch, fix it first and re-validate this step, before starting the upgrade procedures.</p>	<ol style="list-style-type: none">1. Validate the IP connectivity between the server and NTP servers by PING.2. Confirm that time is synchronized on each server using the following CLI shell command: <pre>ntpq -np</pre>3. Confirm that date is correct on each server.4. Check that BIOS clock is synced with the clock using the following CLI shell command: <pre>hwclock</pre>
THIS PROCEDURE HAS BEEN COMPLETED		

4.6 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 12.1.2, each ISO image size is about 1.0 Gigabytes.

4.6.1 Deploying Policy Upgrade Software to Servers

There are four possible software images in this upgrade (CMP, MPE, MPE-Li, and MRA). 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, the MPE-Li image deployed to the MPE-Li servers and the MRA image deployed to the MRA servers.

IMPORTANT: *If the deployed image type (CMP, MPE, MPE-LI, or MRA) 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. Or, if multiple images are copied into the /var/TKLC/upgrade directory, the upgrade will fail.

4.6.2 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.*

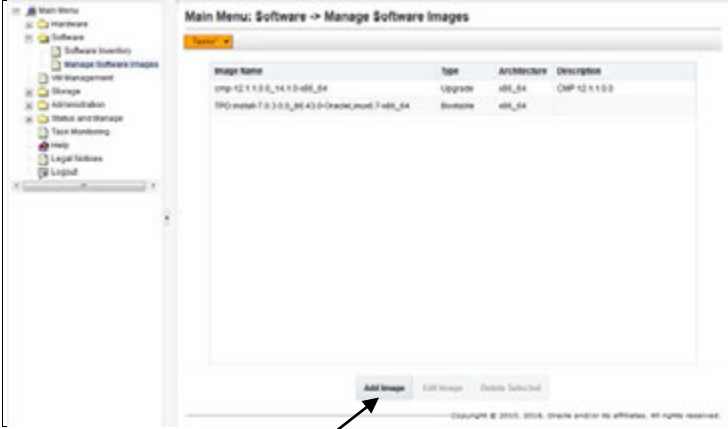
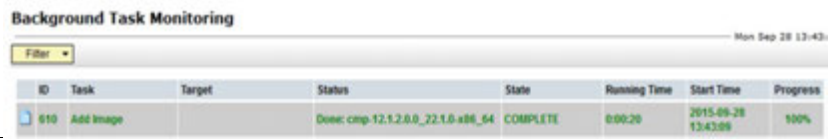
NOTES:

- 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.

Software Upgrade Procedure

Step	Procedure	Result
1. <input type="checkbox"/>	PM&C GUI: Verify that there are no release 12.1.2 ISO files on the server	Log on to the PM&C Server GUI Software → Manage Software Images Confirm that the release 12.1.2 ISO files do not exist. If there are files, remove them.
2. <input type="checkbox"/>	SSH to PM&C server as admusr	<ol style="list-style-type: none"> Log on as admusr to the PM&C server. Change Target directory to <code>/var/TKLC/upgrade</code> and ensure there is at least of 3.0 GB free disk space available. <pre>\$cd /var/TKLC/upgrade</pre> <pre>\$df -h /var/TKLC</pre> <p>NOTE: If there are ISO files in the <code>/var/TKLC/upgrade</code> directory, you can remove the files to free up disk space or add the files to the PM&C repository.</p>
3. <input type="checkbox"/>	Copy release 12.1.2 ISO files to the target directory in the PM&C server	<p>Transfer all release 12.1.2 ISO files (CMP, MPE/MPE-Li, MRA) into directory <code>/var/TKLC/upgrade</code> using one of the following methods:</p> <ul style="list-style-type: none"> SCP/WGET command in the following steps outline in this Procedure USB drive <p>NOTE: If the directory becomes full, you may have to use the <code>scp</code> 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 <code>/var/TKLC/smac/image/isoimages/home/smacftpusr</code> directory which has more available space.</p>
4. <input type="checkbox"/>	Check the checksum file	<ol style="list-style-type: none"> Transfer the <code>md5sum.out</code> file to the <code>/var/camiant/tmp</code> directory. Use the concatenate command, <code>cat</code>, to see the value of the checksum. <p>EXAMPLE</p> <pre>[root@CMP-JB-126 tmp]# cat md5sum.out</pre> <pre>cca84e669c8db680f3264a93fe83aab7/home/build/build/PLATFORM-</pre> <pre>70/iso/cmp-12.1.2.x.x.x.iso [root@CMP-JB-126 tmp]#</pre> <ol style="list-style-type: none"> Verify that the checksum value is the same as the value in the <code>md5sum.out</code> file. <p>EXAMPLE</p> <pre>[root@CMP-JB-126 iso]# md5sum cmp-12.1.2.x.x.x.iso</pre> <pre>cca84e669c8db680f3264a93fe83aab7 cmp-12.1.2.x.x.x.iso [root@CMP-</pre> <pre>JB-126 iso]#</pre>

Software Upgrade Procedure

Step	Procedure	Result
5. <input type="checkbox"/>	PM&C GUI: Adding the new release 12.1.2 ISO files	<p>Software → Manage Software Images</p> <p>1. Click Add Image to select the ISO files that were transferred to the PM&C server.</p>  <p>Path: /var/TKLC/smac/image/isoimages/home/smac/pusr/cmp-12.1.2.0 (▼) Description: CMP 12.1.2 Add New Image</p> <p>2. Click OK on the pop-up</p>
6. <input type="checkbox"/>	PM&C GUI: Verify that the ISO files were added successfully	<p>Software → Manage Software Images</p> <p>The status of the image being added can be monitored using the Task Monitoring menu with the screen display as the following:</p>  <p>NOTE: The added ISO files are now stored in the /var/TKLC/smac/image/repository directory</p>
THIS PROCEDURE HAS BEEN COMPLETED		

4.6.3 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:

- 4.6.3.1 Manual Distribution
- 4.6.3.2 PM&C Distribution

4.6.3.1 Manual Distribution

Step	Procedure	Result
1. <input type="checkbox"/>	Transfer ISO files to Policy server.	<p>Transfer release 12.1.2 ISO files (CMP, MPE/MPE-Li, and MRA) into /var/TKLC/upgrade directory on the respective server using one of the following methods:</p> <ul style="list-style-type: none"> • SCP/WGET command • USB drive <p>If the images are on a server in the same network, <code>scp</code> the files using the CLI.</p> <ul style="list-style-type: none"> • Copy CMP software ISO file to ONE of the other CMP servers: <pre>\$sudo scp cmp-12.1.2.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/</pre> • Copy MPE software ISO to ONE of the other MPE servers: <pre>\$sudo scp mpe-12.1.2.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/</pre> • Copy MPE-Li software ISO to ONE of the other MPE-Li servers: <pre>\$sudo scp mpe-li-12.1.2.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/</pre> • Copy MRA software ISO to ONE of the other MRA servers: <pre>\$sudo scp mra-12.1.2.0.0_22.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/</pre> <p>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.</p>
THIS PROCEDURE HAS BEEN COMPLETED		

Software Upgrade Procedure

4.6.3.2 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:

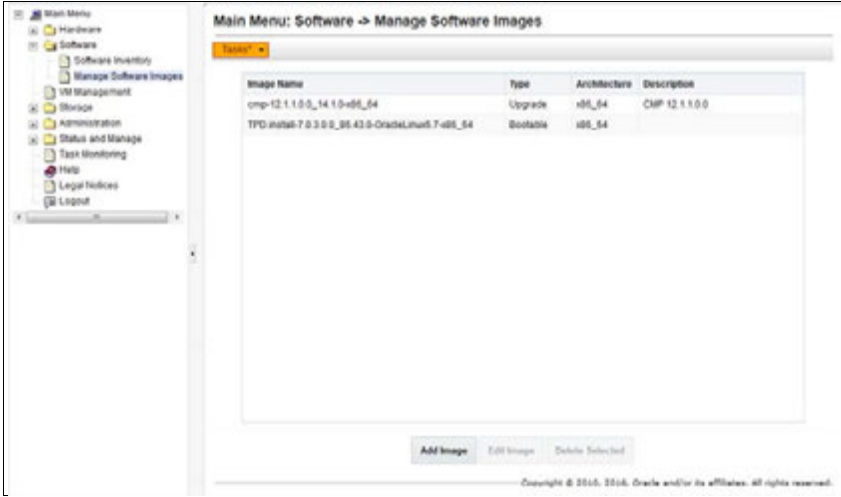
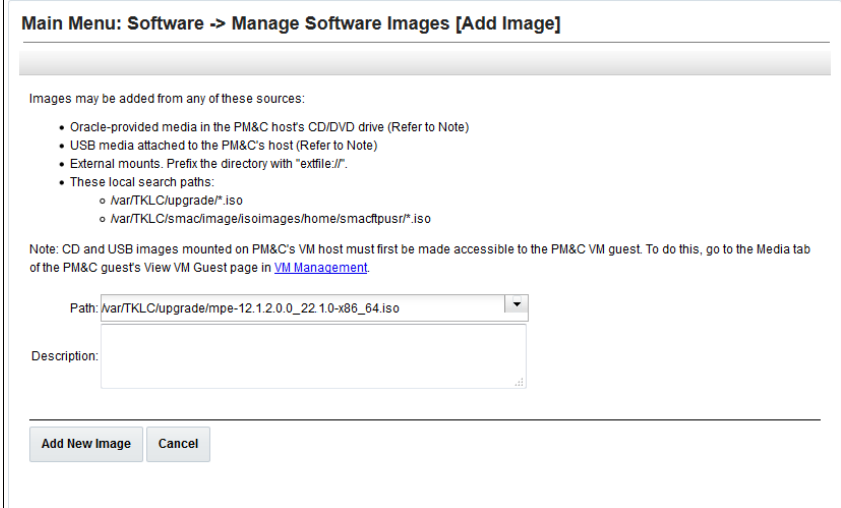
- Media mounted in the CD/DVD drive of the PM&C host
- USB media attached to the PM&C host
- External mounts (prefix the directory with extfile://)
- These local search paths:
 - /var/TKLC/upgrade/
 - /var/TKLC/smac/image/isoimages/home/smacftpusr/

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.

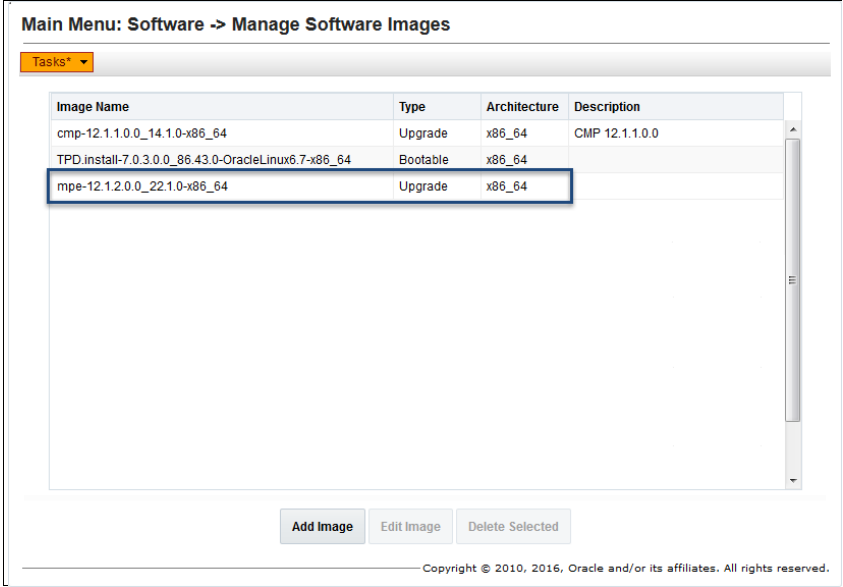
The following procedure assumes the ISO file is located in the directory /var/TKLC/upgrade on the PM&C server.

Step	Procedure	Result
1. <input type="checkbox"/>	Log in to PM&C	<p>Open a browser, enter the URL of the PM&C server, and log in as guiadmin.</p> <p>The PM&C Main Menu opens. For example:</p> 

Software Upgrade Procedure


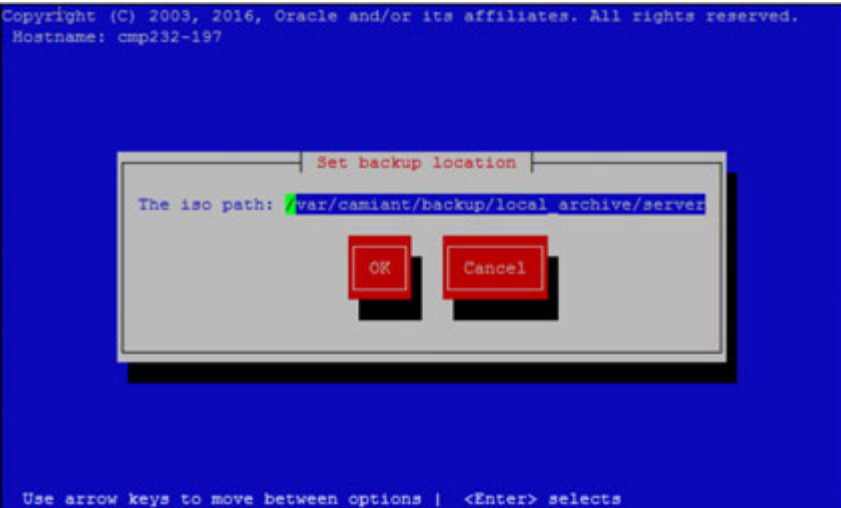
Step	Procedure	Result
2. <input type="checkbox"/>	Select the ISO image	<p>1. Select Main Menu > Software > Manage Software Images</p> <p>The Manage Software Images page opens. For example:</p>  <p>2. Click Add Image (at the bottom of the page). The Manage Software Images [Add Image] page opens. For example:</p>  <p>Select the ISO file from the Path dropdown list and click Add New Image.</p> <p>Tip: You can enter a description of the ISO file before adding it.</p> <p>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.</p>

Software Upgrade Procedure

Step	Procedure	Result
3. <input type="checkbox"/>	Move the ISO file to the repository	<p>Click OK to move the file (or Cancel to copy it).</p> <p>The ISO file is loaded into the PM&C image repository in the background.</p> <p>Tip: You can click the Tasks dropdown list to check the progress of the task.</p> <p>When the upload is complete, the ISO file appears in the list. For example:</p> 
4. <input type="checkbox"/>	Verify that the image is no longer in the directory	<p>Enter the following command:</p> <pre>\$ sudo ls /var/TKLC/upgrade \$</pre>
5. <input type="checkbox"/>	Load addition files	If you are loading multiple ISO files into the image repository, repeat steps 2–4 until all files are loaded.
6. <input type="checkbox"/>	Remove media	When you finish, remove the CD/DVD media or unmount the USB device.
THIS PROCEDURE HAS BEEN COMPLETED		

4.6.4 Backups and Backup Locations

Perform the Backups prior to the Maintenance Window period.

Step	Procedure	Result
1. <input type="checkbox"/>	<p>SSH CLI/iLO: Access the server to be backed up</p> <p>NOTE: System backup is done on active CMP servers ONLY.</p>	<p>IMPORTANT: Server backups (each CMP, MPE/MPE-Li, and MRA server—active/standby/spare), and the system backup (from active CMP), must be collected and readily accessible for recovery operations.</p> <ol style="list-style-type: none"> 1. Login into the active Primary CMP server. 2. Navigate to the following through platcfg utility. <pre>\$sudo su - platcfg</pre> 3. Policy Configuration→Backup and Restore→server backup Provide the ISO backup filename in the default backup location path of: <pre>/var/camiant/backup/local_archive/serverbackup/<filename.iso></pre>  4. Navigate to the following using the platcfg utility. <pre>\$sudo su - platcfg</pre> 5. Policy Configuration→Backup and Restore→system backup Provide the ISO backup filename in default backup location path of: <pre>/var/camiant/backup/local_archive/systembackup/<filename.tar.gz></pre> 

Software Upgrade Procedure

Step	Procedure	Result
2. <input type="checkbox"/>	SSH CLI/iLO: Verify the backup ISO file	<p>If default location is accepted in the previous step, change to the following directory and verify the file.</p> <pre> \$ cd /var/camiant/backup/local_archive/serverbackup \$ ls <hostname>-mpe_12.1.2.0.0_22.1.0-serverbackup-2016<xx><xx><xxxx>.iso \$ cd /var/camiant/backup/local_archive/serverbackup \$ ls <hostname>-mra_12.1.2.0.0_22.1.0-serverbackup-2016<xx><xx><xxxx>.iso cd /var/camiant/backup/local_archive/serverbackup \$ ls <hostname>-cmp-12.1.2.0.0_22.1.0-serverbackup-2016<xx><xx><xxxx>.iso \$ cd /var/camiant/backup/local_archive/systembackup \$ ls <hostname>-cmp12.1.2.0.0_22.1.0-systembackup-2016<xx><xx><xxxx>.tar.gz </pre>
3. <input type="checkbox"/>	Copy backup files.	<p>1. Copy files to remote server or local workstation/laptop.</p> <p>Example of a remote server copy.</p> <pre>\$ sudo scp /var/camiant/backup/local_archive/systembackup/xx_tar.gz <ip_address_of_backup_repository></pre> <p>Example of a local workstation/laptop copy.</p> <pre>\$sudo scp /var/camiant/backup/local_archive/serverbackup/xx.iso <ip_address_of_backup_repository></pre> <p>2. Remove the backup ISO file from the TPD Sever.</p> <pre>\$sudo rm <backup_filename.iso></pre>
4. <input type="checkbox"/>	Identify backup location	<p>Backup location is:</p> <p>_____</p> <p>Instructions to access to backups are as follows:</p> <p>_____</p> <p>_____</p> <p>_____</p>
THIS PROCEDURE HAS BEEN COMPLETED		

4.6.5 Changing Non-Default Root and admusr Passwords

4.6.5.1 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-12.1.1 to 12.1.2 and above. To prevent those issues, the following procedure has been created.

4.6.5.2 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 12.1.2, they will be expired post upgrade.

IMPORTANT: The following procedure should be executed prior to the upgrade to 12.1.2 only if the root or admusr passwords are non-default.

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

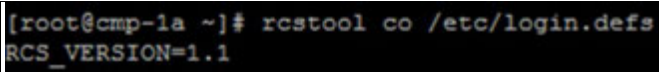
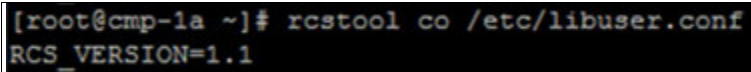
1. Standby CMPs
2. Active CMPs
3. Standby MPEs/MRAs
4. Spare MPEs/MRAs
5. Active MPEs/MRAs

Step	Procedure	Result
1. <input type="checkbox"/>	Login to the server (MRA/CMP/MPE)	<ul style="list-style-type: none"> For an upgrade from 11.5/12.0/12.1.1, login as admusr and change to root using the following command: <pre>\$sudo su</pre> <pre>login as: admusr Using keyboard-interactive authentication. Password:</pre> For an upgrade from 10.5, login as root. <pre>[root@derek local]# ssh root@10.113.0.31 root@10.113.0.31's password:</pre>
2. <input type="checkbox"/>	Check the password field of root and admusr	<p>Issue the following</p> <pre>#egrep '^(root admusr)' /etc/shadow</pre> <p>EXAMPLE OUTPUT</p> <pre>root:\$6\$mErKrEsA\$83n5G8dR3CgBJmEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc .Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7::: admusr:\$6\$mUstAfa\$gn2B8Tsw1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A 5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825:0:99999:7:::</pre> <p>NOTES:</p> <ul style="list-style-type: none"> 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 4

Software Upgrade Procedure

Step	Procedure	Result
3. <input type="checkbox"/>	Order to perform the change	<p>Perform steps 5-15 on each server in the following order:</p> <ol style="list-style-type: none"> Standby CMP Active CMP Standby MPEs/MRAs Spare MPEs/MRAs Active MPEs/MRAs
4. <input type="checkbox"/>	Login to the Server (MRA/CMP/MPE)	<ul style="list-style-type: none"> For an upgrade from 11.5/12.0, login as admusr and change to root using the following command: <pre>\$sudo su</pre> <pre>login as: admusr Using keyboard-interactive authentication. Password:</pre> For an upgrade from 10.5, login as root. <pre>[root@derek local]# ssh root@10.113.0.31 root@10.113.0.31's password:</pre>
5. <input type="checkbox"/>	Checkout revisions	<p>Issue the following command:</p> <pre>#rcstool co /etc/pam.d/system-auth</pre> <pre>[root@cmp-1a ~]# rcstool co /etc/pam.d/system-auth RCS_VERSION=1.1</pre>
6. <input type="checkbox"/>	Modify the system-auth file	<ol style="list-style-type: none"> Open the system-auth file. <pre>#vi /etc/pam.d/system-auth</pre> Modify the file. Change the md5 value to sha512 <p>Current Line:</p> <pre>password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok</pre> <p>Modified Line:</p> <pre>password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok</pre> <pre>##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</pre>
7. <input type="checkbox"/>	Save the file	<ul style="list-style-type: none"> If the file required changing: <pre>#rcstool ci /etc/pam.d/system-auth</pre> If the file was already configured: <pre>#rcstool unco /etc/pam.d/system-auth</pre>

Software Upgrade Procedure

Step	Procedure	Result
8. <input type="checkbox"/>	Checkout revisions for login.defs file	<pre>#rcstool co /etc/login.defs</pre> 
9. <input type="checkbox"/>	Edit login.defs file	<p>Shadow password suite configuration</p> <ol style="list-style-type: none"> Open the login.defs file. <pre>#vi /etc/login.defs</pre> Change the encrypt method from MD5 to SHA12. Current Line: <pre>ENCRYPT_METHOD MD5</pre> Modified Line: <pre>ENCRYPT_METHOD SHA512</pre> <p>NOTE: The line to edit is near the bottom of the file.</p> Comment out the following line if necessary. <pre>MD5_CRYPT_ENAB yes</pre>
10. <input type="checkbox"/>	Save the File	<ul style="list-style-type: none"> If the file required changing <pre>#rcstool ci /etc/login.defs</pre> If the file already was configured <pre>#rcstool unco /etc/login.defs</pre>
11. <input type="checkbox"/>	Checkout revisions for the libuser.conf file	<p>Checkout the file.</p> <pre># rcstool co /etc/libuser.conf</pre> 
12. <input type="checkbox"/>	Edit the libuser.conf file	<p>Open the libuser.conf file and change the crypt style from md5 to sha12</p> <pre>#vi /etc/libuser.conf</pre> <ul style="list-style-type: none"> Current Line: <pre>crypt_style = md5</pre> Modified Line: <pre>crypt_style = sha512</pre> <p>NOTE: The line to edit is close to the top of the file.</p> <p>After setting the password, the passwords are now successfully encrypted and are using SHA512 (the strongest hash algorithm).</p>
13. <input type="checkbox"/>	Save the File	<ul style="list-style-type: none"> If the file required changing <pre>#rcstool ci /etc/libuser.conf</pre> If the file already was configured <pre>#rcstool unco /etc/libuser.conf</pre>

Software Upgrade Procedure

Step	Procedure	Result
14. <input type="checkbox"/>	Set the admusr and root passwords	<ul style="list-style-type: none">For root user <code>#passwd root</code>For admusr user: <code>#passwd admusr</code> <p>NOTE: After setting the password, the passwords are now successfully encrypted and are using SHA512 (the strongest hash algorithm).</p>
15. <input type="checkbox"/>	Verify	Logout of the current session and then login using the new password credentials.
THIS PROCEDURE HAS BEEN COMPLETED		

5. SOFTWARE UPGRADE CAUTIONS

Before upgrade, users must perform the system health check section. This check ensures that the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if upgrade can proceed with alarms.

****** WARNING ******

If the server being upgraded is not in a Normal state, the server should be brought to the Normal state before the upgrade process is started. [Normal state is generally determined by lack of alarms.]

****** WARNING ******

Please read the following notes on upgrade procedures:

Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:

- Session banner information such as *time* and *date*.
- System-specific configuration information such as *hardware locations*, *IP addresses*, and *hostnames*.
- ANY information marked with "XXXX" or "YYYY." Where appropriate, instructions are provided to determine what output should be expected in place of "XXXX or YYYY"
- Aesthetic differences unrelated to functionality such as browser attributes: *window size*, *colors*, *toolbars*, and *button layouts*.

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A check box should be provided. For procedures which are executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).

Captured data is required for future support reference if Oracle Technical Services is not present during the upgrade. Any CLI level windows should be logged.

6. UPGRADE CMP CLUSTERS (10.5 TO 12.1.2)

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

NOTE: If you are using Veritas NetBackup there are additional steps to perform before starting this procedure. See the Maintenance Operation Procedure (MOP) for the Netbackup.

6.1 Upgrade CMP Clusters Overview

1. Upgrade the primary CMP cluster
 - a. Use the CMP GUI—System Maintenance (10.5), to place Primary Standby CMP into Force-Standby state
 - b. Use the CMP GUI—System Maintenance (10.5), to upgrade the Primary Force-Standby CMP server
 - c. Use the CMP GUI—System Maintenance (10.5), to perform Switch Force-Standby on the Primary CMP cluster
 - d. Log back into the CMP GUI and upgrade the remaining Primary CMP Force-Standby server using the 12.1.2 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 CMP servers may be deployed as 2 georedundant 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.

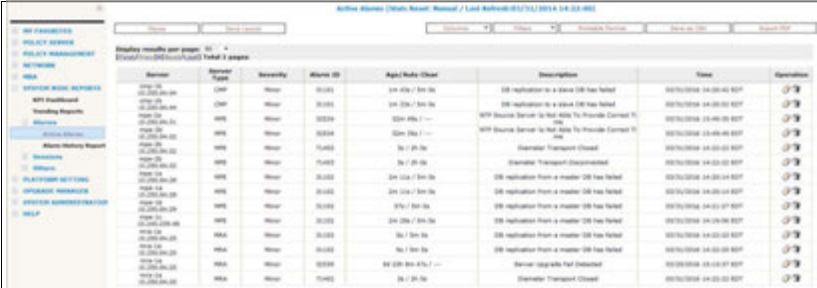
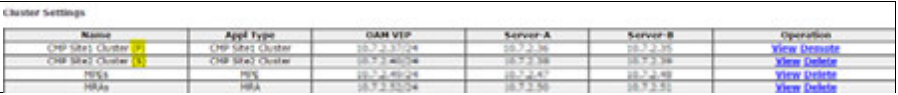
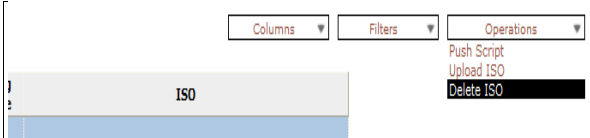
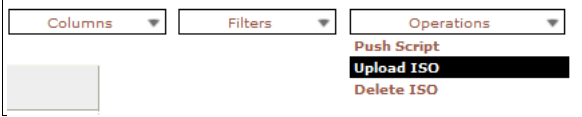
Identify the CMP sites to be upgraded here, and verify which site is the Primary and which site is the Secondary site:

CMP Sites Georedundant 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 Address_____		
Server-A Status _____		
Server-B Hostname _____		
Server-B IP Address_____		
Server-B Status _____		


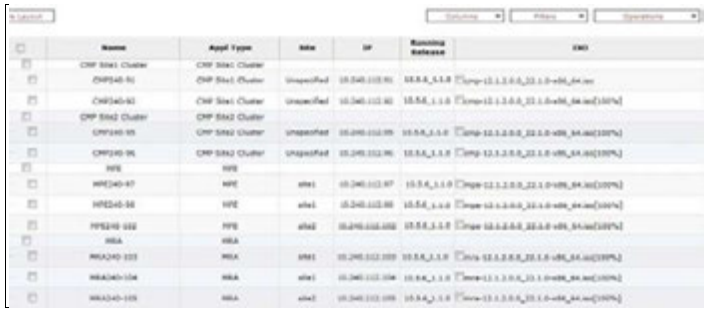
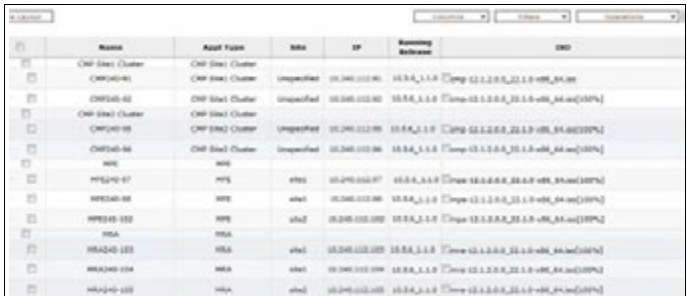
IMPORTANT:

- CMP servers **MUST** be upgraded first, before the MPE or MRA clusters
- 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. <input type="checkbox"/>	CMP GUI: Verify alarm status.	<p>Navigate to System Wide Reports → Alarms→Active Alarms</p> <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Identify and record the CMP clusters	<p>Navigate to Platform Setting→Topology Settings → All Clusters</p>  <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI Access into Primary CMP Server— Remove old ISO files from servers.	<p>Upgrade Manager → ISO Maintenance</p> <ol style="list-style-type: none"> 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.  <ol style="list-style-type: none"> Click OK to continue and wait until the successful deletion message appears Wait until the ISO Maintenance page is refreshes showing that the ISO column blank
4. <input type="checkbox"/>	CMP GUI: Distribute ISO files to CMP/MPE/MRA servers NOTE: This step depends on the ISO type. Distribute ISO files accordingly.	<p>Upgrade Manager → ISO Maintenance</p> <ol style="list-style-type: none"> (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 25. Select Operations→Upload ISO  <ol style="list-style-type: none"> Fill in the dialog with the following information: Mode: Select SCP

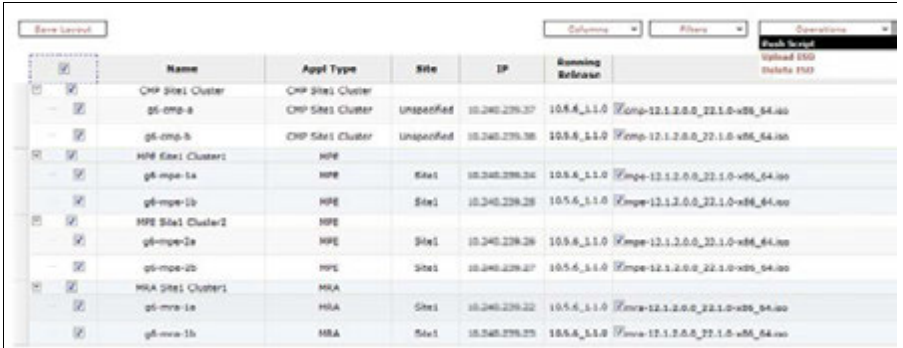
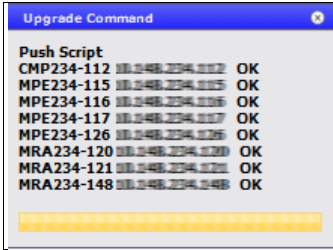

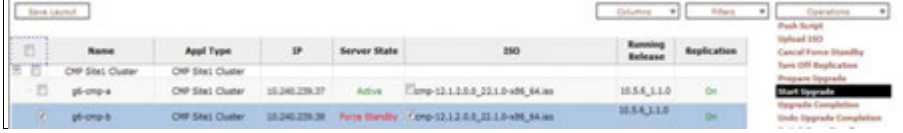
Software Upgrade Procedure

Step	Procedure	Result
		<p>ISO Server Hostname/IP: <IP_address_where_ISO_files_are_located></p> <p>User: root</p> <p>Password: <root_password_for_the_server></p> <p>Source ISO file full path: /var/TKLC/upgrade/</p>  <p>5. Click Add.</p> <p>When completed, the ISO column will be populated with the ISO filename and a notification of [100%]</p> 
5. <input type="checkbox"/>	CMP GUI: Verify ISO file distribution to all the servers	<p>Upgrade Manager → ISO Management</p> <ul style="list-style-type: none"> Verify that the release 12.1.2 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%] <p>NOTE: For those 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.</p> 
6. <input type="checkbox"/>	CMP GUI: Verify status of CMP clusters	<ol style="list-style-type: none"> Navigate to Upgrade Manager → System Maintenance Confirm the CMP clusters have the following: <ul style="list-style-type: none"> Active/Standby status Running release of 10.5 version Replication ON Release 12.1.2 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

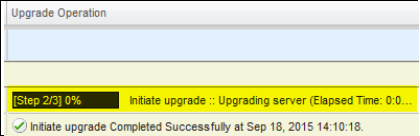
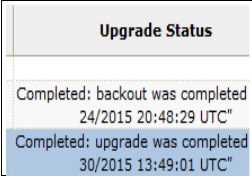
Software Upgrade Procedure

Step	Procedure	Result
7. <input type="checkbox"/>	SSH CLI Primary Active CMP: exchange keys	<p>Exchange keys to all servers from the Site 1 Active Primary CMP. Login as root user.</p> <ol style="list-style-type: none"> Login as root. <div data-bbox="706 289 1300 359" data-label="Text"> <pre>[root@derek local]# ssh root@10.113.0.31 root@10.113.0.31's password: </pre> </div> Exchange the keys. <div data-bbox="604 422 1347 627" data-label="Text"> <pre>mount -o loop /var/TKLC/upgrade/cmp-12.1.2.0.0_22.1.0-x86_64.iso /mnt/upgrade/ cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin cd / umount /mnt/upgrade qpSSHKeyProv.pl --prov --user=root</pre> </div> <div data-bbox="623 646 1386 772" data-label="Text"> <pre>Last login: Mon Apr 11 22:19:29 2016 from 10.182.167.137 [root@NEWTON-MR6-CMP-SA-A ~]# qpSSHKeyProv.pl --prov --user=root The password of root in topology: </pre> </div> <p>NOTE: You are required to enter the PASSWORD for user root</p> Verify that the Keys are exchanged successfully with all the server clusters. <div data-bbox="604 871 945 894" data-label="Text"> <pre>\$sudo qpSSHKeyProv.pl --check</pre> </div> <p>Example</p> <div data-bbox="604 955 1276 1457" data-label="Text"> <pre>Connecting to root@mpe-1c (10.250.zz.zz) ... Connecting to root@cmp-1b (10.250.xx.xx) ... Connecting to root@mra-1a (10.250.yy.y) ... [13/16] Provisioning SSH keys on mra-1b (10.250.ww.w) ... [14/16] Provisioning SSH keys on mra-1a (10.250.yy.yy) ... [15/16] Provisioning SSH keys on mpe-1c (10.250.zz.zz) ... [16/16] Provisioning SSH keys on cmp-1b (10.250.xx.xx) ... SSH keys are OK.</pre> </div>


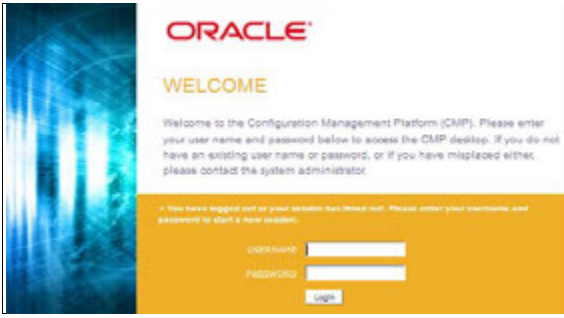
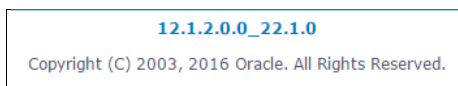
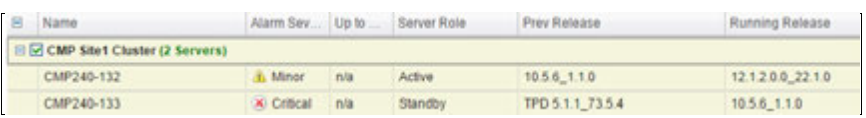
Software Upgrade Procedure

Step	Procedure	Result
8. <input type="checkbox"/>	CMP GUI: Push the release 12.1.2 upgrade scripts to all servers in the segment topology	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select all the servers in the topology as shown. Select Operations→Push Script. It is safe to run the push script multiple times as needed.  <ol style="list-style-type: none"> Click OK to continue the operation. <p>Operation successful.</p>  <p>NOTE: Give the push script a minute to complete</p>
9. <input type="checkbox"/>	CMP GUI: Set Force—Standby mode on the Standby CMP—Primary cluster	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select the checkbox for the Standby CMP Server at the Primary Site Select Operations→Force Standby.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The Standby CMP server state will be changed to Force Standby</p>
10. <input type="checkbox"/>	<p>CMP GUI: Upgrade the Force-Standby CMP server at the primary site</p> <p>NOTE: This will take approximately 40 minutes to complete.</p>	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select the Force-Standby CMP Server at the Primary Site. Select Operations→Start Upgrade.  <ol style="list-style-type: none"> Click OK to continue with the operation. <p>In the Upgrade Operation column, it will show the Progress bar along with the upgrade activities.</p>



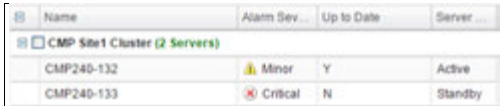
Software Upgrade Procedure

Step	Procedure	Result
		 <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server</p> <p><u>Expected Major Alarm</u></p> <p>31233 HA Path Down</p> <p><u>Expected Minor Alarms</u></p> <p>31114 DB replication over SOAP has failed 31106 Database merge to parent failure 31107 Database merge from child failure</p> <p>Wait until the 'upgrade was completed....' status message appears</p>  <p><i>IMPORTANT: If there is other status message appeared other than the '...upgrade was completed...' message, stop here and contact Oracle Technical Services to troubleshoot and determine if a rollback should be executed.</i></p>
11. <input type="checkbox"/>	CMP GUI: Verify that the upgrade completed successfully	<p>Upgrade Manager → System Maintenance</p> <p>Successful upgrade status will show release 12.1.2 in the Running Release and the Upgrade Status columns.</p> <p>NOTE: Expect the server state role to still shown as Force Standby—same as prior to the upgrade.</p> <p><i>IMPORTANT: Any Sync Broken indicator (🔌) signifies that the data replication between the two servers of the cluster is not synced yet. Do not continue if there is a Sync Broken indicator for the server that was upgraded.</i></p>
12. <input type="checkbox"/>	CMP GUI: Verify alarms	<p>System Wide Reports → Active Alarms</p> <p>Alarm(s) ID: 70025 QP Slave database is a different version than the master is expected. –The alarm will be cleared after the cluster is fully upgraded.</p>

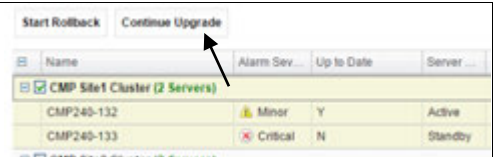
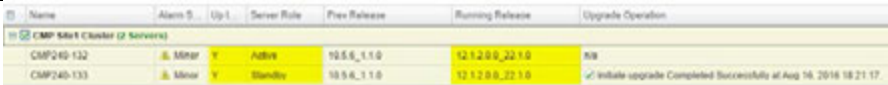
Software Upgrade Procedure

Step	Procedure	Result
13. <input type="checkbox"/>	CMP GUI: Switch the upgraded release 12.1.2 CMP server to Active	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select the checkbox for the CMP cluster to be switched—primary cluster only Select Operations → Switch ForceStandby  <ol style="list-style-type: none"> Click on OK to continue with the operation and a successful message appears. <p>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.</p> <ol style="list-style-type: none"> Close and re-open the browser.
14. <input type="checkbox"/>	CMP GUI: Login to the CMP server VIP	<ol style="list-style-type: none"> Close the current CMP GUI browser tab. Open another browser tab using the same CMP VIP address. <p>The Policy Management release 12.1.2 CMP GUI login form should appear as shown—login username and password credentials are the same as the pre-upgrade credentials.</p> 
15. <input type="checkbox"/>	CMP GUI: Verify new Policy Management release	<p>Navigate to Help→About. Verify the release displayed is 12.1.2</p> 
16. <input type="checkbox"/>	CMP GUI: Critical alarms	<p>The following alarm is seen until the SQL Database matches the master (12.1.2).</p> <ul style="list-style-type: none"> 70025 QP Slave database is a different version than the master 31101 Database replication to slave failure <p>These alarms are expected and will remain until all CMP servers are upgraded.</p> <p>NOTE: The Upgrade Manager will show the same alarms.</p>
17. <input type="checkbox"/>	CMP GUI: Verify the Policy Management release 12.1.2 CMP is Active	<p>Upgrade→Upgrade Manager</p>  <p>As noted, the active CMP server is now running release 12.1.2 and the new interface for Upgrade Director is now in effect.</p>

Software Upgrade Procedure

Step	Procedure	Result																				
18. <input type="checkbox"/>	Primary Active CMP: ssh to primary active CMP and copy iso to /var/camiant/iso	<div><div>1. Logon to the primary active CMP as admusr and copy the 12.1.2 ISO file to the /var/camiant/iso directory: <pre>\$sudo cp /var/TKLC/upgrade/cmp-12.1.2.iso /var/camiant/iso/</pre></div><div>2. Verify the copy by using the following command: <pre>\$ ls /var/camiant/iso/</pre></div></div>																				
19. <input type="checkbox"/>	CMP GUI: Locate the new 12.1.2 Upgrade Manual	<div><div>Upgrade → Upgrade Manager<div><div>1. Select the Current ISO. In this case it is labeled Install Kit.</div><div></div><div>This opens a dialog box that lists the contents of the /var/camiant/iso directory.</div><div>2. Highlight the ISO file and click the button located in the bottom right-hand corner of the window.</div><div></div><div>3. When the confirmation message appears, click OK.</div><div>Within a few seconds, the Up to date column transitions from n/a to Y (meaning up-to-date) or N (meaning needs upgrade).</div><div></div></div></div></div>																				
20. <input type="checkbox"/>	CMP GUI: New alarms introduced with 12.1.2	<div><div>The following minor alarms, along with the active critical alarm, will now be active.</div><div><table><thead><tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th></tr></thead><tbody><tr><td>Mar 12, 2015 09:22 AM EDT</td><td>Minor</td><td>70501</td><td>The Cluster is running different versions of software</td></tr><tr><td>Mar 12, 2015 09:22 AM EDT</td><td>Minor</td><td>70500</td><td>The system is running different versions of software</td></tr></tbody></table><div><table><thead><tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th></tr></thead><tbody><tr><td>Dec 15, 2015 09:58 AM EST</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td></tr></tbody></table></div></div></div>	Occurrence	Severity	Alarm ID	Text	Mar 12, 2015 09:22 AM EDT	Minor	70501	The Cluster is running different versions of software	Mar 12, 2015 09:22 AM EDT	Minor	70500	The system is running different versions of software	Occurrence	Severity	Alarm ID	Text	Dec 15, 2015 09:58 AM EST	Critical	70025	The MySQL slave has a different schema version than the master.
Occurrence	Severity	Alarm ID	Text																			
Mar 12, 2015 09:22 AM EDT	Minor	70501	The Cluster is running different versions of software																			
Mar 12, 2015 09:22 AM EDT	Minor	70500	The system is running different versions of software																			
Occurrence	Severity	Alarm ID	Text																			
Dec 15, 2015 09:58 AM EST	Critical	70025	The MySQL slave has a different schema version than the master.																			

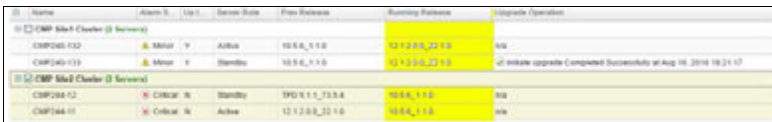
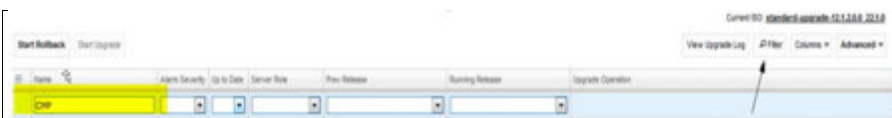
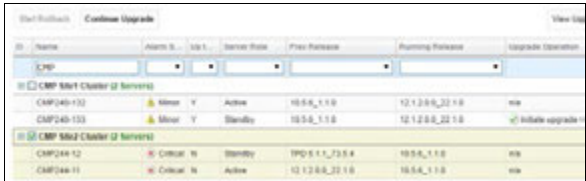
Software Upgrade Procedure

Step	Procedure	Result
21. <input type="checkbox"/>	<p>CMP GUI: Complete the upgrade of the Primary CMP cluster</p> <p>NOTE: The remaining CMP server upgrade will take approximately 40 minutes to complete.</p>	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the Primary Site 1 CMP cluster Click Continue Upgrade.  <ol style="list-style-type: none"> Click OK on the pop-up message to continue the upgrade on the remaining server in the CMP cluster <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>31233 HA Path Down 70004 QP Processes down for maintenance</p> <p><u>Expected Minor Alarms</u></p> <p>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</p>
22. <input type="checkbox"/>	<p>CMP GUI: Verify the status of upgraded CMP server.</p>	<p>Upgrade → Upgrade Manager</p>  <p>Successful upgrade status will show the following for both servers in the Primary CMP cluster:</p> <ul style="list-style-type: none"> 12.1.2 in the Running Release column for both server A √ in the Up to Date column Active/Standby <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical Alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>31233 HA Path Down</p>

Software Upgrade Procedure

Step	Procedure	Result
		70004 QP Processes down for maintenance Expected Minor Alarms 31114 DB replication over SOAP has failed 31106 Database merge to parent failure 31107 Database merge from child failure 31101 Database replication to slave failure 70503 Server Forced Standby 70507 Upgrade In Progress 70500 System Mixed Version 70501 Cluster Mixed Version
23. <input type="checkbox"/>	Proceed to next upgrade procedure	Verify the following information: <ul style="list-style-type: none"> Primary Site-1 is running release 12.1.2 Secondary Site, if applicable, is on release 10.5 All C Level Nodes will be on release 10.5 Proceed to the next procedure if there is a GR CMP to upgrade. If not, skip to section 10.
THIS PROCEDURE HAS BEEN COMPLETED		

6.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP cluster	Upgrade → Upgrade Manager <ul style="list-style-type: none"> Primary CMP is completely upgraded to 12.1.2 Secondary CMP cluster is on 10.5 
2. <input type="checkbox"/>	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.  <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP Server cluster at Site-2 Click Continue Upgrade.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.</p> <p>This will continue to upgrade the standby server only in the CMP cluster</p>

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

Expected Critical alarm

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

Expected Major Alarm

- 70004** QP Processes down for maintenance

Expected Minor Database Replication 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

LOG FILE from the GUI showing complete on the 1st server on the secondary site.

ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
6	6	PreFlight Check	8/16/2016 22:30:51	8/16/2016 22:31:06	0:00:14	Server	CMP244-12	Success	Manual	User initiated action
7	6	Initiate upgrade	8/16/2016 22:31:06	8/16/2016 23:09:07	0:38:01	Server	CMP244-12	Success	Autom.	Automatic action-initia
8	6	Modify the replication attr	8/16/2016 22:31:06	8/16/2016 22:31:08	0:00:01	Cluster	CMP Site2 Cluster	Success	Autom.	Automatic action for m
9	6	Start for replication to synchro	8/16/2016 23:09:07	8/16/2016 23:09:18	0:00:10	Server	CMP244-12	Success	Autom.	Automatic action wait

3. ☐ CMP GUI: Continue to upgrade 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 specific action will take a minute to complete. Wait until the upgraded server is active, as shown below.

ID	Name	Alarm Desc	Up To	Server Role	Prev Release	Running Release
CMP Site1 Cluster (2 Servers)						
CMP240-132	Minor	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	
CMP240-133	Minor	Y	Standby	10.5.6_1.1.0	12.1.2.0.0_22.1.0	
CMP Site2 Cluster (2 Servers)						
CMP244-12	Minor	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	
CMP244-11	Critical	N	Standby	12.1.2.0.0_22.1.0	10.5.6_1.1.0	

- 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 upgrading the remaining CMP *hostname*.

Software Upgrade Procedure

		 <p>6. Click OK to confirm and continue with the operation.</p> <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance</p> <p><u>Expected Minor Database Replication Alarms</u></p> <p>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</p>
4.	<input type="checkbox"/> CMP GUI: Verify that the upgrade completed successfully.	<p>Upgrade → Upgrade Manager</p> <p>Successful upgrade status will show release 12.1.2 in the Running Release and the Upgrade Operation columns.</p>
5.	<input type="checkbox"/> CMP GUI: Verify alarms	<p>System Wide Reports → Alarms → Active Alarms</p> <p>Following expected Minor Alarm ID:</p> <p>70500 System Mixed Version</p>
6.	<input type="checkbox"/> Procedure is complete.	<p>Verify the following information:</p> <ul style="list-style-type: none"> • All CMP clusters upgrades are complete and running release 12.1.2. • All MRA and MPE clusters are running release 10.5 • The Policy Management system is running in mixed-version mode.
THIS PROCEDURE HAS BEEN COMPLETED		

7. UPGRADE CMP CLUSTERS (11.5 TO 12.1.2)

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

7.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster
 - a. Use the CMP GUI—System Maintenance (11.5), to place Primary Standby CMP into Force-Standby
 - b. Use the CMP GUI—System Maintenance (11.5), to upgrade the Primary Force-Standby CMP server
 - c. Use the CMP GUI—System Maintenance (11.5), 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 12.1.2 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 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 Georedundant 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 Address _____

Server-A Status _____

Server-B Hostname _____

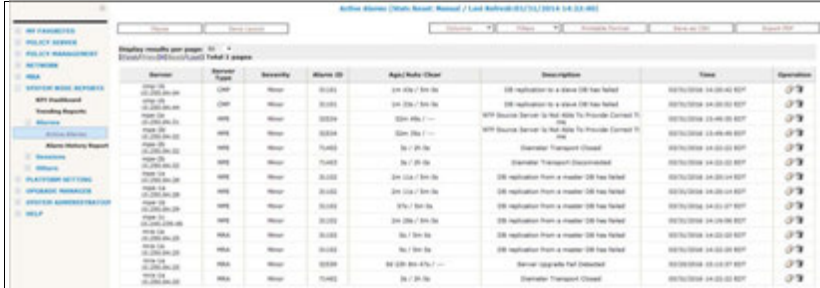
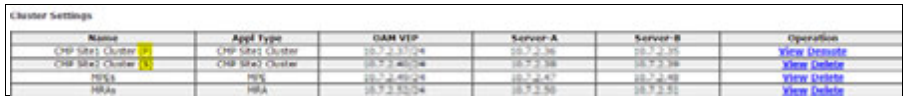
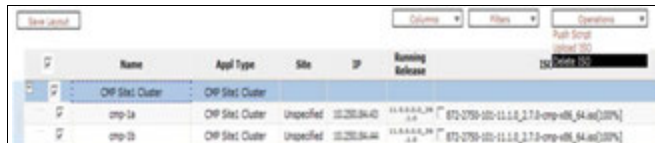
Server-B IP Address _____

Server-B Status _____

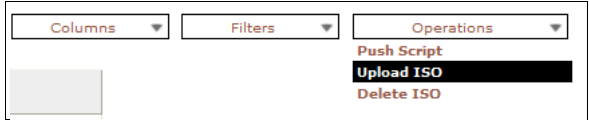

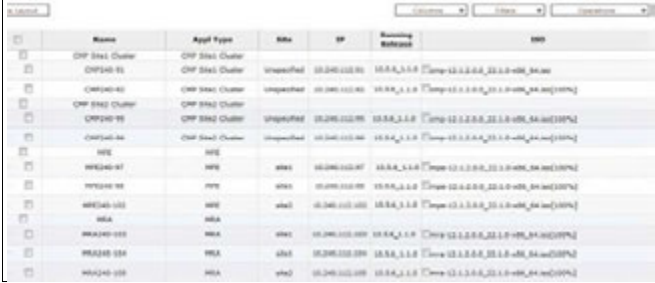
IMPORTANT:

- CMP servers **MUST** be upgraded first, before the MPE or MRA clusters
- Site-1 CMP **MUST** be upgraded to the new release first, before the Site-2 CMP(if applicable)

7.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify alarm status.	<p>System Wide Reports → Alarms→Active Alarms</p> <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Identify and record the CMP cluster(s)	<p>Navigate to Platform Setting→Topology Settings → All Clusters</p>  <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Verify status of CMP clusters	<p>Upgrade Manager → System Maintenance</p> <p>Confirm the CMP clusters have the following:</p> <ul style="list-style-type: none"> Active/Standby status Running release of 11.5 version Replication ON Release 12.1.2 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
4. <input type="checkbox"/>	CMP GUI Access into Primary CMP Server: Remove old ISO files from servers.	<p>Upgrade Manager → ISO Maintenance</p> <ol style="list-style-type: none"> Select the servers that show any old ISO files. Select the server cluster and select Operations→Delete ISO to delete the older ISO files.  <ol style="list-style-type: none"> Click OK to continue and 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. <input type="checkbox"/>	CMP GUI: Distribute ISO files to CMP/MPE/MRA servers	<p>Upgrade Manager → ISO Maintenance</p> <ol style="list-style-type: none"> (Optional but Preferred) Filter CMP/MPE/MRA servers One application at a time, select one server type (MPE, MRA, or CMP) to be

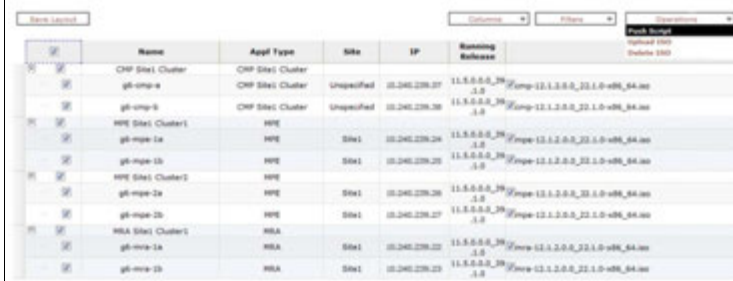
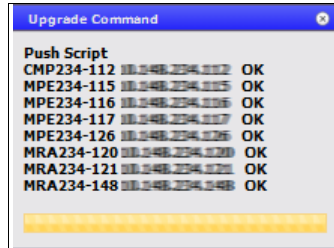
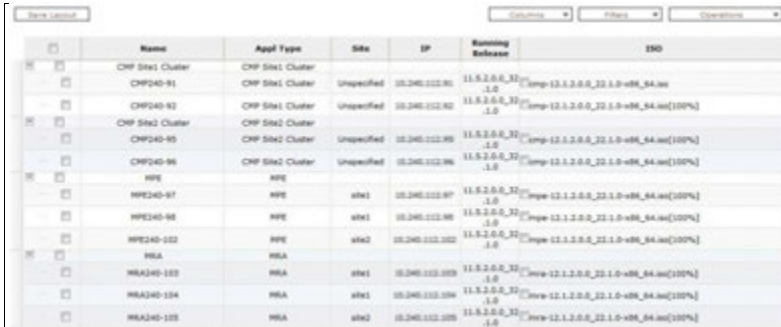
Software Upgrade Procedure

Step	Procedure	Result
	<p>NOTE: This step depends on the ISO file type. Distribute ISO files accordingly.</p>	<p>upgraded.</p> <p>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 25.</p> <p>3. Select Operations → Upload ISO</p>  <p>4. Fill in the dialog with the following information:</p> <p>Mode: Select SCP</p> <p>ISO Server Hostname/IP: <i><IP_address_where_ISO_files_are_located></i></p> <p>User: admusr</p> <p>Password: <i><admusr_password_for_the_server></i></p> <p>Source ISO file full path: <i>/var/TKLC/upgrade/</i></p>  <p>5. Click Add.</p> <p>When completed, the ISO column will be populated with the ISO filename and a notification of [100%]</p> 


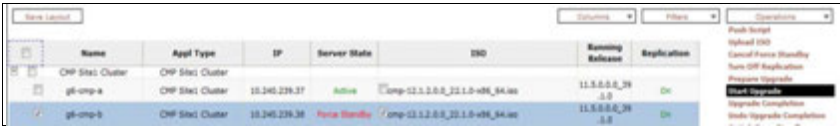
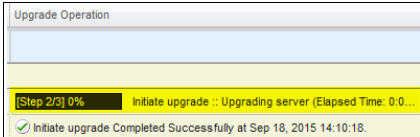
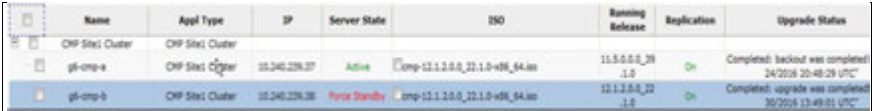
Software Upgrade Procedure

Step	Procedure	Result
6. <input type="checkbox"/>	SSH CLI Primary Active CMP: Exchange keys	<ol style="list-style-type: none"> Exchange keys to all servers from the site 1 Active Primary CMP. Login as admusr user. <pre>\$sudo mount -o loop /var/TKLC/upgrade/cmp-12.1.2.0.0_22.1.0-x86_64.iso /mnt/upgrade/</pre> <pre>\$sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin</pre> <pre>\$cd /</pre> <pre>\$sudo umount /mnt/upgrade</pre> <pre>\$sudo qpSSHKeyProv.pl --prov</pre> <pre>[admusr@cmp-1b upgrade]\$ sudo qpSSHKeyProv.pl --prov</pre> <pre>The password of admusr in topology:</pre> <p>NOTE: You are required to enter the PASSWORD for user admusr</p> Verify that the keys are exchanged successfully with all the server clusters. <pre>\$sudo qpSSHKeyProv.pl --check</pre> <p>EXAMPLE</p> <pre>Connecting to admusr@mpe-1c (10.250.zz.zz) ...</pre> <pre>Connecting to admusr@cmp-1b (10.250.xx.xx) ...</pre> <pre>Connecting to admusr@mra-1a (10.250.yy.y)</pre> <pre>...</pre> <pre>[13/16] Provisioning SSH keys on mra-1b (10.250.ww.w) ...</pre> <pre>[14/16] Provisioning SSH keys on mra-1a (10.250.yy.yy) ...</pre> <pre>[15/16] Provisioning SSH keys on mpe-1c (10.250.zz.zz) ...</pre> <pre>[16/16] Provisioning SSH keys on cmp-1b (10.250.xx.xx) ...</pre> <pre>SSH keys are OK.</pre>


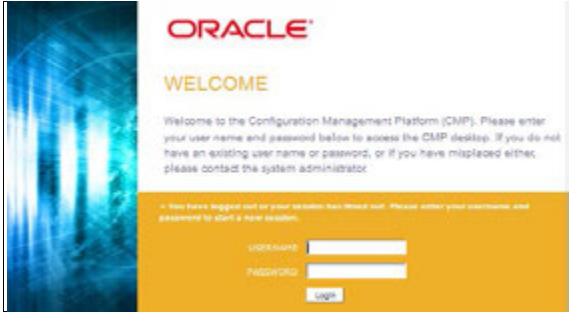
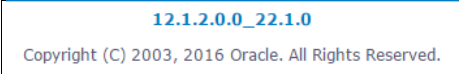
Software Upgrade Procedure

Step	Procedure	Result
7. <input type="checkbox"/>	CMP GUI: Push the release 12.1.2 upgrade scripts to all servers in the segment topology	<p>Upgrade Manager → ISO Maintenance</p> <ol style="list-style-type: none"> Select all the servers in the topology as shown in the figure. Select Operations→Push Script. <p>NOTE: It is safe to run the push script multiple times as needed)</p>  <ol style="list-style-type: none"> Click OK to continue the operation. <p>Operation successful.</p>  <p>NOTE: Give the push script a minute to complete</p>
8. <input type="checkbox"/>	CMP GUI: Verify ISO file distribution to all the servers	<p>Upgrade Manager → ISO Management</p> <ul style="list-style-type: none"> Verify that the release 12.1.2.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%] <p>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.</p> 


Software Upgrade Procedure

Step	Procedure	Result
9. <input type="checkbox"/>	CMP GUI: Set Force Standby mode on the Standby CMP in the Primary cluster	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select the checkbox for the Standby CMP Server at Primary Site Select Operations→Force Standby  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The Standby CMP server state will be changed to Force Standby.</p>
10. <input type="checkbox"/>	CMP GUI: Upgrade the Force-Standby CMP server at the primary site NOTE: This will take approximately 40 minutes to complete.	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Check Force-Standby CMP Server at the Primary Site. Select Operations→Start Upgrade.  <ol style="list-style-type: none"> Click OK to continue with the operation. <p>The Upgrade Operation column shows a progress bar along with the upgrade activities.</p>  <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server</p> <p><u>Expected Major Alarm</u></p> <p>31233 HA Path Down</p> <p><u>Expected Minor Alarms</u></p> <p>31114 DB replication over SOAP has failed 31106 Database merge to parent failure 31107 Database merge from child failure</p> <p>Wait until 'Completed: upgrade was completed...' appears in the Upgrade Status column</p>  <p>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.</p>


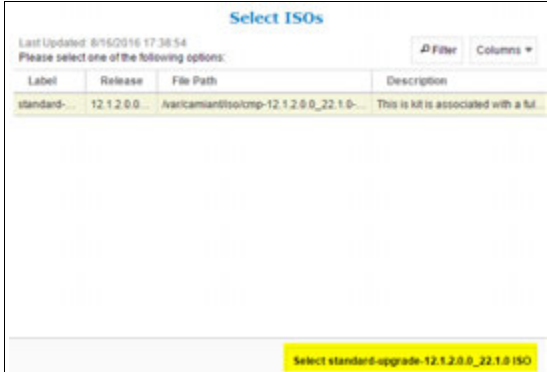
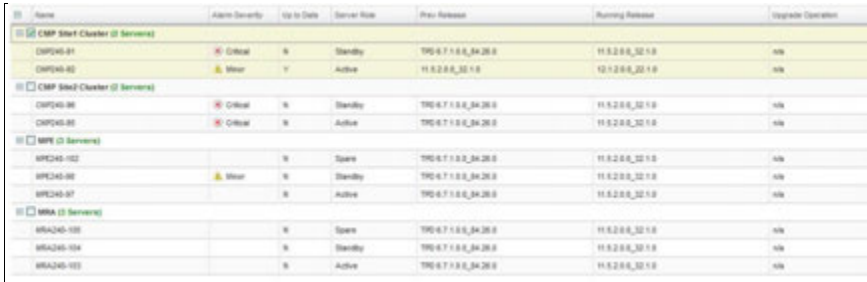
Software Upgrade Procedure

Step	Procedure	Result
11. <input type="checkbox"/>	CMP GUI: Verify that the upgrade completed successfully	<p>Upgrade Manager → System Maintenance</p> <ul style="list-style-type: none"> Successful upgrade status will show release 12.1.2 in the Running Release and Upgrade Operation columns. <p>NOTE: Expect the Server State column to show Force Standby. This is the same as the status prior to the upgrade.</p> <p>IMPORTANT: Any Sync Broken indicator (🔴) signifies that the data replication between the two servers of the cluster is not synced yet. Do not continue if there is a Sync Broken indicator on the server that was upgraded.</p>
12. <input type="checkbox"/>	CMP GUI: Verify alarms	<p>System Wide Reports → Active Alarms</p> <p>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.</p>
13. <input type="checkbox"/>	CMP GUI: Switch the upgraded release 12.1.2 CMP server to Active	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select the checkbox for the CMP cluster to be switched—primary cluster only, and Select Operations→Switch ForceStandby  <ol style="list-style-type: none"> Click OK to continue with the operation and a successful message appears. <p>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.</p> <ol style="list-style-type: none"> Close the browser and re-open.
14. <input type="checkbox"/>	CMP GUI: Login to the CMP server VIP	<p>Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address.</p> <p>The Policy Management release 12.1.2 CMP GUI login form should appear as shown—login username and password credentials are the same as the pre-upgrade.</p> 
15. <input type="checkbox"/>	CMP GUI: Verify new Policy Management release	<p>Navigate to Help→About. Verify the release displayed is 12.1.2</p> 

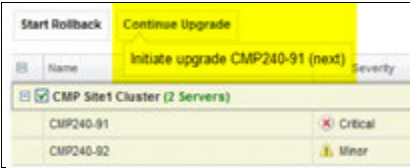
Software Upgrade Procedure

Step	Procedure	Result
16. <input type="checkbox"/>	CMP GUI: Critical alarms	<p>The following critical alarm will be seen until the SQL Database matches the master (12.1.2):</p> <p>70025 QP Slave database is a different version than the master</p> <p>The following minor alarm will also be seen:</p> <p>31101 Database replication to slave failure</p> <p>These alarms are expected and will remain until all CMPs have been upgraded to the same version.</p> <p>NOTE: The Upgrade Manager will show the same alarms.</p>
17. <input type="checkbox"/>	CMP GUI: Verify the Policy Management release 12.1.2 CMP is Active	<p>Upgrade → Upgrade Manager</p>  <p>As noted, the Active CMP server is now running release 12.1.2.</p>
18. <input type="checkbox"/>	Primary Active CMP: ssh to primary active CMP and copy iso to /var/camiant/iso	<p>5. Logon to the primary active CMP as admusr and copy the 12.1.2 ISO file to the /var/camiant/iso directory:</p> <pre>\$sudo cp /var/TKLC/upgrade/cmp-12.1.2.iso /var/camiant/iso/</pre> <p>6. Verify the copy by using the following command:</p> <pre>\$ls /var/camiant/iso/</pre>


Software Upgrade Procedure

Step	Procedure	Result												
19. <input type="checkbox"/>	CMP GUI: Locate the new 12.1.2 upgrade manual	<p>Upgrade → Upgrade Manager</p> <p>1. Select the Current ISO. In this case it is labeled Install Kit.</p> <div></div> <p>This will open a dialog box with a description of the ISO that was copied into /var/camiant/iso</p> <p>2. Highlight the ISO file and click the button located in the bottom right-hand corner of the window.</p> <div></div> <p>3. When the confirmation dialog displays, clickOK.</p> <p>Within a few seconds, the Up to Date column transitions from n/a to Y (meaning up-to-date) or N (meaning needs upgrade).</p> <div></div>												
20. <input type="checkbox"/>	CMP GUI: New alarms introduced with 12.1.2	<p>The following minor alarms, along with the already active critical alarms, will now be active.</p> <table><tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th></tr><tr><td>Mar 12, 2015 09:22 AM EDT</td><td>Minor</td><td>70501</td><td>The Cluster is running different versions of software</td></tr><tr><td>Mar 12, 2015 09:22 AM EDT</td><td>Minor</td><td>70500</td><td>The system is running different versions of software</td></tr></table>	Occurrence	Severity	Alarm ID	Text	Mar 12, 2015 09:22 AM EDT	Minor	70501	The Cluster is running different versions of software	Mar 12, 2015 09:22 AM EDT	Minor	70500	The system is running different versions of software
Occurrence	Severity	Alarm ID	Text											
Mar 12, 2015 09:22 AM EDT	Minor	70501	The Cluster is running different versions of software											
Mar 12, 2015 09:22 AM EDT	Minor	70500	The system is running different versions of software											


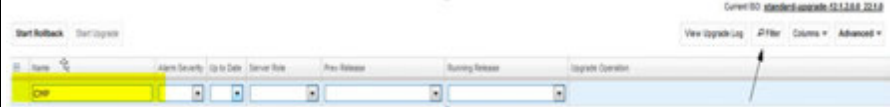
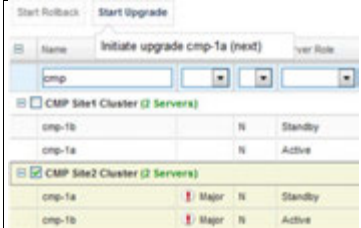
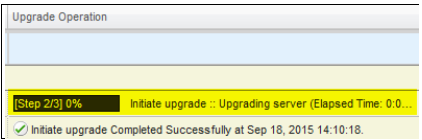
Software Upgrade Procedure

Step	Procedure	Result
21. <input type="checkbox"/>	<p>CMP GUI: Complete the upgrade of the Primary CMP cluster</p> <p>NOTE: Remaining CMP server will take approximately 40 minutes to complete.</p>	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the Primary Site 1 CMP cluster Click Continue Upgrade.  <ol style="list-style-type: none"> Click OK to continue the upgrade on the remaining server in the CMP cluster <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>31233 HA Path Down 70004 QP Processes down for maintenance</p> <p><u>Expected Minor Alarms</u></p> <p>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</p>


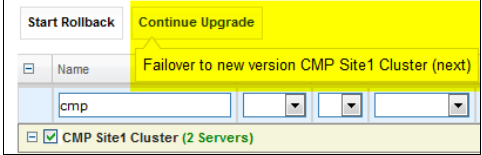

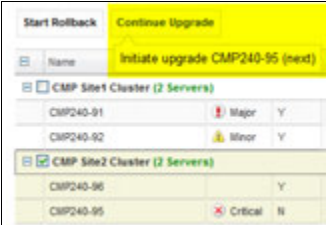
Software Upgrade Procedure

Step	Procedure	Result
22. <input type="checkbox"/>	CMP GUI: Verify the status of upgraded CMP server.	<p>Upgrade → Upgrade Manager</p>  <ul style="list-style-type: none"> • Successful upgrade status will show both servers running release 12.1.2 in the Running Release column. • Active/Standby state for both servers in the Primary CMP cluster. • Active alarms to NOTE <p><u>Expected Critical Alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarms</u></p> <p>31233 HA Path Down 70004 QP Processes down for maintenance</p> <p><u>Expected Minor Alarms</u></p> <p>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 70503 Server Forced Standby 70507 Upgrade In Progress 70500 System Mixed Version 70501 Cluster Mixed Version</p>
23. <input type="checkbox"/>	Proceed to next upgrade procedure	<p>Verify the following information:</p> <ul style="list-style-type: none"> • Primary Site-1 is running release 12.1.2 • Secondary site—if applicable, is on release 11.5 • All C level nodes will be on release 11.5 <p>Proceed to the next procedure if there is a georedundant CMP to upgrade. If not, skip to section 10</p>
THIS PROCEDURE HAS BEEN COMPLETED		

7.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP cluster	Upgrade → Upgrade Manager <ul style="list-style-type: none"> Primary CMP is completely upgraded to 12.1.2 Secondary CMP cluster is on 11.5 
2. <input type="checkbox"/>	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.  <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP Server cluster at Site-2 Click Start Upgrade.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.</p> <p>This will continue to upgrade the standby server only in the CMP cluster</p> <p>The Upgrade Operation column shows a progress bar along with the upgrade activities.</p>  <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events</p> <p>Expected Critical alarm</p> <p>31283 Lost Communication with server 70001 QP_procMgr failed 70025 QP Slave database is a different version than the master</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Database replication Alarms</p> <p>70503 Server Forced Standby 70507 Upgrade In Progress</p>

Software Upgrade Procedure

		<p> 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 </p> <p>LOG FILE from the GUI showing complete on the 1st server on the secondary site.</p> 
3.	<input type="checkbox"/> CMP GUI: Continue upgrade of the Secondary CMP cluster	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP Server cluster at Site-2 Click Continue Upgrade. Notice the message 'Failover to new version...'  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. The specific action will take a minute to complete. Wait until the upgraded server is active, as shown below.  <ol style="list-style-type: none"> 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.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. During the upgrade activities, the following alarms may be generated and considered normal reporting events. <p>Expected Critical alarm</p> <p> 31283 Lost Communication with server 70025 QP Slave database is a different version than the master </p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Database replication Alarms</p> <p> 70503 Server Forced Standby 70507 Upgrade In Progress </p>

Software Upgrade Procedure

		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
4. <input type="checkbox"/>	CMP GUI: Verify that the upgrade completed successfully.	Upgrade → Upgrade Manager Successful upgrade status will show the release 12.1.2 in the Running Release and the Upgrade Operation columns.
5. <input type="checkbox"/>	CMP GUI: Verify alarms	System Wide Reports → Alarms → Active Alarms The following Minor alarm is expected: 70500 System Mixed Version
6. <input type="checkbox"/>	Procedure is complete.	Verify the following information: <ul style="list-style-type: none"> • All CMP clusters upgrades are complete and running release 12.1.2. • All MRA and MPE clusters are running release 11.5 • The Policy Management system is running in mixed-version mode.
THIS PROCEDURE HAS BEEN COMPLETED		

8. UPGRADE CMP CLUSTERS (12.0 TO 12.1.2)

This procedure will upgrade the Site-1 CMP cluster first, and if needed, upgrade the Site-2 CMP cluster in a single maintenance window.

8.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster
 - a. Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 1
 - b. Start upgrade
 - c. Failover
 - d. Log back into the CMP GUI
 - e. Continue upgrade
2. Upgrade Secondary CMP cluster
 - a. Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2
 - b. Start upgrade
 - c. 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 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 Georedundant 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 Address _____

Server-A Status _____

Server-B Hostname _____

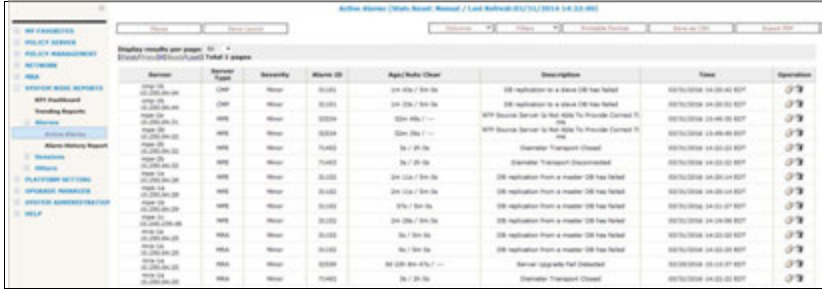
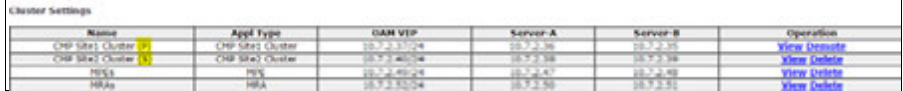
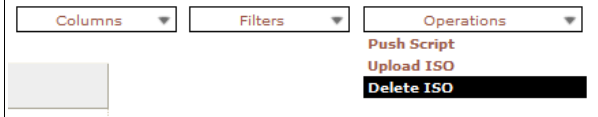
Server-B IP Address _____

Server-B Status _____



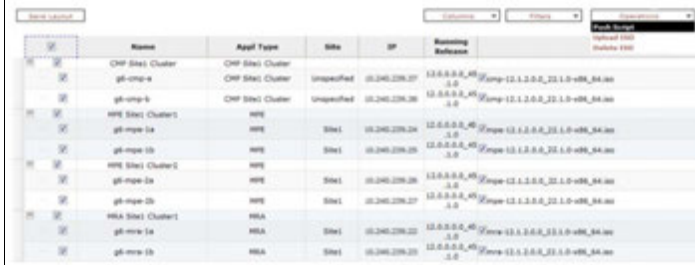
IMPORTANT:

- CMP servers **MUST** be upgraded first, before the MPE or MRA clusters
- Site-1 CMP **MUST** be upgraded to the new release first, before the Site-2 CMP

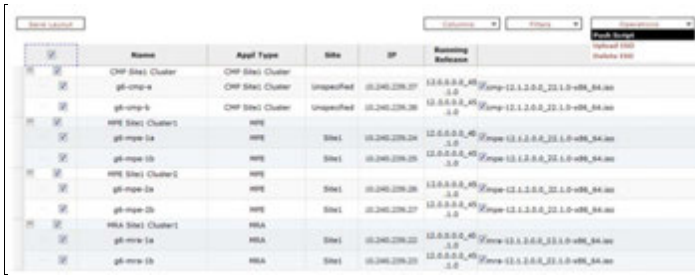
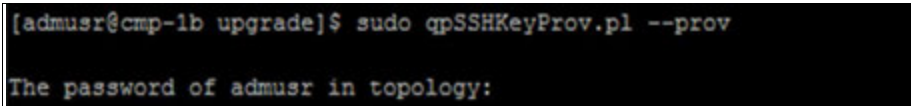
8.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify alarm status.	<p>System Wide Reports → Alarms→Active Alarms</p> <ul style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Identify and record the CMP cluster(s)	<p>Navigate to Platform Setting→Topology Settings → All Clusters</p>  <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP clusters	<p>Upgrade Manager → System Maintenance</p> <p>Confirm the CMP clusters have the following:</p> <ul style="list-style-type: none"> Active/Standby status Running release of 12.0.2 version Replication ON Release 12.1.2 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
4. <input type="checkbox"/>	CMP GUI Access into Primary CMP Server— Remove old ISO files from servers.	<p>Upgrade → ISO Maintenance</p> <ol style="list-style-type: none"> Select the servers that show old ISO files. Select the server cluster and select Operations →Delete ISO to remove any older ISO files.  <ol style="list-style-type: none"> Click OK to continue and wait until seeing the successful deletion message Wait until the ISO Maintenance page is refreshed and the ISO column will be blank.

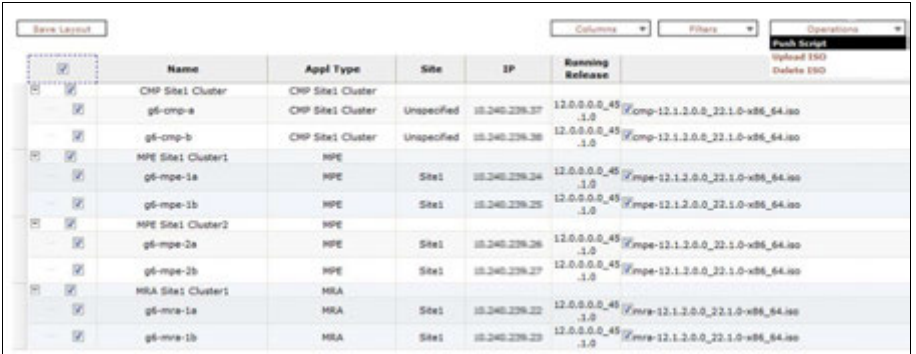
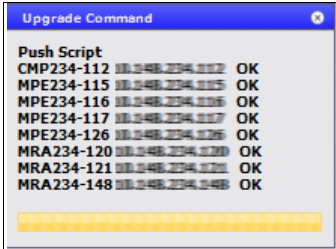
Software Upgrade Procedure

Step	Procedure	Result
5. <input type="checkbox"/>	<p>CMP GUI: Distribute ISO files to CMP/MPE/MRA servers</p> <p>NOTE: This step depends on the ISO file type. Distribute ISO files accordingly.</p>	<p>Upgrade → ISO Maintenance</p> <ol style="list-style-type: none"> (Optional but preferred) Filter CMP/MPE/MRA servers One application at a time, select one server type (MPE, MRA, or CMP) to be upgraded. <ul style="list-style-type: none"> 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 25. Select Operations → Upload ISO  <ol style="list-style-type: none"> Fill in the dialog with the following information: <ul style="list-style-type: none"> Mode: Select SCP ISO Server Hostname/IP: <i><IP_address_where_ISO_files_are_located></i> User: admusr Password: <i><admusr_password_for_the_server></i> Source ISO file full path: <i>/var/TKLC/upgrade/<server_type_iso_filename></i>  <ol style="list-style-type: none"> Click Add. <p>When completed, the ISO column will be populated with the ISO filename and a notification of [100%]</p> 

Software Upgrade Procedure

Step	Procedure	Result
6. <input type="checkbox"/>	CMP GUI: Verify ISO distribution to all the server	<p>Upgrade → ISO Management</p> <ul style="list-style-type: none"> Verify that the release 12.1.2 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%] <p>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.</p> 
7. <input type="checkbox"/>	SSH CLI Primary Active CMP: exchange keys	<ol style="list-style-type: none"> Exchange keys to all servers from the Site 1 Active Primary CMP. Login as admusr user. <pre>\$sudo qpSSHKeyProv.pl --prov</pre>  <p>NOTE: You are required to enter the PASSWORD for user admusr</p> Ensure that the Keys are exchanged successfully with all the server clusters. <pre>\$sudo qpSSHKeyProv.pl --check</pre> <p>EXAMPLE</p> <pre>Connecting to admusr@mpe-1c (10.250.zz.zz) ... Connecting to admusr@cmp-1b (10.250.xx.xx) ... Connecting to admusr@mra-1a (10.250.yy.y) ... [13/16] Provisioning SSH keys on mra-1b (10.250.ww.w) ... [14/16] Provisioning SSH keys on mra-1a (10.250.yy.yy) ... [15/16] Provisioning SSH keys on mpe-1c (10.250.zz.zz) ... [16/16] Provisioning SSH keys on cmp-1b (10.250.xx.xx) ... SSH keys are OK.</pre>

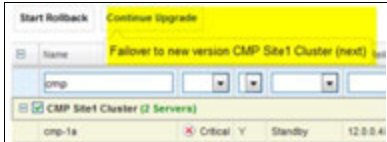
Software Upgrade Procedure

Step	Procedure	Result
8. <input type="checkbox"/>	CMP GUI: Push the release 12.1.2 upgrade scripts to all servers in the segment topology	<p>Upgrade Manager → System Maintenance</p> <ol style="list-style-type: none"> Select all the servers in the topology as shown. Select Operations→Push Script. It is safe to run the push script multiple times as needed.  <ol style="list-style-type: none"> Click OK to continue the operation. <p>Operation successful.</p>  <p>NOTE: Give the push script a minute to complete</p>
9. <input type="checkbox"/>	Primary Active CMP: ssh to primary active CMP and copy iso to /var/camiant/iso	<ol style="list-style-type: none"> Logon to the primary active CMP as admusr and copy the 12.1.2 ISO file to the /var/camiant/iso directory: <pre>\$sudo cp /var/TKLC/upgrade/cmp-12.1.2.iso /var/camiant/iso/</pre> Verify the copy by using the following command: <pre>\$ ls /var/camiant/iso/</pre>

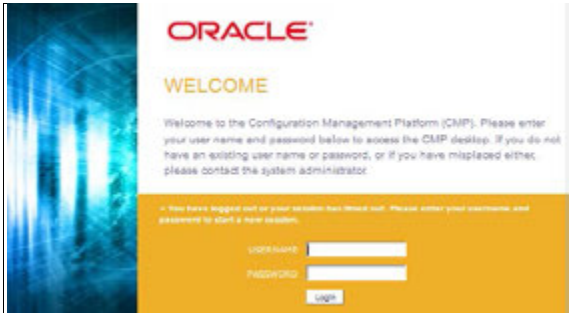
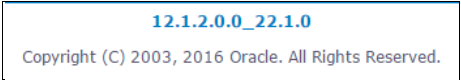



Software Upgrade Procedure

Step	Procedure	Result
10. <input type="checkbox"/>	CMP GUI: Locate the new 12.1.2 upgrade manual	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> 1. Select the Current ISO. In this case it is labeled Install Kit. <div data-bbox="626 285 1364 384" data-label="Image"> </div> <p>A dialog box with a description of the ISO file that was copied into the /var/camiant/iso directory opens.</p> 2. Highlight the ISO file and click the button located in the bottom right-hand corner of the window. <div data-bbox="722 533 1265 903" data-label="Image"> </div> 3. 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. <input type="checkbox"/>	CMP GUI: Upgrade Primary CMP cluster NOTE: This will take approximately 30 minutes to complete.	<p>Upgrade → Upgrade Manager</p> <p>NOTE: The Filter button can be used to show only the CMP servers. Enter in CMP in the Name field.</p> <div data-bbox="552 1150 1443 1262" data-label="Image"> </div> <ol style="list-style-type: none"> 1. Select the checkbox for the Primary CMP Server cluster 2. Click Start Upgrade. <div data-bbox="812 1352 1180 1463" data-label="Image"> </div> 3. 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. <div data-bbox="786 1680 1205 1816" data-label="Image"> </div> <p>Upgrade Operation will change to completed when done.</p>


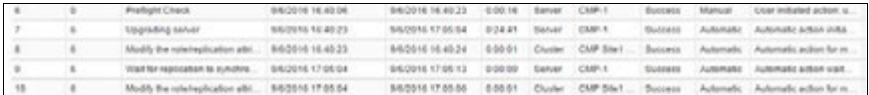

Software Upgrade Procedure

Step	Procedure	Result																																																	
		<p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 31227 HA availability status failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance</p> <p><u>Expected Minor Database replication Alarms</u></p> <p>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</p> <p>Upgrade is complete on the first CMP server in the cluster when the 'Completed successfully' message appears in the Upgrade Operation column.</p>																																																	
12. <input type="checkbox"/>	CMP GUI: Verify that the upgrade is successful	<p>Upgrade → Upgrade Manager</p> <p>View the cluster.</p> <p>Verify the following information:</p> <ul style="list-style-type: none">One server is on 12.1.2The other server in the cluster is on 12.0.The Up to Date column shows Y for the 12.1.2 server and N for the 12.0 server. <table><thead><tr><th>Name</th><th>Alarm Sev.</th><th>Up to</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr></thead><tbody><tr><td colspan="7">CMP Site1 Cluster (2 Servers)</td></tr><tr><td>CMP-2</td><td> Critical</td><td>Y</td><td>Standby</td><td>12.0.0.0_45.1.0</td><td>12.1.2.0_22.1.0</td><td> Initiate upgrade Co</td></tr><tr><td>CMP-1</td><td> Minor</td><td>N</td><td>Active</td><td>TFD 6.7.0.0_84.11.0</td><td>12.0.0.0_45.1.0</td><td>n/a</td></tr><tr><td colspan="7">CMP Site2 Cluster (2 Servers)</td></tr><tr><td>CMP-4</td><td></td><td>N</td><td>Standby</td><td>TFD 6.7.0.0_84.11.0</td><td>12.0.0.0_45.1.0</td><td>n/a</td></tr><tr><td>CMP-3</td><td></td><td>N</td><td>Active</td><td>TFD 6.7.0.0_84.11.0</td><td>12.0.0.0_45.1.0</td><td>n/a</td></tr></tbody></table>	Name	Alarm Sev.	Up to	Server Role	Prev Release	Running Release	Upgrade Operation	CMP Site1 Cluster (2 Servers)							CMP-2	Critical	Y	Standby	12.0.0.0_45.1.0	12.1.2.0_22.1.0	Initiate upgrade Co	CMP-1	Minor	N	Active	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a	CMP Site2 Cluster (2 Servers)							CMP-4		N	Standby	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a	CMP-3		N	Active	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a
Name	Alarm Sev.	Up to	Server Role	Prev Release	Running Release	Upgrade Operation																																													
CMP Site1 Cluster (2 Servers)																																																			
CMP-2	Critical	Y	Standby	12.0.0.0_45.1.0	12.1.2.0_22.1.0	Initiate upgrade Co																																													
CMP-1	Minor	N	Active	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a																																													
CMP Site2 Cluster (2 Servers)																																																			
CMP-4		N	Standby	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a																																													
CMP-3		N	Active	TFD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	n/a																																													
13. <input type="checkbox"/>	CMP GUI: Continue to upgrade CMP cluster	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none">Select the checkbox for the Primary CMP Server clusterClick Continue Upgrade. Notice the message 'Failover to new version...' <div></div> <ol style="list-style-type: none">Click OK to confirm and continue with the operation. <p>The specific action will take a minute to complete.</p>																																																	

Software Upgrade Procedure

Step	Procedure	Result
14. <input type="checkbox"/>	CMP GUI: Login to the CMP server VIP	<p>Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address.</p> <p>The Policy Management release 12.1.2 CMP GUI login form should appear as shown—login and password credentials are the same as the pre-upgrade.</p> 
15. <input type="checkbox"/>	CMP GUI: Verify new Policy Management release	<p>Navigate to Help→About. Verify the release displayed is 12.1.2</p> 
16. <input type="checkbox"/>	CMP GUI: Critical alarms	<p>Critical alarm 70025, QP Slave database is a different version than the master, is seen until the SQL Database matches the master (12.1.2). This alarm is expected and remains until all CMP servers are upgraded to the same version.</p> <p>Current Critical Alarms</p>  <p>Current Minor Alarms</p>  <p>NOTE: The Upgrade Manager will show alarms as well.</p>
17. <input type="checkbox"/>	CMP GUI: Verify the Policy Management release 12.1.2 CMP is Active	<p>Upgrade→Upgrade Manager</p> <p>Verify the following</p> <ul style="list-style-type: none"> Active server is running release 12.1.2 Standby server is on the previous release 


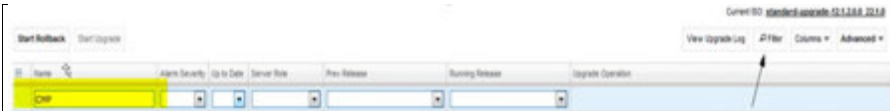
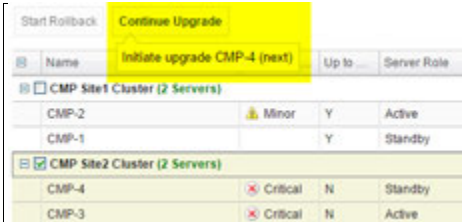
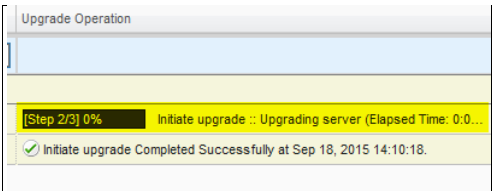
Software Upgrade Procedure

Step	Procedure	Result
18. <input type="checkbox"/>	<p>CMP GUI: Complete the upgrade of the Primary CMP cluster</p> <p>NOTE: Remaining CMP server will take approximately 30 minutes to complete.</p>	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Primary CMP Server cluster Click Continue Upgrade. Notice the message 'Initiate upgrade...' when hovering over the button.  <ol style="list-style-type: none"> Click OK to continue the upgrade on the remaining server in the CMP cluster <p>NOTE: The server that is being upgraded will go into an OOS state.</p> <p>Expected Critical alarm</p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Alarms</p> <p>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</p>
19. <input type="checkbox"/>	<p>CMP GUI: Tracking the upgrade complete</p>	<p>Upgrade → Upgrade Manager</p> <p>The last step in the upgrade for the first CMP cluster will be to wait for replication to complete.</p> <p>From the Upgrade tab:</p> 
20. <input type="checkbox"/>	<p>CMP GUI: Verify the status of upgraded CMP server.</p>	<p>Upgrade Manager → Upgrade Manager</p>  <p>Successful upgrade status will show the following for both servers in the Primary CMP cluster:</p> <ul style="list-style-type: none"> 12.1.2 in the Running Release column for both server A Y in the Up to Date column Active or Standby state for both servers in the Primary CMP cluster.

Software Upgrade Procedure

Step	Procedure	Result
21. <input type="checkbox"/>	Proceed to next upgrade procedure	<p>Verify the following information:</p> <ul style="list-style-type: none"> Primary Site-1 is running release 12.1.2 Secondary Site is on release 12.0 <p>Proceed to the next procedure to upgrade the secondary CMP cluster.</p>
THIS PROCEDURE HAS BEEN COMPLETED		

8.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	<p>CMP GUI: Verify status of CMP cluster</p>	<p>Upgrade → Upgrade Manager</p> <ul style="list-style-type: none"> Primary CMP is completely upgraded to 12.1.2 Secondary CMP cluster is on 12.0 
2. <input type="checkbox"/>	<p>CMP GUI: Upgrade Secondary CMP cluster</p> <p>NOTE: This will take approximately 30 minutes to complete.</p>	<p>Upgrade → Upgrade Manager</p> <p>NOTE: The Filter button can be used to show only the CMP servers. Enter CMP on the Name field.</p>  <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP Server cluster at Site-2 Click Continue Upgrade. When hovering over the button, it will read 'Initiate upgrade CMP-4 (next)'  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.</p> <p>This will continue to upgrade the standby server only in the CMP cluster</p> <p>The Upgrade Operation column shows a progress bar along with the upgrade activities.</p> 

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

Expected Critical alarm

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

Expected Major Alarm

- 70004** QP Processes down for maintenance

Expected Minor Alarms

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

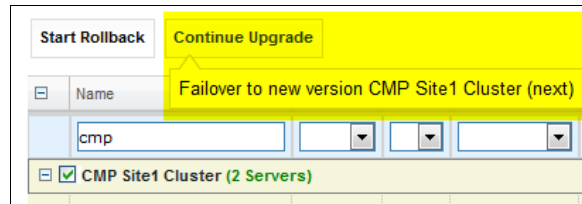
LOG FILE from the GUI showing complete on the 1st server on the secondary site.

740	0	initiate upgrade	9/26/2015 20:18:17	9/26/2015 20:18:11	0:00:14	Server	intg-cmp-10	Success	Manual	User initiated action: upgrade
741	740	upgrading server	9/26/2015 20:18:11	9/26/2015 20:18:12	0:00:01	Server	intg-cmp-10	Success	Automatic	Automatic action: initiate upgrade
742	740	Verify the replication attributes of the ...	9/26/2015 20:18:11	9/26/2015 20:18:15	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cl...
743	740	Wait for replication to synchronize	9/26/2015 20:18:15	9/26/2015 20:18:17	0:00:10	Server	intg-cmp-10	Success	Automatic	Automatic action: wait for replicat...

3. ☐ **CMP GUI: Continue upgrade of the Secondary CMP cluster**

Upgrade → Upgrade Manager

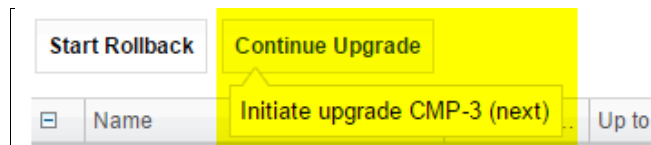
1. Select the checkbox for the Secondary CMP Server cluster at Site-2
2. Click **Continue Upgrade**. Notice the message 'Failover to new version CMP Site 1'



3. Click **OK** to confirm and continue with the operation.
The specific action will take a minute to complete. Wait until the upgraded server is active, as shown below.

Name	Alarm Sev...	Up to ...	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
CMP-2	Minor	Y	Active	12.0.0.0_45.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully
CMP-1		Y	Standby	12.0.0.0_45.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully
CMP Site2 Cluster (2 Servers)						
CMP-4		Y	Active	12.0.0.0_45.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully
CMP-3	Critical	N	Standby	TPD 6.7.0.0_84.11.0	12.0.0.0_45.1.0	na

4. Select the checkbox for the Secondary CMP Server cluster at Site-2
5. Click **Continue Upgrade**. When hovering over the button, the message will display the next action, which is upgrading the remaining CMP.



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

Software Upgrade Procedure

		<p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance</p> <p><u>Expected Minor Alarms</u></p> <p>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</p>
4. <input type="checkbox"/>	CMP GUI: Verify that the upgrade completed successfully.	<p>Upgrade → Upgrade Manager</p> <p>Successful upgrade status will show release 12.1.2 in the Running Release column and the Upgrade Operation.</p> <p>Also, under Upgrade Operation it will show 'Initiate Upgrade Completed Successfully' with the correct date and time.</p>
5. <input type="checkbox"/>	CMP GUI: Verify alarms	<p>System Wide Reports → Alarms → Active Alarms</p> <p><u>Expected Minor Alarms</u></p> <p>70500 System Mixed Version</p>
6. <input type="checkbox"/>	Procedure is complete.	<p>Verify the following information:</p> <ul style="list-style-type: none"> • All CMP clusters upgrades are complete and running release 12.1.2. • All MRA and MPE clusters are running release 12.0 • The Policy Management system is running in mixed-version mode.
THIS PROCEDURE HAS BEEN COMPLETED		

9. UPGRADE CMP CLUSTERS (12.1.1 TO 12.1.2)

This procedure will upgrade the Site-1 CMP cluster first, and if needed, upgrade the Site-2 CMP cluster in a single maintenance window.

9.1 Upgrade CMP Clusters Overview

1. Upgrade Primary CMP cluster
 - a. Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 1
 - b. Start upgrade
 - c. Failover
 - d. Log back into the CMP GUI
 - e. Continue upgrade
2. Upgrade Secondary CMP cluster
 - a. Use the CMP GUI, **Upgrade → Upgrade Manager** and upgrade the CMP Secondary Site 2
 - b. Start upgrade
 - c. 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 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.

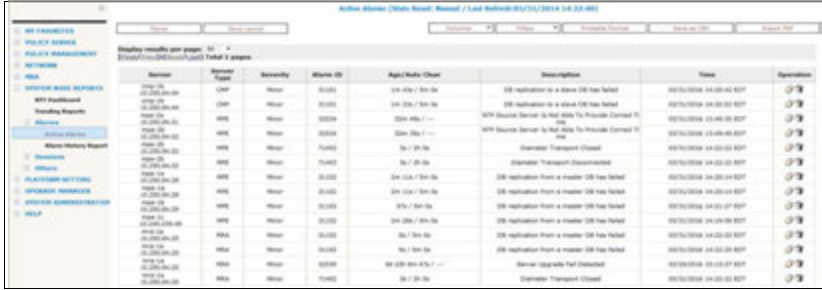
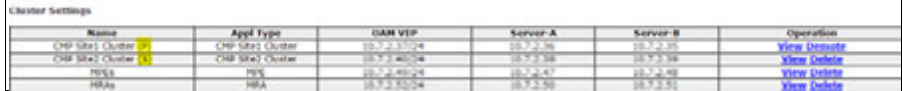
Identify the CMP sites to be upgraded, and verify which site is the Primary site and which site is the Secondary site:

CMP Sites Georedundant 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 Address _____		
Server-A Status _____		
Server-B Hostname _____		
Server-B IP Address _____		
Server-B Status _____		

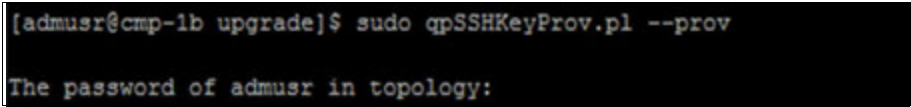
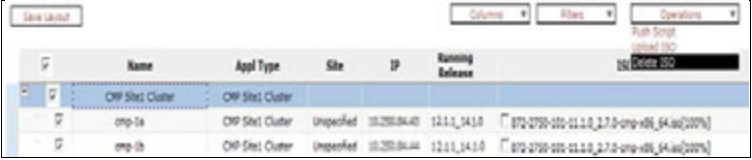
IMPORTANT:

- CMP servers **MUST** be upgraded first, before the MPE or MRA clusters
- Site-1 CMP **MUST** be upgraded to the new release first, before the Site-2 CMP

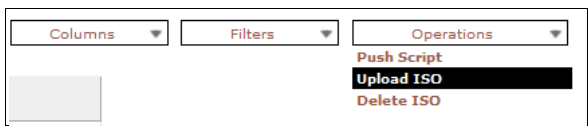



9.1.1 Upgrade Primary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify alarm status.	<p>System Wide Reports → Alarms→Active Alarms</p> <ul style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Identify and record the CMP cluster(s)	<p>Navigate to Platform Setting→Topology Settings → All Clusters</p>  <ol style="list-style-type: none"> 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. <input type="checkbox"/>	CMP GUI: Verify status of CMP clusters	<p>Upgrade → Upgrade Manager</p> <p>Confirm the CMP clusters have the following:</p> <ul style="list-style-type: none"> Active/Standby status Running release of 12.1.1version Release 12.1.2 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


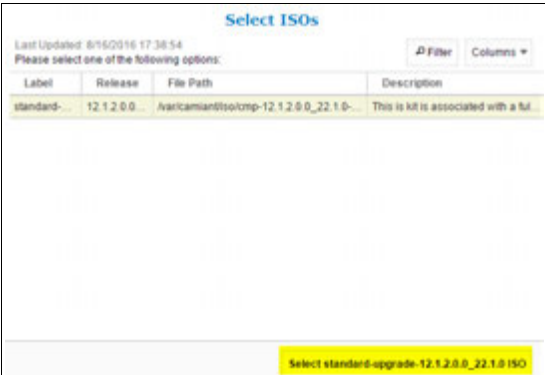
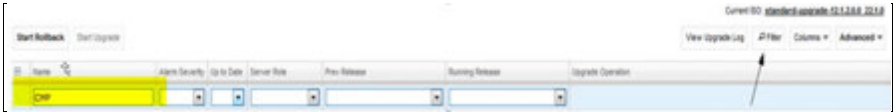

Software Upgrade Procedure

Step	Procedure	Result
4. <input type="checkbox"/>	SSH CLI Primary Active CMP: Exchange keys	<ol style="list-style-type: none"> Exchange keys to all servers from the Site 1 Active Primary CMP. Login as admusr user. <pre>\$sudo qpSSHKeyProv.pl --prov</pre>  <p>NOTE: You are required to enter the PASSWORD for user admusr</p> Ensure that the Keys are exchanged successfully with all the server clusters. <pre>\$sudo qpSSHKeyProv.pl --check</pre> <p>EXAMPLE</p> <pre>Connecting to admusr@mpe-1c (10.250.zz.zz) ... Connecting to admusr@cmp-1b (10.250.xx.xx) ... Connecting to admusr@mra-1a (10.250.yy.y) ... [13/16] Provisioning SSH keys on mra-1b (10.250.ww.w) ... [14/16] Provisioning SSH keys on mra-1a (10.250.yy.yy) ... [15/16] Provisioning SSH keys on mpe-1c (10.250.zz.zz) ... [16/16] Provisioning SSH keys on cmp-1b (10.250.xx.xx) ... SSH keys are OK.</pre>
5. <input type="checkbox"/>	CMP GUI Access into Primary CMP Server—Remove old ISO files from servers.	<p>Upgrade → ISO Maintenance</p> <ol style="list-style-type: none"> Select the servers that show old ISO files. Select the server cluster and select Operations → Delete ISO to remove any older ISO files.  <ol style="list-style-type: none"> Click OK to continue and wait until seeing the successful deletion message. Wait until the ISO Maintenance page is refreshed and the ISO column will be blank.

Software Upgrade Procedure

Step	Procedure	Result
6. <input type="checkbox"/>	<p>CMP GUI: Distribute ISO files to CMP/MPE/MRA servers</p> <p>NOTE: This step depends on the ISO file type. Distribute ISO files accordingly.</p>	<p>Upgrade → ISO Maintenance</p> <ol style="list-style-type: none"> (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 25. Select Operations → Upload ISO  <ol style="list-style-type: none"> 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>  <ol style="list-style-type: none"> Click Add. <p>When completed, the ISO column will be populated with the ISO filename and a notification of [100%]</p> 
7. <input type="checkbox"/>	<p>CMP GUI: Verify ISO distribution to all the server</p>	<p>Upgrade → ISO Management</p> <ul style="list-style-type: none"> Verify that the release 12.1.2 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%] <p>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.</p> 

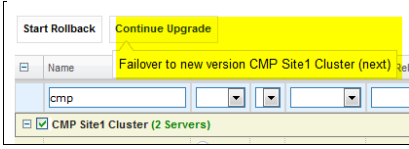
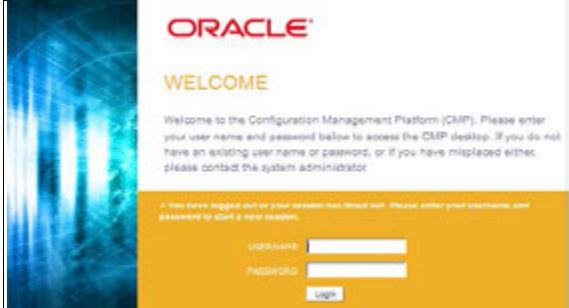
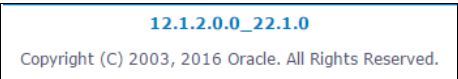


Software Upgrade Procedure

Step	Procedure	Result
8. <input type="checkbox"/>	Primary Active CMP: ssh to primary active CMP and copy iso to /var/camiant/iso directory	<p>Logon to the primary active CMP as admusr and copy the 12.1.2 ISO file to the following directory:</p> <pre>/var/camiant/iso</pre> <pre>\$sudo cp /var/TKLC/upgrade/cmp-12.1.2.iso /var/camiant/iso/</pre> <p>Verify the copy by using the following command:</p> <pre>\$ ls /var/camiant/iso/</pre>
9. <input type="checkbox"/>	CMP GUI: Locate the new 12.1.2 Upgrade Manager	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the Current ISO. In this case it is labeled Install Kit.  <p>A dialog box with a description of the ISO that was copied into /var/camiant/iso directory opens.</p> Highlight the ISO file and click the button located in the bottom right-hand corner of the window.  When the confirmations message displays, click OK. <p>Within a few seconds, the Up to Date column transition from Y (meaning up-to-date) or N (meaning needs upgrade).</p>
10. <input type="checkbox"/>	CMP GUI: Upgrade Primary CMP cluster NOTE: This will take approximately 30 minutes to complete.	<p>Upgrade → Upgrade Manager</p> <p>NOTE: The Filter button can be used to show only the CMP servers. Enter in CMP in the Name field.</p>  <ol style="list-style-type: none"> Select the checkbox for the Primary CMP Server cluster Click Continue Upgrade.  Click OK to confirm and continue with the operation. <p>The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.</p>

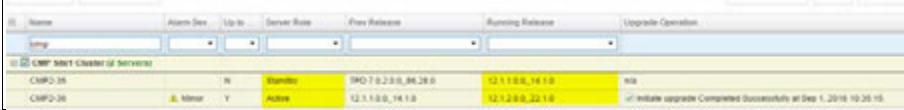
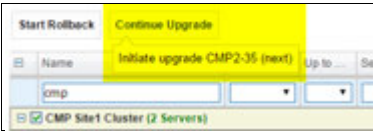

Software Upgrade Procedure

Step	Procedure	Result																																																																
		<p>This will continue to upgrade the standby server only in the CMP cluster</p> <p>The Upgrade Operation column shows a progress bar along with the upgrade activities.</p> <div><div>Upgrade Operation</div><div><div>[Step 2/3] 0%</div><div>Initiate upgrade :: Upgrading server (Elapsed Time: 0:0...</div><div>Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:18.</div></div></div> <p>Upgrade Operation column will change to completed when done.</p> <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 31227 HA availability status failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance</p> <p><u>Expected Minor Database replication Alarms</u></p> <p>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</p> <p>Upgrade is complete on the first CMP server in the cluster when the 'Completed successfully' message appears in the Upgrade Operation column.</p>																																																																
11. <input type="checkbox"/>	CMP GUI: Verify the upgrade is successful	<p>Upgrade → Upgrade Manager</p> <p>View the cluster.</p> <p>Verify the following information:</p> <ul style="list-style-type: none">One server is on 12.1.2Other server in the cluster is on 12.1.The Up to Date column shows Y for the 12.1.2 server and N for the 12.1.1server. <table><thead><tr><th>ID</th><th>Name</th><th>Alarm Sev</th><th>Up to</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr></thead><tbody><tr><td colspan="8">CMP</td></tr><tr><td colspan="8">CMP Site1 Cluster (2 Servers)</td></tr><tr><td></td><td>CMP2-35</td><td>Minor</td><td>N</td><td>Active</td><td>TPD 7.0.2.0.0_86.28.0</td><td>12.1.1.0.0_14.1.0</td><td>n/a</td></tr><tr><td></td><td>CMP2-36</td><td></td><td>Y</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.1.2.0.0_22.1.0</td><td>Initiate upgrade Completed Successfully</td></tr><tr><td colspan="8">CMP Site2 Cluster (2 Servers)</td></tr><tr><td></td><td>CMP2-38</td><td></td><td>N</td><td>Standby</td><td>TPD 7.0.2.0.0_86.28.0</td><td>12.1.1.0.0_14.1.0</td><td>n/a</td></tr><tr><td></td><td>CMP2-39</td><td></td><td>N</td><td>Active</td><td>TPD 7.0.2.0.0_86.28.0</td><td>12.1.1.0.0_14.1.0</td><td>n/a</td></tr></tbody></table>	ID	Name	Alarm Sev	Up to	Server Role	Prev Release	Running Release	Upgrade Operation	CMP								CMP Site1 Cluster (2 Servers)									CMP2-35	Minor	N	Active	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a		CMP2-36		Y	Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully	CMP Site2 Cluster (2 Servers)									CMP2-38		N	Standby	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a		CMP2-39		N	Active	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a
ID	Name	Alarm Sev	Up to	Server Role	Prev Release	Running Release	Upgrade Operation																																																											
CMP																																																																		
CMP Site1 Cluster (2 Servers)																																																																		
	CMP2-35	Minor	N	Active	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a																																																											
	CMP2-36		Y	Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_22.1.0	Initiate upgrade Completed Successfully																																																											
CMP Site2 Cluster (2 Servers)																																																																		
	CMP2-38		N	Standby	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a																																																											
	CMP2-39		N	Active	TPD 7.0.2.0.0_86.28.0	12.1.1.0.0_14.1.0	n/a																																																											

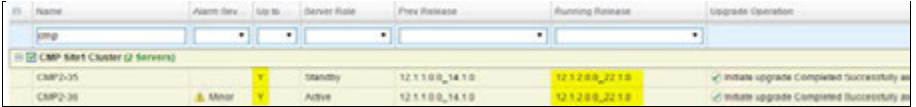
Software Upgrade Procedure

Step	Procedure	Result
12. <input type="checkbox"/>	CMP GUI: Continue upgrade of the CMP cluster	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Primary CMP Server cluster Click Continue Upgrade. Notice the message 'Failover to new version CMP Site 1'  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. <p>The specific action will take a minute to complete.</p>
13. <input type="checkbox"/>	CMP GUI: Log into the CMP server VIP	<p>Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address.</p> <p>The Policy Management release 12.1.2 CMP GUI login form should appear as shown—login and password credentials are the same as the pre-upgrade.</p> 
14. <input type="checkbox"/>	CMP GUI: Verify new Policy Management release	<p>Navigate to Help→About. Verify the release displayed is 12.1.2</p> 
15. <input type="checkbox"/>	CMP GUI: Critical alarms	<p>Critical alarm 70025, QP Slave database is a different version than the master, is seen until the SQL Database matches the master (12.1.2). This alarm is expected and remains until all CMP servers are upgraded to the same version.</p>  <p>Current Minor Alarms</p>  <p>NOTE: The Upgrade Manager will show alarms as well.</p>


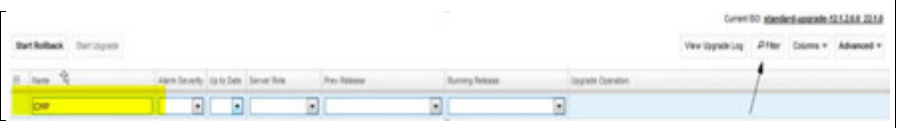
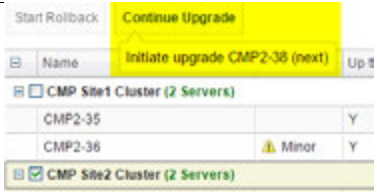
Software Upgrade Procedure

Step	Procedure	Result
16. <input type="checkbox"/>	CMP GUI: Verify the Policy Management release 12.1.2 CMP is Active	Upgrade→Upgrade Manager Verify the following <ul style="list-style-type: none"> Active server is on running release 12.1.2 Standby server is on the previous release 
17. <input type="checkbox"/>	CMP GUI: Complete the upgrade of the Primary CMP cluster NOTE: Remaining CMP server will take approximately 30 minutes to complete.	Upgrade → Upgrade Manager <ol style="list-style-type: none"> Select the checkbox for the Primary CMP Server cluster Click Continue Upgrade. When hovering over the button, the message displays the next action, which is to initiate the upgrade of the remaining CMP.  Click OK to continue the upgrade on the remaining server in the CMP cluster NOTE: Server getting upgraded will go OOS <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
18. <input type="checkbox"/>	CMP GUI: Tracking the upgrade complete	Upgrade → Upgrade Manager The last step in the upgrade for the first CMP cluster is to wait for the replication to complete. From the Upgrade tab: 

Software Upgrade Procedure

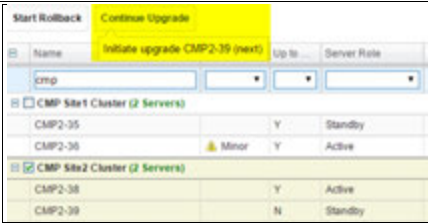
Step	Procedure	Result
19. <input type="checkbox"/>	CMP GUI: Verify the status of upgraded CMP server.	Upgrade → Upgrade Manager Successful upgrade status will show the following for the servers in the Primary CMP cluster: <ul style="list-style-type: none"> • Successful upgrade status will show both servers running release 12.1.2 in the Running Release column and Y for both servers in the Up to Date column • Active/standby state for both servers in the Primary CMP cluster. 
20. <input type="checkbox"/>	Proceed to next upgrade procedure	Verify the following information: <ul style="list-style-type: none"> • Primary Site-1 is running release 12.1.2 • Secondary site is on release 12.0 Proceed to the next procedure to upgrade the secondary CMP cluster.
THIS PROCEDURE HAS BEEN COMPLETED		

9.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP cluster	Upgrade → Upgrade Manager <ul style="list-style-type: none"> • Primary CMP is completely upgraded to 12.1.2 • Secondary CMP cluster is on 12.1 
2. <input type="checkbox"/>	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.  <ol style="list-style-type: none"> 1. Select the checkbox for the Secondary CMP Server cluster at Site-2 2. Click the Continue Upgrade.  <ol style="list-style-type: none"> 3. Click OK to confirm and continue with the operation. <p>The specific action taken will be determined by the Upgrade Manager and based on the specific version change being performed.</p> <p>This will continue to upgrade the standby server only in the CMP cluster</p>

		<p>The Upgrade Operation column shows a progress bar along with the upgrade activities.</p> <div><div>Upgrade Operation</div><div><div>Step 2/3 0%</div><div>Initiate upgrade :: Upgrading server (Elapsed Time: 0.0...</div></div><div>Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:18.</div></div> <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events:</p> <p>Expected Critical alarm</p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Alarms</p> <p>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</p> <p>LOG FILE from the GUI showing complete on the 1st server on the secondary site.</p> <table><tr><th>ID</th><th>TS</th><th>MsgType</th><th>MsgText</th><th>MsgTime</th><th>MsgDate</th><th>MsgFrom</th><th>MsgTo</th><th>MsgStatus</th><th>MsgAction</th><th>MsgComment</th></tr><tr><td>740</td><td>0</td><td>MsgTypeCheck</td><td>9/20/2015 20:10:17</td><td>9/20/2015 20:10:17</td><td>0 00:14</td><td>Server</td><td>9/20/2015-18</td><td>Success</td><td>Manual</td><td>User initiated action: upgrade/ser...</td></tr><tr><td>741</td><td>740</td><td>Upgrading server</td><td>9/20/2015 20:10:17</td><td>9/20/2015 20:10:17</td><td>0 00:15</td><td>Server</td><td>9/20/2015-18</td><td>Success</td><td>Automatic</td><td>Automatic action: upgrade/ser...</td></tr><tr><td>742</td><td>740</td><td>Verify the replication attributes of the...</td><td>9/20/2015 20:10:17</td><td>9/20/2015 20:10:17</td><td>0 00:17</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td><td>Automatic action for managing cl...</td></tr><tr><td>743</td><td>740</td><td>Wait for replication to synchronize</td><td>9/20/2015 20:10:17</td><td>9/20/2015 20:10:17</td><td>0 00:18</td><td>Server</td><td>9/20/2015-18</td><td>Success</td><td>Automatic</td><td>Automatic action: wait/replica...</td></tr></table>	ID	TS	MsgType	MsgText	MsgTime	MsgDate	MsgFrom	MsgTo	MsgStatus	MsgAction	MsgComment	740	0	MsgTypeCheck	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:14	Server	9/20/2015-18	Success	Manual	User initiated action: upgrade/ser...	741	740	Upgrading server	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:15	Server	9/20/2015-18	Success	Automatic	Automatic action: upgrade/ser...	742	740	Verify the replication attributes of the...	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:17	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cl...	743	740	Wait for replication to synchronize	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:18	Server	9/20/2015-18	Success	Automatic	Automatic action: wait/replica...	
ID	TS	MsgType	MsgText	MsgTime	MsgDate	MsgFrom	MsgTo	MsgStatus	MsgAction	MsgComment																																																
740	0	MsgTypeCheck	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:14	Server	9/20/2015-18	Success	Manual	User initiated action: upgrade/ser...																																																
741	740	Upgrading server	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:15	Server	9/20/2015-18	Success	Automatic	Automatic action: upgrade/ser...																																																
742	740	Verify the replication attributes of the...	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:17	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cl...																																																
743	740	Wait for replication to synchronize	9/20/2015 20:10:17	9/20/2015 20:10:17	0 00:18	Server	9/20/2015-18	Success	Automatic	Automatic action: wait/replica...																																																
3.	<div><input type="checkbox"/></div> <div>CMP GUI: Continue Upgrade Secondary CMP cluster</div>	<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none">Select the checkbox for the Secondary CMP Server cluster at Site-2Click Continue Upgrade. Notice the message 'Failover to new version CMP Site 1' <div><div>Start Rollback</div><div>Continue Upgrade</div><div>Failover to new version CMP Site1 Cluster (next)</div><div>cmp</div><div><input checked="" type="checkbox"/> CMP Site1 Cluster (2 Servers)</div></div> <ol style="list-style-type: none">Click OK to confirm and continue with the operation. <p>This action takes some time to complete. Wait until the upgraded server is active, as shown below.</p> <table><tr><th>ID</th><th>Name</th><th>Alarm Date</th><th>Up To</th><th>Service State</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Op</th></tr><tr><td colspan="8">CMP Site1 Cluster (2 Servers)</td></tr><tr><td>CMP0-05</td><td></td><td></td><td></td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.1.2.0.0_13.1.0</td><td>Initiate upg</td></tr><tr><td>CMP0-06</td><td></td><td></td><td></td><td>Active</td><td>12.1.1.0.0_14.1.0</td><td>12.1.2.0.0_13.1.0</td><td>Initiate upg</td></tr><tr><td colspan="8">CMP Site2 Cluster (2 Servers)</td></tr><tr><td>CMP0-05</td><td></td><td></td><td></td><td>Active</td><td>12.1.1.0.0_14.1.0</td><td>12.1.2.0.0_13.1.0</td><td>Initiate upg</td></tr><tr><td>CMP0-06</td><td></td><td></td><td></td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.1.2.0.0_13.1.0</td><td>Initiate upg</td></tr></table> <ol style="list-style-type: none">Select the checkbox for the Secondary CMP Server cluster at Site-2Click Continue Upgrade. When hovering over the Continue Upgrade button, the message will display the next action, which is upgrading the remaining CMP.	ID	Name	Alarm Date	Up To	Service State	Prev Release	Running Release	Upgrade Op	CMP Site1 Cluster (2 Servers)								CMP0-05				Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg	CMP0-06				Active	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg	CMP Site2 Cluster (2 Servers)								CMP0-05				Active	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg	CMP0-06				Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg
ID	Name	Alarm Date	Up To	Service State	Prev Release	Running Release	Upgrade Op																																																			
CMP Site1 Cluster (2 Servers)																																																										
CMP0-05				Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg																																																			
CMP0-06				Active	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg																																																			
CMP Site2 Cluster (2 Servers)																																																										
CMP0-05				Active	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg																																																			
CMP0-06				Standby	12.1.1.0.0_14.1.0	12.1.2.0.0_13.1.0	Initiate upg																																																			

Software Upgrade Procedure

		 <p>6. Click OK to confirm and continue with the operation.</p> <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>31283 Lost Communication with server 70001 QP_procmgr failed 70025 QP Slave database is a different version than the master</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance</p> <p><u>Expected Minor Alarms</u></p> <p>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</p>
4. <input type="checkbox"/>	CMP GUI: Verify that the upgrade completed successfully.	<p>Upgrade → Upgrade Manager</p> <ul style="list-style-type: none"> Successful upgrade status will show release 12.1.2 in the Running Release and Upgrade Operation columns. In the Upgrade Operation column, the message 'Initiate Upgrade Completed Successfully...' with the correct date and time is shown.
5. <input type="checkbox"/>	CMP GUI: Verify alarms	<p>System Wide Reports → Alarms → Active Alarms</p> <p><u>Expected Minor Alarms</u></p> <p>70500 System Mixed Version</p>
6. <input type="checkbox"/>	Procedure is complete.	<p>Verify the following information:</p> <ul style="list-style-type: none"> All CMP clusters upgrades are complete and running release 12.1.2. All MRA and MPE clusters are running release 12.1.1 The Policy Management system is running in mixed-version mode.
THIS PROCEDURE HAS BEEN COMPLETED		

10. MPE AND/OR MRA UPGRADE

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

NOTES:

- An upgrade of up to 4 clusters can be running at the same time.
- MPE and MRA clusters can be upgraded at the same time.

10.1 Upgrade Preparation

10.1.1 Configuration Preparation

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Access into CMP server	Use the supported browser to login as the admin user or as a user with administrative privileges.
2. <input type="checkbox"/>	CMP GUI: Verify current Upgrade Manager status and software release 12.1.2 ISO files	Upgrade → Upgrade Manager <ul style="list-style-type: none">• 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 12.1.2 ISO files are available for all CMP, MPE, and MRA clusters. One ISO per Server• Verify that the CMP cluster is upgraded successfully and running Policy Management release 12.1.2
THIS PROCEDURE HAS BEEN COMPLETED		

Software Upgrade Procedure

10.2 Upgrade MRA and MPE Servers

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

This procedure is applicable for a 10.5, 11.5, 12.0, or 12.1.1 upgrade to 12.1.2.

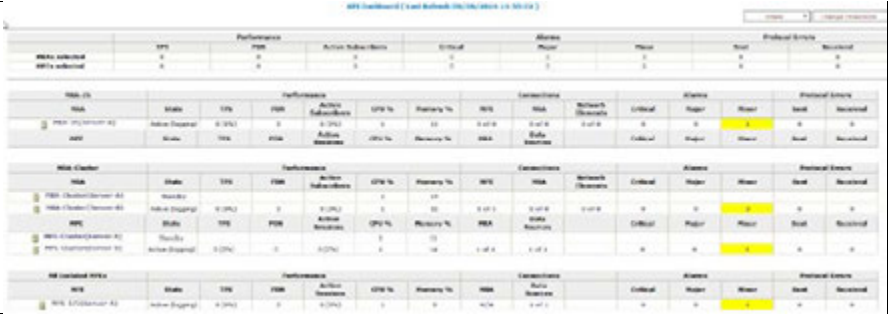
This section can be replicated for each site/segment to be upgraded, allowing you to add cluster and site specific information.

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

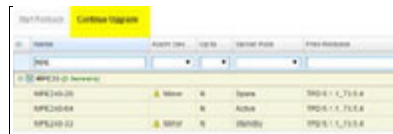
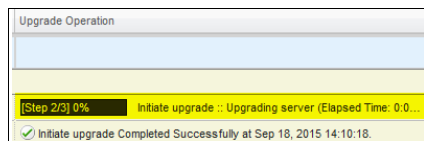
1. Select and start upgrade on a cluster using the CMP Upgrade Manager.
2. Failover one cluster at a time
3. Re-apply configuration one cluster at a time
4. Continue to upgrade the spare server
5. Continue upgrade on remaining server
6. (MPE only) Re-apply configuration one MPE cluster at a time

NOTES:

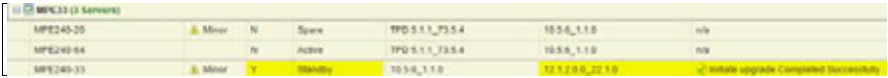

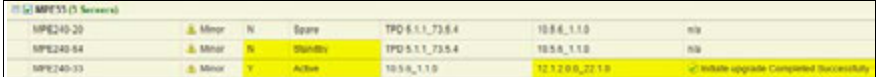
- All CMP clusters must be upgraded to Policy Management release 12.1.2 prior to executing the following procedures.
- Four (4) clusters can be running the upgrade at one time.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 12.1.2.

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Health Checks on the MPE/MRA servers to be upgraded	<p>Perform the following:</p> <ol style="list-style-type: none"> 1. Check for current Active Alarms 2. Reset MPE/MRA counters to make a baseline <ul style="list-style-type: none"> - For the MPE: Policy Server→Configuration→<server_name>→Reports → Reset Counters - For the MRA: MRA→Configuration→<server_name>→Reports → Reset Counters 3. Go to the KPI Dashboard and capture a screenshot. System Wide Reports → KPI Dashboard 


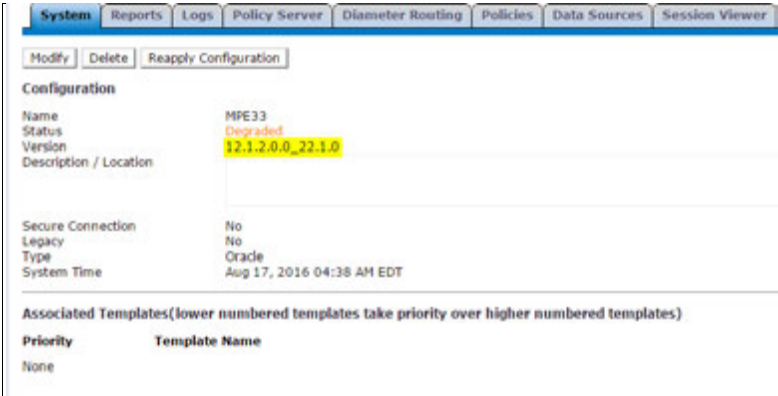
Software Upgrade Procedure

Step	Procedure	Result																																																																																																									
2. <input type="checkbox"/>	CMP GUI: Verify upgrade status of selected MPE/MRA site/segment	Upgrade → Upgrade Manager Verify information for the MRAs/MPE servers: <ul style="list-style-type: none">Current release 10.5, 11.5, 12.0, or 12.1.1 installedActive/Standby/Spare statusISO version to be deployed is 12.1.2.Verify the current ISO files are 12.1.2 by going to Upgrade→ISO Maintenance <table border="1"><thead><tr><th></th><th>Name</th><th>Appl Type</th><th>Site</th><th>IP</th><th>Running Release</th><th>ISO</th></tr></thead><tbody><tr><td></td><td>CMP Site1 Cluster</td><td>CMP Site1 Cluster</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>CMP240-132</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.148.240.132</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>CMP240-133</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.148.240.133</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>CMP Site2 Cluster</td><td>CMP Site2 Cluster</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>CMP244-11</td><td>CMP Site2 Cluster</td><td>Unspecified</td><td>10.148.244.11</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>CMP244-12</td><td>CMP Site2 Cluster</td><td>Unspecified</td><td>10.148.244.12</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MPE33</td><td>MPE</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>MPE240-33</td><td>MPE</td><td>site1</td><td>10.148.240.33</td><td>10.5.6_1.1.0</td><td>mpe-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MPE240-64</td><td>MPE</td><td>site1</td><td>10.148.240.64</td><td>10.5.6_1.1.0</td><td>mpe-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MPE240-20</td><td>MPE</td><td>site2</td><td>10.148.240.20</td><td>10.5.6_1.1.0</td><td>mpe-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MRA270</td><td>MRA</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>MRA240-70</td><td>MRA</td><td>site1</td><td>10.148.240.70</td><td>10.5.6_1.1.0</td><td>mra-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MRA240-166</td><td>MRA</td><td>site1</td><td>10.148.240.166</td><td>10.5.6_1.1.0</td><td>mra-12.1.2.0.0_22.1.0-x86_64.iso</td></tr><tr><td></td><td>MRA240-28</td><td>MRA</td><td>site2</td><td>10.148.240.28</td><td>10.5.6_1.1.0</td><td>mra-12.1.2.0.0_22.1.0-x86_64.iso</td></tr></tbody></table>		Name	Appl Type	Site	IP	Running Release	ISO		CMP Site1 Cluster	CMP Site1 Cluster						CMP240-132	CMP Site1 Cluster	Unspecified	10.148.240.132	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso		CMP240-133	CMP Site1 Cluster	Unspecified	10.148.240.133	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso		CMP Site2 Cluster	CMP Site2 Cluster						CMP244-11	CMP Site2 Cluster	Unspecified	10.148.244.11	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso		CMP244-12	CMP Site2 Cluster	Unspecified	10.148.244.12	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso		MPE33	MPE						MPE240-33	MPE	site1	10.148.240.33	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso		MPE240-64	MPE	site1	10.148.240.64	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso		MPE240-20	MPE	site2	10.148.240.20	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso		MRA270	MRA						MRA240-70	MRA	site1	10.148.240.70	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso		MRA240-166	MRA	site1	10.148.240.166	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso		MRA240-28	MRA	site2	10.148.240.28	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso
	Name	Appl Type	Site	IP	Running Release	ISO																																																																																																					
	CMP Site1 Cluster	CMP Site1 Cluster																																																																																																									
	CMP240-132	CMP Site1 Cluster	Unspecified	10.148.240.132	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	CMP240-133	CMP Site1 Cluster	Unspecified	10.148.240.133	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	CMP Site2 Cluster	CMP Site2 Cluster																																																																																																									
	CMP244-11	CMP Site2 Cluster	Unspecified	10.148.244.11	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	CMP244-12	CMP Site2 Cluster	Unspecified	10.148.244.12	12.1.2.0.0_22.1.0	cmp-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MPE33	MPE																																																																																																									
	MPE240-33	MPE	site1	10.148.240.33	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MPE240-64	MPE	site1	10.148.240.64	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MPE240-20	MPE	site2	10.148.240.20	10.5.6_1.1.0	mpe-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MRA270	MRA																																																																																																									
	MRA240-70	MRA	site1	10.148.240.70	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MRA240-166	MRA	site1	10.148.240.166	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
	MRA240-28	MRA	site2	10.148.240.28	10.5.6_1.1.0	mra-12.1.2.0.0_22.1.0-x86_64.iso																																																																																																					
3. <input type="checkbox"/>	CMP GUI: Upgrade clusters NOTE: 4 clusters can be running the upgrade process at one time. NOTE: The upgrade of a single server takes approximately 40 minutes to complete.	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 1. Select the checkbox for the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click Continue Upgrade  3. 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. Expected Critical Alarms 31283 Lost Communication with server 70001 QP_procmgr failed 31227 HA availability status failed Expected Major Alarm 70004 QP Processes down for maintenance Expected Minor Alarms 70503 Server Forced Standby																																																																																																									


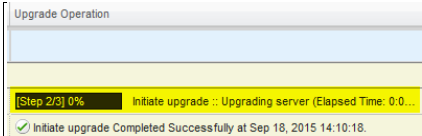
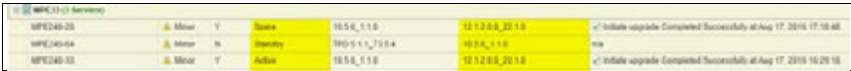
Software Upgrade Procedure

Step	Procedure	Result
		<p> 70507 Upgrade In Progress 70500 System Mixed Version 70501 Cluster Mixed Version 31114 DB replication over SOAP has failed 31106 Database merge to parent failure 31107 Database merge from child failure 31101 Database replication to slave failure 31282 HA Management Fault 78001 Rsync Failed </p> <p>Upgrade is complete on the first server in the cluster when the 'Completed Successfully' message appears in the Upgrade Operation column. The server will go back to Standby state when the upgrade completes.</p>  <p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p>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:</p> <p>Expected Minor Alarms</p> <p> 78001 Rsync Failed 70500 System Mixed Version 70501 Cluster Mixed Version 70503 Server Forced Standby </p>
4. <input type="checkbox"/>	<p>CMP GUI: Continue to upgrade the MRA/MPE clusters. Next operation is a failover</p> <p>NOTE: 4 clusters can be running the upgrade process at one time.</p>	<p>Fail over ONE cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster.</p> <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the cluster (one cluster at a time) (can be an MRA or MPE) Click Continue Upgrade. When hovering over the button, it will say 'Failover to new version...'  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will start to failover the cluster. <p>Wait until failover completes before failing over the next cluster, this will take a minute or two to complete. Verify the 12.1.2 server is now active. The process is complete when there is an active/standby at site 1 and spare at site 2.</p> 

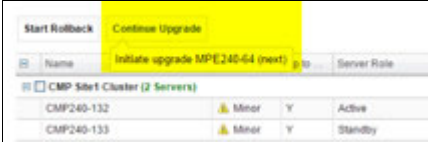
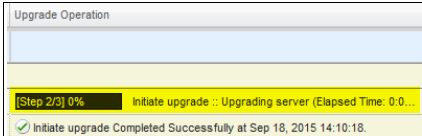
Software Upgrade Procedure

Step	Procedure	Result
5. <input type="checkbox"/>	CMP GUI: Reapply configuration on MPE/MRA cluster that completed the upgrade successfully.	<p>For MPE: PolicyServer → Configuration → <MPE_cluster_name> → System</p> <p>For MRA: MRA → configuration → <MRA_cluster> → System</p> <p>The selected cluster will show different releases for the Active and Standby servers with Config mismatch. This is expected.</p> <ol style="list-style-type: none"> Select Operations → Reapply Configuration NOTE: A progress bar appears for the MPE reapply configuration only The MRA reapply configuration does not display the progress bar.  <ol style="list-style-type: none"> Note the version is successfully changed to the upgraded release 12.1.2. <p>NOTE: The status still showing as Degraded. This is a normal reporting event as the servers are in different releases.</p> 
6. <input type="checkbox"/>	CMP GUI: Current alarms	<p>During the upgrade activities, the following alarms may be generated and considered normal reporting events.</p> <p><u>Expected Critical alarm</u></p> <p>None</p> <p><u>Expected Major Alarm</u></p> <p>None</p> <p><u>Expected Minor Alarms</u></p> <p>70503 Server Forced Standby 70502 Cluster Replication Inhibited 70500 System Mixed Version 70501 Cluster Mixed Version 71402 Connectivity Lost 78001 Rsync Failed 31101 Database replication to slave failure</p>
7. <input type="checkbox"/>	CMP GUI: Continue upgrade of the MRA/MPE clusters. Next operation is initiate upgrade on the Standby server	<p>Continue The upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters may be running upgrade at one time.</p> <p>NOTE: 4 clusters can be running the upgrade process at one time.</p>



Software Upgrade Procedure

Step	Procedure	Result
		<p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for a cluster. <ul style="list-style-type: none"> 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...'  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin the final server upgrade of the cluster <p>Wait until the cluster reports OOS before selecting the next cluster</p> <p>Follow the progress in the Upgrade Operation column.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Alarms</p> <p>70503 Server Forced Standby 70507 Upgrade In Progress 70500 System Mixed Version 70501 Cluster Mixed Version 78001 Rsync Failed 70502 Cluster Replication Inhibited</p> <p>Upgrade is complete on the spare server in the georedundant cluster when:</p> <ul style="list-style-type: none"> 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). <p>The Active and Spare servers are on release 12.1.2 and the current standby will be on 10.5, 11.5, 12.0, or 12.1.1.</p> 

Software Upgrade Procedure

Step	Procedure	Result
8. <input type="checkbox"/>	CMP GUI: If traffic does not become active within 90 seconds	Upgrade Manager → System Maintenance If traffic is active, go to step 10. <ul style="list-style-type: none"> Select the checkbox for the partially upgraded cluster, and select Operations → RollBack. Release 10.5, 11.5, 12.0, or 12.1.1 MPE server should become active and resume handling traffic.
9. <input type="checkbox"/>	CMP GUI: Reapply configuration back to release 10.5, 11.5, 12.0, or 12.1.1	<ol style="list-style-type: none"> Policy Server → Configuration → <mpe_cluster name> → System tab or MRA → Configuration → <mpe_cluster name> → System tab Click Reapply Configuration <ul style="list-style-type: none"> Verify that the version is changed from 10.5, 11.5, 12.0, or 12.1.1, and the action report success. If NOT, contact Oracle support to consider backing out of the partially upgraded cluster.
10. <input type="checkbox"/>	CMP GUI: Continue to upgrade the MRA/MPE clusters. Next operation is Initiate upgrade on the standby server NOTE: 4 clusters can be running the upgrade process at one time.	<p>Continue the upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters may be running the upgrade at one time.</p> <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for a cluster <ul style="list-style-type: none"> 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 remaining MRA or MPE.  <p>3. Click OK to confirm and continue with the operation. It will begin the final server upgrade of the cluster</p> <p>Wait until the cluster reports OOS before selecting the next cluster</p> <p>Follow the progress in the Upgrade Operation column.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p>

Software Upgrade Procedure

Step	Procedure	Result
		<p><u>Expected Minor Alarms</u></p> <p> 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 </p> <p>Upgrade is complete on the third server in the georedundant cluster when:</p> <ul style="list-style-type: none"> 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)  <p>All clusters are now running release 12.1.2</p>
11. <input type="checkbox"/>	CMP GUI: (MPEonly) Reapply configuration on the MPE cluster that completed the upgrade successfully.	<p>MPE only</p> <ol style="list-style-type: none"> PolicyServer → Configuration → <MPE_cluster_name> → System Select Operations→Reapply Configuration <p>NOTE: A progress bar appears for the MPE reapply configuration.</p> 
12. <input type="checkbox"/>	Repeat steps 1–10 for the next MPE or MRA clusters	<p>Proceed with next cluster(s)</p> <p>MPE cluster _____</p> <p>MPE cluster _____</p> <p>MPE cluster _____</p> <p>MPE cluster _____</p> <p>MRA cluster _____</p> <p>NOTE: If you are using Veritas NetBackup there are additional steps to perform after an upgrade. See the Maintenance Operation Procedure (MOP) for the Netbackup.</p>
13. <input type="checkbox"/>	ACCEPT UPGRADE REQUIREMENT	With release 12.1.2, the Accept Upgrade step is NOT required. It will be embedded as part of the next release upgrade procedure.
THIS PROCEDURE HAS BEEN COMPLETED		

11. POST UPGRADE HEALTH CHECK

NOTE: This section is used when the entire topology is running release 12.1.2.

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the upgrade is successful on all CMP/MRA/MPE clusters.	Upgrade → Upgrade Manager View the Up to Date, Running Release, and Upgrade Operation columns
2. <input type="checkbox"/>	CMP GUI: View current alarms	Navigate to System Wide Reports→Alarms→Active Alarms Only Possible alarms are the following.
3. <input type="checkbox"/>	CMP GUI: View current KPIs	Navigate to System Wide Reports→KPIDashboard
4. <input type="checkbox"/>	CMP GUI: View trending reports	Navigate to System Wide Reports→Trending Reports
5. <input type="checkbox"/>	CMP GUI: Replication stats	Navigate to System Wide Reports→Others→MPE/MRA Rep Stats
THIS PROCEDURE HAS BEEN COMPLETED		

12. BACKOUT (ROLLBACK)

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 the Technical Services and Escalation team before initiating the Backout procedure. They will determine the appropriate course of recovery options.

12.1 Backout Sequence

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

1. Backout MRA/MPE—Use Upgrade Manager
2. Backout the Secondary CMP cluster (if applicable) —Use Upgrade Manager
3. Backout the Primary CMP cluster:
 - For 10.5 or 11.5 backout, use Upgrade Manager and the System Maintenance Manager
 - For 12.0 or 12.1.1 backout, the Upgrade Manager will be used for all components.

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

NOTE: In the case of an MPE/MRA, the upgrade/backout is NOT complete until the operator does a Reapply Configuration from the CMP. The MRA/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 backout if other Policy servers (MPEs and MRAs) are still on the upgraded release.

NOTE: If Veritas NetBackup is being used on a 10.5 Policy Management system, see the Maintenance Operation Procedure for additional backout steps.

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 10.5, 11.5, 12.0, or 12.1.1 (MRA, MPE, CMP) with Active, Standby, or Spare status.

Expected pre-conditions:

1. Primary Active CMP is on release 12.1.2
2. Cluster is of MPE, MRA or CMP
3. One server of target cluster is on release 12.1.2 in Active role
4. One server of target cluster is on release 12.1.2 in either Standby, Force Standby, or Spare

12.3.1 Backout Sequence

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

Software Upgrade Procedure

12.3.1.1 Required Cluster Backout Sequence (Reverse of the Upgrade Sequence)

1. MRAs and MPEs, Site 1 and Site-2 clusters—Uses current Upgrade Manager
2. CMP Site-2 cluster (if applicable)—Uses current Upgrade Manager
3. CMP Site-1 cluster—Uses current Upgrade Manager and System Maintenance for 10.5 or 11.5, and Upgrade Manager only for 12.0 and 12.1

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

12.3.1.2 Overview on Backout/Rollback MRA/MPE cluster

NOTE: The following procedure should be used to backout a 12.1.2 cluster to Policy 10.5, 11.5, 12.0, or 12.1.1.

This will preserve the cluster as a georedundant MRA cluster.

1. Use the Upgrade Manager in the CMP GUI to begin the backout of the MRA/MPE cluster
2. Wait until complete
3. Use the Upgrade Manager in the CMP GUI to continue the backout of the MRA/MPE cluster
4. Failover
5. Reapply the configuration
6. Use the Upgrade Manager in the CMP GUI to continue the backout of the MRA/MPE cluster

12.3.1.3 Backout Secondary CMP (If applicable)

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

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

12.3.1.4 Backout Primary CMP (10.5)

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

1. Use the Upgrade Manager in the CMP GUI to backout the Primary standby CMP cluster
2. Log back in to the Primary CMP VIP
3. Use the 10.5 System Maintenance to complete backout of the Primary CMP cluster

12.3.1.5 Backout Primary CMP (11.5)

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 System Maintenance to complete backout of the Primary CMP cluster

12.3.1.6 Backout Primary CMP (12.0 and 12.1.1)



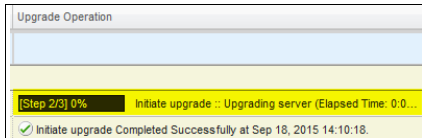
Use the CMP GUI (Upgrade Manager) to backout the CMP cluster.

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 MPE/MRA Cluster

NOTE: If you are using Veritas NetBackup there are additional steps to perform before a backout. See the Maintenance Operation Procedure (MOP) for Netbackup.

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of affected clusters	<p>Upgrade → Upgrade Manager</p> <p>Confirm status of the cluster to be backed out:</p> <ul style="list-style-type: none"> Primary Active CMP is on release 12.1.2 MPE/MRA is on release 12.1.2 Up to Date column shows Y for all servers <p>EXAMPLE</p> 
2. <input type="checkbox"/>	CMP GUI: Rollback standby server—MPE/MRA 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.	<p>Select the upgraded clusters to backout.</p> <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the cluster. <ul style="list-style-type: none"> Select one cluster at a time. 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.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin the backout process. <p>Follow the progress in the Upgrade Operation column.</p>  <p>The server backing out will go into the OOS state and the spare server will now take over as standby.</p> <p>Wait until the server goes to an OOS state before selecting the next cluster to backout.</p> <p>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.</p>

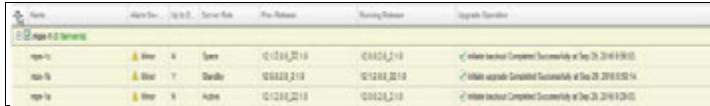
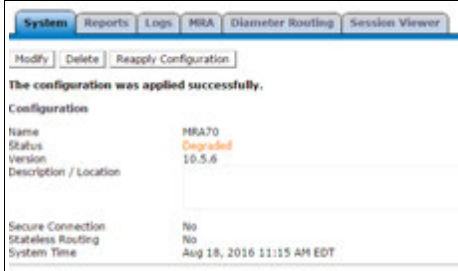
Software Upgrade Procedure

Step	Procedure	Result																																			
		<p><u>Expected Critical Alarms</u></p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procMgr failed</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance 31233 HA Path Down</p> <p><u>Expected Minor Alarms</u></p> <p>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</p> <p>Backout is complete when the following message 'Initiate backout completed successfully' shows in the Upgrade Operation column. The server will show running release of 10.5, 11.5, 12.0, or 12.1.1 and return to standby with an N in the Up to Date column.</p> <table><thead><tr><th>Name</th><th>Alarm Set</th><th>Up to Date</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr></thead><tbody><tr><td colspan="7">mpe-4 (3 Servers)</td></tr><tr><td>mpe-1</td><td></td><td>Y</td><td>Spare</td><td>10.0.2.0_2.1.0</td><td>12.1.2.0_2.2.1.0</td><td>✓ Initiate upgrade Completed Successfully at Sep 28, 2015 7:32:15</td></tr><tr><td>mpe-1b</td><td></td><td>Y</td><td>Active</td><td>10.0.2.0_2.1.0</td><td>12.1.2.0_2.2.1.0</td><td>✓ Initiate upgrade Completed Successfully at Sep 28, 2015 8:50:14</td></tr><tr><td>mpe-1a</td><td>Minor</td><td>N</td><td>Standby</td><td>10.0.2.0_2.1.0</td><td>10.0.2.0_2.1.0</td><td>✓ Initiate backout Completed Successfully at Sep 28, 2015 8:28:01</td></tr></tbody></table>	Name	Alarm Set	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation	mpe-4 (3 Servers)							mpe-1		Y	Spare	10.0.2.0_2.1.0	12.1.2.0_2.2.1.0	✓ Initiate upgrade Completed Successfully at Sep 28, 2015 7:32:15	mpe-1b		Y	Active	10.0.2.0_2.1.0	12.1.2.0_2.2.1.0	✓ Initiate upgrade Completed Successfully at Sep 28, 2015 8:50:14	mpe-1a	Minor	N	Standby	10.0.2.0_2.1.0	10.0.2.0_2.1.0	✓ Initiate backout Completed Successfully at Sep 28, 2015 8:28:01
Name	Alarm Set	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation																															
mpe-4 (3 Servers)																																					
mpe-1		Y	Spare	10.0.2.0_2.1.0	12.1.2.0_2.2.1.0	✓ Initiate upgrade Completed Successfully at Sep 28, 2015 7:32:15																															
mpe-1b		Y	Active	10.0.2.0_2.1.0	12.1.2.0_2.2.1.0	✓ Initiate upgrade Completed Successfully at Sep 28, 2015 8:50:14																															
mpe-1a	Minor	N	Standby	10.0.2.0_2.1.0	10.0.2.0_2.1.0	✓ Initiate backout Completed Successfully at Sep 28, 2015 8:28:01																															
3. <input type="checkbox"/>	<p>CMP GUI: Continue the backout of the MRA/MPE clusters. Next operation is initiate backout on the spare server</p> <p>NOTE: Up to 4 clusters can be backed out at the same time, selecting one at a time.</p>	<p>Select the partially backed out cluster to backout.</p> <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none">Select the checkbox for the cluster.<ul style="list-style-type: none">Select one cluster at a time.Can be an MRA or MPE cluster.Click Continue Rollback. When hovering over the button, it will inform you to initiate backout. <table><thead><tr><th colspan="2">Continue Rollback</th><th colspan="2">Resume Upgrade</th></tr><tr><td colspan="2">Initiate backout MRA240-28 (Back) to 10</td><td>Up to Date</td><td>Server Role</td></tr></thead><tbody><tr><td colspan="4">MRA</td></tr><tr><td colspan="4">MRA79 (3 Servers)</td></tr><tr><td>MRA240-166</td><td>Minor</td><td>Y</td><td>Active</td></tr><tr><td>MRA240-28</td><td>Minor</td><td>Y</td><td>Spare</td></tr><tr><td>MRA240-79</td><td>Minor</td><td>N</td><td>Standby</td></tr></tbody></table> <ol style="list-style-type: none">Click OK to confirm and continue with the operation. <p>Wait until the server fails over before selecting the next cluster. This will take a minute or two.</p> <p>Follow the progress in the Server Role column. The Server will show OOS in the server role until the backout completes. Wait for the server to show Standby in the Server role column.</p>	Continue Rollback		Resume Upgrade		Initiate backout MRA240-28 (Back) to 10		Up to Date	Server Role	MRA				MRA79 (3 Servers)				MRA240-166	Minor	Y	Active	MRA240-28	Minor	Y	Spare	MRA240-79	Minor	N	Standby							
Continue Rollback		Resume Upgrade																																			
Initiate backout MRA240-28 (Back) to 10		Up to Date	Server Role																																		
MRA																																					
MRA79 (3 Servers)																																					
MRA240-166	Minor	Y	Active																																		
MRA240-28	Minor	Y	Spare																																		
MRA240-79	Minor	N	Standby																																		


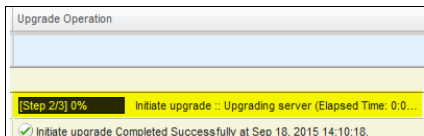
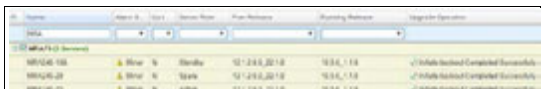
Software Upgrade Procedure

Step	Procedure	Result																																																
		<p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance 31233 HA Path Down 31126 Audit blocked</p> <p>Expected Minor Alarms</p> <p>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</p> <p>Backout is complete when the initiate backout completed successfully message shows in the Upgrade Operation column. The server will go back to running release of 10.5, 11.5, 12.0, or 12.1.1.</p> <table><thead><tr><th>ID</th><th>Name</th><th>Alarm S.</th><th>Up L.</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr></thead><tbody><tr><td colspan="8">MRA</td></tr><tr><td colspan="8">MRA70 (3 Servers)</td></tr><tr><td>MRA240-100</td><td></td><td>Minor</td><td>Y</td><td>Active</td><td>10.5.0, 11.0</td><td>12.1.2.0.0, 22.1.0</td><td>Initiate upgrade Completed Successfully</td></tr><tr><td>MRA240-28</td><td></td><td>Minor</td><td>N</td><td>Spare</td><td>12.1.2.0.0, 22.1.0</td><td>10.5.0, 11.0</td><td>Initiate backout Completed Successfully</td></tr><tr><td>MRA240-70</td><td></td><td>Minor</td><td>N</td><td>Standby</td><td>12.1.2.0.0, 22.1.0</td><td>10.5.0, 11.0</td><td>Initiate backout Completed Successfully</td></tr></tbody></table>	ID	Name	Alarm S.	Up L.	Server Role	Prev Release	Running Release	Upgrade Operation	MRA								MRA70 (3 Servers)								MRA240-100		Minor	Y	Active	10.5.0, 11.0	12.1.2.0.0, 22.1.0	Initiate upgrade Completed Successfully	MRA240-28		Minor	N	Spare	12.1.2.0.0, 22.1.0	10.5.0, 11.0	Initiate backout Completed Successfully	MRA240-70		Minor	N	Standby	12.1.2.0.0, 22.1.0	10.5.0, 11.0	Initiate backout Completed Successfully
ID	Name	Alarm S.	Up L.	Server Role	Prev Release	Running Release	Upgrade Operation																																											
MRA																																																		
MRA70 (3 Servers)																																																		
MRA240-100		Minor	Y	Active	10.5.0, 11.0	12.1.2.0.0, 22.1.0	Initiate upgrade Completed Successfully																																											
MRA240-28		Minor	N	Spare	12.1.2.0.0, 22.1.0	10.5.0, 11.0	Initiate backout Completed Successfully																																											
MRA240-70		Minor	N	Standby	12.1.2.0.0, 22.1.0	10.5.0, 11.0	Initiate backout Completed Successfully																																											
4. <input type="checkbox"/>	<p>CMP GUI: Continue the backout of the MRA/MPE clusters. Next operation is failover to previous release.</p> <p>NOTE: Up to 4 clusters can be backed out at the same time, selecting one at a time.</p>	<ol style="list-style-type: none">Select the cluster to backout. Current state of the cluster needs to be as follows.<ul style="list-style-type: none">Spare server on previous releaseActive server on release 12.1.2Standby Server on previous release<p>Upgrade → Upgrade Manager</p>Select the checkbox for the cluster (one cluster at a time) (can be an MRA or MPE)Click Continue Rollback. When hovering over the button, it will inform you to failover to old version <div><p>Continue Rollback Become Upgrade</p><p>Failover to old version MRA70 (back)</p><p>MRA</p><p>MRA70 (3 Servers)</p><p>MRA240-100 Minor Y Active</p><p>MRA240-28 Minor N Spare</p><p>MRA240-70 Minor N Standby</p></div> <ol style="list-style-type: none">Click OK to confirm and continue with the operation. It will begin to failover.																																																

Software Upgrade Procedure

Step	Procedure	Result
		<p>Wait until the server fails over before selecting the next cluster. This will take a minute or two.</p> <p><u>Expected Critical Alarms</u></p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance 31233 HA Path Down 31126 Audit blocked</p> <p><u>Expected Minor Alarms</u></p> <p>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</p> <p>State of the cluster will look like the following when the failover completes.</p> 
5. <input type="checkbox"/>	<p>CMP GUI: Reapply the configuration to the MPE/MRA cluster that completed the failover successfully.</p>	<p>For MPE: PolicyServer → Configuration → <MPE_cluster_name> → System</p> <p>For MRA: MRA → Configuration → <MRA_cluster> → System</p> <p>The selected cluster will have the status shown as Degraded. This status is expected</p> <ol style="list-style-type: none"> Click Reapply Configuration. <ul style="list-style-type: none"> The MPE opens a dialog box showing the progress of the reapply process. The MRA will not show anything. Note the version is successfully changed to the previous release. The following figure shows 10.5.  <p>NOTE: The status still showing Degraded is a normal reporting event because the servers currently have different releases.</p>

Software Upgrade Procedure


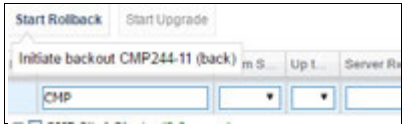
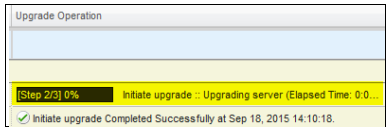
Step	Procedure	Result
6. <input type="checkbox"/>	<p>CMP GUI: Complete backout of cluster(s)</p> <p>NOTE: The backout of a single server takes approximately 30 minutes to complete.</p> <p>NOTE: Up to 4 clusters can be backed out at the same time, selecting one at a time.</p>	<ol style="list-style-type: none">1. Select the partially upgraded cluster to backout. Upgrade → Upgrade Manager2. Select the checkbox for the cluster (one cluster at a time) (can be an MRA or MPE)3. Click Continue Rollback. When hovering over the button, it will inform you of the current standby server to be rolled back. 4. Click OK to confirm and continue with the operation. It will begin the backout process. <p>Follow the progress in the Upgrade Operation column.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance 31233 HA Path Down 31126 Audit blocked</p> <p>Expected Minor Alarms</p> <p>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</p> <p>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 previous release and show active/standby/spare</p> 

Software Upgrade Procedure

Step	Procedure	Result
7. <input type="checkbox"/>	Current alarms	Minor alarms expected: 31282 HA Management Fault 78001 Rsync Failed 70500 System Mixed Version
8. <input type="checkbox"/>		Repeat this Procedure for remainder of MPE and MRA servers, if not fully backed out yet.
9. <input type="checkbox"/>	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		

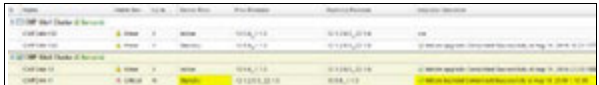

12.3.4 Backout Fully Upgraded Secondary CMP Cluster

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 10.5 or 11.5 System Maintenance option. For Rollback to release 12.0 and 12.1, the Upgrade Manager is used.

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP clusters	<p>Upgrade → System Maintenance</p> <p>Confirm status of the cluster to be backed out</p> <ul style="list-style-type: none"> Primary Active CMP is on release 12.1.2 Standby server are on release 12.1.2 Up to Date column shows Y for all servers <p>NOTE: The Filter button can be used to show only the CMP servers. Enter CMP in the Name field.</p> 
2. <input type="checkbox"/>	<p>CMP GUI: backout secondary CMP cluster</p> <p>NOTE: The backout of a single server takes approximately 40 minutes to complete.</p>	<ol style="list-style-type: none"> Select Secondary CMP cluster to backout. <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the secondary CMP cluster Click Start Rollback. When hovering over the button, it will inform you of the server to get backed out.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin to backout. The server will go into an OOS server Role <p>Follow the progress in the Upgrade Operation column.</p>  <p>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.</p>

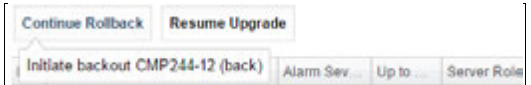
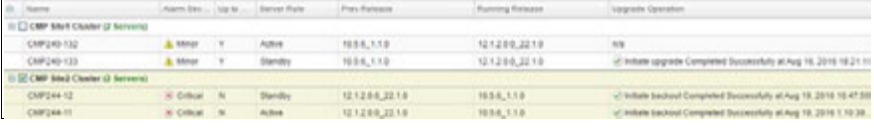
Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 10.5 or 11.5 System Maintenance option. For Rollback to release 12.0 and 12.1, the Upgrade Manager is used.

Step	Procedure	Result
		<p><u>Expected Critical Alarms</u></p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p><u>Expected Major Alarm</u></p> <p>70004 QP Processes down for maintenance 31233 HA Path Down 31126 Audit blocked</p> <p><u>Expected Minor Alarms</u></p> <p>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</p> <p>Backout of the server is complete when the backout completed successfully message shows in the Upgrade Operation column. The server will go back to standby state and show the previous release.</p> 
3. <input type="checkbox"/>	CMP GUI: Continue the backout. Next operation is failover	<ol style="list-style-type: none"> Select Secondary CMP cluster. <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP cluster Click Continue Rollback. When hovering over the button, it will inform you to failover.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin the failover process. Wait until the previous release becomes active before continuing <p><u>Expected Critical Alarm</u></p> <p>70025 QP Slave database is a different version than the master</p> <p><u>Expected Minor Alarms</u></p> <p>70503 Server Forced Standby 70501 Cluster Mixed Version 78001 Rsync Failed 70500 System Mixed Version</p>

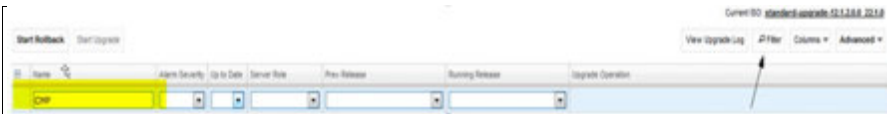
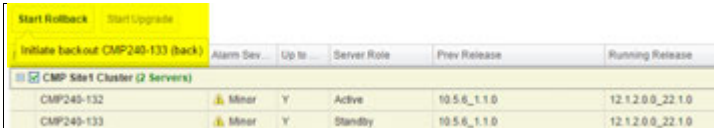
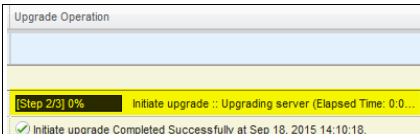
Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 10.5 or 11.5 System Maintenance option. For Rollback to release 12.0 and 12.1, the Upgrade Manager is used.

Step	Procedure	Result
4. <input type="checkbox"/>	<p>CMP GUI: Continue the backout. Next operation is initiate backout</p>	<ol style="list-style-type: none"> Select Secondary CMP cluster. <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Secondary CMP cluster Click Continue Rollback. When hovering over the button, it will inform you to rollback.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin the failover process. Follow the progress of the status in the Server Role column.  <p>Expected Critical alarm</p> <p>70025 QP Slave database is a different version than the master</p> <p>Expected Minor Alarms</p> <p>70500 System Mixed Version</p>
THIS PROCEDURE HAS BEEN COMPLETED		

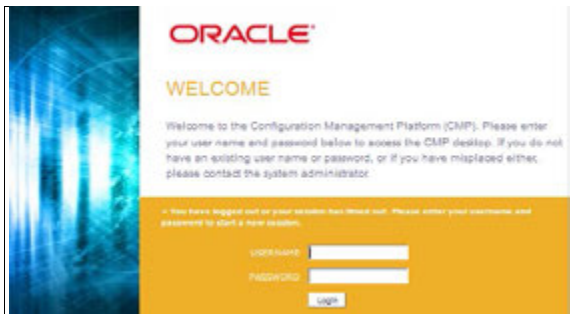
12.3.5 Backout Fully Upgraded Primary CMP Cluster

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster. For rollback to 10.5 or 11.5, use both the Upgrade Manager and System Maintenance. For rollback to release 12.0 or 12.1, only use the Upgrade Manager.

Step	Procedure	Result
1. <input type="checkbox"/>	CMP GUI: Verify the status of the CMP clusters	<p>Upgrade Manager → System Maintenance</p> <p>Confirm status of the cluster to be backed out:</p> <ul style="list-style-type: none"> Primary Active CMP is on release 12.1.2 Secondary CMP cluster is on release 10.5, 11.5, 12.0, or 12.1.1 Up to Date column shows Y for all servers in the primary CMP cluster <p>NOTE: The Filter button can be used to show only the CMP servers. Enter CMP in the Name field.</p> 
2. <input type="checkbox"/>	CMP GUI: backout standby Primary CMP cluster NOTE: backout of one server will take approximately 40 minutes to complete.	<ol style="list-style-type: none"> Select Primary CMP cluster to backout. <p>Upgrade → Upgrade Manager</p> <ol style="list-style-type: none"> Select the checkbox for the Primary CMP cluster Click Start Rollback. When hovering over the button, it will inform you of the server to get backed out.  <ol style="list-style-type: none"> Click OK to confirm and continue with the operation. It will begin to backout. The server will go into an OOS server Role <p>Follow the progress of the status in the Upgrade Operation column.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <ul style="list-style-type: none"> 31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed 31236 HA Link Down <p>Expected Major Alarm</p> <ul style="list-style-type: none"> 70004 QP Processes down for maintenance 31233 HA Path Down <p>Expected Minor Alarms</p> <ul style="list-style-type: none"> 31114 DB replication over SOAP has failed 31106 Database merge to parent failure



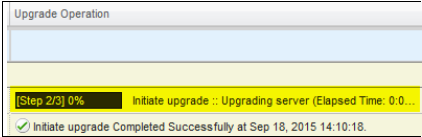
Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster. For rollback to 10.5 or 11.5, use both the Upgrade Manager and System Maintenance. For rollback to release 12.0 or 12.1, only use the Upgrade Manager.

Step	Procedure	Result																																
		<div>31107 Database merge from child failure</div> <div>31101 Database replication to slave failure</div> <div>31102 Database replication from master failure</div> <div>31113 DB replication manually disabled</div> <div>70503 Server Forced Standby</div> <div>70507 Upgrade In Progress</div> <div>70500 System Mixed Version</div> <div>70501 Cluster Mixed Version</div> <div>78001 Rsync Failed</div> <div>70502 Cluster Replication Inhibited</div> <div>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.</div> <div><table><tr><th>ID</th><th>Name</th><th>Alerts Sev.</th><th>12.0</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th><th>Upgrade Operation</th></tr><tr><td colspan="8">CMP Site1 Cluster (2 Servers)</td></tr><tr><td>CMP240-132</td><td></td><td>Minor</td><td>Y</td><td>Active</td><td>10.5.6_1.1.0</td><td>12.1.2.0.0_22.1.0</td><td>NA</td></tr><tr><td>CMP240-133</td><td></td><td>Critical</td><td>N</td><td>Standby</td><td>12.1.2.0.0_22.1.0</td><td>10.5.6_1.1.0</td><td>Initiate Backout Completed Successfully at Aug 10, 2019 14:30:00</td></tr></table></div>	ID	Name	Alerts Sev.	12.0	Server Role	Prev Release	Running Release	Upgrade Operation	CMP Site1 Cluster (2 Servers)								CMP240-132		Minor	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	NA	CMP240-133		Critical	N	Standby	12.1.2.0.0_22.1.0	10.5.6_1.1.0	Initiate Backout Completed Successfully at Aug 10, 2019 14:30:00
ID	Name	Alerts Sev.	12.0	Server Role	Prev Release	Running Release	Upgrade Operation																											
CMP Site1 Cluster (2 Servers)																																		
CMP240-132		Minor	Y	Active	10.5.6_1.1.0	12.1.2.0.0_22.1.0	NA																											
CMP240-133		Critical	N	Standby	12.1.2.0.0_22.1.0	10.5.6_1.1.0	Initiate Backout Completed Successfully at Aug 10, 2019 14:30:00																											
3. <input type="checkbox"/>	CMP GUI: Continue the backout. Next operation is failover	<div>1. Select Primary CMP cluster.</div> <div>Upgrade → Upgrade Manager</div> <div>2. Select the checkbox for the Secondary CMP cluster</div> <div>3. Click Continue Rollback. When hovering over the button, it will inform you to failover.</div> <div><div>Continue Rollback Resume Upgrade</div><div>Fallover to old version CMP Site1 Cluster (back) Up to: Server Role</div><table><tr><td colspan="4">CMP Site1 Cluster (2 Servers)</td></tr><tr><td>CMP240-132</td><td>Minor</td><td>Y</td><td>Active</td></tr><tr><td>CMP240-133</td><td>Critical</td><td>N</td><td>Standby</td></tr></table></div> <div>4. Click OK to confirm and continue with the operation. It will begin the failover process.</div> <div>Failover takes a couple minutes.</div>	CMP Site1 Cluster (2 Servers)				CMP240-132	Minor	Y	Active	CMP240-133	Critical	N	Standby																				
CMP Site1 Cluster (2 Servers)																																		
CMP240-132	Minor	Y	Active																															
CMP240-133	Critical	N	Standby																															
4. <input type="checkbox"/>	CMP GUI: Log back in to the Primary CMP VIP	<div>After failover, you will be required to log back in to the CMP GUI using the Primary CMP VIP.</div> <div><div></div></div>																																
5. <input type="checkbox"/>	CMP GUI: Verify release	<div>Navigate to Help→About. Verify the release number is displayed as 10.5, 11.5, 12.0, or 12.1.1.</div> <div><ul style="list-style-type: none">If Rollback is for release 10.5 or 11.5, continue with step 6.If Rollback is for release 12.0 and 12.1, continue with step 8</div>																																

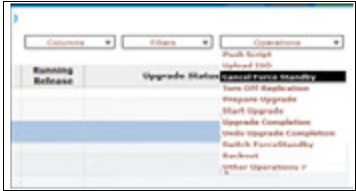

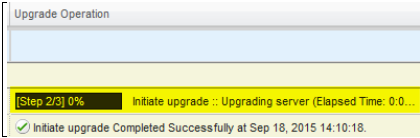
Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster. For rollback to 10.5 or 11.5, use both the Upgrade Manager and System Maintenance. For rollback to release 12.0 or 12.1, only use the Upgrade Manager.

Step	Procedure	Result
6. <input type="checkbox"/>	<p>CMP GUI (release 10.5 or 11.5): Continue the backout of the Primary CMP cluster</p> <p>NOTE: backout of one server will take approximately 30 minutes to complete.</p>	<p>Upgrade → System Maintenance</p> <ol style="list-style-type: none"> Select the checkbox for the remaining server in the Primary CMP cluster. The server will be on 12.1.2 and show Forced Standby in the Server State column.  <ol style="list-style-type: none"> Select Operations→Backout  <ol style="list-style-type: none"> Click OK to continue <p>Follow the progress in the Upgrade Operation column. Wait until the server to backout comes to backout complete.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Alarms</p> <p>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</p>

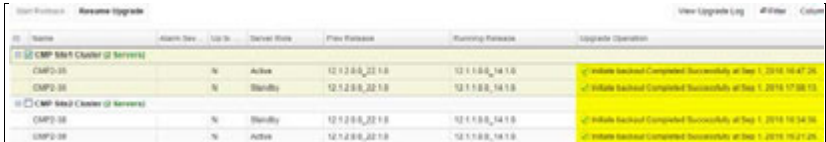
Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster. For rollback to 10.5 or 11.5, use both the Upgrade Manager and System Maintenance. For rollback to release 12.0 or 12.1, only use the Upgrade Manager.

Step	Procedure	Result
7. <input type="checkbox"/>	CMP GUI: Remove Forced Standby	<p>Upgrade → System Maintenance</p> <p>Select the checkbox for the remaining server in the Primary CMP cluster. The server will be on 10.5 or 11.5 and show Forced Standby in the Server State column.</p> <p>NOTE: A refresh of the current screen may be necessary at the 40 minute mark.</p> <p>Select Operations→Cancel Forced Standby</p> 
The backout procedure is now completed for releases 10.5 or 11.5. Go to step 9 and perform the final Syscheck.		
8. <input type="checkbox"/>	<p>CMP GUI (release 12.0 and 12.1): Continue the backout of the Primary CMP cluster</p> <p>NOTE: The backout of one server takes approximately 40 minutes to complete.</p>	<ol style="list-style-type: none"> 1. Select Primary CMP cluster to complete the backout. 2. Select Upgrade → Upgrade Manager 3. Select the checkbox for the Primary CMP cluster 4. 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.  <ol style="list-style-type: none"> 5. Click OK to confirm and continue with the operation. It will begin to backout. Server will go in an OOS server Role <p>Follow the progress in the Upgrade Operation column.</p>  <p>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.</p> <p>Expected Critical Alarms</p> <p>31283 Lost Communication with server 31227 HA availability status failed 70001 QP_procmgr failed</p> <p>Expected Major Alarm</p> <p>70004 QP Processes down for maintenance</p> <p>Expected Minor Alarms</p> <p>70503 Server Forced Standby 70507 Upgrade In Progress 70500 System Mixed Version 70501 Cluster Mixed Version</p>

Software Upgrade Procedure

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager—followed by the Primary CMP Site-1 cluster. For rollback to 10.5 or 11.5, use both the Upgrade Manager and System Maintenance. For rollback to release 12.0 or 12.1, only use the Upgrade Manager.

Step	Procedure	Result
		<p> 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 </p> <p>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.</p> 
9. <input type="checkbox"/>	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		

APPENDIX A. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE AND HOTLINES

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

1. Log into 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>